

17 October 2012

COMMISSION PROPOSAL ON A GENERAL DATA PROTECTION REGULATION

KEY MESSAGES

- 1 The General Data Protection Regulation should contribute to the achievement of greater harmonisation towards the establishment of a true Digital Single Market.
- 2 However, the Commission proposal is overly prescriptive and detailed in a way that creates more administrative burden and compliance costs for companies without a proportionate privacy benefit. In this way, it discourages digital innovation and competitiveness.
- 3 The proposal introduces far-reaching documentation obligations, data protection impact assessments, prior consultations and authorisations that will disproportionately increase administrative burden for companies with no benefits for consumers.

WHAT DOES BUSINESSEUROPE AIM FOR?

- BUSINESSEUROPE does not support the changes in the definition of data subject's consent compared to the current directive, as they will make the process too cumbersome and prescriptive. In case of continued business relationships, these requirements are an unnecessary supplementary administrative burden.
- The numerous provisions on secondary rulemaking (delegated and implementing acts) undermine legal predictability and risk neutralising the effectiveness of the provisions by complicating the data protection regime.
- Despite the fact that effective and high- quality enforcement is essential, the proposed sanctions are excessive and disproportionate. In our view, particularly in cases of first and non-intentional non-compliance, a warning procedure as well as pre-requisites for renouncing from inflicting sanctions should be considered.
- In addition, we are worried about the impact of the proposal on data processing in the employer/employee relationship. In several Member States, collective agreements and employees' consent to the processing of their data by employers



are also the basis of legal data processing. This practice should be maintained. Otherwise, administrative burden will increase while employees' situation will not improve.

- It is extremely important to clarify the distinction between the liabilities of the data controller and those of the data processor. Indeed, some confusion can be observed in several provisions of the regulation on this matter. Data processor obligations should continue to be controlled by and specified in contractual clauses between controller and processor.

17 October 2012

BUSINESSEUROPE COMMENTS ON THE COMMISSION PROPOSAL FOR A GENERAL DATA PROTECTION REGULATION

I. INTRODUCTION

The Commission adopted on 25 January 2012 proposals to review the current EU data protection framework (directive 95/46/EC). BUSINESSEUROPE will focus its comments on the proposal for a General Data Protection Regulation [COM(2012), 11].

We support the aim of the proposal to achieve greater harmonisation towards a Digital Single Market for Europe. In a data-driven age, it is important to get data protection rules right for European businesses and consumers and ensure legal certainty. Effective digital solutions, more competition across Europe and a more efficient public sector depend on citizen's trust in information and communications technology (ICT).

We also welcome the single Data Protection Authority (DPA) concept based on the "main establishment" of a company principle sometimes referred to as a "one-stop-shop" for compliance. This should simplify and streamline companies' relations with data protection authorities.

We are concerned about the overall approach to draft the proposal with respect to a data controller and not the enterprise as a whole. This could give rise to confusion as to what the main establishment is or where the "one-stop-shop" for compliance might be as an organisation could be a data controller in multiple Member States.

Furthermore, the proposal not only determines what obligations apply but how they are implemented in an overly detailed way without reflecting the realities of today's technologies and taking account of other specific regulation (e.g. consumer law, contractual law, employment law, collective agreements, national legislation on privacy, sectorial requirements). This will create unnecessary burden, increase costs without a proportionate privacy benefit, discourage digital innovation and competitiveness, as companies will be pushed to invest in administrative compliance rather than growth.

We believe that regulators need to craft the "what" is expected and remain clear and comprehensive regarding the "how". Accordingly, the proposal should provide enough flexibility to allow different organisations to implement the most effective technical and organisational measures, fit for the nature and structure of each respective organisation to ensure optimal data protection. Instead of the detailed and prescriptive rules an organisational accountability obligation would be more effective.

The proposal should have been more "future-proofed" by giving sufficient consideration to businesses' activity online and how it may change in a short amount of time. This is particularly relevant for work in the cloud. The requirement to inform individuals of the level of protection in any country to which their data may be transferred (Article 14(1g)) is not workable in practice in the context of data stored in the cloud. Article 30 also demands appropriate security measures to be agreed between processors and controllers, and here a form of security certification could be introduced for cloud

service providers. In other areas, the proposal does not provide sufficient clarity as to who is responsible for data published via social media networks.

In addition, we are worried about the impact of the proposal on data processing in the employer/employee relationship. In several Member States, collective agreements and employees' consent to the processing of their data by employers are also the basis of legal data processing. This practice should be maintained. Otherwise, administrative burden will increase while employees' situation will not improve. In that respect, we also refer to provisions in articles 153-155 in the Treaty on the Functioning of the European Union (TFEU).

BUSINESSEUROPE will develop its concerns in its detailed comments below. If these shortcomings are not effectively addressed by Member States and the European Parliament, they will outweigh the positive elements of the Commission proposal.

II. DETAILED COMMENTS

DEFINITIONS

1. DEFINITION OF PERSONAL DATA

We believe that various key definitions in the Commission proposal suffer from ambiguities. This will adversely affect the aim of ensuring legal certainty and also impact other principles of the proposal such as consent and profiling.

Such an example is the linking of the definitions of "data subject" and "personal data", meaning that personal data is defined as "any information relating to a data subject". A person is a data subject as soon as he or she is reasonably to be expected traceable by "means reasonably likely to be used by the controller or by any other natural or legal person". In our view, this is too broad and lacks clarity. Moreover, naming for e.g. IP addresses and cookies as measures by use of which data subjects can be identified seems to broaden this definition of data subject. Combined with the recital 24 of the proposal which stipulates that such factors need not necessarily be considered as personal data in all circumstances, this blurs the legal framework. Therefore, a clarification is needed whether IP addresses, IP ports or cookies etc. are included in the definition "personal data" and if the answer is positive, what the circumstances referred to in recital 24 mean, when they shall not be considered as "personal data".

To offset possible huge cost of compliance and legal uncertainty a clear definition is needed making data "personal data" only when this is in the context of processing of this data where it is supposed to be "personal data".

One should consider the unintended consequences that an overly broad definition could have, especially when read in combination with the more explicit requirements of consent. The need to use IP addresses for a variety of security and authentication purposes both directly and indirectly would be undermined as bad-faith actors are unlikely to consent to the capture of such information if they believe it will be used to prevent the acts they are executing. This is an example of the need to tailor more

narrowly the draft in order to address specific and compelling public policy issues while not resulting in undue burden or unintended consequences.

2. DEFINITION OF LEGAL PERSONS

Furthermore, the proposal explicitly states (recital 12) that the protection afforded by the regulation should not be claimed with regard to the processing of data which concern legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person.

From this wording, the reference to the undertakings seems to be only limited to those “established as legal persons” and not to undertakings in general. By contrast, the relevant element to identify an undertaking should be the economic activity (as stated in article 4, n. 15 “enterprise means any entity engaged in an economic activity, irrespective of its legal form, thus including, in particular, natural and legal persons, partnerships or associations regularly engaged in an economic activity”). Therefore, it would be better to modify recital 12 in order to avoid misunderstandings, and to simply refer to “undertakings” in general, instead of “undertakings established as legal persons”.

3. DEFINITION OF DATA CONCERNING HEALTH

In addition, the proposal defines data concerning health as information which relates to the physical or mental health of an individual, or the provision of health services to the individual. This definition is impossible to implement in practice.

Purely administrative data should therefore be excluded explicitly from this definition.

CONSENT (ARTICLES 4, 7 AND 8 AND LABOUR MARKET)

1. DEFINITION OF CONSENT

Individuals should have the right to make an informed choice about how their data will be processed. BUSINESSSEUROPE believes that the provisions of the proposal on consent should not hinder a sensible and flexible processing of data and use of services.

We do not support the changes in the definition of consent as they will make the process too cumbersome and prescriptive. In case of continued business relationships, these requirements are an unnecessary supplementary administrative burden.

This is likely to turn consent into a box-ticking exercise rather than a way for data subjects to control their data. The number of forms and tick boxes that users need to complete will increase. Online services will be negatively affected, as users will be an additional click away from accessing the product, services, content they are interested in. It must remain possible for consumers to provide implicit consent i.e. in the process of registration.

In addition, online service providers would be seriously hindered, while the personal data they ask for (name, address), are necessary to give their clients a good and fast service.

2. EMPLOYER/EMPLOYEE RELATIONSHIP

In particular, it should be possible to give consent in the employment relationship. The presumption that the employment relationship is of questionable nature in preamble 34 concerning consent is unfounded and unacceptable. In the employment context consent is often given in areas where it is in the employees' interest that their personal data is processed. Otherwise, employees would be deprived from deciding how their personal data is used. For example it is beneficial for the employers and the employee that the employee in relevant situations can consent that the employer process information with regard to his/hers health, holiday, parental leave, income tax, criminal convictions, education, and wage.

Example 1: In Belgium the consent of the employee is, amongst others, used as the legal basis for transferring specific data of employees from an affiliate or subsidiary company to the mother company located outside of Europe. This is allowed on the basis of article 22, §1, 1° of the Belgian privacy act (cfr. Art. 44 of the proposal). This kind of operation is not harmful for the employees. In many cases it's even an advantage for them, because it leads to more employee mobility within multinational companies.

Example 2: Another example can be found in the area of the private employment agencies and recruitment offices. When a candidate employee presents himself at such an agency/office in Belgium, it is crucial that the agency/office transmits some of his personal data (e.g. his curriculum vitae) to candidate employers. The personal data are thus processed in order to help the candidate employee find a job. The candidate employee is asked to give his consent for this.

Example 3: In Germany, the consent is, amongst others, used as the legal basis to publish contact details and photos of their employees on the company website. This allows clients to directly contact the responsible person in charge. Without the possibility of the employee to give consent on the publication of his or her photo the employer is not able to maintain this important service for the customer-client relation in the future.

3. CONSENT IN PROCESSING PERSONAL DATA OF A CHILD

Regarding consent in the context of processing personal data of a child, the proposal lacks clarity concerning the harm to children it aims to prevent. It seems that mere processing of personal data of children is seen as harmful. However, one should identify types of processing that are harmful and focus on preventing those.

Article 8 needs further clarifications regarding when information society services are "directly offered to a child" and what "verifiable consent" of a child's parent or custodian is. To avoid hampering the development of services addressed to children,

such as educational ones, the article should also explicitly clarify that consent might be obtained by electronic means.

The proposed definition of „child“ in article 4 may also pose problems between different Member States where currently national legislation defines this differently based on national preferences and stemming from different historical origins.

MINIMUM PROCESSING PRINCIPLE (ARTICLE 5)

The Commission proposal stipulates that personal data must be limited to the minimum necessary in relation to the purposes for which they are processed. While data minimization is an important principle that tries to assure proportionate and relevant collection of information regarding its use, such a provision might lead to a situation in which a supervisory body will question the scope of data collected, even if the data subject gave its consent for the processing. The regulation should not replace the ability of the individual to control the use of their information and should focus more on the rules related to data processing as opposed to the material scope of collected and processed data where it has been consented to.

LAWFULNESS OF DATA PROCESSING (ARTICLE 6)

This article sets out the criteria within which it would be lawful to process personal data, and is therefore a very critical part of the proposed regulations. It is therefore also very important that this article is proportionate and avoids unintended consequences.

Firstly, the article should clarify under 6(c) that processing is necessary where the data controller needs to comply with domestic or international regulations (such as financial regulations) guidance and industry codes of practice as well as legal obligations. Furthermore, article 6 paragraph 1 (b) and (c) of the draft regulation provides that processing of personal data must be possible in performance of a contract or a legal obligation. This fails to take adequate account of national specificities.

For instance, in Germany and other Member States collective agreements such as sectoral and company-level agreements rank equally with legislation enacted by the state and hence can provide the basis for legal data processing. Collective agreements guarantee a balanced level of data protection. In this regard, the company-level agreement serves primarily to give concrete form to unspecified legal concepts in data protection legislation for companies and their employees and to organise legally secure procedures. For this reason, such rules meet the objective of practical data protection in a better and more sustainable way than statutory requirements. Hence, it must be ensured that collective agreements such as sectoral and company-level agreements can remain a legal basis for data processing.

Example of company-level agreements: Introduction and use of an employee identification card (including the possibility for cashless paying in the staff restaurant), implementation and analysis of employee surveys.
--



Secondly, it is essential that data processing for the legitimate interests of third parties under 6 (f) must continue to remain possible as under the 1995 data protection directive, provided that the necessary conditions are met. This is indispensable for the day-to-day business activities of many companies such as in magazine publishing, where the use of third party addresses is important for reaching new customers. Without the modification of this paragraph contacting customers would be limited to only current readers.

RIGHTS IN RELATION TO RECIPIENTS (ARTICLE 13)

An obligation on controllers to communicate any rectification or erasure to each recipient would be very burdensome. It would always involve “disproportionate effort”, especially with regard to technical or unessential rectifications. Also in cases when data are disseminated for example on an internet website or in places open to the public, exercising recipients’ rights could lead to a situation in which, following a data subject’s request to erase personal data, the data would have to be made public again.

RIGHT OF ACCESS FOR DATA SUBJECT (ARTICLE 15)

It is appropriate that data subjects should have access to their personal data.

However, the proposal to waive the fee for processing subject access requests risks leading to a significant increase in frivolous requests, which would be difficult and expensive for companies to manage. A nominal fee as in the current directive helps weed out such requests resulting in a more proportionate and manageable for businesses to process system. Alternatively, a time restriction for such requests could be considered as is the case in the Polish law on data protection, according to which a request can be submitted once every 6 months.

RIGHT TO BE FORGOTTEN AND TO ERASURE (ARTICLE 17)

It has to be underlined that this new right will have negative consequences for the transaction models of online services and for the functioning of banks, credit registers and other institutions, which for the purpose of safeguarding further transactions and detect potential abuses to prevent fraud, process personal data related to credit or transactional history.

Example 1: Allowing a person with bad credit history to demand for its erasure might hamper responsible lending and have serious economic consequences. Erasure of credit history can be also disadvantageous for a person who fulfilled his/her credit obligations in the past and would like to obtain another credit.

Example 2: Buying platform where comments of users on a seller/buyer performance are the main source of verifying somebody’s credibility. If an unfair seller is allowed to ask for erasure of all of his data after closing his account on the platform, how can a data controller assure that the same user will not open another account and continue fraudulent transactions?



It should be noted that the intention of this article is to delete data allowing for identification of a natural person from a public perspective (and not with the use of internal structures of the service provider, where such data should still be kept due to security policy and other applicable provisions of law). Moreover, it is required to separate personal data processed by an administrator from personal data published by a data subject (hosting) on which an administrator has no impact as to its publishing.

Furthermore, it should be stressed that the provisions obliging controllers to remove all the links are in many cases practically impossible, since they would require them to determine who had access to disseminated information and who copied it. It is not possible to effectively inform third parties (including those who were not authorised by the controller to publish personal data) about a request made by a data subject, because it is unworkable to determine who copied the data which was made public or which websites refer to these data.

Lastly, one should recall that requirements already exist to retain information for only the amount of time relevant to the use and purpose of collection. This obligation flows with the information so that each party that receives information has such obligations. Under the right to be forgotten such obligation is placed on the initial collector of the information with, as highlighted above, unworkable obligations to delete information on sites beyond their control. It would seem that the proposed solution is both less workable and more limited in coverage than the existing obligations. Ultimately this new right will be confusing for consumers, since there are many situations in which personal data cannot be erased for valid and legal reasons.

DATA PORTABILITY (ARTICLE 18)

The Commission proposal introduces a new right to data portability which is designed to allow individuals to change services more easily by giving them the right to obtain a copy of their data from the controller in an electronic format making it possible to transfer their personal data to another service provider. This proposal also allows the Commission to specify technical standards for the transmission of data, which goes against the principle of „technological neutrality“.

The proposal does not really reflect the technical reality. Data received from a controller cannot be easily – or at all – used as it is in other services as e.g. companies have different kinds of formats and ways of processing data that are designed to fit with the other aspects of their services and products.

In practice, the proposed right could mean that processor would have to collect the required data from different data bases as companies may have more than one database. After this all data should be transformed into a format that may not be used by the companies for its own purposes. If this process cannot be automated (automation would naturally mean costs as well), it would require human resources.

We fully support the data subjects’ right of access and right to object as defined in the current data protection regime but cannot support the proposed right to data portability. This proposal does not belong to a data protection legislation piece.

RIGHT TO OBJECT (ARTICLE 19)

The proposal transfers the burden of proof from data subjects, who under the current directive have to show their particular situation to controllers. According to the proposal, the latter would be obliged to demonstrate “compelling legitimate grounds for the processing” even if they process the data in accordance with article 6. This solution will impose another burden on administrators and needs to be revised.

PROFILING (ARTICLE 20)

A balanced regulation of profiling is important for ensuring consumer trust.

However, the proposed changes in the Commission proposal in relation to measures based on profiling lack clarity. If the proposal is meant to cover many rather routine data processing operations that are developed to satisfy consumer demand (e.g. services that remember consumers’ preferences), it fails to acknowledge the fact that profiling is often a basis for a good customer service and not always simply a means for additional marketing. Additionally, in certain sectors profiling is a necessity (for instance in the insurance or banking sectors).

Provisions on profiling need to allow profiling for legitimate interests and purposes that are for e.g. intended to respond to consumer demands. In other words, there is no need to require additional and specific conditions for this type of profiling.

RESPONSIBILITY OF THE CONTROLLER (ARTICLE 22.3)

This provision adds layers of burdensome bureaucracy for businesses and supervisory authorities, as they are obliged to assess the adequacy of the measures adopted in order to fulfil the general obligations and be legally responsible in case of breaches. On the other hand, the scheme of responsibility proposed by the regulation considers data processing as risky, and therefore giving the controller the burden of proof. Accordingly, it is the controller who is obliged to demonstrate that it has adopted all the necessary measures to avoid the damage and that the damage was not ascribable to it.

As a consequence, recruiting “independent internal or external auditors” to verify the effectiveness of the measures should be subject to the free choice of the controller. Assuming this, paragraph 3 of article 22 should be deleted and the following paragraph 4 should be modified adapting the references to the verifications of effectiveness.

DATA PROTECTION BY DESIGN AND BY DEFAULT (ARTICLE 23)

The proposed regulation contains new provisions on data protection by design and by default.

While we consider both valuable guiding principles for companies, they should not be dictated in a top-down way in a regulation, which ignores the specific context of the circumstances of the company, the nature of the information, the infrastructure and

numerous other factors. The provision on data protection by default is an example of a poorly defined rule that will create legal uncertainty. Instead it should aim to set clear expectations for what privacy by default should achieve while allowing flexibility for how each company should set about achieving it.

Industry is best placed to determine what constitutes privacy by design applied in practice and we strongly question the need for articles 23.3 and 23.4 legitimizing the European Commission's power to propose delegated acts and technical standards via implementing acts."

PROCESSOR AND CONTROLLER RELATION (ARTICLES 4, 24 AND 26)

The proposed regulation specifies in article 4.6 the definition of the processor, as processing "on behalf of the controller" and, as mentioned in article 26, "only on instructions from the controller". It is also stipulated in article 26 that the carrying out of processing between processor and controller is governed "by a contract or other legally binding act".

In case of erroneous process, the articulation between articles 26.4 and 24 is unambiguous: If a processor processes personal data other than as instructed by the controller, the processor shall be considered to be a controller in respect of that processing and shall be subject to the rules on joint controllers laid down in article 24.

For example, the proposed regulation requires the processor to provide full documentation on the data processing (Article 28). In reality, most processors do not have the knowledge required to fulfil this obligation (for example, a cloud computing provider). The processor would be fully liable for the data processing carried out by it on behalf of the controller (Article 77). The processor might not even know the content of the processing carried out. In addition, it would become much more difficult to engage data processors, because the controller has to specify the conditions of the data processing (Article 4 (5)), which takes away flexibility needed to provide cost efficient services and adds substantial bureaucracy.

We see incoherence and inconsistency in several provisions of the draft regulation, leading to confusion between the controller and the processor obligation. It imposes for instance several obligations without distinction between processors and controllers (designation of a Data Protection Officer (DPO) – article 35; documentation requirements – article 28 etc.).

Under the current directive, processors are directed by controllers on what to do with the data they are provided. They rely on the controllers' assertions and instructions related to the data and act accordingly pursuant to the terms of the contractual arrangement between them. With the new proposals, processors will no longer be able to rely on controller assertions related to the data. They will need to have independent knowledge of the data needlessly expanding the scope of persons with detailed knowledge of the data. Furthermore processors will no longer be able to rely on controllers' instructions related to the data as they will need to evaluate those instructions in relation to their obligations. Since there is more than one compliant way to treat the data, this will decrease legal certainty and undermine the trust in the

controller processor relations. Processor obligations should continue to be controlled by and specified in contractual clauses between controller and processor.

A clear distinction should be made between the liabilities of the controller and those of the processor. In practice it would become confusing if both parties are liable for the same obligations.

Since the controller decides for which purposes the processing of personal data is done, he should be sole responsible for this. In his contract with the processor he should foresee the necessary guarantees to allow him to recover the damages that are due to the processor.

Example 1: The notification of a data breach to the national authority should be an obligation for the controller, not for the processor. The controller should however foresee in his contract with the processor that the processor should notify him of any data breach. (article 31)

Example 2: Only the controller should be liable for the mandatory privacy impact assessment. (article 33 and recital 66)

Other examples of this unnecessary double liability can be found in the articles 28 (documentation), 29 (co-operation with the supervising authority), 30 (security of processing), 34 (prior authorization and prior consultation), 35 (DPO) and 77 (right to compensation and liability).

For the same reasons as those mentioned above, the requirement to ask the prior permission of the controller before enlisting another processor (sub-contractor) is not acceptable (Article 26.2 (d)).

DOCUMENTATION, PRIVACY IMPACT ASSESSMENTS AND PRIOR CONSULTATIONS AND AUTHORISATIONS (ARTICLES 28, 33 AND 34)

1. DOCUMENTATION

The proposal introduces far-reaching documentation obligations as well as requirements on data protection impact assessments and prior consultations and authorisations which would significantly increase administrative burden for both controllers and processors.

The proposed documentation obligations are very detailed and the Commission is mandated to lay down standard forms for the documentation. We believe that data processing can be documented well in many ways and no specific method should be mandated. The obligation is disproportionate since it covers almost all processes. Documenting will be a very extensive process. The obligation will trigger high costs also for low-risk processes.

Example: The Italian privacy code (article 37), in line with articles 18 and 19 of the Directive 95/46/CE, limits the obligation of notification only to some kinds of data processing, namely to the risky ones, while the new obligation proposed would be to maintain all the documentation with no distinction. Moreover, this obligation does not indicate a maximum period for the maintenance of the documentation. This way, the new provision would introduce an unjustified burden for controllers, who would have no option but to fill hundreds of documents a day (for enterprises) including information already made known before.

As a consequence, Article 28 should be deleted as well as all references to it within the regulation (e.g. Article 22 paragraph 2a).

2. PRIVACY IMPACT ASSESSMENTS/PRIOR CONSULTATIONS

While the general obligations of diligence and planning should be maintained, prescriptive provisions on privacy impact assessments risk creating a „tick-box“ approach to data protection and should be re-considered. Privacy impact assessments are internal processes designed to identify and remedy risks to systems and processes in their development. Trying to turn such processes that often contain sensitive and proprietary organisational information into public accountability processes undermines the very essence of the process. There is no question that the results of such assessments may provide useful information to Data Protection Authorities in specific investigations or review of corporate processes. However, there should not be an obligation to file them in the ordinary course or otherwise publish results. We cannot emphasise strongly enough, how important a flexible framework is.

The proposed provisions on privacy impact assessments and prior consultations will add layers of burdensome bureaucracy for businesses and supervisory authorities but also consumers without reflecting best practices of planning and assessment work done by companies. One should also recall that simple registration filings were faced with substantial, sometimes multi-year, backlogs at many of the Data Protection Authorities. Delays in processing assessment of systems could severely impact the speed of deployment and implementation of systems limiting both innovation and competitiveness in the EU. There should be no prior consultation obligation for data processing which according to the assessment is in compliance with data protection legislation.

Also the obligation to consult data subjects or their representatives should be deleted or limited to specialised categories of data where the risks are high as it could e.g. risk the confidentiality of information and trade secrets, if a blanket approach is adopted.

Example 1: Article 33 foresees a mandatory privacy impact assessment where processing operations represent specific risks. The cost of such a privacy impact assessment is estimated between € 10.000 and 30.000, which is disproportionate.

Example 2: This obligation risks re-introducing in the Italian legal system a merely formal and bureaucratic document (so called “DPS”), with no utility with regard to data protection as it is only a collection of information and a description of overall aspects of data processing. The experience reached within the Italian system proves that such a fulfilment brings only useless costs and burdens, with no benefits in terms of data protection.

DATA BREACH NOTIFICATIONS (ARTICLES 4, 31 AND 32)

Mandatory notification requirements for all breaches, even minor ones, would impose significant compliance burden not only on controllers but also on supervisory authorities. They would aggravate “notification fatigue” amongst consumers and give them a false picture of security regarding companies. Only companies with good security will be able to identify breaches. Providers with poor security will fail to identify and notify any breaches. Therefore, they will appear secure for the end-users.

It should also be stressed that the 24-hours deadline for data breach notifications is in many cases unrealistic. Very often internal verification procedures of companies, aiming at assessing whether a data breach took place, last longer than 24 hours. If data breaches are notified before verification has been completed, this will lead in a series of corrective notifications and these will not improve data subjects’ trust.

Instead of the current proposal, a duty to notify the supervisory authority and data subjects without undue delay (but without strict deadlines) could be justified in data breaches that cause serious harm to data subjects and require action by data subjects to minimize the harm. Even in that case, the definition of data breach should be narrowed since the scope is too wide to be workable.

In addition, the obligation offers insufficient incentives for applying effective privacy-measures. Even when encrypted -non readable- data are lost, the supervisory authority should be notified. This is disproportional and does not stimulate organizations to take certain measures. An exception for encrypted 'data' should be in place.

Example: A company manager loses his or her laptop, containing personal data of another data subject. This laptop however is very well secured (encoded, encrypted) and so it is highly unlikely that the person who finds/stole it will be able to access the information on the laptop. In cases like these a notification to the supervisory authority has no added value.

DATA PROTECTION OFFICERS (DPOs) (ARTICLES 35, 36 AND 37)

The proposed regulation would make data protection officers mandatory for all public authorities, companies employing more than 250 persons, or controllers and processors whose core activities consist of processing operations which require regular and systematic monitoring of data subjects.



The proposal grants DPOs with a strong position (at least a two-year appointment, vague basis for dismissal). In addition, management should have the right to manage and dismiss the DPO according to collective agreements on the labour market.

Different kinds of organizational set-ups can result in effective data protection and current practices in Member States should be respected. Prescriptive and detailed provisions would be costly and burdensome in particular for organisations where data processing forms only a marginal part of their activities.

If such a regulation is adopted, companies with a DPO should be released from bureaucratic data reporting obligations in return.

TRANSFERS BY WAY OF APPROPRIATE SAFEGUARDS (ARTICLE 42)

Companies often have to transfer data to a third country or international organisation and this article provides safeguards for those transfers. The increased requirement for consent for international transfers risks disrupting emerging digital business models. For example in the newspaper industry, this will be feasible where consumers pay for content and already have a contract with the consumer, but will be much more difficult for free access models, where this requirement could impose a new relationship between the newspaper and the reader.

The requirement to obtain authorisation from the supervisory authority where transfers take place on the data controller's own standard contract clauses (Article 42(2)(d) contract clauses between the controller or processor) is also bureaucratic and burdensome and likely to lead to unnecessary delays in doing business.

The proposed regulation should specifically include the EU-U.S. Safe Harbor program as an appropriate safeguard enabling data transfers. Although as we understand from various communications that the Safe Harbor remains in place under the proposed regulation, it will be important to refer explicitly to this mechanism in an article or recital in order to avoid confusion.

BINDING CORPORATE RULES (ARTICLE 43)

Even though Binding Corporate Rules (BCRs) are more streamlined than in the past and work effectively once established, the administrative burden they continue to pose should be addressed. The utility of BCRs can also be enhanced by expanding their applicability across not just within groups of companies. If a company and its subsidiaries have a valid BCR it should be possible for them to transfer data to another company with a valid BCR. Today global information flows are not limited within groups of companies but exist across value chains. The regulation should reflect and enable that reality.

In order to reduce bureaucratic burden, intra-group data transfers have to be simplified. Unfortunately, the European Commission has not taken the opportunity to create a provision on intra-group data transfer which ensures legal certainty for data transfer not only within the EU but also beyond. The new data protection provisions envisaged with the regulation must be used to close this gap.

COMPETENCE OF SUPERVISORY AUTHORITIES (ARTICLE 4, 51)

BUSINESSEUROPE supports the "one-stop shop" approach enshrined in the draft regulation as it should simplify relations between businesses and supervisory authorities.

However, the regulation has to make sure that the single competent authority is comprehensively informed about all aspects which are relevant in the case concerned. The current wording of the proposal raises the need of clarity in the definition of main establishment (« *where the purposes, conditions and means of the processing of personal data are taken* ») and in the criteria to solve conflicts regarding the role of the supervisory authorities in cases of a business carrying out its activities in several Member States.

ADMINISTRATIVE SANCTIONS (ARTICLE 79)

The proposed regulation introduces very high administrative sanctions for violations based on a "one-size-fits-all" approach.

Example 1: Article 79.5.b. states that the supervisory authority *shall* impose a fine up to € 500.000 or 1% of an enterprise's worldwide turnover, to anyone who, *intentionally or negligently*, does not comply with the right to be forgotten or to erasure.

Example 2: Article 79.6 (h) foresees a fine of € 1.000.000 or 2% of an enterprise's worldwide turnover in case they intentionally or negligently, do not alert or notify a personal data breach.

BUSINESSEUROPE considers a competition law approach regarding the system of sanctions as inappropriate and unacceptable in the context of data protection legislation. In competition law, the sanction system is based on economic studies and understanding of the negative impacts of anti-competitive behaviour to the market dynamics which justifies the turnover-based way of calculating fines. This is not the case for the proposed administrative sanctions.

Even though effective and high- quality enforcement is essential, the proposed sanctions are excessive and disproportionate. Any sanction levied should be proportionate to the impact on data subjects. In our view, particularly in cases of first and non-intentional non-compliance, a warning procedure as well as pre-requisites for renouncing from inflicting sanctions should be considered (for ex. in case where a controller removed the risk of data protection breach and took all measures to avoid them in the future.).

Finally, there is no question that the application of the new regulation will lead to confusion. It will be difficult to differentiate between good faith efforts at compliance and mere negligence in the early stages of its application. Clearly greater emphasis should be placed on intentional violations of the regulation.



Reconsideration on the nature grouping and scope of transgressions in relation to fines should also occur as many minor and administrative failures of compliance are associated with a disproportionate range of fines. There should be a mechanism that gives companies the possibility to defend themselves against the allegations made by the supervisory authority (e.g. a right to be heard before any decision is taken). Supervisory authorities should not be obliged to fine shortcomings. This draconian and disproportionate range of fines may also have a chilling effect on digital innovation in the EU at a time when it can ill afford such potential limitation on growth and economic development.

COLLECTIVE REDRESS (ARTICLE 73, 75, 76)

Although support to data subjects regarding data protection is useful, the taking over by bodies, organizations or associations and bundling of supposed infringements will lead to business models based upon buying and exploiting claims. This will create a claim culture, where organizations will stop innovating or will have to take insurance policies, at the expense of the consumer cost or products and services. In addition, the European Commission is still assessing an overall approach to collective redress in the EU. Therefore, we believe it is inappropriate to come forward with a sector-specific proposal, before a general framework is agreed.

DELEGATED ACTS AND IMPLEMENTING ACTS (ARTICLE 86)

The proposed regulation includes 26 provisions that grant the Commission the power to adopt delegated acts and 19 provisions that allow the Commission to adopt implementing acts. There is hardly an issue that would not be substantially affected by delegated or implementing act. This is in many instances contrary to article 290 of the TFEU, which limits the use of delegated acts to “other than essential elements of an area”.

The numerous provisions on secondary rulemaking undermine legal predictability and risk neutralising the effectiveness of the provisions by complicating the data protection regime. They would mean that legislation would be constantly evolving and achieving compliance would be extremely difficult. The problematic nature of the provisions is further underlined by the fact that compliance with data protection legislation often requires significant and time-consuming data system investments.

We therefore call for a review of the provisions on secondary rulemaking and a limitation of the provisions on delegated acts and implementing acts, when justified, only to non-essential elements. Delegated acts and implementing acts should not for e.g. mandate business processes or technologies.

PROCESSING OF PERSONAL DATA AND FREEDOM OF EXPRESSION (ARTICLE 80)

The current directive allows companies in the business of journalism appropriate allowances to process personal data in the interests of freedom of expression.



In the context of the proposed regulation, it would be helpful to have more certainty around the freedom of expression exemption (Art 80) as this could be of concern for news businesses (i.e. to avoid that Member States decide what the freedom of expression exemption should look like). Unless there is more clarity in the proposed regulation we could have a situation where information from a news story had to be deleted in one jurisdiction but not in another due to countries applying different balancing tests.

RELATIONSHIP BETWEEN REGULATION AND DIRECTIVE 2002/58/EC (DPEC)

Many businesses will be subject to obligations under both the Regulation and DPEC. The wording of Article 89 paragraph 1 is not straightforward to apply, although it appears to be on the face of it.

We need further clarity to understand how the delineation between the two is intended to operate in practice.

* * *



GENERAL DATA PROTECTION REGULATION SUGGESTIONS FOR AMENDMENTS

INDEX

- [Definition of personal data \(article 4\(1\)\)](#)
- [Main establishment \(articles 3 and 4 \(13\)\)](#)
- [Consent \(article 4 \(8\)\)](#)
- [Data protection and intermediary liability \(article 2\(3\)\)](#)
- [Right to be forgotten \(article 17\)](#)
- [Privacy by default / privacy by design \(article 23\)](#)
- [Sanctions \(article 79\)](#)

DEFINITION OF PERSONAL DATA (ARTICLE 4 (1))

BACKGROUND

While the current Directive 95/46/EC is centered around a definition of 'personal data', the proposed Regulation instead defines who is a 'data subject'. The change of approach is determined by the Commission's willingness to make the consumer the focal point of the reform. To ensure maximum protection of personal data, the Regulation lowered the threshold for identifying personal data stating that data are personal if "identifiable" by any "third party" ("by any other natural or legal person") with the consequence of virtually making any information to qualify as personal.

PROBLEM(S) IDENTIFIED

The personal data definition proposed by the Commission has been considerably broadened to cover an unlimited amount of information, irrespective of their nature or the context in which they are processed or whether they are anonymised/pseudonymised or not, or whether the controller had any intention to identify a user.

This is due to the fact that the relevant angle to determine 'identifiability' of a person is not limited, as has previously been the case, to the perspective of the controller, but has been extended to the perspective of 'any other natural or legal person', irrespective of the relationship with the controller. For instance, an IP address can arguably not be personal data to a website operator while it is for the access provider that assigned it. According to the current text proposal, the simple fact that a third party (in the example the access provider) is able to identify the individual on the basis of information available to him renders such information as personal *per se* also for the website provider.

This circumstance removes incentive for companies to invest in privacy enhancing measures as there will be no secure way to anonymise or pseudonymous information any longer. Coupled with the new "explicit consent" requirement, this broad definition of personal data is particularly problematic, as virtually any information will require the users' explicit consent. Rules applying to such a broad definition risk to be unworkable in practice and to generate legal uncertainty.

Finally, by mentioning 'online identifiers' 'location data', the definition of data subject is not technologically neutral.

PROPOSED SOLUTION(S)

In order to make the definition of personal data workable in practice, a "context based approach" should be introduced in the definition. This means that the personal character of the data should depend on who is processing it, how, and for what purpose:

- Data should only be considered as personal where it is reasonably likely that, based on the context, the data controller or processor has the intention to use data in a way that requires personal identification of the data subject or where there is a realistic risk of such identification.
- The reference to "online identifier" and "location data" is not technology neutral and should be deleted. Additionally, as to online identifiers, if we consider them to be IP-addresses, they are already included in the broader definition of "identification number".
- A clear definition of pseudonymous data should be introduced. Also, in cases where data is used to distinguish between users, rather than identifying them, the data should not be considered as personal.
- Anonymised data should be defined in the text as not being personal data.
- The lawful grounds for processing (article 6) should also be modified to reflect the specificities of pseudonymous and anonymous data.
- Finally, the reference to delegated acts should be deleted.

General Data Protection Regulation Article 2

Definitions

For the purposes of this Regulation:

(1) 'data subject' means an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller **or by any other natural or legal person, in particular** by reference to an identification number, **location data, online identifier** or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;

(2) 'personal data' means any information **relating to** a data subject;

Amendments Article 4

Definitions

For the purposes of this Regulation:

(1) 'data subject' means an identified natural person or a natural person who can, **based on the context of the specific processing**, be identified, directly or indirectly, by means reasonably likely to be used by the controller **or the processor** ~~or by any other natural or legal person~~, **including** in particular by reference to an identification number, ~~location data, online identifier~~ or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person; **these means factors as such need not necessarily be considered as personal data in all circumstances;**

(2) 'personal data' means any information **used to directly or indirectly identify** ~~relating to~~ a data subject;

NEW (3) Pseudonymous data means any personal data that has been collected, altered or otherwise processed in such a way that any personal characteristics, such as the name or other personal identifiers, are replaced with a code so that the data

subject can no longer be identified or that identifiability would require a disproportionate amount of time, cost and effort.

NEW (4) “Anonymous data” means any information that has been collected, altered or otherwise processed in such a way that it cannot be attributed to a data subject.

RECITALS

NEW

Pseudonymisation is the process of disguising identities. The aim of such a process is to be able to collect additional data relating to the same individual without having to know his identity (i.e. research and statistics). Pseudonymisation can be done in a retraceable way by using correspondence lists for identities and their pseudonyms or by using two-way cryptography algorithms for pseudonymisation. Key-coded data are a classical example of pseudonymisation. Information relates to individuals that are earmarked by a code, while the key making the correspondence between the code and the common identifiers of the individuals (like name, date of birth, address) is kept separately.

(23) The principles of protection should apply to any information concerning an identified or identifiable person. To determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used **either** by the controller **or by any other person** to identify the individual. The principles of data protection should not apply to data rendered anonymous in such a way that the data subject is no longer identifiable.

(23) The principles of protection should apply to any information concerning an identified or identifiable person. To determine whether a person is identifiable, account should be taken of all the means **that are technically feasible, do not involve a disproportionate effort, and are** likely reasonably to be used ~~either~~ by the controller **or the processor** ~~by any other person~~ to identify the individual, **based on the context of the specific processing. In cases where data is used to distinguish between data subjects, rather than identifying them, these data shall be considered as pseudonymous personal data.** The principles of data protection should not apply to data rendered anonymous in such a way that the data subject is no longer identifiable, **taking into account the technological “state of the art”.**

Article 2

Material Scope

(...)

Article 2

Material Scope

(...)

2. This Regulation does not apply to the processing of personal data:

- (a) in the course of an activity which falls outside the scope of Union law, in particular concerning national security;
- (b) by the Union institutions, bodies, offices and agencies;
- (c) by the Member States when carrying out activities which fall within the scope of Chapter 2 of the Treaty on European Union;
- (d) by a natural person without any gainful interest in the course of its own exclusively personal or household activity;
- (e) by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

Article 6

Lawfulness of processing

1. Processing of personal data shall be lawful only if and to the extent that at least one of the following applies:

- (a) the data subject has given consent to the processing of their personal data for one or more specific purposes;
- (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- (c) processing is necessary for compliance with a legal obligation to which the controller is subject;
- (d) processing is necessary in order to protect the vital interests of the data subject;
- (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- (f) processing is necessary for the purposes of the legitimate interests pursued by a controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks;

2. This Regulation does not apply to the processing of personal data:

- (a) in the course of an activity which falls outside the scope of Union law, in particular concerning national security;
- (b) by the Union institutions, bodies, offices and agencies;
- (c) by the Member States when carrying out activities which fall within the scope of Chapter 2 of the Treaty on European Union;
- (d) by a natural person without any gainful interest in the course of its own exclusively personal or household activity;
- (e) by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties;

(f) that has been rendered anonymous

Article 6

Lawfulness of processing

1. Processing of personal data shall be lawful only if and to the extent that at least one of the following applies:

- (a) the data subject has given consent to the processing of their personal data for one or more specific purposes;
- (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- (c) processing is necessary for compliance with a legal obligation to which the controller is subject;
- (d) processing is necessary in order to protect the vital interests of the data subject;
- (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- (f) processing is necessary for the purposes of the legitimate interests pursued by a controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks;

NEW (g) processing is necessary for the implementation of technical security

measures or mechanisms to ensure the protection of personal data or for the prevention of fraud;

NEW (h) processing of pseudonymous data is lawful, provided that the data subject does not object;

NEW (i) processing of anonymised data is lawful at all times.

(...)

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the conditions referred to in point (f) of paragraph 1 for various sectors and data processing situations, including as regards the processing of personal data related to a child.

(...)

~~5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the conditions referred to in point (f) of paragraph 1 for various sectors and data processing situations, including as regards the processing of personal data related to a child.~~



MAIN ESTABLISHMENT (ARTICLES 3 AND 4 (13))

BACKGROUND

With the proposed Regulation, the Commission intends to truly harmonise the rules governing the processing of personal data in the European Union and clarify the rules on applicable law. It is proposed to put in place one single set of data protection rules (i.e. the Regulation) applicable throughout the EU coupled with a so called “one stop shop” enforcement system, establishing the competence of one single national data protection authority (DPA), in particular where companies operate and process personal data in more than one Member State. Purpose of the creation of the one-stop-shop is to achieve consistent application of the Regulation throughout all Member States, provide legal certainty and reduce administrative burdens for data controllers and processors. The one stop shop is determined on the basis either of the “main establishment” of a company within the EU or, where a company’s main establishment is outside the EU, the “place of residence of the consumer” who is being offered products or services or whose behavior is being monitored. As concerns the second circumstance, the idea is to extend the extra territorial application of the Regulation to any processing of personal data even if carried in a third country.

PROBLEM(S) IDENTIFIED

- Article 4 (13) defines the “main establishment” differently for data controllers vis-à-vis to data processors. **As regards the controller**, main establishment means the place of its establishment in the Union where the main decisions as to the purposes, conditions and means of the processing of personal data are taken. If no such decisions are taken in the Union, the main establishment is the place where the main processing activities in the context of the activities of an establishment of a controller in the Union take place. **As regards the processor**, main establishment means the place of its central administration in the Union. The reasoning behind this different regime for controllers and processors is, however, unclear.
- Article 51(2) of the Regulation foresees that the competent authority, providing the one-stop shop, is the supervisory authority of the Member State in which the controller or processor has its main establishment. Consumers, however, will be able to issue a complaint in their own country even if the controller or processor is established elsewhere (Article 73). However, the Regulation is silent on the question of how supervisory authorities should act when receiving a complaint concerning a controller whose main establishment is in a different country. Furthermore, it is unclear how cooperation between the different data protection authorities would work in practice, so putting at risk the creation of a level playing field in the EU.
- The fact that the Regulation applies to any processing of personal data in the context of activities of an establishment in the Union, even if this processing takes place outside of the EU, means that EU rules apply whenever actors operating in third countries target EU users (Article 3). It could be particularly complex for international companies operating from different geographical regions of the world if they have to implement potentially conflicting legislation, i.e. their own national law and within the EU.
- Applicable law criteria in those cases where national law builds on or exempts from the Regulation should be clearly laid out.

PROPOSED SOLUTION(S)

- A uniform definition of main establishment for both data controller and processor should be considered
- The term 'main establishment' requires further clarification. It could be understood as the company's central administration. Objective criteria need to be elaborated to define it and a clear reference to the role of the "representative" for those companies established outside the EU should be foreseen.
- For groups of undertakings, the designation of the 'main establishment' should apply to all entities part of the group established in the Union. The lead DPA for the company's main establishment should be competent to supervise all processing carried out by all entities of the group as far as they are subject to the Regulation
- The cooperation and consistency mechanism between DPAs needs to be strengthened further to allow for a true one stop shop. DPAs who receive a complaint or have others reasons to investigate with respect to a controller whose main establishment is located in a Member State different from the consumer's place of residence should be required to refer the matter to the lead DPA. The latter should be leading for all privacy matters concerning companies with a main establishment in its jurisdiction
- The extra territorial application of the Regulation vis-à-vis controllers established in third countries processing personal data of EU citizens should be clarified to only cover situations where goods and services are specifically targeted at EU citizens. In particular¹, due account must be taken of the jurisprudence of the European Court of Justice.

General Data Protection Regulation

Article 4

Definitions

(13) 'main establishment' means as regards the controller, the place of **its establishment** in the Union where the main decisions as to **the purposes, conditions and means of** the processing of personal data are taken; if no decisions as to **the purposes, conditions and means of** the processing of personal data are taken in the Union, the main establishment is the place where the **main processing activities in the context of the activities of an establishment of a controller** in the Union **take place. As regards the processor, 'main establishment' means the place of its central administration in the Union;**

Amendments

Article 4

Definitions

(13) 'main establishment' means, as regards the controller **and the processor**, the place of **their its-establishment central administration** in the Union, **or in the absence of such administration, the place** where the main decisions as to ~~the purposes, conditions and means of~~ the processing of personal data are taken, **in accordance with their respective competences**; if no decisions as to ~~the purposes, conditions and means of~~ the processing of personal data are taken in the Union, the main establishment is the place where the **controller or processor has its representative** ~~main processing activities in the context of the activities of an establishment of a controller~~ in the Union ~~take place. As regards the processor, 'main establishment' means the place of its central administration in the Union;~~

¹ In the Hotel Alpenhof GesmbH v Oliver Heller case (C-144/09), the ECJ elaborated objective criteria that can be used to assess the intention of an operator to expressly target EU citizens such as the use of a language or a currency other than the language or currency generally used in the country in which the operator is established, the possibility of making and confirming the reservation in that other language, the use of a top-level domain name with the .eu suffix or other than that of the country in which the merchant is established.

NEW 13 (a) The designation of the ‘main establishment’ should apply to all entities part of a group of undertakings established in the Union

NEW 13 (b) The controller and processor shall communicate their main establishment to the competent supervisory authority.

Article 51

Competence

(...)

2. Where the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union, and the controller or processor is established in more than one Member State, the supervisory authority of the main establishment of the controller or processor shall be competent for the supervision of the processing activities of the controller or the processor in all Member States, without prejudice to the provisions of Chapter VII of this Regulation.

(...)

Article 3

Territorial scope

(...)

2. This Regulation applies to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are related to:
(a) the offering of goods or services to such data subjects in the Union; or
(b) the monitoring of their behaviour.

Article 51

Competence

(...)

2. Where the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union, and the controller or processor is established in more than one Member State, the supervisory authority of the main establishment of the controller or processor shall be competent for the supervision of the processing activities of the controller or the processor in all Member States **and, in the case of a group of undertakings, of any member of the group**, without prejudice to the provisions of Chapter VII of this Regulation.

NEW 3. Where the controller or processor has designated a representative in the Union pursuant to Article 25, the supervisory authority of the establishment of the representative in accordance with Article 25.4 shall be competent for the supervision, in all Member States, of all processing activities of that controller or processor.

(...)

Article 3

Territorial scope

(...)

2. This Regulation applies to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities, **including the monitoring of behaviour**, are related to ~~(a) the targeted~~ offering of goods or services to such data subjects in the Union; ~~or~~
~~(b) the monitoring of their behaviour.~~

(...)

RECITAL

(20) In order to ensure that individuals are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects residing in the Union by a controller not established in the Union should be subject to this Regulation where the processing activities are related to the offering of goods or services to such data subjects, **or to the monitoring of the behaviour of such data subjects.**

(27) The main establishment of a controller **in the Union** should be determined according to objective criteria **and** should imply the effective and real exercise of management activities determining the main decisions as to the **purposes, conditions and means of processing** through stable arrangements. This criterion should not depend whether the processing of personal data is actually carried out at that location; the presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute such main establishment and are therefore no determining criteria for a main establishment. **The main establishment of the processor should be the place of its central administration in the Union.**

(...)

RECITAL

(20) In order to ensure that individuals are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects residing in the Union by a controller not established in the Union should be subject to this Regulation where the processing activities, **including the monitoring of the behaviour of such data subjects,** are related to the ~~targeted~~ offering of goods or services to such data subjects, ~~or to the monitoring of the behaviour of such data subjects~~ **in accordance with the jurisprudence of the European Court of Justice and based on objective criteria that can be used to assess the intention of an operator to target EU citizens such as the use of a language or a currency other than the language or currency generally used in the country in which the operator is established, the possibility of making and confirming the transaction in that other language, the use of a top-level domain name with the .eu suffix or other than that of the country in which the operator is established.**

(27) The main establishment of a controller **or a processor in the Union should be the place of their central administration which should be determined according to the following objective criteria: the location of the group's European headquarter or the location of the company within the group with delegated data protection responsibilities. In the absence of a central administration, the main establishment is the place where the main decisions as to the purposes, conditions and means of processing are taken.** ~~and,~~ **As regards the controller, the main establishment** should imply the effective and real exercise of management activities determining the main decisions as to the ~~purposes, conditions and means of processing~~ through stable arrangements. This criterion should not depend whether the processing of personal data is actually carried out at that location; the presence and use of technical means and technologies for processing personal data or

processing activities do not, in themselves, constitute such main establishment and are therefore no determining criteria for a main establishment. ~~The main establishment of the processor should be the place of its central administration in the Union.~~



CONSENT (ARTICLE 4 (8))

BACKGROUND

The Regulation sets stricter thresholds as compared to the current Directive 95/46 by defining consent as "freely given specific, informed and explicit indication" of an individual's wishes. The requirement for consent to always be "explicit", irrespective of the context for which consent is being obtained or the risks involved in the processing operation for the individual, could be construed as always requiring a "yes" response to having one's personal data processed. According to Recital 25 of the Regulation, explicit consent can be provided "either by a statement or by a clear affirmative action", but would not encompass consent implied from individuals' actions or behaviour.

PROBLEM(S) IDENTIFIED

The proposed approach is too formalistic and rigid, creates uncertainty and practical problems, without adding anything to individuals' data protection. In fact the current and future technology environment allows for consent to be inferred or implied from users' actions. However, this would not meet the threshold set in Article 4 (8) for explicit consent. This is even more restrictive for Internet operators if one considers that - in conjunction with Article 7 (Conditions for consent) - an increased reliance is introduced on (explicit) consent as the preferred legal basis for data processing over other possible grounds as foreseen in Article 6 (Lawfulness of processing), i.e. processing for the performance of a contract; for compliance with legal obligation; for the purposes of a legitimate interest pursued by a controller.

Finally, article 7 (4) states that consent cannot be used in case of 'significant imbalance' between the position of the data subject and the controller. This provision is confusing and might risk creating a situation where companies with bargaining power will never be able to rely on consent.

PROPOSED SOLUTION(S)

A context based approach should be introduced allowing the controller to select the most appropriate way/mechanism of providing information, obtaining meaningful consent and offering control to data subjects, depending on the context of the specific data use and the risks involved for data subjects. The "explicit" requirement should be replaced by a more flexible criterion that, while guaranteeing a higher level of protection of data subjects, would make the Regulation more technology neutral and, particularly, not chill technology innovation.

General Data Protection Regulation

Article 4

Definitions

For the purposes of this Regulation:

(8) 'the data subject's consent' means any freely given specific, informed and **explicit** indication of his or her wishes by which the

Amendments

Article 4

Definitions

For the purposes of this Regulation:

(8) 'the data subject's consent' means any freely given specific, informed and **verifiable** ~~explicit~~ indication of his or her wishes by which the data subject, either by a statement or **through his behavior** ~~by a clear affirmative~~

data subject, either by a statement or **by a clear affirmative action**, signifies agreement to personal data relating to them being processed;

Article 7

Conditions for consent

1. The controller shall bear the burden of proof for the data subject's consent to the processing of their personal data for specified purposes.

2. If the data subject's consent is to be given in the context of a written declaration which also concerns another matter, the requirement to give consent must be presented distinguishable in its appearance from this other matter.

3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

4. Consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller.

RECITAL

(25) Consent should be given **explicitly** by any appropriate method enabling a freely given specific **and** informed indication of the data subject's wishes, either by a statement or **by a clear affirmative action by the data subject**, ensuring that individuals are aware that they give their consent to the processing of personal data, including by ticking a box when visiting an Internet website or by any other statement or **conduct** which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data. Silence or inactivity should therefore not constitute consent. Consent

action, signifies agreement to personal data relating to them being processed;

Article 7

Conditions for consent

1. The controller shall bear the burden of proof for the data subject's consent to the processing of their personal data for specified purposes. **If the data processed by the controller do not permit the controller to identify the data subject, the controller shall not be obliged to acquire additional information in order to identify the data subject for the sole purpose of proving his consent.**

2. If the data subject's consent is to be given in the context of a written declaration which also concerns another matter, the requirement to give consent must be presented distinguishable in its appearance from this other matter.

3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

4. Consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller **in accordance with EU and Member States' law.**

RECITAL

(25) Consent should be given *explicitly* by any appropriate method enabling a freely given specific, *and* informed **and verifiable** indication of the data subject's wishes. **This indication can be given either by a statement (including a clear affirmative action) or through the behavior of the data subject, ~~by a clear affirmative action by the data subject,~~ ensuring that individuals are aware that they give their consent to the processing of personal data, including by ticking a box when visiting an Internet website or by any other statement or **behavior** ~~conduct~~ which clearly indicates in this context**

should cover all processing activities carried out for the same purpose or purposes. If the data subject's consent is to be given following an electronic request, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.

(32) Where processing is based on the data subject's consent, the controller should have the burden of proving that the data subject has given the consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware that and to what extent consent is given.

*(33) In order to ensure free consent, it should be clarified that consent does not provide a valid legal ground where the individual has no genuine and free choice and is subsequently not able to refuse or withdraw consent **without detriment**.*

(34) Consent should not provide a valid legal ground for the processing of personal data, where there is a clear imbalance between the data subject and the controller. This is especially the case where the data subject is in a situation of dependence from the controller, among others, where personal data are processed by the employer of employees' personal data in the employment context. Where the controller is a public authority, there would be an imbalance only in the specific data processing operations where the public authority can impose an obligation by virtue of its relevant public powers and the consent cannot be deemed as freely given, taking into account the +interest of the data subject.

the data subject's acceptance of the proposed processing of their personal data. Silence or inactivity should therefore not constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. If the data subject's consent is to be given following an electronic request, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.

*(32) Where processing is based on the data subject's consent, the controller should have the burden of proving that the data subject has given the consent to the processing operation. **If the data processed by the controller, however, do not permit the controller to identify the data subject, the controller shall not be obliged to acquire additional information in order to identify the data subject for the sole purpose of proving his consent.** In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware that and to what extent consent is given.*

*(33) In order to ensure free consent, it should be clarified that consent does not provide a valid legal ground where the individual has no genuine and free choice and is subsequently not able to refuse or withdraw consent **without detriment**.*

*(34) Consent should not provide a valid legal ground for the processing of personal data, where there is a clear imbalance between the data subject and the controller **in accordance with EU and Member States' law**. This is especially the case where the data subject is in a situation of dependence from the controller, among others, where personal data are processed by the employer of employees' personal data in the employment context. Where the controller is a public authority, there would be an imbalance only in the specific data processing operations where the public authority can impose an obligation by virtue of its relevant public powers and the consent cannot be deemed as freely given, taking into account the interest of the data subject.*



DATA PROTECTION AND INTERMEDIARY LIABILITY (ARTICLE 2(3))

BACKGROUND

Both the EU data protection rules and the intermediary liability regime of the E-Commerce Directive are of major importance to online intermediaries. However, the interpretation of, and interplay between, these two legal instruments is unclear, leading to a number of legal challenges for Internet operators. Indeed, Article 1 (5) (b) of the E-commerce Directive states that the Directive does not apply to "questions relating to information society services covered by Directive 95/45/EC (...) [Data Protection Directive]". There is a risk that authorities could make online intermediaries fully liable for data protection violations by third parties, even in the case where the intermediary "expeditiously" takes down illegal content upon being made aware of the breach of data protection rules, in the meaning of Article 14 of the E-Commerce Directive.

PROBLEMS IDENTIFIED

As it currently stands, it is not clear whether the protection granted by the E-Commerce Directive does apply to circumstances where an intermediary is dealing with personal data. The lack of confirmation deprives the intermediary of a needed legal protection. In order to address this shortcoming, the Commission introduced an explicit reference in the scope of the Regulation referring to the E-Commerce Directive (Article 2, 3). This allows an intermediary to be subject to data protection obligations only if it is acting as a controller because only a controller is in the position to take decisions related to the processing of personal data. Accordingly, while service providers should be held liable for their own collection and use of personal data of individuals (i.e., when they act as controllers), this same liability needs to be limited where it concerns data protection issues related to third party use of online services.

PROPOSED SOLUTION(S)

In order to address the legitimate concerns of the intermediaries, a clarification of the scope of the Regulation to the E-Commerce Directive regime should be introduced in the text.

Directive 95/46/EC

**General Data Protection Regulation
RECITAL**

NEW

The liability limitations of the Directive on Electronic Commerce 2000/31/EC are horizontal in nature and therefore apply to relevant activities of all information society service providers. This Regulation establishes the rules for the processing of personal data, determines what constitutes a privacy and data

protection infringement, while the Directive on Electronic Commerce sets out the conditions by which an information service provider is liable for third party infringements of the law. In the interest of legal certainty for European citizens and businesses, the clear and distinct roles of the two instruments need to be respected.

This consistency can be ensured by holding service providers, other than controllers, acting only as conduits or merely providing automatic, intermediate and temporary storage or storage of information provided by a recipient of the service or allowing or facilitating the search of or access to personal data, shall not be responsible for personal data transmitted or otherwise processed or made available by or through them.



RIGHT TO BE FORGOTTEN (ARTICLE 17)

BACKGROUND

One of the main goals of the Regulation is to put data subjects in control of their personal data. In addition to the existing general right to erasure under the current Directive 95/46/EC (where article 12 requires controllers to erase personal data at the request of the data subject where the data can no longer be processed in accordance with the law), the Regulation tries to reinforce this right for the online environment. Indeed it requires controllers that have made information available about an individual public (whether this happened upon request of the individual or not) to inform “third parties” that are processing the data of the request of the data subject to erase any links to, or copy, or replications of the data (so called Right to be Forgotten).

PROBLEM(S) IDENTIFIED

The obligation for data controllers to inform third parties that are processing the data of the request of the data subject is vague as to the procedure to be used and risks to be extremely difficult to implement in practice. For an Internet provider it is not always possible to identify who has accessed the data and might be processing it. Furthermore, the fact that the obligation also concerns data that were consciously made public by the user makes it even more unreasonable to require the Internet provider to inform every potential “third party” (concept not defined by the Regulation) of the wishes of the data subject to have the data deleted. In that case, the obligation to inform third parties should lie with the data subject instead of the controller. Finally, the Regulation states that where erasure is carried out, data cannot be processed further. The complete removal of all data, however, could negatively affect the capability of the controller to verify or prove compliance with the requests of the data subject.

PROPOSED SOLUTION(S)

The proposed rules regarding the right to be forgotten and corresponding obligations for controllers should be clarified. The interest of the user to be forgotten and the legitimate interests pursued by the controller for processing need to be balanced.

The obligation for controllers should only apply vis-à-vis recipients of data to whom the controller has transferred the data (i.e. when a contractual relation exists). This situation, however, is already covered by article 13, which foresees that “the controller shall communicate any rectification or erasure to each recipient to whom the data have been disclosed unless this proves impossible or involves a disproportionate effort”. Therefore article 17 (2) does not add anything to what already exists in the proposed Regulation and should be deleted.

Additionally, article 17 (8) (saying that where erasure is carried out, the data cannot otherwise be processed) should be modified in a way to allow the controller to verify or prove compliance with the requests of the data subject, or to allow processing for billing purposes.

General Data Protection Regulation

Article 17

Right **to be forgotten** and to erasure

Amendments

Article 17

Right to be forgotten and to erasure

(...)

2. Where the controller referred to in paragraph 1 has made the personal data public, it shall take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible, to inform third parties which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data. Where the controller has authorised a third party publication of personal data, the controller shall be considered responsible for that publication.

(...)

8. Where the erasure is carried out, the controller shall not otherwise process such personal data.

RECITAL

(53) Any person should have the right to have personal data concerning them rectified **and a 'right to be forgotten'** where the retention of such data is not in compliance with this Regulation. In particular, data subjects should have the right that their personal data are erased and no longer processed, where the data are no longer necessary in relation to the purposes for which the data are collected or otherwise processed, where data subjects have withdrawn their consent for processing or where they object to the processing of personal data concerning them or where the processing of their personal data otherwise does not comply with this Regulation. This right is particularly relevant, when the data subject has given their consent as a child, when not being fully aware of the risks involved by the processing, and later wants to remove such personal data especially on the Internet. However, the further retention of the data should be allowed where it is necessary for historical, statistical and scientific research purposes, for reasons of public interest in the area of public health, for exercising the right of freedom of expression, when required by law or where there is a reason to restrict the processing of the data instead of erasing them.

(...)

~~2. Where the controller referred to in paragraph 1 has made the personal data public, it shall take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible, to inform third parties which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data. Where the controller has authorised a third party publication of personal data, the controller shall be considered responsible for that publication.~~

(...)

8. Where the erasure is carried out, the controller shall not otherwise process such personal data, **unless to prove compliance with the data subject's request or to allow processing for billing purposes.**

RECITAL

(53) Any person should have the right to have personal data concerning them rectified ~~and a~~ 'right to be forgotten' where the retention of such data is not in compliance with this Regulation. In particular, data subjects should have the right that their personal data are erased and no longer processed, where the data are no longer necessary in relation to the purposes for which the data are collected or otherwise processed, where data subjects have withdrawn their consent for processing or where they object to the processing of personal data concerning them or where the processing of their personal data otherwise does not comply with this Regulation. This right is particularly relevant, when the data subject has given their consent as a child, when not being fully aware of the risks involved by the processing, and later wants to remove such personal data especially on the Internet. However, the further retention of the data should be allowed where it is necessary for historical, statistical and scientific research purposes, for reasons of public interest in the area of public health, for exercising the right of freedom of expression, when required by law, **to prove compliance with the data subject's request, to allow processing for billing purposes** or where there is a reason to restrict the processing of the data instead of

erasing them.

(54) To strengthen the 'right to be forgotten' in the online environment, the right to erasure should also be extended in such a way that a controller who has made the personal data public should be obliged to inform third parties which are processing such data that a data subject requests them to erase any links to, or copies or replications of that personal data. To ensure this information, the controller should take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible. In relation to a third party publication of personal data, the controller should be considered responsible for the publication, where the controller has authorised the publication by the third party.

~~(54) To strengthen the 'right to be forgotten' in the online environment, the right to erasure should also be extended in such a way that a controller who has made the personal data public should be obliged to inform third parties which are processing such data that a data subject requests them to erase any links to, or copies or replications of that personal data. To ensure this information, the controller should take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible. In relation to a third party publication of personal data, the controller should be considered responsible for the publication, where the controller has authorised the publication by the third party.~~



PRIVACY BY DEFAULT / PRIVACY BY DESIGN (ARTICLE 23)

BACKGROUND

The principles of data protection by design and data protection by default have been included explicitly in the proposed Regulation. Article 23 obliges the controller to implement processes allowing for data protection aspects to be carefully considered both at design and implementation stage of products and services. The new provision (article 23 (1)) frames the obligation of the controller to implement these principles both at the time of the determination of the means for processing and at the time of the processing itself, and to do so in the context of “the state of the art and the cost of implementation” while ensuring that “appropriate technical and organisational measures and procedures” are in place.

PROBLEM(S) IDENTIFIED

Article 23 (2) which deals with privacy by default, is redundant as it is limited to repeating the principle of “data minimisation” already contained in Article 5 of the Regulation (i.e. data retention/collection should be limited to those data which are strictly necessary for the processing). Additionally, the article mandates that the collection of data by default be justified according to “each specific purpose of the processing”, ignoring the fact that some perfectly legitimate and socially desirable uses data may be unknown at the time of collection. Finally, the new provision empowers the Commission to “lay down technical standards”. The imposition of such standards would create legal, investment and development uncertainty and hinder, rather than promote, user privacy.

PROPOSED SOLUTION(S)

- Privacy by design should be implemented by industry according to the means it has at its disposal, based on the most appropriate mechanisms for the specific business model and on the accountability principle. Therefore, the reference to delegated acts should be deleted.

- Any reference to privacy by default should be deleted as Article 5 of the Regulation already set obligations on data minimisation.

General Data Protection Regulation Article 23

Data protection by design and by default

(...)

2. The controller shall implement mechanisms for ensuring that, **by default**, personal data shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data **only those personal data are processed which are necessary for each**

Amendments Article 23

Data protection by design and by default

(...)

2. The controller shall implement mechanisms for ensuring that, ~~by default~~, personal data shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data ~~only those personal data are processed which are necessary for each specific purpose of the~~

specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals.

3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures and mechanisms referred to in paragraph 1 and 2, in particular for data protection by design requirements applicable across sectors, products and services.

4. The Commission may lay down technical standards for the requirements laid down in paragraph 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

(61) The protection of the rights and freedoms of data subjects with regard to the processing of personal data require that appropriate technical and organizational measures are taken, both at the time of the design of the processing and at the time of the processing itself, to ensure that the requirements of this Regulation are met. In order to ensure and demonstrate compliance with this Regulation, the controller should adopt internal policies and implement appropriate measures, which meet in particular the principles of data protection by **design and data protection by default**.

~~processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals.~~

~~3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures and mechanisms referred to in paragraph 1 and 2, in particular for data protection by design requirements applicable across sectors, products and services.~~

~~4. The Commission may lay down technical standards for the requirements laid down in paragraph 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).~~

(61) The protection of the rights and freedoms of data subjects with regard to the processing of personal data require that appropriate technical and organizational measures are taken, both at the time of the design of the processing and at the time of the processing itself, to ensure that the requirements of this Regulation are met. In order to ensure and demonstrate compliance with this Regulation, the controller should adopt internal policies and implement appropriate measures, which meet in particular the principles of data protection by ~~design and data protection by default~~.



SANCTIONS (ARTICLE 79)

BACKGROUND

The Commission wishes to strengthen the role of national Data Protection Authorities (DPAs) by enabling them to issue fines that are sufficiently dissuasive. While Directive 95/46EC left it to the Member States to lay down in national law the sanctions to be imposed in case of infringement (Article 24), the proposed Regulation foresees specific sanctions to be issued by national DPAs.

PROBLEM(S) IDENTIFIED

Article 79 of the proposed Regulation foresees that, depending on the violation, companies can be sanctioned with a fine ranging from 0,5% to up to 2% of their annual worldwide turnover. This approach would be burdensome for SMEs but also create an uneven playing field between multinational companies and companies without global outreach.

PROPOSED SOLUTION(S)

The reference to companies' global turnover should be deleted and the turnover should be capped at the maximum amount that can be imposed.

The word 'shall' in article 79 (4 – 6) should be replaced by 'may' in order to provide DPAs with flexibility in deciding whether or not it is necessary to impose a fine at all.

The proportionality of breaches allocated to the highest category of sanction should be re-considered (i.e. breaching the provision requiring maintenance of documentation triggers a fine of 0.5% of global annual turnover, which is disproportionate considering that this is a simple administrative fault without substantial damage to individuals. In general fines should be reserved to most substantial and severe breaches).

As regards the calculation of the amount of the sanction, the following circumstances should be considered:

- the actual damage suffered by the data subject or the actual risk of suffering a damage;
- the presence of aggravating circumstance such as repeated violations, refusal to cooperate or deliberate violations causing substantial damage;
- the presence of mitigating circumstances such as measures taken by the controller or processor to ensure compliance with the Regulation, immediate termination of the violation upon knowledge or cooperation with enforcement processes.

Finally, the consistency mechanism should be used to cover divergences in the application of the administrative sanctions.

General Data Protection Regulation
Article 79

Administrative sanctions

(...)

2. The administrative sanction shall be in each individual case effective, proportionate and

Amendments
Article 79

Administrative sanctions

(...)

2. The administrative sanction shall be in each individual case effective, proportionate and

dissuasive. The amount of the administrative fine shall be **fixed** with due regard to the nature, gravity and duration of the breach, the intentional or negligent character of the infringement, the degree of responsibility of the natural or legal person and of previous breaches by this person, the technical and organisational measures and procedures implemented pursuant to Article 23 and the degree of cooperation with the supervisory authority in order to remedy the breach.

(...)

4. The supervisory authority **shall** impose a fine up to 250 000 EUR, **or in case of an enterprise up to 0,5 % of its annual worldwide turnover**, to anyone who, **intentionally or negligently**:

(a) does not provide the mechanisms for requests by data subjects or does not respond promptly or not in the required format to data subjects pursuant to Articles 12(1) and (2);

(b) charges a fee for the information or for responses to the requests of data subjects in violation of Article 12(4).

5. The supervisory authority **shall** impose a fine up to 500 000 EUR, or in case of an enterprise up to 1 % of its annual worldwide turnover, to anyone who, **intentionally or negligently**:

(a) does not provide the information, or does provide incomplete information, or does not provide the information in a sufficiently transparent manner, to the data subject pursuant to **Article 11**, Article 12(3) and Article 14;

dissuasive. **The decision to impose an administrative fine or t**The amount of the administrative fine shall be **fixed determined** with due regard to the nature, gravity and duration of the breach, **the actual damage or risk of suffering a damage caused to the data subject**, the intentional or negligent character of the infringement, **the immediate termination upon knowledge of the infringement**, the degree of responsibility of the natural or legal person and of previous breaches by this person, **the repeated violation of the same provision, the refusal to cooperate**, the technical and organizational measures and procedures implemented pursuant to Article 23 and the degree of cooperation with the supervisory authority in order to remedy the breach.

(...)

4. The supervisory authority ~~shall~~**may** impose a fine up to 250 000 EUR, ~~or in case of an enterprise up to 0,5 % of its annual worldwide turnover~~, to anyone who, ~~intentionally or negligently~~:

(a) does not provide the mechanisms for requests by data subjects or does not respond promptly or not in the required format to data subjects pursuant to Articles 12(1) and (2);

(b) charges a fee for the information or for responses to the requests of data subjects in violation of Article 12(4);

NEW (c) provides not transparent information and communication relating to the processing of personal data to the data subject in violation of Article 11.

5. The supervisory authority ~~shall~~**may** impose a fine up to 500 000 EUR, to anyone who, ~~intentionally or negligently~~:

(a) does not provide the information, or does provide incomplete information, or does not provide the information in a sufficiently transparent manner, to the data subject pursuant to ~~Article 11~~, Article 12(3) and Article 14;

(...)

6. The supervisory authority **shall** impose a fine up to 1 000 000 EUR or, **in case of an enterprise up to 2 % of its annual worldwide turnover**, to anyone who, **intentionally or negligently**:

(...)

(e) does not adopt internal policies or does not implement appropriate measures for ensuring and demonstrating compliance pursuant to Articles 22, 23 and 30;

(...)

RECITAL

(120) In order to strengthen and harmonise administrative sanctions against infringements of this Regulation, each supervisory authority should have the power to sanction administrative offences. This Regulation **should** indicate these offences and the upper limit for the related administrative fines, which should be fixed in each individual case proportionate to the specific situation, with due regard in particular to the nature, gravity **and** duration of the breach. The consistency mechanism **may also** be used to cover divergences in the application of administrative sanctions.

(...)

6. The supervisory authority ~~shall~~ **may** impose a fine up to 1 000 000 EUR or, ~~in case of an enterprise up to 2 % of its annual worldwide turnover~~, to anyone who, ~~intentionally or negligently~~:

(...)

(e) does not adopt internal policies or does not implement appropriate measures for ensuring and demonstrating compliance pursuant to Articles 22, **except from §2, 23 and 30**;

(...)

RECITAL

(120) In order to strengthen and harmonise administrative sanctions against infringements of this Regulation, each supervisory authority should have the power to sanction administrative offences. This Regulation ~~should~~ **indicates** these offences and the upper limit for the related administrative fines, which should be fixed in each individual case proportionate to the specific situation, with due regard in particular to the nature, gravity, ~~and~~ duration of the breach, **the actual damage or risk of suffering a damage caused to the data subject, the intentional or negligent character of the infringement, the immediate termination upon knowledge of the infringement, the degree of responsibility of the natural or legal person and of previous breaches by this person, the repeated violation of the same provision, the refusal to cooperate, the technical and organizational measures and procedures implemented pursuant to Article**. The consistency mechanism ~~may~~ **should also** be used to cover divergences in the application of administrative sanctions.

**EMMA and ENPA position on the proposed
“General Data Protection Regulation” (COM (2012) 11)**

The Commission proposal for a General Data Protection Regulation of 25 January 2012 impacts various activities of newspaper and magazine publishers' businesses.

As well as affecting **editorial press freedom**, it also impacts **press distribution** for both the consumer and the business to business press **and the future development of the digital press**, and therefore the economic sustainability of magazines and newspapers across Europe. Furthermore, given the broad scope for delegated acts by the Commission proposal, the framework for data protection in the future remains to a large extent uncertain and unpredictable for European companies. **EMMA and ENPA would like to highlight the following comments in particular:**

1. The need to safeguard press distribution for the consumer press as well as the business to business press, in order to preserve readership and media pluralism

A press subscription is a product that must be explained, but which has no dedicated retail outlet. In order to safeguard press distribution, direct marketing without prior consent is therefore crucial.

Up to 40% of subscribers to certain magazines and newspapers in various Member States depend on the current possibility to carry out direct marketing without prior consent. It should be noted that there are only marginal objection rates to receiving direct marketing by mail without prior consent (e. g. less than 10 objections out of 100,000 letters).

This approach is also necessary for “**controlled circulation**” **business to business** and special interest magazines, as they are also sent to targeted addressees (e.g., doctors, computer and financial specialists etc) without the recipients' prior consent.

The current approach **poses the serious risk of a dramatic loss of subscribers and decrease in circulation** of many titles across the EU where these publications are dependent on subscriptions sales and press distribution.

Under the current Directive, publishers are able to process personal data for the legitimate interest of the data controller, as well as third parties, on condition that strict information requirements are met and consumers have the right to object (as in the proposed Regulation under [Art 19](#)). The proposed Regulation, however, **limits how businesses such as publishers can communicate with existing and potential readers.**

Unlike under the current rules, the wording **does not allow publishers to process personal data for the legitimate interest of third parties**, restricting it to only the data controller (under [Art 6\(1\)\(f\)](#)). This would mean it would no longer be possible to have access to addresses of third parties, which is crucial for reaching interested parties. It is therefore **imperative that this possibility is reintroduced**. This is especially **important for the thousands of SMEs**, which can neither afford big media advertising, nor masses of unaddressed direct mail.

Furthermore, there are several other provisions in the proposal that would threaten press distribution. These include the restriction on data processing for **purposes other than those for which the data were originally collected** under [Article 6 \(4\)](#), which can in fact be in the interest of the customer for various reasons. In addition, there are **extended information obligations** ([Art 14](#)) with the threat of a fine that amounts to over 1% of the global turnover of a company and the provision on **profiling** ([Art 20](#)).

2. Need to preserve editorial press freedom, to ensure a free and independent, quality press

Exemptions for journalistic data processing are essential to ensure that journalists and publishers can continue fulfilling their democratic mission as regards investigating, researching, writing, checking, editing - whether or not leading to publication of material - as well as publication, dissemination, and archiving of articles without any obstacles, and to ensure that sources are adequately protected.

The Commission proposal leaves it up to the Member States to provide for such exemptions under Article 80. However, as the provisions of the Regulation will directly restrict journalistic data processing (i.e., without national implementation), the **chapters exempted from applying to journalistic data processing under Article 80 must also be directly binding, without further modification.** Otherwise, existing standards of protection of editorial press freedom could be endangered as it cannot be foreseen whether all Member States will introduce new robust exemptions without hesitation.

There is also no conflict with the subsidiarity principle here: journalistic activities foreseen to be excluded from the data protection Regulation via the exemption for journalistic data processing, can still be covered by media, libel and privacy laws and enforced at national level.

3. Need to secure the future development of the digital press, by avoiding unnecessary bureaucratic burdens and ensuring key elements for a positive online user experience

Newspaper and magazine publishers are facing many challenges as regards digitization and are **investing** in the development of digital business models to finance their editorial products across all platforms. They need to be able to interact easily with their readers, especially in the digital environment, to be able to **adapt to their readers' needs**. The proposal in its current form would unnecessarily increase **bureaucratic burdens** for publishers:

The “**right to be forgotten and to erasure**” ([Art 17](#)) rightly does not apply to data processing for “journalistic purposes”, which according to [Recital 121](#) would also include readers’ digital commentaries and opinion forums. As the latter have become an important element of the digital offerings of publishers, an obligation to delete such comments at the request of not only the person posting the comment, but also **the person being commented on** with the threat of a fine of 500,000 euros or up to 1% of worldwide turnover for an enterprise ([Art 79](#)), would be disproportionate, in many cases it would also be impracticable, and unduly interfere with the (often pseudonymous) dialogue which is only understandable if the entire context is published.

The Regulation’s provisions on **consent**, which has to be “explicit” by “a statement or a clear affirmative action” under [Art 4\(8\)](#), would be too restrictive, particularly for the many SMEs who do not have the advantage of having log-in systems like established global digital players, which make it easier to obtain consent. For example, new rules which demand explicit consent for **profiling** ([Art 20\(2\)c](#)) could potentially hinder digital business models, including advertising. It would also be hard to verify that a person providing consent was authorised to do so and not **a child** under 13 ([Art 8\(1\)](#)). These bureaucratic burdens, further exacerbated by e.g., stringent rules on rights of information ([Art 14](#)) and access for the data subject ([Art 15](#)), threaten to create barriers to potential customers engaging with publishers, while discouraging consumer, B2B and special interest publishers from offering innovative services.

More generally, we are concerned by the **many delegated acts** foreseen by the Commission to expand further these and many other provisions in the draft. Given the significant implications, we believe that any future changes must be subject to the full democratic EU law-making process.

CONTACTS:

Sophie Scrive
ENPA Deputy Director
Contact: sophie.scrive@enpa.be

Catherine Starkie
EMMA Senior Legal Adviser
Contact: catherine.starkie@magazinemedi.eu

**ENPA and EMMA Position paper on
PROPOSAL FOR A DATA PROTECTION REGULATION, 25 JANUARY 2012
(COM(2012) 11)**

Introduction

The Commission proposal for a draft Data Protection Regulation of 25 January 2012 impacts various activities of newspaper and magazine publishers' businesses. As well as affecting editorial press freedom, it also impacts press distribution for both the consumer and the business to business press and therefore the economic sustainability of magazines and newspapers across Europe. Furthermore, given the broad scope for delegated acts by the Commission proposal, the framework for data protection in the future remains to a large extent uncertain and unpredictable for European companies.

Given the fundamental importance of the press for any democracy, it is essential that the long term prosperity of a pluralistic, diverse and independent media is safeguarded. It is therefore important that an adequate balance is found between the legitimate interest of individuals with regard to the processing of their personal data and the free movement of such data. It is essential that the revision of the current data protection framework does not lead to an increase in the already substantial regulatory and administrative requirements, which cannot be fulfilled, in particular by European small and medium sizes companies.

ENPA, the European Newspaper Publishers' Association, and EMMA, the European Magazine Media Association would like to highlight the following points in particular in this paper:

KEY CONCERNS FOR MAGAZINE AND NEWSPAPER PUBLISHERS

1. A robust, directly applicable exemption for processing of personal data for journalistic purposes is crucial to preserve editorial press freedom and safeguard a free and independent, quality press (for further details see point 21, below).

2. The possibility for the press to continue to be able to reach out to potential new as well as current subscribers via direct marketing is essential to safeguard press distribution for the consumer as well as the business to business press, in order to preserve readership, future press subscriptions and media pluralism (for further details see points 4, 5, 6, 7, 9, 11, 12, 15, 17 below).

3. The future of the digital press must not be jeopardized: publishers today are innovating and investing in business models to take full advantage of the opportunities provided by new technology to serve their readers on all platforms. The sustainability of newspaper and magazine content on all platforms depends on advertising and digital subscriptions, as well as e-commerce. It is therefore essential that the Regulation does not restrict these possibilities and make it difficult for publishers to be able to interact easily with their readers, and adapt to their needs (for further details see points 1-12, 14, 15 and 17 below).

Concerns of magazine and newspaper publishers in more detail (in chronological order by Article)

1. Definition of personal data (Articles 4(1) and 4(2) and Recital 24)

According to the definitions in these provisions, all data, which can be related directly or indirectly to any particular person, can be considered as personal data. This broad definition covers a wide scope of applications as it simply refers to the general possibility of being able to identify a natural person. This problem is underlined in Recital 24 which points out that identification numbers, location data, online identifiers and other specific factors as such “need not necessarily be considered as personal data in all circumstances”, while not completely excluding this possibility.

This wide scope and the associated requirements for the processing of practically all data, leads to an unmanageable burden for companies, which does not seem to be justifiable, even from a consumer protection standpoint.

Furthermore the wide definition of personal data does not take into account the possibility to use pseudonyms of the user data. This is foreseen, for example, in the German Federal Data Protection Act in order to exclude the identification of the data subject or to make it significantly more difficult. This possibility to use pseudonyms for user profiles, in combination with the right to object of the person concerned, should also remain possible.

In order not to extend the scope disproportionately, it is the knowledge or the knowledge capabilities of the data controller that must be the basis for determining whether a person is identifiable. It should also be made clear that the possibility to identify a person indirectly is not sufficient. Article 4 (2) should therefore be amended, so an actual identification is required and not just the abstract possibility of identification.

To increase legal certainty, it would be also appropriate to include within the list of various definitions set out under Article 4 "special categories of personal data". This definition – in line with Article 9 on processing of "special categories of personal data" - should cover information which shows the racial or ethnic origin, political beliefs, religion or belief or membership of a trade union as well as genetic data, data concerning health or sex life and data relating to criminal convictions or related security measures. this group of sensitive data should also be taken into account when determining other obligations of the data controller (see proposed amendment to Article 31).

2. Explicit consent (Article 4(8))

The full consequences of the data subject's consent having to be "explicit" in future remain unclear, but this inevitably poses the risk of further restrictions online and offline:

- a) **It remains unclear if implied consent is still possible** (e.g. by inserting a business card into an appropriate box.). In this regard the specific characteristics of the selected communication channel have to be taken into account. Offers such as mobile applications and websites are typically used differently than, for example, postcards and forms. The possibility to grant consent therefore has to be adapted to the respective medium, if necessary in the form of an implied consent. The call for explicit consent is therefore problematic not only for traditional means of communication, but also precludes future technical innovations.
- b) **Relationship with E-Privacy Directive.** The requirement for explicit consent also raises the question of whether this has any impact on the ability to express the required consent in certain circumstances through browser settings in the context of the E-Privacy Directive (Recital 66 of Directive 136/2009).

- c) **No consent where there is significant imbalance (Article 7(4)).** It is also unclear when there is a “significant imbalance” between the position of the data subject and the controller, in which case under Article 7(4), consent would not provide a legal basis for data processing. In this respect, Recital 34 just states that this is especially the case where the data subject is in a situation of dependence from the controller. This explanation cannot, however, sufficiently explain all possible applications.
- d) **Competitive advantage for global business models based on log-in systems.** The requirement of explicit consent generally favours large international companies such as free e-mail providers or social networks, which base their business models on log-in systems. For those companies it is relatively simple to obtain the required consent of their customers, due to the direct contact inherent in the system with their customers.

The requirement that consent must be explicit poses also the serious risk that consumers will be more likely to give their consent to large global companies, which they are already familiar with and may have already created a comprehensive profile, than to unknown, smaller companies operating at a national level and which are less in the public view.

Many companies, including many publishers, allow free access to their content without any such restraints. Any direct contact with the customer to obtain consent (such as respective pop-up windows on websites) will therefore carry the **risk of being perceived by the user as a disturbance** and therefore as a negative aspect of the offering. This approach risks resulting in a **huge competitive disadvantage for publishers.**

At the same time, it is questionable how far the provision of explicit consent contributes to the protection of privacy, insofar as consumers often quickly click ‘YES’ in order to reach the particular webpage they are looking for, without paying full attention to what they are agreeing to. This puts into question the real value of providing explicit consent.

3. Definition of "child" (Article 4 (18)) and related obligations

The draft Regulation refers to children in several provisions (and therefore to the age limit of 18 years as defined in Article 4(18)), e.g. in the provisions about the right to be forgotten (Article 17, Recital 53), information requirements (Article 11, Recital 46) or profiling (Recital 58).

The general **classification of anyone under 18 years as a child appears inappropriate** given the different stages of development and experience of children, teens and young adults. Also the reference by the Commission to the United Nations Convention on the rights of the child cannot justify this. The Convention contains essential standards for the protection of children, but is not however intended to establish a universal definition of "children". The limit of 18 years chosen is especially questionable given the fact that consent of the parents or guardians in accordance with Article 8(1) is required for the processing of personal data of a child below the age of 13, which is directly offered as a service of the information society.

Recital 38 states that there needs to be “careful assessment” of whether the right to process data, which is lawful if it is in the “legitimate interests” of the data controller data processing, is overridden “where the data subject is a child” (as required under Article 6(1)(f)). In reality, it is questionable as to whether there would actually be the possibility to do so.

If an age verification was required for every contact this would be pose **significant burden for enterprises and numerous business models.** This approach raises the question of how companies can determine in a legally appropriate way, whether the respective services are viewed or requested by a child, especially as regards their digital business models. As it would be very difficult to know for sure if the data subject was in fact a child, companies might feel obliged to not go ahead and process data, which would not be proportionate given the various data processing operations which might be applicable under this article.

4. Principles relating to personal data processing (Article 5).

It is difficult to understand the need for having a list of "principles" in addition to the regulatory requirements in Article 6. These principles, if retained, would constitute an unreasonable burden for businesses taking into account the associated costs and additional efforts they would result in. It is particularly important that the requirements contained in Article 5 (b) should be deleted in this regard.

It is also not appropriate to impose on the controller a general responsibility for compliance with the Regulation.

5. Conditions for lawful processing of data (Article 6)

A **press subscription is a product that must be explained**, but which has no dedicated retail outlet which would allow a publishers' representative, for example, to explain it to a potential customer. In order to safeguard press distribution, direct marketing is therefore crucial.

Article 6 sets out which conditions must be met for the lawful processing of personal data. One of the six alternatives contained in Article 6 has to be met. Consent is one alternative, but not the only one. This is also appropriate because it reflects the fact that there are many different situations where data must be processed.

a) Article 6 (1)(f)

Under Article 6(1)(f), the Regulation continues to allow businesses such as publishers to communicate with potential customers where there is a "legitimate interest" of the data controller, on the condition that strict information requirements are met (Article 14) and consumers have control with the right to object to receiving any further communications (Article 19).

However, the wording does not guarantee that publishers can continue to address potential new readers via direct marketing without prior consent as the possibility to process personal data also for **legitimate interest of third parties** is not included in the text anymore. This is, however, in many cases the necessary condition to conduct direct marketing. Only this possibility ensures that necessary legitimate data processing procedures like the transfer of address lists, the purchase or renting of addresses or the conduct of certain marketing measures by specialized service providers of services can continue to be employed. **This alternative must therefore be reintroduced. This is especially important for the thousands of SMEs, which can neither afford big media advertising nor masses of unaddressed direct mail.**

If the **possibility to process personal data for legitimate interest of third parties is not reintroduced as is the case in the current Directive, this poses the serious risk of a dramatic loss of new subscribers and decrease in circulation of many titles across the EU dependent on subscriptions sales and press distribution.** This is even more significant when considering the direct applicability of the Regulation. In many Member States a large percentage of the subscription circulation of certain newspapers and magazines depends on direct marketing by letters sent to third-party addresses without prior consent, which is permitted by national laws based on Article 7 (f) and Article 14 Directive 95/46/EC under the condition of information to the addressee and his right to object.

- As regards the **consumer press**, figures we have received from national publishers' associations, as well as individual publishers, in the following Member States show that such marketing letters to third party addressees without consent account for the following percentage of subscribers for various publications: in Germany (up to 20%, as regards regional and local newspapers: a recent inquiry revealed that 20 % of new subscriptions and up to 50 % of new temporary subscriptions

depend on direct marketing via addressed letters without prior consent; France (up to 42%); Sweden (up to 46%); Portugal (up to 95%); UK (up to 45%).

- As regards the **business press**, B2B magazines are often sent to their readers (e.g., doctors, computer and financial specialists etc.) based on special address lists of the respective target group for free and without prior consent. This so-called '**controlled circulation**' (which accounts for up to 90% of the readership of some business titles in some Member States) is necessary to advertise for a subscription of the magazine but also to secure the required reach in order to attract advertisers and therefore to finance the magazine. This would simply not be possible anymore if this form of marketing was not allowed. The benefits to both customers and publishers from this approach can be contrasted with the marginal objection rates to receiving direct marketing by mail without prior consent (e.g., less than 10 objections out of 100,000 letters).

The Regulation's proposed wording also raises the question of whether external service centres (e.g., subscription fulfillment houses) to which publishers provide personal data to distribute their magazines, would be in breach of the Regulation.

Information and control guarantee the right of self-determination of the consumer. This is guaranteed in the proposal for a regulation. It is stipulated that an individual must be informed about the processing (Article 14) and may object to it (Article 19 (1)). Specifically for direct marketing, a provision was introduced according to which the person concerned has not only the right to object to the processing of their personal data for direct marketing purposes, but must also explicitly be informed about this right (Article 19 (2)).

It must also be ensured that no requirements are introduced, that can only be relatively easily fulfilled by large, globally active companies but not by the majority of small and medium-sized enterprises in Europe (see point 2(d) above for further details). In addition, there is the practical concern that the broad definition of personal data would lead to an inflation of consent requests to the user and to a huge volume of data in the databases of the companies.

Furthermore, when discussing direct marketing it must not be forgotten that the aim is to create a legal framework for the processing of personal data. The problem of annoying advertising or unsolicited messages is already sufficiently regulated in the Unfair Commercial Practices Directive 2005/29/EC (in particular Articles 6, 7, 8 and 9) and the E-Privacy Directive 2002/58/EC (see in particular Article 13).

b) Article 6 (4)

The current wording also does not guarantee that publishers can continue to address existing customers. The conditions for a legitimate change of purpose for further processing must take account of all possible forms of data processing. Data processing for purposes other than to those for which the data were originally collected can be necessary and in the interest of the customer for various reasons. It must, for example, remain possible for press publishers to send addressed direct marketing letters to their own readers or former readers, to inform them about a new subscription offer for a new or even the same publication, even if those readers have not originally given their prior consent to the use of their address also for this specific purpose. Another example is informing a relevant target group about the launch of a new B2B magazine after the success of a certain topic at a trade fair.

Such a change of purpose must be permitted if the conditions for data processing without prior consent within the meaning of Article 6 (1) are fulfilled. The proposal foresees this in Article 6 (4) only for the alternatives of Article 6 (1) (a) to (e) but not for Article 6 (1) (f). There is however no reason for such a limitation. On the contrary, this would lead to the anomaly that for personal data, which has been previously collected or used, including with consent for the original use, stricter rules would be applied than for such data that has never been used (i. e. Article 6 (1) f) would not apply). This limitation should therefore be removed and Article 6 (4) should generally refer to Article 6 (1).

6. Conditions for consent (Article 7)

- a) The establishment of additional requirements for consent must not result in excessive demands that cannot properly be implemented in practice. In particular, the requirement in Article 7 (1), that consent has to be granted for specified purposes, should be deleted. This deletion will avoid long and complex texts having to be used for declarations of consent which are not read by users but regarded as a nuisance.
- b) In Article 7 (3), it should be clarified that the original recipient of the consent provided is the sole addressee of the withdrawal of consent. This clarification is essential for cases where the data related to the consent provided are passed on to third parties or published. Furthermore, where there are contractual or statutory "special agreements" in place, these rules apply and have priority over Article 7 (3).
- c) In Article 7 (4), it should also be clarified that any assessment of a "significant imbalance" between a data subject and controller must always relate to individual cases and to the specific consent provided.

7. Information to the data subject (Article 14)

The extension of already considerable information requirements that the data controller is obliged to provide the data subject under Article 14 is apparently aimed at data processing in an online environment. It would be unacceptable however if, as a consequence, traditional and proven marketing channels could no longer be used, because the tremendous amount of required information can simply not be adequately provided. The draft Regulation does not take into account the following:

- a) In order to be able to continue to provide appropriate press distribution, it has to be possible to provide information in a general way. The requirement that information has to include the contract terms and general conditions (Article 14(1)(b)), where the processing is necessary for the performance of a contract or to conduct pre-contractual measures, is in particular not practical for direct marketing activities that take place by mail or by phone, as opposed to online. While we have doubts that the information required would in fact bring any added value for data protection. In many cases, **the provision of this information e.g. on an order card, as regularly used for subscriptions, will simply be impossible.**
- b) In many cases it **will not be possible to pre-determine the period of data storage (Article 14(1)(c)) in advance.** At the time of conclusion of a subscription for an unlimited period it is impossible to know the length of the subscription period, and thus for how long the personal data has to be stored. Even after the termination of the contractual relationship there might be a legitimate interest to continue using the respective data.
- c) The obligation to **indicate the contact details of the supervisory authority (Article 14(1)(e)) combined with the liability for any incorrect information** will be a further burden for businesses.
- d) It is unnecessary for the data subject to be informed about the recipients or categories of recipients **(Article 14 (1)(f))** of the data in circumstances under which he would already expect that data to be forwarded without receiving such information (for example to a subcontractor).
- e) Information about the intention of the data controller "to transfer the data to a third country or international organisation and on the level of protection afforded by that third country or international organisation by reference to an adequacy decision by the Commission" (Article 14(1)(g)), **can often not be realised in a practical manner.** It must be considered that this requirement would already apply if only parts of the data processing, e.g., the invoice processing or material management, take place in a third country. In particular, it is difficult to see how information requirements on the respective level of data protection in a third country could easily be met via certain traditional marketing channels (e.g. a postcard, letter).

- f) The already extensive information requirements are even more amplified by a blanket clause obliging the data controller to provide any other information necessary to guarantee fair processing in respect of the data subject, having regard to the specific circumstances in which the personal data are collected (Article 14(1)(h)). This **provision will not provide legal certainty for individual companies** as regards which information must be made available in each individual case.
- g) The information provided to the data subject as to whether the provision of personal data is mandatory or voluntary and the possible consequences of failure to provide such data (Article 14(2)) does not only extend the amount of information to be provided, but would in many cases be **unnecessary since it would already arise from the context** (e.g., the indication of a delivery address for the delivery of a subscription is necessary in order to receive the respective newspaper or magazine). However, it must be at least possible to provide this information using representations appropriate to the circumstances (e. g. asterixes to indicate the mandatory information).
- h) Where the personal data is not collected from the data subject, the data subject has to be informed according to Article 14(3), as regards the source from which the personal data originated. This general obligation is too extensive and not necessary, particularly in light of the fact that the respective data could also come from public sources or may have been published by the data subject in question.
- i) The requirements regarding when information has to be provided (Article 14(4)) do not take into account the fact that data are usually obtained in traditional press distribution on completion of the order form, etc. The obligation to provide this amount of information would mean that **this sort of distribution would simply be no longer feasible**.
- j) For the many publishers that still depend on traditional practices for gathering and processing personal data (e.g., with regard to subscription marketing that is highly dependent on traditional tools, such as postcards or return coupons) it would in many cases be **impossible to fulfill the new information requirements** suggested under Article 14. Furthermore, the threat of huge fines of up to 1% of the worldwide annual turnover of the company which does not provide information or provides information in an incomplete or insufficiently transparent manner (under Article 79(5)(a)) leads to a **significant risk that businesses will want to avoid**. It therefore **needs to strike a better balance between transparency and practicability**.
- k) The **exemption to the information requirements** under Article 14 (1)–(3) set out in Article 14 (5) (a) – i.e., where the data subject already has the information referred to in those paragraphs - **needs to be extended** to those cases where the data subject has to expect a respective data processing procedure based on their experience of common practices. This scenario should be treated in the same way as those cases where the person already has the information.
- l) In addition, the **information requirements should not apply where communication of the respective information is impossible**, regardless of whether the data have been collected from the person concerned or not. The Commission proposal is disproportionate on this point by limiting this exception to only cases where data are not collected from the data subject. This limitation should therefore be deleted from Article 14 (5)(b).

8. Right of access (Article 15)

Under the suggested new rules on the right of access, which go further than the current rules, many of the requirements for controllers are excessive and would pose the risk of being an unmanageable burden on many publishing houses:

- a) The data subject now has the right to “obtain from the data controller at any time, on request, confirmation as to whether or not personal data relating to the data subject are being processed”. This creates an **unreasonable burden**.

Our comments on the need for information obligations to be significantly reduced in the context of Article 14 are also valid here. In many cases, the obligation to inform the data subject will not be practicable. Many publishers for example do not use “plain data” for the representation of certain internal transactions, but certain variables instead (e.g., specific figures which correspond to specific products or processes). Apart from the fact that the information about the relevant data could possibly affect trade secrets of the company (e.g., relating to internal processes), the advantage gained by consumers in these cases would, we believe, most likely be accordingly low.

Furthermore, it is unclear what is meant by the requirement in Article 15 (1) (h) to provide information about “the significance and envisaged consequences of such processing, at least in the case of measures referred to in Article 20”. We believe that this extension of the information requirements is unnecessary.

- b) The obligation in Article 15(2) to provide the information in electronic form when the data subject has made the request in electronic form **poses unmanageable risks to businesses**. It is generally not possible for a company to verify if the person about which information has been requested is the same person requesting the information, where the request has been made in an electronic format. Therefore such a requirement poses a significant risk of obliging businesses to disclose data to unauthorized people. It should therefore only be incorporated as an alternative, but not as a duty.
- c) Exclusion of right of access. The right of access shall give the data subject the possibility to understand who has stored which personal data about him. This right is therefore taking account of the fact, that the data subjects often do not have their own access to their personal data. In certain cases however this interest of the data subject does not prevail any longer, if for example the data subject already has the information (Article 14 (5) a). The same must apply when the data subject has access to the stored personal data at any time (e.g. via a customer profile on the Internet). An interest in information that might justify a right of access does also not exist, if the processed personal data are publicly accessible.

9. Right to be forgotten and to erasure (Article 17)

The right to be forgotten and to erasure in Article 17 could be extremely problematic for readers' contributions (e.g. comments, contributions to opinion forums, product reviews, etc.) in the context of professional journalistic offerings. Furthermore, these requirements might also be a significant burden to other forms of data processing, for example regarding the processing of an objection in the sense of Article 19.

- a) First of all, Article 17 itself is worded so broadly that it allows for not only deletion of people's own posts, but also the deletion of posts by others referring to another person, by giving the right to request deletion of content *relating to* the person concerned.
- b) It is **questionable whether the exemption in Article 17(3)(a) for exercising the right of freedom of expression in accordance with Article 80 is sufficient for publishing houses**. While this exception would indeed have a wider scope with a broad definition of journalistic activity (in Recital 121), it is not clear whether this broad definition will remain.
- c) **Requiring publishers to delete commentaries** of readers, not only under instructions from the person posting the comment, but also from someone that this person was commenting on (e.g., a powerful person that does not particularly like what has been written) with the threat of a fine of 500,000 euros or up to 1% of worldwide turnover for an enterprise (Article 79), is **disproportionate** and would interfere with the (often pseudonymous) dialogue which is only understandable if the entire context is published.

- d) Furthermore, such an obligation leads to a **considerable burden for web site operators, but also for companies that process the corresponding data by traditional means**. This applies equally to the obligation contained in Article 17 (2), to inform third parties about the desired deletion. This obligation should therefore be deleted.
- e) As regards **direct marketing**, the problem might arise that a person asks for the deletion of data about him/herself because he objects to the processing of his data for future direct marketing. However to comply with the proposed rules, his address must be blocked, and not deleted, to avoid his address being used for future promotional activities. Article 17 (4) refers to cases where instead of a deletion of data, the data processing might be restricted. It is nevertheless questionable whether this provision indeed covers all relevant cases. The Commission points out in the explanatory memorandum to its proposal for a regulation under section 3.4.3.3 that it wants to avoid the ambiguous expression "blocking". However, it has to be ensured that at least cases and particular situations like the one described above are also regarded as an exception.

This could be clarified, for example, by deleting the possibility for the data subject to object to the processing of personal data pursuant to Article 19 (under Article 17 (1) (c)) and specifying that instead of erasure, a limitation of the data processing is also possible if the data processing officer must retain the data. There should also be the possibility to waive erasure if the deletion is associated with a disproportionate effort; affects the legitimate interests of the data subject; precludes the predominant legitimate interests of the data controller or a third party; the attribution of the data stored to the data subject based on the information provided would necessitate disproportionate effort; or the data subject has not been identified itself with sufficient certainty.

10. Right to data portability (Article 18)

The right to data portability, and in particular the obligation to grant to the data subject the opportunity to transmit their personal data and any other information provided by the data subject in an electronic format which is commonly used into another automated processing system, will in many cases be **difficult to realise**.

Many publishing houses do not save the data in a standard electronic format which is commonly used, but use specific formats, tailored to their specific needs. A relevant transmission would be in many cases not only be technically difficult, but in addition would not necessarily reveal any relevant information concerning the data subject, since the corresponding data are often not presented as plain data, but it is rather variables that are used.

If this right is maintained, however, it has to be ensured at the very least that the data controller is not disproportionately burdened. In particular it must be possible to charge the person concerned for the costs associated with this purpose.

11. Right to object (Article 19)

The new formulation of the right to object in Article 19 creates legal uncertainty for businesses and unnecessarily makes them vulnerable to huge fines:

- a) The proposal foresees a general right to object in Article 19 (1) and thereby changes the current effective and proven provision on objection set out in Article 14 (a) of Directive 95/46/EC where the data subject has the right to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him. There are no known practical problems in this area which would justify or necessitate such a legislative

change. This is particularly significant as the Regulation will now apply directly and thus without the flexibility of the Directive.

- b) It is not taken into account that it may be necessary to retain certain data even after objection. In this respect it is preferable that the wording used in Article 14 (a) of the current Directive- is also used in the new Regulation.
- c) Furthermore, it would be clearer if the legal consequences for an objection being upheld were set out on a case-specific basis in paragraphs 1 and 2, rather than being regulated under Article 19(3). Paragraph 1 should therefore specify that in cases of justified objection the processing by the controller may no longer refer to this data. In paragraph 2, it should be clarified that in the case of a justified objection the processing by the controller may no longer refer to this data for direct marketing.
- d) Another problem is that it is not clear when the information about the right to object can be regarded as **"intelligible"** as defined in Article 19 (2). In addition, it is not taken into account that a clear, explicit and understandable notice is also possible, where - such as on a post card - due to limited space a spatial separation from other information is not possible. This leads to considerable legal uncertainty, which can have significant consequences for companies because under Article 79 (6) (c) a violation of this obligation is threatened with a fine of up to 2% of the global annual turnover of the company.
- e) The question also arises as to whether it is not already a **prohibited use or processing according to Article 19(3), if the data processing company records the objection of the data subject** to its personal data, which is probably regularly required in order to comply with the respective obligation.

12. Profiling (Article 20)

The future of newspaper and magazine publishers depend on their ability to respond to users' demands for innovative digital offers on various platforms (online, tablets, mobile, smart phones, etc). These challenges not only concern how editorial content can be received under various forms, but also how advertising can be displayed in the digital environment. Article 20 relating to profiling, which goes beyond the current EU rules on automated individual decisions (Article 15 of Directive 95/46/EC), **threatens to prevent the development of digital publishing** and the competitiveness of the European press in the digital environment by the burdens it creates.

Due to the general formulation of Article 20 there is the risk that this provision might also **significantly burden traditional and proven business models or even make them impossible**:

- a) It is not defined, in particular, when and which consequences of a measure **"significantly affect"** a person. Therefore it cannot be excluded that certain forms of direct marketing activities or certain forms of controlled circulation of journals could be affected by this provision. In addition, this provision could have an impact on online advertising methods such as e.g., so-called online behavioural advertising.
- b) Furthermore, it is not clear which conditions a measure must fulfill to be based solely on automated processing of data. This is especially true for cases where the corresponding data processing is automated but based on previously determined criteria. The scope of the provision has been extended in comparison to the current Directive (Article 15) to those measures intended to analyse or predict certain personal aspects related to the data subject.

It cannot therefore be excluded that numerous data processing processes that are important for publishers, such as **measures within the framework of customer relationship management**, or certain forms of interest-based advertising that might be relevant as an important form of advertising in the online publishing sector, also fall under this provision, and **may be negatively impacted**.

- c) Due to its large scope, this provision **could even apply to certain forms of data processing, which do not identify a particular person**, such as the creation of pseudonymous or even anonymous user profiles for the purpose of excluding the identification of the data subject or to make it significantly more difficult. As pointed out in Recital 24 identification numbers, location data, online identifiers and other specific factors as such, do not necessarily need to be considered as personal data in all circumstances, but it is also not completely excluded from the scope of the provision. Therefore, there is still the possibility that this could include certain forms of data processing which are relevant for publishers, such as certain ways of contacting their own customers, certain forms of direct marketing or new forms of online advertising, etc.

In this case, the strict requirements of Article 20(2) would then also be applicable for those measures, and the processing would be subject to the general requirement of consent of the data subject, if the profiling is not carried out during the course of entering into or fulfilling the contract or authorized by an EU or Member State law. Furthermore, it is not taken into account that certain national rules already provide for a variety of data processing procedures more detailed rules. The German Telemedia Act (Telemediengesetz), for example, ensures the necessary consumer protection by introducing a prohibition of merging pseudonymous user profiles with the owner of the profile combined with a penalty and the right to object for the individual. It also remains unclear how anonymous profiling would affect the interests of the person which is unknown to the data processing entity.

- d) Although certain forms of data processing continue to be regulated under the provisions of the E-Privacy Directive (such as e.g. the setting and reading of cookies), other forms could end up being covered by the Data Protection Regulation. Those could be considered as profiling measures in terms of the Regulation and the more stringent requirements of the Regulation would therefore apply to them.

13. Responsibility of the controller (Article 22)

The obligations of the controller laid down in the draft Regulation would in many cases constitute a significant burden for companies. Due to the general concerns relating to the obligations laid down in Article 34 concerning prior authorisation of data processing, the reference to this provision in the obligations in Article 22 (2) (d) should be deleted.

To clarify that the review of the effectiveness of the procedures established by the controller can continue to be carried out, for example, by the internal auditor or the company's data protection officer, the ambiguous definition that the control must be carried out by independent internal or external auditors should be deleted.

In addition, it cannot be excluded that the processor also employs staff not involved in the data processing. There is no reason to demand the fulfillment of strict confidentiality obligations for these employees. Article 26 (2) (b)) should therefore be changed so that this requirement must only be satisfied as regards those staff which are entrusted with the processing.

It is also not obvious why under Article 26 (2) (h) there is a general obligation for the processor to provide information. It should be considered sufficient when the information is made available upon request.

14. Data protection by design and by default (Article 23)

The requirements for the implementation of data protection by design and by default require assessment by the companies concerned, having regard to the state of the art and the cost of implementation, which **especially for small and medium-sized companies will not be easy to realise.**

The application of this provision would in many cases impose a subjective view on users as regards what data protection settings should look like. This raises the question as to how consistent such a requirement is with the overall concept of a responsible consumer, who is usually regarded as being able to make an informed decision.

Furthermore, there is also the risk that such a general determination leaves no room for privacy settings that are more adapted to the individual needs and which can be stricter, less extensive or simply differentiated. For example, modern browser settings already provide users with the choice, as to whether they want to accept cookies in general, for the current browser session only, or on a case by case basis.

15. Processor (Article 26)

The possibility to undertake data processing by outsourcing it to data processors is essential for many businesses and business processes. Therefore, it must be ensured that the review of the regulatory framework does not make these proven and important forms of outsourcing of certain tasks practically impossible. Against this background it should be considered sufficient in Article 26 (1) that the selected processor provides reasonable assurance for compliance with the respective obligations under the Regulation. The term currently used - "guarantee" - could easily be misunderstood.

16. Co-operation with the supervisory authority (Article 29 and Article 53)

It has to be ensured that the review of the regulatory framework does not lead to a mixing of responsibilities. It has to be ensured that the data controller does not become the deputy of the supervisory authority. However, there is this very risk in view of the formulation of Article 29 (1), which might be interpreted as broad obligations of the controller. It should rather be stressed in this provision, that the authority should advise and support the controller, the processors and any representative of the controller with regard to their typical needs. In addition, it should be made clear that the obligations of the controller, the processor and any representative of the controller vis-à-vis the supervisory authority alone is to provide it with the information necessary for the performance of its investigative powers under Article 53. The duties and powers of the supervisory authority are exhaustively regulated in Article 52 and 53 respectively of the draft, so further specifications contained in Article 29 (2) should consequently also be deleted.

17. Bureaucratic burden on businesses must be reduced

One of the aims of the Regulation is to reduce bureaucratic burdens for companies. This will only be achieved if, in return, there are no new burdensome requirements introduced, such as extensive information (e.g. Articles 14, 15), documentation (Article 28), notification (Art. 31, 32) and consultation requirements (Articles 33, 34).

18. Certification (Article 39)

The requirement in Article 39 for the Commission and Member States to encourage the establishment of data protection certification mechanisms and of data protection seals and marks runs the risk that such certification can easily lead to a *de facto* mandatory certification requirement for businesses.

This is especially true if such certification gives the impression to the public that only the certified processes, technologies, products or services meet a certain data protection level.

Furthermore, certification requirements could result in a competitive advantage for large and financially strong businesses compared to SMEs which cannot afford costly measures.

19. Right to lodge a complaint and to engage in court proceedings (Articles 73, 76)

The Regulation now extends the right to lodge a complaint and engage in court proceedings for any individual, organisation or association which aims to protect data subjects' rights and interests concerning the protection of their personal data..

We believe that the right for e.g., civil society associations to engage in, or pursue, legal proceedings along with supervisory authorities would lead to a confusing co-existence of roles and more legal uncertainty.

20. Sanctions and fines for breaches of data protection law (Article 79)

The fines for breaches of data protection legislation have increased significantly under the proposed Regulation. General fines of up to 0.5%, 1% or 2% of annual worldwide turnover of the company are foreseen, compared to e.g., German Law which foresees fines of up to 300.000 Euros (which can only be exceeded if this amount does not exceed the economic advantage of the offender).

This increase is unjustified, especially with regard to some of the provisions which foresee fines in case of a breach (e.g. insufficient compliance with the extensive information requirements in Article 79(5)(a)).

The obligations are also often provided by general clauses or formulations which leave room for wide interpretations. This could lead to a situation that companies cannot oversee all their duties and obligations in an acceptable and manageable manner. The uncertainty created by Article 79 as regards legal obligations, combined with the significant amount of the fines, amounts to a considerable and unacceptable risk for companies.

21. Exemption for processing of data for journalistic purposes (Article 80)

An exemption for journalistic data processing is essential to ensure that journalists and publishers can continue fulfilling their democratic mission as regards investigating, reporting, writing and publishing editorial content without any obstacle, and to ensure that sources are adequately protected. Even though the Commission proposes to retain the existing exemption for journalistic data processing, it has to be ensured that with the change to a Regulation the level of protection will not be lowered:

- a) The **chapters referred to in Article 80 must be immediately and without further modification excluded from applying to journalistic data processing**. The Commission proposal continues to leave it up to the Member States to provide for such exemptions. The current national exemptions in force in the Member States would no longer be applicable under the new Regulation and it cannot be foreseen whether all Member States will introduce new robust exemptions without hesitation. Any implementation of this provision by Member States carries the risk of restrictions to the existing standards of protection of editorial press freedom.
- b) Furthermore, the **exemption should be extended to Articles 73, 74, 76 and 79** of Chapter VIII (on Remedies, Liabilities and Sanctions). This is because they include elements such as complaints to the supervisory authority, which are not suitable considering that the exemption for journalistic purposes is supposed to avoid supervision. We also believe that the current wording of Article 80, by listing the titles of each chapter before each chapter number, could lead to a misinterpretation that it is not the chapter as a whole which is to be excluded from the application but only some parts of the

chapter (e.g. only the general principles in chapter II rather than the whole of the chapter entitled “general principles”).

- c) It should be underlined that this direct application of the exemption is **consistent with the subsidiarity principle**. The journalistic activities which are foreseen to be excluded from the data protection Regulation via the exemption for journalistic data processing, can still be covered by media, libel and privacy laws. These are mainly characterized by national laws and are therefore covered by Member States' fundamental rights. This means they are thus open to legal action via Member States' constitutional courts.
- d) It should also be noted that the proposal suggests that activities are “journalistic” if ‘the object of these activities is the disclosure to the public of information, opinions or ideas, irrespective of the medium which is used to transmit them. They should not be limited to media undertakings and may be undertaken for profit-making or for non-profit making purposes’ (see recital 121). It **must be ensured, however, that the protection of the editorial processing of the press is not weakened** as a result of these non-journalistic expressions of opinion also be covered in the definition.

22. Relationship with the E-Privacy Directive (Article 89)

Article 89 now clarifies that the E-Privacy Directive takes precedence over the Data Protection Regulation for those cases regulated in it. It is an important step that it has been made clear that the Data Protection Regulation introduces no duties other than those that are envisaged in the E-Privacy-Directive. Nevertheless, the wording of the Article must not inadvertently undermine the aim of the Regulation in this regard by conferring additional rights to individuals. In addition, not all data processing processes relevant for digital business models fall under the E-Privacy Directive, in which case the Data Protection Regulation would apply. Therefore, it is quite likely that this might lead to further restrictions.

23. Delegated acts

Delegated acts are not the proper instrument to regulate or to specify the right of privacy. In particular, discussions in and with the European Data Protection Committee cannot replace the democratic process.

Data protection legislation has to achieve the sometimes difficult balance between the legitimate interests of the individual and the communication needs of a modern economy. The result of this balancing process can have far-reaching effects on consumers and businesses, and should therefore not be left to a single institution.

In addition, due to the use of numerous general clauses and the reservation of the adoption of delegated acts at various points of the proposed Regulation, it is practically impossible for companies to predict which obligations will actually be implemented. This entails not only the risk of further restrictions, but also leads to significant legal uncertainty for businesses.

CONTACTS:

Sophie Scrive
ENPA Deputy Director
Sophie.scrive@enpa.be
+32 (0)2 551 0197

Catherine Starkie
EMMA Senior Legal Adviser
Catherine.starkie@magazinemedie.eu
+32 (0)2 536 0602

Data Protection Reform – a view from the consumer credit reference agencies

About ACCIS

The Association of Consumer Credit Information Suppliers (ACCIS <http://www.accis.eu/>) is an international non-profit trade association bringing together 37 consumer credit reference agencies in 27 European countries and associate members from all other continents and provides the largest representative group of credit reference agencies in the world. Credit reporting agencies sit at the heart of financial systems providing a critical service to help banks and other creditors make decisions about credit and risk in the financial services, communications and energy and water industries. These services impact on consumers and businesses helping organisations make responsible lending decisions based on accurate and verifiable data about the history on financial commitments and behaviour of applicants and customers. In all cases, those services operate transparently and are accessed in accordance with data protection regulations and/ or other specific regulations (i.e. banking law).

Overview

Whilst the data protection reform is welcome – the rise of social networks and the increasing reliance on the internet in our daily lives indeed makes it urgent – there are particular aspects of the draft Regulation (European Commission, 2012) that, whilst well meaning, could have serious repercussions for the users of consumer credit reference agencies, whether lenders, consumers or businesses. It is the view of ACCIS that the changes emanating from the review of the Data Protection Directive (European Commission, 1995) are primarily intended to tackle problems with social networks and could have unintended consequences elsewhere. So, for example, it is hard to envisage how reliable creditworthiness checks could be carried out in Europe if the right to be forgotten, (if applied to unpaid debts) is not tempered with some pragmatism. The consequences could be disastrous primarily for consumers but also for the future of financial services and commerce.

Summary

1. ACCIS supports the aims of the draft Regulation in seeking to raise and harmonise the overall level of protection for individuals across Member States.
2. ACCIS is concerned that the draft Regulation may have serious, adverse consequences for the users of credit reference agency services by reducing the amount of available data and restricting how it may be used. ACCIS believes these consequences are unintended.
3. Credit reference agency services are widely recognised as being essential to the effective operation of a developed economy. Disruption to those services would have a detrimental impact on the flow of credit to individuals and businesses (particularly small and medium-sized enterprises). This in turn would hinder economic recovery and growth in the EU.
4. There could also be very serious consequences for consumers and small businesses. More would become excluded as credit could be harder to secure for those with less data, whilst others may become over indebted if granted credit they cannot repay. In many respects, credit reference agency services play a crucial role in consumer protection. Decision-making by lenders would become slower, less objective and less fair. There would also be a significantly increased exposure to fraud.

5. ACCIS' main concerns are in respect of:

1. Right to be forgotten (Article 17),
2. Right to data portability (Article 18),
3. Restrictions on automated profiling (Article 20);
4. Data minimisation (Article 5);
5. The legitimate interests condition (Article 6);
6. Notification of a personal data breach (Article 31),
7. Data protection impact assessment (Article 33),
8. Administrative sanctions (Article 79),

Please see the attached appendix for more details on our proposed amendments.

ACCIS position paper on the EC's proposed data protection Regulation (COM (2012) 11 final) ("the draft Regulation")

Amendment 1

**Principles relating to personal data processing
Article 5 – paragraph 1 – point c**

Text proposed by the Commission

(c) adequate, relevant, and *limited to the minimum necessary* in relation to the purposes for which they are processed; they shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data;

Amendment

(c) adequate, relevant, and *proportionate limited to the minimum necessary* in relation to the purposes for which they are processed; they shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data;

Amendment 2

**Principles relating to personal data processing
Article 5 – paragraph 1 – point d**

Text proposed by the Commission

(d) accurate and kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

Amendment

(d) accurate and *where necessary*, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without *undue* delay;

Justification

Credit reference agency services depend on, and are made more effective by, access to large amounts of relevant data, from which the most predictive will be extracted and used according to the profile of the individual or business and the purpose for which a decision is being made. It is necessary for a credit reference agency ("CRA") to hold data for significant periods of time, and in relation to an individual's previous addresses and/or identities.

Credit reference agency services are created in line with current data protection requirements, and:

- *whilst credit reference agencies do hold and/or make available a range of data for modelling purposes that data will be used to determine which provides the most statistically effective contribution to a decision. Thus, data will only ever be used in a scoring model if it is predictive of the outcome being assessed. Different models will*

- use different data depending on the product, market, applicant and outcome being assessed. ; and
- retain data only for so long as necessary. ACCIS works with regulators and in line with existing legislation to ensure there are appropriate limits for the length of time data is retained, and that these limits are transparent to consumers.

The draft Regulation is contrary to other EU legislation. For example, the importance of having access to data above a “minimum necessary” level in the context of credit reference agency services is recognised in the following:

- The Consumer Credit Directive (2008/46/EC) requires creditors to assess a consumer’s creditworthiness on the basis of “sufficient information” before the conclusion of a credit agreement (Article 8 of that Directive);
- The proposed Directive of the European Parliament and the Council on credit agreements relating to residential property (2011/0062 (COD)), which requires creditors to conduct a “thorough” assessment of a consumer’s creditworthiness, using information from “relevant” sources (Article 14 of that draft Directive).

ACCIS believes that personal data should be proportionate to the processing purposes, in order to allow a degree of flexibility for individual industries.

Amendment 3

Lawfulness of processing

Article 6 – paragraph 1 – point f

Text proposed by the Commission

(f) processing is necessary for the purposes of the legitimate interests pursued by *a* controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks.

Amendment

(f) processing is necessary for the purposes of the legitimate interests pursued by *the a* controller *or by the third party or third parties to whom the data are disclosed*, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks.

Amendment 4

Lawfulness of processing

Article 6 – paragraph 4

Text proposed by the Commission

4. Where the purpose of further processing is not compatible with the one for which the personal data have been collected, the processing must have a legal basis at least in one of the grounds referred to in *points (a) to (e) of* paragraph 1. This shall in particular apply

Amendment

4. Where the purpose of further processing is not compatible with the one for which the personal data have been collected, the processing must have a legal basis at least in one of the grounds referred to in ~~points (a) to (e)~~ of paragraph 1. This shall in particular

to any change of terms and general conditions of a contract.

apply to any change of terms and general conditions of a contract.

Justification

The legitimate interests condition is of fundamental significance to CRA's across the EU. Much of the processing carried out by CRAs is undertaken for the legitimate interests of their clients. Similarly, lenders (in the widest definition being any organisation providing goods or services ahead of payment) who contribute data to the shared databases operated by CRAs will often rely on the legitimate interests of the CRAs. The long-established network of data sharing which underpins many credit reference agency services is therefore heavily dependent on the words proposed above being included in the draft Regulation (as they are currently included in Directive 95/46/EC).

By not repeating the provisions of the current legislation, there is a material risk that credit reference agencies' ability to effectively serve their clients and help them assess customers' ability to meet their financial obligations will be adversely affected. ACCIS believes that the removal of these words may not have been intentional, as the wording "a controller" is ambiguous in this respect. As a consequence, a definition of "third party" should be given in Article 4 of the draft Regulation (see Article 2 f) of the Directive 95/46/EC).

Furthermore, CRAs rely on a constant flow of data. In cases of a change of purpose during the data processing, this should be also possible under the conditions of Article 6 paragraph 1 f), which is not included in the reference of Article 6 paragraph 4 (only "(a) to (e)", not "(a) to (f)"). Otherwise, the processing of relevant and predictive data would not be possible any longer.

Amendment 5

Procedures and mechanisms for exercising the rights of the data subject

Article 12 – paragraph 2

Text proposed by the Commission

2. The controller shall inform the data subject without delay and, at the latest within one month of receipt of the request, whether or not any action has been taken pursuant to Article 13 and Articles 15 to 19 and shall provide the requested information. This period may be prolonged for a further month, if several data subjects exercise their rights and their cooperation is necessary to a reasonable extent to prevent an unnecessary and disproportionate effort on the part of the controller. The information shall be given in writing. Where the data subject makes the request in electronic form, the information shall be provided in electronic form, unless otherwise requested by the data subject.

Amendment

2. The controller shall inform the data subject without delay and, at the latest within one month of receipt of the request, whether or not any action has been taken pursuant to Article 13 and Articles 15 to 19 and shall provide the requested information. This period may be prolonged for a further month, if several data subjects exercise their rights and their cooperation is necessary to a reasonable extent to prevent an unnecessary and disproportionate effort on the part of the controller. The information shall be given in writing. Where the data subject makes the request in electronic form, the information shall be provided in electronic form, unless otherwise requested by the data subject ***or unless the controller has reason to believe that providing the information in electronic form***

would create a significant risk of fraud.

Justification

Releasing certain data in electronic form such as credit files could result in modification or identity theft when provided to consumers. Release of data from credit reference agencies should be dependent upon authentication checks which satisfy criteria set out by the agency holding the data to prevent interception, misuse, fraudulent use or modification.

Amendment 6

Procedures and mechanisms for exercising the rights of the data subject Article 12 – paragraph 4

Text proposed by the Commission

4. The information and the actions taken on requests referred to in paragraph 1 shall be free of charge. Where requests are manifestly excessive, in particular because of their repetitive character, the controller may charge a fee for providing the information or taking the action requested, or the controller may not take the action requested. In that case, the controller shall bear the burden of proving the manifestly excessive character of the request.

Amendment

4. The charges for taking action or providing information upon the request of data subject referred to in paragraph 1 shall not exceed actual costs of handling the requests born by the controller.

Justification

Existing legal requirements determine the manner in many EU Member States concerning access to credit files by consumers. The ability for credit reference agencies to charge a nominal fee allows for coverage of costs incurred in relation to follow up enquiries, and is commonly used mechanism to confirm the identity of the applicant and so prevent fraud.

Amendment 7

Right to be forgotten and to erasure Article 17 – paragraph 1 – point c

Text proposed by the Commission

(c) the data subject objects to the processing of personal data pursuant to Article 19;

Amendment

(c) the data subject objects to the processing of personal data pursuant to Article 19, and the objection is upheld;

Justification

This amendment is designed to ensure that a data subject cannot simply make an objection under Article 19, therefore triggering the principle of the Right to be Forgotten, where the objection would be without merit.

Amendment 8

Right to be forgotten and to erasure
Article 17 – paragraph 3 – point f (new)

*Text proposed by the Commission**Amendment*

(f) for prevention or detection of fraud, confirming identity, and/or determining creditworthiness, or ability to pay.

Justification

It would not be appropriate for individuals to be able to delete data about themselves which is held for legitimate reasons in line with existing legislation.

Amendment 9

Right to object
Article 19 – paragraph 1

*Text proposed by the Commission**Amendment*

1. The data subject shall have the right to object, on grounds relating to their particular situation, at any time to the processing of personal data which is based on points (d), (e) and (f) of Article 6(1), unless the controller demonstrates ~~compelling~~ legitimate grounds for the processing which override the interests or fundamental rights and freedoms of the data subject.

1. The data subject shall have the right to object, on grounds relating to their particular situation, at any time to the processing of personal data which is based on points (d), (e) and (f) of Article 6(1), unless the controller demonstrates legitimate grounds for the processing which override the interests or fundamental rights and freedoms of the data subject.

Justification

This amendment is designed to demonstrate that legitimate grounds should be sufficient grounds for processing, as per Article 6.

Amendment 10

Measures based on profiling

Article 20 – paragraph 1

Text proposed by the Commission

1. Every natural person shall have the right not to be subject to a measure which produces legal effects concerning this natural person or significantly affects this natural person, and which is based solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour.

Amendment

1. Every natural person shall have the right **to request** not to be subject to a measure which produces legal effects concerning this natural person or significantly affects this natural person, and which is based solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour.

Amendment 11

Measures based on profiling

Article 20 – paragraph 2 – point c

Text proposed by the Commission

(c) is *based on the data subject's consent, subject to the conditions laid down in Article 7 and to suitable safeguards.*

Amendment

(c) is **consistent with the requirements of Article 6 and of this Article 20** ~~based on the data subject's consent, subject to the conditions laid down in Article 7 and to suitable safeguards.~~

Amendment 12

Measures based on profiling

Article 20 – paragraph 2 – point d (new)

Text proposed by the Commission

Amendment

(d) Data controllers should notify the data subject where such processing takes place and give the individual the right to have any such decision reviewed.

Justification

The scope of Article 20(1) is potentially very wide and could be regarded as covering scoring models. Scoring models are used extensively across the EU by businesses:

President:	Neil Munroe • Equifax Ltd • 25 Chapel Street • LONDON • UK • GB-NW1 5DS • Tel. +44 207 298 3055 • Fax: +44 20 7723 7555 • e-mail: president@accis.eu
Secretary General:	Feriel Saouli • ACCIS • Rue Defacqz 52 • BE-1050 BRUSSELS • Tel. +32 2 536 86 73 • Fax: +32 2 645 79 99 • e-mail: gen@accis.eu
Registered office:	ACCIS IVZW • Rue Defacqz 52 • BE-1050 BRUSSELS • Company number BE 0884.372.853 • RLP BRUSSELS

- to help determine credit-worthiness, and to identify fraud and money-laundering;
- to provide reassurance with regard to an individual's ability to afford repayments; and
- to manage credit accounts and collections.

Credit and other scoring systems are widely recognised to be highly effective, transparent, consistent, and non-discriminatory ways of assimilating and balancing fairly large amounts of (often conflicting) data in order to make decisions.

Profiling for the purposes of credit scoring can be clearly distinguished from profiling for social media purposes, not least in that this profiling is clearly notified to the individual in advance. Credit scoring has public interest benefits in supporting economic growth, and it has personal benefits for data subjects. It allows consumers the benefit of transparent, quick and objective decision-making in connection with credit applications, and protects them against the very serious consequences of taking on credit they cannot afford to repay.

The wording of Article 20 threatens the continued use of these models. At a time when the issue of indebtedness is high on the European agenda, ACCIS would suggest that data subject rights are better protected by rights individuals can use in connection with this processing (such as ensuring that the data used in automated profiling is accurate, and that decisions can be reviewed), rather than a broad restriction on specific types of processing. With these protections in place, automated profiling should be permitted if it is otherwise in compliance with the provisions of the draft Regulation.

APPENDIX 1

The Nature and Importance of Credit Reference Agency Services**1. The Nature of Credit Reference Agency Services**

1.1. The services of a credit reference agency ("CRA") can differ between Member States, dependent on the nature and ownership of the credit bureau (for example, whether it is publically or privately operated). Main activities that these services can include are briefly as follows:

- When an individual makes an application for credit such as a mortgage or a loan, or for other services that involve credit such as a mobile telephone agreement, the services of a CRA can be used to verify and/or authenticate the individual, and to indicate whether the application may be fraudulent;
- Credit reference and related data can be used to help determine whether an individual should be accepted (according to criteria set by the lender), and if so the terms on which credit will be granted;
- Credit reference and related data (often in combination with other data obtained by the decision-making organisation) may be used manually for underwriting in its "raw" form, or managed in a more automated manner through decision-making systems which may also incorporate credit scoring techniques;
- Similar services can be used to monitor and manage accounts once they have been set up;
- If accounts go into arrears or default, and if the account holder absconds without leaving a forwarding address, the services of a CRA can assist with tracing and contacting an individual, and determining the strategies which should be applied to collecting any overdue amounts.

1.2. ACCIS members, and other CRA's across the EU, provide a complex range of services in these areas. Many of these depend on advanced data-sharing arrangements, and are designed to achieve the following:

- Tools to combat fraud and identity theft;
- Provision of technologies to allow for quick and efficient decision-making. (Credit reference agency services facilitate access by individuals and businesses (including SME's) to credit and other services in a way which is consistent with their expectations in a technological world. This particularly requires rapid (sometimes instantaneous) and effective decision-making, delivered in convenient ways, often in situations where there is no face-to-face contact between lender and borrower, and where the use of paper and the burden on the individual to provide supporting evidence are both kept to a minimum);
- Responsible lending, so that individuals and businesses do not become over-exposed to levels of debt which they cannot support;
- The efficient management of accounts and the minimisation of bad debt (the occurrence of which inevitably increases the cost of credit for responsible borrowers);
- The fair and lawful treatment of individuals and businesses.

- 1.3. Services such as these are widely used in a number of situations in which mainstream goods and services which are the subject of credit are offered in the EU. The assessment of credit applications using automated decision-making processes is almost inextricably embedded in many sectors, which can include finance, banking, retail, utilities and telecommunications.

2. The Importance of Credit Reference Agency Services

- 2.1. Credit reference agency services are widely recognised as being essential to the effective operation of credit in a modern economy. The free flow of responsibly managed credit to consumers and businesses is widely recognised as being essential to economic growth:

“Well functioning financial markets contribute to sustainable growth and economic development...Credit reporting is a vital part of a country’s financial infrastructure and is an activity of public interest.”

(The World Bank: “General Principles for Credit Reporting.” Consultative Report, March 2011).

“Small firms benefit from credit bureaus.”

(International Finance Corporation presentation entitled “Global Credit Bureau Program” September 2010)

“...empirical evidence has provided plenty of evidence supporting the claim that credit sharing institutions have a positive effect on lending to the private sector. For instance, Jappelli and Pagano (2002) show that strong credit-sharing institutions are positively related to the size of the credit market. Other empirical studies, including Jappelli and Pagano (1993), Love and Mylenko (2003), Galindo and Miller (2001) and Powell, et al. (2004) have shown that credit is more abundant when borrowers and lenders benefit from credit-sharing institution.”

(OECD Discussion Paper on Credit Information Sharing)

“Data protection and the right to privacy are fundamental to the establishment of a private credit bureau. Governments should ensure that a legal framework is in place that protects privacy but does not stifle the creation of private credit bureaus.”

(OECD Discussion Paper on Credit Information Sharing)

- 2.2. As well as performing this vital role, credit reference agency services are widely recognised as being the best way of producing fair and effective decisions in relation to credit in a modern economy.

“Historically, credit would be granted on the basis of a credit officer’s personal knowledge of the debtor. Robust credit reporting systems capture most of this information and sometimes even facts that might not be disclosed to credit officers. Moreover, creditors are generally able to access credit reporting information at a fraction of the cost and time of traditional lending mechanisms. At the same time, credit reporting systems support unbiased decision-making as such decisions are based on objective and correct data. This last feature favours segments of the population that may have been denied credit in the past due to some form of prejudice (e.g. assuming that a low-income individual is always a bad debtor.”

(The World Bank: “General Principles for Credit Reporting.” Consultative Report, March 2011).

- 2.3. By ensuring that individuals do not take on credit obligations which they are unable to manage, credit reference agency services help to ensure that individuals are less likely to be exposed to the potentially very serious personal consequences which can result from over-indebtedness.
- 2.4. ACCIS would contend that credit reference agency services are essential to the successful operation of the EU economy, and that any material restriction placed on existing, legitimate activities in these areas would have implications far beyond the effect on the revenues of CRAs. As well as detrimental impact on the economy and society at large, any such restriction would have particular adverse consequences for individuals and small businesses.

Amazon EU Sarl

Proposed amendments to MEP Gallo's opinion on data protection

Amendment 1

Proposal for a regulation

Recital 20

Text proposed by the Commission

(20) In order to ensure that individuals are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects residing in the Union by a controller not established in the Union should be subject to this Regulation where the processing activities are related to the offering of goods or services to such data subjects, or to the monitoring of the behaviour of such data subjects.

Amendment

(20) In order to ensure that individuals are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects residing in the Union by a controller not established in the Union, **and where this Regulation would not otherwise apply**, should be subject to this Regulation where the processing activities are related to the offering of goods or services **that are specifically targeted at** such data subjects, or to the monitoring of the behaviour of such data subjects.

Or. en

Justification

This amendment is consistent with the amendment to Art. 3.2.

Amendment 2

Proposal for a regulation

Recital 23

Text proposed by the Commission

(23) The principles of protection should apply to any information concerning an identified or identifiable person. To determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used **either** by the controller **or by any other person** to identify the individual. The principles of data protection should not apply to **data rendered anonymous in such a way that the data subject is no longer identifiable**.

Amendment

(23) The principles of protection should apply to any information concerning and identified or identifiable person. To determine whether a person is identifiable, account should be taken of all the means **that are technically feasible, do not involve a disproportionate effort, and are** likely reasonably to be used by the controller **or the processor in the context of the specific processing activity and with the intention** to identify the individual. **Account shall also be taken of the technical and organizational measures put in place by the controller or processor to prevent identification of the individual.** The principles of data protection shall not apply to **processors when processors are not required to identify data subjects as part of their processing activities and where the use of such technical and organizational measures render it substantially unlikely for the processor to identify the data subject.**
Data that has been collected, altered or otherwise processed in such a way that its controller or processor can no longer attribute it to a data subject

or that such attribution would require a disproportionate amount of time, cost and effort (anonymous data), shall not be considered as personal data for that controller or processor. This shall also apply in cases where the controller or processor has replaced any personal identifiers contained in the data with a code, provided and as long as the code does neither alone nor together with other data available to the controller or processor allow identification of the data subject.

Data that has been collected, altered or otherwise processed in such a way that the data subject's name and other identifying features have been replaced with another identifier so that identifiability of the data subject is considerably impeded (pseudonymous data) shall be considered as personal data.

The principles of data protection shall not apply to data that has been collected, altered or otherwise processed with the sole purpose of rendering it anonymous, pseudonymous or unable to be identified by the controller or processor.

Or. en

Justification

This amendment is consistent with the amendment to Art. 4.1. points (1), (2) and new (2a).

Amendment 3

Proposal for a regulation

Recital 24a (new)

Text proposed by the Commission

Amendment

Where service providers process data without being able to access personal data by means that are technically feasible, do not involve a disproportionate effort, and are reasonably likely to be used by a controller or a processor to take knowledge of the content of such data, such service providers shall be qualified as mere conduits pursuant to Article 12 of the Directive 2000/31/EC----- and shall not be responsible for any personal data transmitted or otherwise processed or made available through them.

Or. en

Justification

This amendment intends to take account of the fact that the traditional controller/processor concept structurally does not cater for many types of cloud computing services particularly where the cloud provider offers simple infrastructure services (processing power, storage, basic computing resources). Such providers are usually data agnostic. They regularly don't know whether information stored on or processed through their infrastructure is personal data and they usually have no control over or ability to access that data, nor do they require such knowledge or access to provide their services. The reality shows that the relation of a number of cloud providers to data is fundamentally different from that of traditional processors. Recognition of such reality will help promote (rather than impede) the further development of cloud computing in Europe. The Regulation should provide for different actors with varying degrees of obligations and liabilities under the data protection laws.

Amendment 4

Proposal for a regulation

Recital 25

Text proposed by the Commission

(25) Consent should be given **explicitly** by any appropriate method enabling a freely given specific and informed indication of the data subject's wishes, **either by a statement or by a clear affirmative action by the data subject**, ensuring that individuals are aware that they give their consent to the processing of personal data, **including by** ticking a box when visiting an Internet website or by any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data. **Silence or inactivity should therefore not constitute consent.** Consent should cover all processing activities carried out for the same purpose or purposes. If the data subject's consent is to be given following an electronic request, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.

Amendment

(25) Consent should be given by any appropriate method, **commensurate to the context of and risk involved with the respective processing activity**, enabling a freely given specific, and informed indication of the data subject's wishes **and** ensuring that individuals are aware that they give their consent to the processing of personal data. **Consent may be given by a statement or an affirmative action by the data subject such as** ticking a box when visiting an Internet website or by any other statement, conduct or **measure** which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data. Consent should cover all processing activities carried out for the same purpose or purposes. If the data subject's consent is to be given following an electronic request, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.

Or. en

Justification

This amendment is consistent with the amendment to Art. 4.1(8).

Amendment 5

Proposal for a regulation

Recital 27

Text proposed by the Commission

(27) The main establishment of **a controller** in the Union should be **determined according to objective criteria and should imply the effective and real exercise of management activities determining the main decisions as to the purposes, conditions and means of processing through stable arrangements. This criterion should not depend whether** the processing of personal data is actually carried out **at that location**; the presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute such main establishment and are therefore no determining criteria for a main establishment. **The main establishment of the processor should be the place of its central administration in the Union.**

Amendment

(27) The main establishment of **an undertaking or a group of undertakings, whether controller or processor**, in the Union should be **designated by the undertaking or group of undertakings and the competent authority should be informed of such designation, subject to the consistency mechanism set out in Article 57. The designation of the main establishment should be based upon the following optional objective criteria:**

- (1) location of the group's European headquarters;**
- (2) location of the entity within the group with delegated data protection responsibilities;**
- (3) location of the entity within the group which is best placed (in terms of management function, administrative burden etc.) to deal with and enforce the rules as set out in this Regulation;**
- (4) location where effective and real management activities are exercised determining the data processing through stable arrangements.**

Priority shall be given to the criteria described under (1) above.

The location where the processing of personal data is actually carried out **shall not be a relevant criteria**; the presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute such main establishment and are therefore no determining criteria for a main establishment.

Or. en

Justification

This amendment is consistent with the amendment to Art. 4(13).

Amendment 6

Proposal for a regulation

Recital 33

Text proposed by the Commission

(33) In order to ensure free consent, it should be clarified that consent does not provide a valid legal ground where the individual has no genuine and free choice and is subsequently not able to refuse or withdraw consent **without detriment**.

Amendment

(33) In order to ensure free consent, it should be clarified that consent does not provide a valid legal ground where the individual has no genuine and free choice and is subsequently not able to refuse or withdraw consent.

Or. en

Justification

The change clarifies that free consent, including the ability to refuse or withdraw consent, cannot be made dependent on whether the data subject may incur a detriment as the result of consent withdrawal. This is particularly the case where benefits and services that are provided in the context of a contractual relationship are dependent upon consent. Withdrawal of consent shall be possible, but only in accordance with the contract's terms and data subjects should be aware that they may not be able to withdraw consent and maintain these benefits or services. The new language emphasizes this point so consumers make a well-reasoned decision before choosing to withdraw consent.

Amendment 7

Proposal for a regulation

Recital 34

Text proposed by the Commission

(34) Consent should not provide a valid legal ground for the processing of personal data, where **there is a clear imbalance between** the data subject **and the controller**. This **is especially** the case where the data subject is in a situation of dependence from the controller, **among others**, where personal data are processed by the employer of employees' personal data in the employment context. Where the controller is a public authority, there would be an imbalance only in

Amendment

(34) Consent should not provide a valid legal ground for the processing of personal data, where **consent is not freely given by** the data subject. This **can be** the case where the data subject is in a situation of **fundamental economic** dependence from the controller **that is** where personal data are processed by the employer of employees' personal data in the employment context. Where the controller is a public authority, there would be an imbalance only in the

the specific data processing operations where the public authority can impose an obligation by virtue of its relevant public powers and the consent cannot be deemed as freely given, taking into account the interest of the data subject.

specific data processing operations where the public authority can impose an obligation by virtue of its relevant public powers and the consent cannot be deemed as freely given, taking into account the interest of the data subject.

Or. en

Justification

The notion of “significant imbalance” lacks clarity and will lead to confusion and legal uncertainty for both consumers and businesses. There is the risk that the utility of consent will be significantly restricted, as there is rarely an equal bargaining power between individuals and businesses. For instance, one could claim that there is significant imbalance where an individual relies upon the usage of a service for his business. Article 4(8) better addresses concerns about protecting consumers by mandating data subject’s consent must be “freely given”.

Amendment 8

Proposal for a regulation

Recital 62

Text proposed by the Commission

(62) The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers **and processor**, also in relation to the monitoring by and measures of supervisory authorities, requires a clear attribution of the responsibilities under this Regulation, including where a controller determines the purposes, conditions and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller.

Amendment

(62) The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers, also in relation to the monitoring by and measures of supervisory authorities, requires a clear attribution of the responsibilities under this Regulation, including where a controller determines the purposes, conditions and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller.

Or. en

Justification

This amendment is meant to clarify wording in line with amendments to Article 26.1 and 26.2.

Amendment 9

Proposal for a regulation

Recital 63

Text proposed by the Commission

(63) Where a controller not established in the Union is processing personal data of data subjects residing in the Union whose processing activities are related to the offering of goods or services **to** such data subjects, or to the monitoring their behaviour, the controller should designate a representative, unless the controller is established in a third country ensuring an adequate level of protection, or the controller is a small or medium sized enterprise or a public authority or body or where the controller is only occasionally offering goods or services to such data subjects. The representative should act on behalf of the controller

Amendment

(63) Where a controller not established in the Union is processing personal data of data subjects residing in the Union whose processing activities are related to the offering of goods or services **that are specifically targeted at** such data subjects, or to the monitoring **of** their behaviour, the controller should designate a representative, unless the controller is established in a third country ensuring an adequate level of protection, or the controller is a small or medium sized enterprise or a public authority or body or where the controller is only occasionally offering goods or services to such data subjects. The representative should act on behalf of the controller and **shall only** be addressed by **the**

and *may* be addressed by *any* supervisory authority.

supervisory authority *of the establishment of the representative*.

Or. en

Justification

The inclusion of the term “targeting” is consistent with the amendment to Art. 3.2. The second change is intended to ensure respect of the EU principle of non-discrimination by affording the benefit of the one stop shop principle also to non-EU controllers who appoint an EU representative. They should benefit from one of the main anchors of the draft Regulation in the same way as EU established companies, given that they are subject to the same rights and obligations of the draft Regulation.

Amendment 10

Proposal for a regulation

Recital 64

Text proposed by the Commission

(64) In order to determine whether *a controller is only occasionally* offering goods or services *to* data subjects residing in the Union, it should be ascertained whether it is apparent from the controller's overall activities that the offering of goods and services to such data subjects is *ancillary to those main activities*.

Amendment

(64) In order to determine whether *the* offering of goods or services *is targeted at* data subjects residing in the Union, it should be ascertained whether it is apparent from the controller's overall activities that the offering of goods and services to such data subjects is *specifically and-intentionally directed at them, taking account of in particular the international nature of the activities, use of a language or a currency other than the language or currency generally used in the controller's country of establishment, the possibility of making and confirming a reservation in that other language, or the use of a top-level domain name with the .eu suffix or other than that of the country in which the controller is established. The mere accessibility of the controller's website by a data subject residing in the Union is insufficient*.

Or. en

Justification

This amendment is consistent with the amendment to Art. 3.2.

Amendment 11

Proposal for a regulation

Recital 65

Text proposed by the Commission

(65) In order to demonstrate compliance with this Regulation, the controller *or processor* should document *each* processing operation. Each controller *and processor* should be obliged to co-operate with the supervisory authority and make this documentation, on request, available to it, *so that it might serve for monitoring those processing operations*.

Amendment

(65) In order to demonstrate compliance with this Regulation, the controller should document *the main* processing operations. Each controller should be obliged to co-operate reasonably with the supervisory authority and make this documentation, on request, available to it.

Or. en

Justification

The proposed documentation obligation is disproportionate since it covers virtually every data processing activity. It risks defeating the objective of the draft Regulation to reduce administrative burdens. The changes aim to achieve effective data protection, by requiring organisations to document their main data processing activities. Processors should not be subject to the documentation requirement as they usually do not have access to data or other processing strategies which remain the remit of the controller. It should be left to the controller and processor to determine contractually who is best placed to adequately document the specific processing activities in compliance with this Regulation.

Amendment 12

Proposal for a regulation

Recital 70

Text proposed by the Commission

(70) Directive 95/46/EC provided for a general obligation to notify processing of personal data to the supervisory authorities. While this obligation produces administrative and financial burdens, it did not in all cases contribute to improving the protection of personal data. Therefore such indiscriminate general notification obligation should be abolished, and replaced by effective procedures and mechanism which focus instead on those processing operations which are likely to present *specific* risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes. In such cases, a data protection impact assessment should be carried out by the controller *or processor* prior to the processing, which should include in particular the envisaged measures, safeguards and mechanisms for ensuring the protection of personal data and for demonstrating the compliance with this Regulation.

Amendment

(70) Directive 95/46/EC provided for a general obligation to notify processing of personal data to the supervisory authorities. While this obligation produces administrative and financial burdens, it did not in all cases contribute to improving the protection of personal data. Therefore such indiscriminate general notification obligation should be abolished, and replaced by effective procedures and mechanism which focus instead on those processing operations which are likely to present *significant* risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes. In such cases, a data protection impact assessment should be carried out by the controller prior to the processing, which should include in particular the envisaged measures, safeguards and mechanisms for ensuring the protection of personal data and for demonstrating the compliance with this Regulation.

Or. en

Justification

The term “specific risk” is too vague and would open up to a seemingly infinite amount of criteria. The scope should be narrowed down to “significant risks” to be reflective of the real concerns. Processors should not be subject to the data impact assessment requirement as they usually do not have access to data or other processing strategies which remain the remit of the controller. In any case, it should be left to the controller and processor to determine contractually who is best placed to undertake an impact assessment, where required under this Regulation.

Amendment 13

Proposal for a regulation

Recital 105

Text proposed by the Commission

In order to ensure the consistent application of this Regulation throughout the Union, a consistency mechanism for co-operation between the supervisory authorities themselves and the Commission should be

Amendment

In order to ensure the consistent application of this Regulation throughout the Union, a consistency mechanism for co-operation between the supervisory authorities themselves and the Commission should be

established. This mechanism should in particular apply where **a** supervisory authority intends to take a measure as regards processing operations that are related to the offering of goods or services **to** data subjects in several Member States, or to the monitoring such data subjects, that might substantially affect the free flow of personal data. ***It should also apply where any supervisory authority or the Commission requests that the matter should be dealt with in the consistency mechanism.*** This mechanism should be without prejudice to any measures that the Commission may take in the exercise of its powers under the Treaties.

established. This mechanism should in particular apply where **the competent** supervisory authority intends to take a measure as regards processing operations that are related to the offering of goods or services ***specifically targeted at*** data subjects in several Member States, or to the monitoring such data subjects, ***and the controller not established in the Union has not appointed a representative in the Union, or as regards processing operations*** that might substantially affect the free flow of personal data. This mechanism should be without prejudice to any measures that the Commission may take in the exercise of its powers under the Treaties.

Or. en

Justification

Companies not established in the Union that are covered by the Regulation should not automatically be subject to the consistency mechanism in all circumstances. The competence of the data protection board with respect to such non- EU companies should be equivalent to that for EU companies. Only if the non-EU company does not appoint a representative is it justified to apply the consistency mechanism. This amendment is also consistent with the amendment to Article 58.1, Article 58.2 as well as Article 3.2 and Article 51.2.

Amendment 14

Proposal for a regulation

Recital 106

Text proposed by the Commission

In application of the consistency mechanism, the European Data Protection Board should, within a determined period of time, issue an opinion, if a ***simple*** majority of its members so decides or if so requested by any supervisory authority or the Commission.

Amendment

In application of the consistency mechanism, the European Data Protection Board should, within a determined period of time, issue an opinion, if a ***qualified*** majority of its members so decides or if so requested by any supervisory authority or the Commission.

Or. en

Justification

Majorities need to be substantial in accordance with current practice.

Amendment 15

Proposal for a regulation

Recital 108

Text proposed by the Commission

There may be an urgent need to act in order to protect the interests of data subjects, in particular when the danger exists that the enforcement of a right of a data subject could be considerably impeded. Therefore, ***a*** supervisory authority should be able to adopt provisional measures with a specified period of validity when applying the consistency mechanism.

Amendment

There may be an urgent need to act in order to protect the interests of data subjects, in particular when the danger exists that the enforcement of a right of a data subject could be considerably impeded. Therefore, ***the competent*** supervisory authority should be able to adopt provisional measures with a specified period of validity when applying the consistency mechanism.

Or. en

Justification

This amendment is consistent with the amendment to Article 51.2.

Amendment 16

Proposal for a regulation

Article 3 – paragraph 2

Text proposed by the Commission

2. This Regulation applies to the processing of personal data of data subjects residing in the Union **by a controller not established in the Union, where** the processing activities are related to:

(a) the offering of goods or services **to** such data subjects in the Union; or

(b) the monitoring of their behaviour.

Amendment

2. This Regulation applies to the processing of personal data of data subjects residing in the Union, **in circumstances when Article 3(1) does not apply, but when** the processing activities **of the controller** are related to:

(a) the offering of goods or services **which are specifically targeted at** such data subjects in the Union; or

(b) the monitoring of their behaviour.

Or. en

Justification

While it is desirable that non-EU companies respect EU data protection standards when processing EU citizens' data, the term "offering" is too broad and unpredictable and does not constitute a valid legal notion in the context of cross-border activities to determine the applicable law and jurisdiction. Companies may not know that their customers are European residents. The wording does not take into account that goods and services may be offered passively online with no clear way to determine the location of the purchaser or end user. The use of the additional term "targeting" can be evaluated by objective criteria, thereby carrying much more legal certainty. It also reflects current EU jurisprudence.

Amendment 17

Proposal for a regulation

Article 4 – paragraph 1 – point 1

Text proposed by the Commission

(1) '**data subject**' means an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or **by any other natural or legal person, in particular** by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;

Amendment

(1) '**Personal data**' means **any information concerning** an identified natural person or a natural person who can be identified ('**data subject**'), directly or indirectly, by means **that are technically feasible, do not involve a disproportionate effort, and are** reasonably likely to be used by the controller **or the processor in the context of the specific processing activity and with the intention to identify the data subject, including** by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person; **these factors as such need not necessarily be considered as personal data in all circumstances;**

Or. en

Justification

The proposed definition is very broad and will effectively result in the strict conditions of the Regulation applying to the vast majority of all processing operations, regardless of the context in which the data is processed, whether the data is attributable to a person, the realistic privacy risk and intention of identification. This all-encompassing approach risks leading to a disruptive consumer experience, particularly in the online environment, and risks removing any incentive for companies to invest in or make use of privacy-enhancing measures and processes as under such an approach any piece of information, even if anonymized, would have to be considered personal. This will, as a result, lead to less privacy protection rather than more, which would directly conflict with the intended objective of the Regulation. The suggested changes are intended to enhance protection of individuals' data by placing the focus on the most relevant data processing operations, on the parties who will have access to the data and by setting true incentives for industry to continuously invest in robust privacy-friendly technologies. In line with recital 24, it should be made clear in the Article 4 itself that it depends on the context whether identification numbers, location data, and online identifiers are to be considered personal data.

Amendment 18

Proposal for a regulation

Article 4 – paragraph 1 – point 2

Text proposed by the Commission

Amendment

(2) **'personal data'** means any **information relating to a data subject**;

(2) **'Anonymous data'** means any **data that has been collected, altered or otherwise processed in such a way that it can no longer be attributed to a data subject, including where any personally identifying features are replaced with a code so that the data subject can no longer be identified, or that such attribution would require a disproportionate amount of time, cost and effort; anonymous data shall not be considered personal data.**

Or. en

Justification

Businesses should be incentivized to anonymize data, which will ultimately strengthen consumers' privacy protection. The changes aim at clarifying the meaning of anonymous data and, in line with recital 23, explicitly excluding such data from the scope of the Regulation.

Amendment 19

Proposal for a regulation

Article 4 – paragraph 1 – point 2a (new)

Text proposed by the Commission

Amendment

(2a) **'pseudonymous data'** means any **personal data that has been collected, altered or otherwise processed in such a way that the data subject's name and other identifying features are replaced with another identifier so that identifiability of the data subject is considerably impeded; pseudonymous data shall be considered as personal data.**

Or. en

Justification

Businesses should be incentivized to invest in and use privacy-enhancing measures, such as pseudonymization, which will ultimately strengthen consumers' privacy protection. The changes aim at ensuring that the Regulation expressly recognises the existence and value of pseudonymous data. Similar approaches in existing data protection laws of some Member States (e.g. Germany) have proven successful.

Amendment 20

Proposal for a regulation

Article 4 – paragraph 1 – point 6

Text proposed by the Commission

(6) 'processor' means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

Amendment

6) 'processor' means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller ***and is able to access personal data by means that are technically feasible, do not involve a disproportionate effort, and are reasonably likely to be used by a controller or a processor to take knowledge of the content of such data;***

Or. en

Justification

This amendment is consistent with the amendment to Recital 24a (new).

Amendment 21

Proposal for a regulation

Article 4 – paragraph 1 – point 8

Text proposed by the Commission

(8) 'the data subject's consent' means any freely given specific, informed ***and explicit*** indication of his or her wishes by which the data subject, either by a statement or ***by a*** clear ***affirmative*** action, signifies agreement to personal data relating to them being processed;

Amendment

(8) 'the data subject's consent' means any freely given specific ***and*** informed indication of his or her wishes by which the data subject, either by a statement or clear action ***or any other appropriate method commensurate to the context of and risk involved with the respective processing activity,*** signifies agreement to personal data relating to them being processed;

Or. en

Justification

Requiring 'explicit' consent as the norm for every data use scenario, irrespective of the context of data processing and the privacy risks for data subjects, is overly formalistic and rigid. It risks inhibiting legitimate and innovative business practices in the off- and online environment and impacting user experience and expectations without adding anything to users' data protection. Consent as a means to gain user acceptance and protect fundamental rights may be devaluated as a consequence of consumers being overloaded with consent requests, making it difficult for them to understand the privacy impact of different data processing operations. The suggested changes aim at allowing for flexibility for businesses, avoiding confusing of consumers and ensuring that there is a role for implied consent in cases where a user's behaviour can safely be interpreted as a decision to accept certain uses of data.

Amendment 22

Proposal for a regulation

Article 4 – paragraph 1 – point 13

Text proposed by the Commission

(13) ‘main establishment’ means *as regards the controller, the place of its establishment in the Union where the main decisions as to the purposes, conditions and means of the processing of personal data are taken; if no decisions as to the purposes, conditions and means of the processing of personal data are taken in the Union, the main establishment is the place where the main processing activities in the context of the activities of an establishment of a controller in the Union take place. As regards the processor, ‘main establishment’ means the place of its central administration in the Union;*

Amendment

(13) ‘main establishment’ means ***the location as designated by the undertaking or group of undertakings, whether controller or processor, subject to the consistency mechanism set out in Article 57, on the basis of, but not limited to, the following optional objective criteria:***

- (1) the location of the European headquarters of a group of undertakings;***
- (2) the location of the entity within a group of undertakings with delegated data protection responsibilities;***
- (3) the location of the entity within the group which is best placed in terms of management functions and administrative responsibilities to deal with and enforce the rules as set out in this Regulation; or***
- (4) the location where effective and real management activities are exercised determining the data processing through stable arrangements.***

The competent authority shall be informed by the undertaking or group of undertakings of the designation of the main establishment.

Or. en

Justification

The ‘one-stop-shop’ approach with respect to the jurisdiction of regulators is particularly crucial for corporate groups operating in several Member States as they require legal certainty as to one ‘lead’ regulator being their single point of contact and by whom they may be addressed, and it is also essential to allow businesses and consumers to fully reap the benefits of the EU Single Market. It also has the potential to cut red tape, provide legal certainty and ensure a consistent and more efficient application of data protection rules across Europe. The current system has led to confusion as to competency questions and to conflicting approaches by regulators as a result of this. However, the proposed ‘main establishment’ terminology is too vague and narrow to work in different situations and provides too much room for diverging interpretation. To take account of today’s business reality and provide for clear-cut and common sense criteria allowing for flexibility and predictability for all stakeholders, one uniform test for determining an organization’s “main establishment” should be applied to “undertakings/groups of undertakings” as the relevant reference point (rather than applying different tests for controller and processor) and based on a set of relevant objective criteria, which a business can choose from in order to officially designate its location of ‘main establishment’, with effects for all processing activities of all entities part of the group. A similar concept to determine the lead DPA exists in relation to Binding Corporate Rules (BCRs) and should for consistency reasons also apply for the purpose of determining the place of ‘main establishment’ in the context of the draft Regulation. This approach will provide for legal certainty required by business while preventing the risk of forum shopping as well as disputes over the place of main establishment.

Amendment 23

Proposal for a regulation

Article 4 – paragraph 1 – point 14

Text proposed by the Commission

Amendment

(14) ‘representative’ means any natural or legal person established in the Union who, explicitly designated by the controller, acts and **may** be addressed by **any** supervisory authority **and other bodies in the Union instead of the controller**, with regard to the obligations of the controller under this Regulation;

(14) ‘representative’ means any natural or legal person established in the Union who, explicitly designated by the controller, acts and **shall only** be addressed by **the supervisory authority of the establishment of the representative**, with regard to the obligations of the controller under this Regulation;

Justification

The change is intended to ensure respect of the EU principle of non-discrimination by affording the benefit of the one stop shop principle also to non-EU controllers who appoint an EU representative. They should benefit from one of the main anchors of the draft Regulation in the same way as EU established companies, given that they are subject to the same rights and obligations of the draft Regulation.

Amendment 24

Proposal for a regulation

Article 4 – paragraph 1 – point 20 (new)

Text proposed by the Commission

Amendment

(20) ‘erasure’ means deleting personal data or rendering it unusable, unreadable, anonymous or indecipherable through the use of appropriate technological protection measures which are widely accepted as effective industry practices or industry standards, when applicable.

Or. en

Justification

This change is aimed at providing flexibility for different technical capabilities. Whether the data is deleted, rendered unusable, unreadable, irreversibly anonymous, or indecipherable, the main goal is that the data subject’s information can no longer be accessed or identified to the extent practicable by the controller or processor. The change of language will also provide assurance and comfort to data subjects in situations where information cannot be fully erased for a variety of reasons. Similar clarifications contained in existing data protection laws of some Member States (e.g. Germany) have proven successful.

Amendment 25

Proposal for a regulation

Article 6 – paragraph 1 – point (g) (new)

Text proposed by the Commission

Amendment

(g) only pseudonymous data is processed.

Or. en

Justification

This amendment is consistent with the amendment to new Art. 4.1(2a)

Amendment 26

Proposal for a regulation

Article 6 – paragraph 4

Text proposed by the Commission

4. Where the purpose of further processing is not compatible with the one for which the personal data have been collected, the processing must have a legal basis at least in one of the grounds referred to in points (a) to (e) of paragraph 1. This shall in particular apply to any change of terms and general conditions of a contract.

Amendment

4. Where the purpose of further processing is not compatible with the one for which the personal data have been collected, the processing must have a legal basis at least in one of the grounds referred to in points (a) to (g) of paragraph 1. This shall in particular apply to any change of terms and general conditions of a contract.

Or. en

Justification

This amendment is consistent with the amendment to new Art. 4.1(2a)

Amendment 27

Proposal for a regulation

Article 7 – Paragraph 2

Text proposed by the Commission

2. If the data subject's consent is to be given in the context of a written declaration which also concerns another matter, the requirement to give consent must be presented distinguishable in its appearance **from this other matter**.

Amendment

2. The controller shall select the method most appropriate to obtain meaningful consent from data subjects. The requirement to give consent must be presented **in a manner** distinguishable in its appearance.

Or. en

Justification

The changes reflect the need to consider differences in the purpose and context for the collection of data. The goal to provide clear information to data subjects is preserved and strengthened. The current wording “distinguishable in its appearance” is vague, which could result in situations where the data subject may be confused as to the importance of each section of the matters. Further, some contractual arrangements are fully dependent upon the data subject providing consent and fully separating consent from other issues may confuse data subjects.

Amendment 28

Proposal for a regulation

Article 7 – Paragraph 3

Text proposed by the Commission

3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

Amendment

3. The data subject shall have the right to withdraw his or her consent at any time, **without prejudice to applicable laws and contractual arrangements**. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

Or. en

Justification

It should be clarified in the Regulation that while data subjects may withdraw their consent at any time, such withdrawal needs to be in accordance with the contractual terms. Many benefits and services that are provided in the context of a contractual relationship are dependent on consent for processing of data. Therefore, when data subjects withdraw consent, they may not be able to maintain these benefits or services. The new language emphasizes this point so consumers make a well-reasoned decision before choosing to withdraw consent.

Amendment 29

Proposal for a regulation

Article 7 – Paragraph 4

Text proposed by the Commission

Amendment

4. Consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller.

Deleted

Or. en

Justification

The notion of “significant imbalance” lacks clarity and will lead to confusion and legal uncertainty for both consumers and businesses. There is the risk that the utility of consent will be significantly restricted, as there is rarely an equal bargaining power between individuals and businesses. For instance, one could claim that there is significant imbalance where an individual relies upon the usage of a service for his business. Article 4(8) better addresses concerns about protecting consumers by mandating data subject’s consent must be “freely given”.

Amendment 30

Proposal for a regulation

Article 19 – Paragraph 1

Text proposed by the Commission

Amendment

1. The data subject shall have the right to object, on grounds relating to their particular situation, at any time to the processing of personal data which is based on points (d), (e) **and** (f) of Article 6(1), unless the controller demonstrates compelling legitimate grounds for the processing which override the interests or fundamental rights and freedoms of the data subject.

1. The data subject shall have the right to object, on grounds relating to their particular situation, at any time to the processing of personal data which is based on points (d), (e), (f) **and (g)** of Article 6(1), unless the controller demonstrates compelling legitimate grounds for the processing which override the interests or fundamental rights and freedoms of the data subject.

Or. en

Justification

This amendment is consistent with the amendment to new Art. 4.1 point 2a. Data subjects’ right to object to data processing shall be extended to the processing of pseudonymous data.

Amendment 31

Proposal for a regulation

Article 20 – Paragraph 2 – point (d) (new)

Text proposed by the Commission

Amendment

(d) is based on pseudonymous data.

Or. en

Justification

This amendment is consistent with the amendment to new Art. 4.1 point 2a. Since the aim of pseudonymous data is to prevent identification of an individual, processing of such data for profiling purposes should be permitted.

Amendment 32

Proposal for a regulation

Article 22 – Paragraph 2a (new)

Text proposed by the Commission

Amendment

2a. Paragraph 2(a), (c), (d) shall not apply to controllers who have appointed a data protection officer pursuant to Article 35.

Or. en

Justification

The appointment of a data protection officer should result in the exemption from administrative burdens, such as the documentation requirement, the obligation to undertake a data impact assessment, prior authorization and consultation. This practice has been widely successful in other Member States (e.g. Germany), encouraging the appointment of DPOs and ultimately leading to increases in both business efficiency and consumer protections.

Amendment 33

Proposal for a regulation

Article 22 – Paragraph 3

Text proposed by the Commission

Amendment

3. The controller shall implement mechanisms to ensure the verification of the effectiveness of the measures referred to in paragraphs 1 and 2. If proportionate, this verification shall be carried out by independent internal or external auditors.

3. The controller shall implement mechanisms to ensure the verification of the effectiveness of the measures referred to in paragraphs 1 and 2. If proportionate, this verification shall be carried out by independent internal or external auditors. ***Measures adhered to by the controller pursuant to Articles 38 and 39 shall be accepted as valid tool to prove compliance with the respective requirements of this Regulation.***

Or. en

Justification

The Regulation should offer clear regulatory incentives to controllers and processors to invest in security and privacy enhancing measures and making use of viable self-regulatory systems and certification schemes via waivers from administrative burdens and simplification mechanisms. Where controllers and processors propose additional safeguards to protect data, which are in line with or go beyond accepted industry standards and who can demonstrate this via conclusive certificates (e.g. via DPO, code of conduct, third party audit), they should benefit from less prescriptive requirements. This would allow for flexibility, legal certainty, less administrative

burden, highest privacy and security standards for data subjects and transparency for regulators.

Amendment 34

Proposal for a regulation

Article 26 – Paragraph 1

Text proposed by the Commission

Amendment

1. Where a processing operation is to be carried out on behalf of a controller, the controller shall choose a processor providing sufficient guarantees to implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject, in particular in respect of the technical security measures and organizational measures governing the processing to be carried out and shall ensure compliance with those measures.

1. Where a processing operation is to be carried out on behalf of a controller **and which involves the processing of data that would permit the processor to reasonably identify the data subject**, the controller shall choose a processor providing sufficient guarantees to implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject, in particular in respect of the technical security measures and organizational measures governing the processing to be carried out and shall ensure compliance with those measures. **The controller remains solely responsible for ensuring compliance with the requirements of this Regulation.**

Or. en

Justification

Where it is technically not feasible for the processor to identify a data subject, e.g. due to the use of proper anonymization techniques, Article 26 shall not apply. The lessening of administrative burdens will incentivize investment in robust anonymisation technology and use of strong system of restricted access, ultimately strengthening data subject protections. The basic principle according to which primary and direct responsibility and liability for processing is incumbent upon the controller should be clearly stated in this Article. There should be no direct obligation and liability for processors beyond the existing status quo.

Amendment 35

Proposal for a regulation

Article 26 – Paragraph 2

Text proposed by the Commission

Amendment

2. The carrying out of processing by a processor shall be governed by a contract or other legal act binding the processor to the controller **and stipulating in particular that the processor shall:**

2. The carrying out of processing by a processor shall be governed by a contract or other legal act binding the processor to the controller. **The controller and processor shall be free to determine respective roles and responsibilities with respect to the requirements of this Regulation, and shall provide for the following:**

Or. en

Justification

Any regulatory allocation of responsibilities between controller and processor needs to take account of the contractual arrangements between the parties, in order to avoid potential contradictions, overlapping responsibilities, duplication of administrative burdens and inefficiencies in enforcement. It is important that the freedom and flexibility for controller-processor arrangements is preserved. Also, processors are often not in a

position to automatically comply with all the requirements as stipulated in Article 26. Processors have limited and distinct obligations that do not simply mirror those of controllers. Independent obligations upon processors will create needless uncertainty in the controller-processor relationship, as processors will need to independently evaluate their obligations vis-à-vis controller instructions. Controller and processor should be free to determine the nature of their relationship to ensure proper levels of protection and best comply with the requirements while at the same time allowing sufficient flexibility for practical business solutions.

Amendment 36

Proposal for a regulation

Article 26 – Paragraph 2 – point a

Text proposed by the Commission

Amendment

(a) act only on instructions from the controller, in particular, where the transfer of the personal data used is prohibited;

(a) **the processor shall** act only on instructions from the controller, in particular, where the transfer of the personal data used is prohibited;

Or. en

Justification

This amendment serves clarification purposes in line with amendments to Article 26.2.

Amendment 37

Proposal for a regulation

Article 26 – Paragraph 2 – point b

Text proposed by the Commission

Amendment

(b) **employ only** staff who have committed themselves to confidentiality **or are under a statutory obligation of confidentiality**;

(b) staff **employed by the processor shall commit** to confidentiality;

Or. en

Justification

This amendment is meant to clarify wording in line with amendments to Article 26.2.

Amendment 38

Proposal for a regulation

Article 26 – Paragraph 2 – point c

Text proposed by the Commission

Amendment

(c) **take all** required measures pursuant to Article 30;

(c) **agreement with respect to the** required measures pursuant to Article 30;

Or. en

Justification

This amendment is meant to clarify wording in line with amendments to Article 26.2.

Amendment 39

Proposal for a regulation

Article 26 – Paragraph 2 – point d

Text proposed by the Commission

Amendment

(d) enlist another processor only with the prior permission of the controller;

deleted

Or. en

Justification

The apportionment of responsibilities between the controller and processor should be left to the parties to agree on and should be appropriately embodied in the contract. The requirement to obtain prior authorization from the controller for the processor to enlist sub-processors imposes burdens with no clear benefit in terms of enhanced data protection. Also, it is not workable particularly in the cloud context and especially if interpreted to require prior authorization to use specific sub-processors. This requirement should be removed.

Amendment 40

Proposal for a regulation

Article 26 – Paragraph 2 – point e

Text proposed by the Commission

Amendment

(e) insofar as this is possible given the nature of the processing, ***create in*** agreement ***with the controller*** the ***necessary*** technical and organizational requirements ***for the fulfilment of*** the controller's ***obligation*** to respond to requests for exercising the data subject's rights laid down in Chapter III;

(e) insofar as this is possible given the nature of the processing ***and the processor's ability to assist with reasonable effort, an*** agreement ***as to the appropriate and relevant*** technical and organizational requirements ***which support the ability of the controller*** to respond to requests for exercising the data subject's rights laid down in Chapter III;

Or. en

Justification

This amendment is consistent with the amendment to Article 26.2. Furthermore, it clarifies the wording to take account of the fact that particularly in the cloud context certain processors are not in a position to assist the controller in complying with information requirements nor to make any determination as to the handling of the personal data.

Amendment 41

Proposal for a regulation

Article 26 – Paragraph 2 – point f

Text proposed by the Commission

Amendment

(f) ***assist the controller in ensuring compliance*** with the obligations pursuant to Articles 30 to 34;

(f) ***insofar as this is possible given the nature of the processing, the information available to the processor and his ability to assist with reasonable effort, an agreement on how compliance will be ensured*** with the obligations pursuant to Articles 28 to 34;

Or. en

Justification

This amendment is consistent with the amendment to Article 26.2 and Article 26.2 point e.

Amendment 42

Proposal for a regulation

Article 26 – Paragraph 2 – point g

Text proposed by the Commission

Amendment

(g) **hand over all results to the controller after the end of the processing and** not process the personal data *otherwise*;

(g) **assurance from the processor that he will** not process the personal data **further after the end of the agreed processing**;

Or. en

Justification

This amendment is consistent with the amendment to Article 26.2. It also takes account of the fact that there may be no results as such to hand over if the data minimisation principle has been effectively applied. Making data available to the supervisory authority should be handled by the controller. Processors typically do not provide due diligence materials to a controller or DPA.

Amendment 43

Proposal for a regulation

Article 26 – Paragraph 2 – point h

Text proposed by the Commission

Amendment

(h) make available to the controller **and the supervisory authority** all information necessary to control compliance with the obligations laid down in this Article.

(h) **agreement that, upon request, the processor will** make available to the controller all **available, relevant and permissible** information necessary to control compliance with the obligations laid down in this Article.

Or. en

Justification

This amendment is consistent with the amendment to Article 26.2 and Article 26.2 point g.

Amendment 44

Proposal for a regulation

Article 26 – Paragraph 3a (new)

Text proposed by the Commission

Amendment

3a. The controller is deemed to have fulfilled the obligations set out in paragraph 1 when employing a processor who has voluntarily self-certified or voluntarily obtained a third party certification, seal or mark showing the implementation of appropriate standard technical and organizational measures in response to the requirements set out in this Regulation.

Or. en

Justification

The Regulation should offer clear regulatory incentives to controllers and processors to invest in security and privacy enhancing measures and making use of viable self-regulatory systems and certification schemes via waivers from administrative burdens and simplification mechanisms. Where controllers and processors propose additional safeguards to protect data, which are in line with or go beyond accepted industry standards and who can demonstrate this via conclusive certificates (e.g. via DPO, code of conduct, third party audit), they should benefit from less prescriptive requirements. This would allow for flexibility, legal certainty, less administrative burden, highest privacy and security standards for data subjects and transparency for regulators.

Amendment 45

Proposal for a regulation

Article 28 – Paragraph 1

Text proposed by the Commission

1. Each controller **and processor** and, if any, the controller's representative, shall maintain documentation of **all** processing operations under its responsibility.

Amendment

1. Each controller and, if any, the controller's representative shall maintain **appropriate** documentation of **the main** processing operations under its responsibility.'

Or. en

Justification

The proposed documentation obligation is disproportionate since it covers virtually every data processing activity. It risks defeating the objective of the draft Regulation to reduce administrative burdens. The changes aim to achieve effective data protection, by requiring organisations to document their main data processing activities. Processors should not be subject to the documentation requirement as they usually do not have access to data or other processing strategies which remain the remit of the controller. This amendment is also consistent with the amendment to Article 26.2.

Amendment 46

Proposal for a regulation

Article 28 – Paragraph 2

Text proposed by the Commission

2. The documentation shall contain **at least** the following information:...

Amendment

2. The documentation shall contain the following information:...

Or. en

Justification

This amendment is consistent with the amendment to Article 28.1.

Amendment 47

Proposal for a regulation

Article 28 – Paragraph 3

Text proposed by the Commission

Amendment

3. The controller **and the processor** and, if any, the controller's representative, shall make the documentation available, on request, to the supervisory authority.

3. The controller and, if any, the controller's representative, shall make the documentation available, on request, to the supervisory authority.

Or. en

Justification

This amendment is consistent with the amendment to Article 26.2, Article 26.2 point g and h, and Article 28.1.

Amendment 48

Proposal for a regulation

Article 28 – Paragraph 4

Text proposed by the Commission

Amendment

4. The obligations referred to in paragraphs 1 and 2 shall not apply to the following controllers **and processors**:

4. The obligations referred to in paragraphs 1 and 2 shall not apply to the following controllers:

Or. en

Justification

This amendment is consistent with the amendment to Article 26.2.

Amendment 49

Proposal for a regulation

Article 33 – Paragraph 1

Text proposed by the Commission

Amendment

1. Where processing operations present **specific** risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller **or the processor acting on the controller's behalf** shall carry out an assessment of the impact of the envisaged processing operations on the **protection of personal data**.

1. Where processing operations **are likely to** present **significant** risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller shall carry out an assessment of the impact of the envisaged processing operations on the **fundamental rights and freedoms of the data subjects**.

Or. en

Justification

This amendment is consistent with the amendment to 26.2. Furthermore, it proposes to limit the requirement for impact assessments to situations involving significant risks for data subjects, in order to funnel the priority towards assuring effective privacy protection rather than fulfilling burdensome administrative requirements. This is in line with the ethos of the data protection reform, which was intended to instil a culture of accountability backed by ex-post oversight rather than perpetuate ex-ante 'box-ticking'.

Amendment 50

Proposal for a regulation

Article 33 – Paragraph 2

Text proposed by the Commission

Amendment

2. The following processing operations in particular present *specific* risks referred to in paragraph 1:

2. The following processing operations in particular *are likely to* present *such significant* risks *as* referred to in paragraph 1:

Or. en

Justification

This amendment is consistent with the amendment to Article 33.1.

Amendment 51

Proposal for a regulation

Article 33 – Paragraph 4

Text proposed by the Commission

Amendment

4. The controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations. ~~deleted~~

Or. en

Justification

Considering the data subject's need to be informed of the data processing in accordance with Article 14, an obligation to consult data subjects as part of the data impact assessment appears misplaced and unnecessary. It could also likely result in compromising important trade secrets.

Amendment 52

Proposal for a regulation

Article 34 – Paragraph 1

Text proposed by the Commission

Amendment

1. The controller **or the processor as the case may be** shall obtain an authorisation from the supervisory authority prior to the processing of personal data, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where a controller or processor adopts contractual clauses as provided for in point (d) of Article 42(2) or does not provide for the appropriate safeguards in a legally binding instrument as referred to in Article 42(5) for the transfer of personal data to a third country or an international organisation.

1. The controller shall obtain an authorisation from the supervisory authority prior to the processing of personal data, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where a controller or processor adopts contractual clauses as provided for in point (d) of Article 42(2) or does not provide for the appropriate safeguards in a legally binding instrument as referred to in Article 42(5) for the transfer of personal data to a third country or an international organisation.

Or. en

Justification

This amendment is consistent with the amendment to Article 26.1 and Article 26.2.

Amendment 53

Proposal for a regulation

Article 34 – Paragraph 2

Text proposed by the Commission

Amendment

2. The controller *or processor acting on the controller's behalf* shall consult the supervisory authority prior to the processing of personal data in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where:

2. The controller shall consult the supervisory authority prior to the processing of personal data in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where:

Or. en

Justification

This amendment is consistent with the amendment to Article 26.1 and Article 26.2.

Amendment 54

Proposal for a regulation

Article 34 – Paragraph 2 – point a

Text proposed by the Commission

Amendment

(a) a data protection impact assessment as provided for in Article 33 indicates that processing operations are by virtue of their nature, their scope or their purposes, likely to present a high degree of *specific* risks; or

(a) a data protection impact assessment as provided for in Article 33 indicates that processing operations are by virtue of their nature, their scope or their purposes, likely to present a high degree of *significant* risks; or

Or. en

Justification

This amendment is consistent with the amendment to Recital 70 and Article 33.1.

Amendment 55

Proposal for a regulation

Article 34 – Paragraph 6

Text proposed by the Commission

Amendment

6. The controller *or processor* shall provide the supervisory authority with the data protection impact assessment provided for in Article 33 and, on request, with any other information to allow the supervisory authority to make an assessment of the compliance of the processing and in particular of the risks for the protection of personal data of the data subject and of the related safeguards.

6. The controller shall provide the supervisory authority with the data protection impact assessment provided for in Article 33 and, on request, with any other information to allow the supervisory authority to make an assessment of the compliance of the processing and in particular of the risks for the protection of personal data of the data subject and of the related safeguards.

Or. en

Justification

This amendment is consistent with the amendment to Article 26.1 and Article 26.2.

Amendment 56

Proposal for a regulation

Article 35 – Paragraph 1

Text proposed by the Commission

Amendment

1. The controller **and** the processor shall designate a data protection officer in any case where:

1. The controller **or** the processor shall designate a data protection officer in any case where:

Or. en

Justification

Only one DPO should be required for all subsidiaries of a group established in the Union, regardless of size and activity, instead of a separate DPO for every Member State in which that entity operates. This allows for consistency and ease of communication for data subjects and supervisory authorities.

Amendment 57

Proposal for a regulation

Article 35 – paragraph 2

Text proposed by the Commission

Amendment

2. In the case referred to in point (b) of paragraph 1, a group of undertakings may appoint a single data protection officer.

2. In the case referred to in point (b) **and (c)** of paragraph 1, a group of undertakings may appoint a single data protection officer.

Or. en

Justification

Only one DPO should be required for all subsidiaries of a group established in the Union, regardless of size and activity, instead of a separate DPO for every Member State in which that entity operates. This allows for consistency and ease of communication for data subjects and supervisory authorities.

Amendment 58

Proposal for a regulation

Article 38 – paragraph 1

Text proposed by the Commission

Amendment

1. The Member States, the supervisory authorities and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various data processing sectors, in particular in relation to:

1. The Member States, the supervisory authorities and the Commission shall encourage the drawing up of **voluntary** codes of conduct **and self-regulatory schemes** intended to contribute to the proper application of this Regulation, taking account of the specific features of the various data processing sectors, in particular in relation to:

Or. en

Justification

This amendment aims to clarify the voluntary nature of self-regulation and to extend the scope of the Article to other self-regulatory mechanisms that have the same function and are hence as viable as codes of conducts.

Amendment 59

Proposal for a regulation

Article 38 – paragraph 2

Text proposed by the Commission

2. Associations and other bodies representing categories of controllers or processors in one Member State which intend to draw up codes of conduct or to amend or extend existing codes of conduct may submit them to an opinion of the supervisory authority in that Member State. The supervisory authority *may* give an opinion whether the draft **code of conduct** or the amendment is in compliance with this Regulation. The supervisory authority shall seek the views of data subjects or their representatives on these drafts.

Amendment

2. Associations and other bodies representing categories of controllers or processors in one Member State which intend to draw up codes of conduct, **self-regulatory schemes or self-certification mechanisms**, or to amend or extend existing codes of conduct, **self-regulatory schemes or self-certification mechanisms**, may submit them to an opinion of the supervisory authority in that Member State. The supervisory authority **shall** give a **binding** opinion whether the draft or the amendment **of such measure** is in compliance with this Regulation. The supervisory authority shall seek the views of data subjects or their representatives on these drafts.

Or. en

Justification

This amendment aims to extend the scope of the Article to other self-regulatory and self-certification mechanisms that have the same function and are hence as viable as codes of conducts.

Amendment 60

Proposal for a regulation

Article 38 – paragraph 3

Text proposed by the Commission

3. Associations and other bodies representing categories of controllers in several Member States may submit draft codes of conduct and amendments or extensions to existing **codes of conduct** to the Commission.

Amendment

3. Associations and other bodies representing categories of controllers **or processors** in several Member States may submit draft codes of conduct, **self-regulatory schemes or self-certification mechanisms**, and amendments or extensions to **such** existing **measures** to the Commission.

Or. en

Justification

This amendment is in line with the amendment proposed to Article 38.1 and 38.2. It also aims to clarify that the Article applies to processors, the omission of which seems to be a drafting error, as processors are included in Article 38.2.

Amendment 61

Proposal for a regulation

Article 39 – paragraph 1

Text proposed by the Commission

1. The Member States and the Commission shall encourage, in particular at European level, the establishment of data protection certification mechanisms and of data protection seals and marks, allowing data subjects to quickly assess the level of

Amendment

1. The Member States and the Commission shall encourage, in particular at European level, the establishment of data protection certification mechanisms, **including self-certification mechanisms**, and of data protection seals and marks, allowing data

data protection provided by controllers and processors. The data protection certifications mechanisms shall contribute to the proper application of this Regulation, taking account of the specific features of the various sectors and different processing operations.

subjects to quickly assess the level of data protection provided by controllers and processors. The data protection certifications mechanisms shall contribute to the proper application of this Regulation, taking account of the specific features of the various sectors and different processing operations. ***They shall be elaborated based on industry-led efforts and in consultation with the supervisory authorities, and shall be capable of global application, affordable and technology neutral.***

Or. en

Justification

This amendment aims to clarify that certification mechanisms and data protection seals and marks should be voluntary, industry-driven, enable competition and allow for innovative solutions for consumers. Given the global nature of the internet and increasing internationalisation of data flows, such certification mechanisms should be open to companies both inside and outside the EEA and be elaborated in consultation with relevant stakeholders. Certification mechanisms can help to reduce compliance burdens and foster competitiveness.

Amendment 62

Proposal for a regulation

Article 51 – paragraph 2

Text proposed by the Commission

2. Where ***the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union, and*** the controller or processor is established in more than one Member State, the supervisory authority of the main establishment of the controller or processor shall be competent for the supervision of ***the*** processing activities of ***the*** controller or the processor in all Member States, ***without prejudice to*** the provisions of Chapter VII of this Regulation.

Amendment

2. ***In situations referred to in Article 3(1) and*** where the controller or processor is established in more than one Member State, the supervisory authority of the main establishment of the controller or processor shall be ***solely*** competent for the supervision of ***all*** processing activities ***that are carried out by or on behalf of that*** controller or processor in all Member States, ***or in the case of a group of undertakings, by any member of the group, as far as they are subject to this Regulation. The competent supervisory authority of the main establishment shall cooperate with other supervisory authorities in accordance with*** the provisions of Chapter VII of this Regulation.

Or. en

Justification

This amendment is consistent with the amendment to Article 4(13). It is intended to further strengthen the so-called one-stop shop concept, according to which the DPA of a company's main establishment is to be the lead for investigative actions and interpreting rules. Other DPAs should serve as liaison point when needed. This language will help to provide consumers and multinational companies with legal certainty as to which competent supervisory authority will have authority to supervise any data processing activities subject to the Regulation. It will also prevent multiple supervisory authorities from sanctioning the same company for the same incident.

Amendment 63

Proposal for a regulation

Article 51 – paragraph 2a (new)

Text proposed by the Commission

Amendment

2a. In situations referred to in Article 3(2) and where the controller has designated a representative in the Union pursuant to Article 25, the supervisory authority of the establishment of the representative shall be solely competent for the supervision, in all Member States, of all processing activities that are carried out by or on behalf of that controller.

Or. en

Justification

This amendment is consistent with the amendment to recital 63. It intends to ensure respect of the EU principle of non-discrimination by affording the benefit of the one stop shop principle also to non-EU controllers who appoint an EU representative. They should benefit from one of the main anchors of the draft Regulation in the same way as EU established companies, given that they are subject to the same rights and obligations of the draft Regulation.

Amendment 64

Proposal for a regulation

Article 52 – paragraph 1

Text proposed by the Commission

Amendment

1. The supervisory authority shall:

1. The **competent** supervisory authority **pursuant to Article 51** shall:

Or. en

Justification

This amendment is consistent with the amendment to Article 51.2.

Amendment 65

Proposal for a regulation

Article 52 – paragraph 3

Text proposed by the Commission

Amendment

3. The supervisory authority shall, upon request, advise any data subject in exercising the rights under this Regulation and, if appropriate, co-operate with the supervisory authorities in other Member States to this end.

3. The **competent** supervisory authority **pursuant to Article 51** shall, upon request, advise any data subject in exercising the rights under this Regulation and, if appropriate, co-operate with the supervisory authorities in other Member States to this end.

Or. en

Justification

This amendment is consistent with the amendment to Article 51.2.

Amendment 66

Proposal for a regulation

Article 53 – paragraph 1

Text proposed by the Commission

Amendment

1. Each supervisory authority shall have the power:

1. **The competent** supervisory authority **pursuant to Article 51** shall have the power:

Or. en

Justification

This amendment is consistent with the amendment to Article 51.2.

Amendment 67

Proposal for a regulation

Article 53 – paragraph 1 – point b

Text proposed by the Commission

Amendment

(b) to order the controller **or the processor** to comply with the data subject's requests to exercise the rights provided by this Regulation;

(b) to order the controller to comply with the data subject's requests to exercise the rights provided by this Regulation;

Or. en

Justification

This amendment is consistent with the amendment to Article 26.1 and 26.2.

Amendment 68

Proposal for a regulation

Article 53 – paragraph 1 – point c

Text proposed by the Commission

Amendment

(c) to order the controller **and the processor**, and, where applicable, the representative to provide any information relevant for the performance of its duties;

(c) to order the controller, and, where applicable, the representative to provide any information relevant for the performance of its duties;

Or. en

Justification

This amendment is consistent with the amendment to Article 26.1 and 26.2.

Amendment 69

Proposal for a regulation

Article 53 – paragraph 1 – point e

Text proposed by the Commission

Amendment

(e) to warn or admonish the controller **or the processor**;

(e) to warn or admonish the controller;

Or. en

Justification

This amendment is consistent with the amendment to Article 26.1 and 26.2.

Amendment 70

Proposal for a regulation

Article 53 – paragraph 2

Text proposed by the Commission

Amendment

2. **Each** supervisory authority shall have the investigative power to obtain from the controller **or the processor**:

2. **The competent** supervisory authority **pursuant to Article 51** shall have the investigative power to obtain from the controller:

Or. en

Justification

This amendment is consistent with the amendments to Article 26.1, 26.2 and 51.2.

Amendment 71

Proposal for a regulation

Article 53 – paragraph 3

Text proposed by the Commission

Amendment

3. **Each** supervisory authority shall have the power to bring violations of this Regulation to the attention of the judicial authorities and to engage in legal proceedings, in particular pursuant to Article 74(4) and Article 75(2).

3. **The competent** supervisory authority **pursuant to Article 51** shall have the power to bring violations of this Regulation to the attention of the judicial authorities and to engage in legal proceedings, in particular pursuant to Article 74(4) and Article 75(2).

Or. en

Justification

This amendment is consistent with the amendments to Article 51.2.

Amendment 72

Proposal for a regulation

Article 53 – paragraph 4

Text proposed by the Commission

Amendment

4. **Each** supervisory authority shall have the power to sanction administrative offences, in particular those referred to in Article 79(4), (5) and (6).

4. **The competent** supervisory authority **pursuant to Article 51** shall have the power to sanction administrative offences, in particular those referred to in Article 79(4), (5) and (6).

Or. en

Justification

This amendment is consistent with the amendments to Article 51.2.

Amendment 73

Proposal for a regulation

Article 53 – paragraph 4a (new)

Text proposed by the Commission

Amendment

4a. The competent supervisory authority pursuant to Article 51 shall serve as the primary contact and reference point for any action to be implemented in accordance with Chapter VII of this Regulation. Other supervisory authorities shall refer any matter concerning a controller under the jurisdiction of the competent supervisory authority to that authority.

Or. en

Justification

This amendment is consistent with the amendments to Article 51.2.

Amendment 74

Proposal for a regulation

Article 55 – paragraph 8

Text proposed by the Commission

Amendment

8. Where a supervisory authority does not act within one month on request of another supervisory authority, the requesting supervisory authorities **shall be competent to take a provisional measure on the territory of its Member State in accordance with Article 51(1) and** shall submit the matter to the European Data Protection Board in accordance with the procedure referred to in Article 57.

8. Where a supervisory authority does not act within one month on request of another supervisory authority, the requesting supervisory authorities shall submit the matter to the European Data Protection Board in accordance with the procedure referred to in Article 57.

Or. en

Justification

This amendment is consistent with the amendments to Article 51.2. The draft Regulation should reflect the practical viability and resources affecting mutual assistance duties between supervisory authorities.

Amendment 75

Proposal for a regulation

Article 55 – paragraph 9

Text proposed by the Commission

Amendment

9. The supervisory authority shall specify the period of validity of such provisional measure. This period shall not exceed three months. The supervisory authority shall, without delay, communicate those measures, with full reasons, to the European Data Protection Board and to the Commission. ~~deleted~~

Or. en

Justification

This amendment is consistent with the amendments to Article 51.2. The draft Regulation should reflect the practical viability and resources affecting mutual assistance duties between supervisory authorities.

Amendment 76

Proposal for a regulation

Article 58 – paragraph 1

Text proposed by the Commission

1. Before **a** supervisory authority adopts a measure referred to in paragraph 2, this supervisory authority shall communicate the draft measure to the European Data Protection Board and the Commission.

Amendment

1. Before **the competent** supervisory authority adopts a measure referred to in paragraph 2, this supervisory authority shall communicate the draft measure to the European Data Protection Board and the Commission.

Or. en

Justification

This amendment is consistent with the amendments to Article 51.2.

Amendment 77

Proposal for a regulation

Article 58 – paragraph 2 – point a

Text proposed by the Commission

(a) relates to processing activities which are related to the offering of goods or services **to** data subjects in several Member States, or to the monitoring of their behaviour; or

Amendment

(a) relates to processing activities which are related to the offering of goods or services **specifically targeted at** data subjects in several Member States, or to the monitoring of their behavior, **and where the controller not established in the Union has not appointed a representative in the territory of the Union**; or

Or. en

Justification

The first part of this amendment is consistent with the amendment to Article 3.2. The second part of this amendment aims to limit the scope of applicability of the consistency mechanism to those cases where consistency of data protection enforcement is truly at stake. It would seem unjustified to automatically apply the consistency mechanism to non-EU established companies that are subject to the Regulation in all circumstances, particularly where these have appointed a representative in the EU. The competence of the data protection board over non- EU established companies that are subject to the Regulation should be equivalent to that over EU companies.

Amendment 78

Proposal for a regulation

Article 58 – paragraph 2 – point c

Text proposed by the Commission

(c) aims at adopting a list of the processing operations subject to prior consultation pursuant to Article 34(5); **deleted**
or

Amendment

Or. en

Justification

This amendment is consistent with the amendment to Article 58.2(a). The consistency mechanism should remain an exceptional mechanism and not a body of appeal of legitimate decisions of the competent Data Protection

Authority. Otherwise there is the risk that the consistency mechanism becomes an appeal mechanism that slows down decision taking and becomes a bureaucratic step to the detriment of all actors.

Amendment 79

Proposal for a regulation

Article 58 – paragraph 3

Text proposed by the Commission

Amendment

3. Any supervisory authority or the European Data Protection Board may request that any matter shall be dealt with in the consistency mechanism, in particular where **a** supervisory authority does not submit a draft measure referred to in paragraph 2 or does not comply with the obligations for mutual assistance in accordance with Article 55 or for joint operations in accordance with Article 56.

3. Any supervisory authority or the European Data Protection Board may request that any matter shall be dealt with in the consistency mechanism, in particular where **the competent** supervisory authority does not submit a draft measure referred to in paragraph 2 or does not comply with the obligations for mutual assistance in accordance with Article 55 or for joint operations in accordance with Article 56.

Or. en

Justification

This amendment is consistent with the amendments to Article 51.2.

Amendment 80

Proposal for a regulation

Article 58 – paragraph 4

Text proposed by the Commission

Amendment

4. In order to ensure correct and consistent application of this Regulation, the Commission may request that any matter shall be dealt with in the consistency mechanism.

4. In order to ensure correct and consistent application of this Regulation, the Commission may request that any matter **related to the category of measures referred to in paragraph 2** shall be dealt with in the consistency mechanism.

Or. en

Justification

This amendment is consistent with the amendments to Article 51.2 point c.

Amendment 81

Proposal for a regulation

Article 58 – paragraph 7

Text proposed by the Commission

Amendment

7. The European Data Protection Board shall issue an opinion on the matter, if the European Data Protection Board so decides by **simple** majority of its members or any supervisory authority or the Commission so requests within one week after the relevant information has been provided according to paragraph 5. The

7. The European Data Protection Board shall issue an opinion on the matter, if the European Data Protection Board so decides by **qualified** majority of its members or any supervisory authority or the Commission so requests within one week after the relevant information has been provided according to paragraph 5. The

opinion shall be adopted within one month by *simple* majority of the members of the European Data Protection Board. The chair of the European Data Protection Board shall inform, without undue delay, the supervisory authority referred to, as the case may be, in paragraphs 1 and 3, the Commission *and* the supervisory authority competent under Article 51 of the opinion and make it public.

opinion shall be adopted within one month by *qualified* majority of the members of the European Data Protection Board. The chair of the European Data Protection Board shall inform, without undue delay, the supervisory authority referred to, as the case may be, in paragraphs 1 and 3, the Commission, the *competent* supervisory *and the controller or processor* of the opinion and make it public.

Or. en

Justification

This amendment is consistent with the amendments to Recital 106 and Article 51.2. The controller or processor should be informed about any opinion of the European Data Protection Board as far as they are concerned by the content of such opinion.

Amendment 82

Proposal for a regulation

Article 58 – paragraph 7

Text proposed by the Commission

8. The *supervisory* authority referred to in paragraph 1 *and the supervisory authority competent under Article 51* shall take account of the opinion of the European Data Protection Board and shall within two weeks after the information on the opinion by the chair of the European Data Protection Board, electronically communicate to the chair of the European Data Protection Board and to the Commission whether it maintains or amends its draft measure and, if any, the amended draft measure, using a standardised format.

Amendment

8. The *competent* supervisory authority referred to in paragraph 1 shall take account of the opinion of the European Data Protection Board and shall within two weeks after the information on the opinion by the chair of the European Data Protection Board, electronically communicate to the chair of the European Data Protection Board and to the Commission whether it maintains or amends its draft measure and, if any, the amended draft measure, using a standardised format.

Or. en

Justification

This amendment is consistent with the amendments to Article 51.2.

Amendment 83

Proposal for a regulation

Article 59 – paragraph 2

Text proposed by the Commission

2. Where the Commission has adopted an opinion in accordance with paragraph 1, the supervisory authority concerned shall take utmost account of the Commission's opinion and inform the Commission and the European Data Protection Board whether it intends to maintain or amend its draft measure.

Amendment

2. Where the Commission has adopted an opinion in accordance with paragraph 1, the *competent* supervisory authority concerned shall take utmost account of the Commission's opinion and inform the Commission and the European Data Protection Board whether it intends to maintain or amend its draft measure.

Or. en

Justification

This amendment is consistent with the amendments to Article 51.2.

Amendment 84

Proposal for a regulation

Article 59 – paragraph 4

Text proposed by the Commission

4. Where the **supervisory** authority concerned intends not to follow the opinion of the Commission, it shall inform the Commission **and** the European Data Protection Board thereof within the period referred to in paragraph 1 and provide a justification. In this case the draft measure shall not be adopted for one further month.

Amendment

4. Where the **competent** supervisory authority concerned intends not to follow the opinion of the Commission, it shall inform the Commission, the European Data Protection Board **and the controller or processor** thereof within the period referred to in paragraph 1 and provide a justification. In this case the draft measure shall not be adopted for one further month.

Or. en

Justification

The first part of the amendment is consistent with the amendment to Article 51.2. The controller or processor should be informed about any decision of the competent supervisory authority as far as they are directly or indirectly, effectively or potentially concerned by the content of such decision.

Amendment 85

Proposal for a regulation

Article 61 – paragraph 1

Text proposed by the Commission

1. In exceptional circumstances, where **a** supervisory authority considers that there is an urgent need to act in order to protect the interests of data subjects, in particular when the danger exists that the enforcement of a right of a data subject could be considerably impeded by means of an alteration of the existing state or for averting major disadvantages or for other reasons, by way of derogation from the procedure referred to in Article 58, it may immediately adopt provisional measures with a specified period of validity. The **supervisory** authority shall, without delay, communicate those measures, with full reasons, to the European Data Protection Board **and to** the Commission.

Amendment

1. In exceptional circumstances, where **the competent** supervisory authority considers that there is an urgent need to act in order to protect the interests of data subjects, in particular when the danger exists that the enforcement of a right of a data subject could be considerably impeded by means of an alteration of the existing state or for averting major disadvantages or for other reasons, by way of derogation from the procedure referred to in Article 58, it may immediately adopt provisional measures with a specified period of validity. The **competent** supervisory authority shall, without delay, communicate those measures, with full reasons, to the European Data Protection Board, the Commission **and the controller or processor**.

Or. en

Justification

The first part of the amendment is consistent with the amendment to Article 51.2. The controller or processor should be informed about any decision of the competent supervisory authority as far as they are directly or indirectly, effectively or potentially concerned by the content of such decision or any measure the competent authority intends to take.

Amendment 86

Proposal for a regulation

Article 61 – paragraph 2

Text proposed by the Commission

Amendment

2. Where **a** supervisory authority has taken a measure pursuant to paragraph 1 and considers that final measures need urgently be adopted, it may request an urgent opinion of the European Data Protection Board, giving reasons for requesting such opinion, including for the urgency of final measures.

2. Where **the competent** supervisory authority has taken a measure pursuant to paragraph 1 and considers that final measures need urgently be adopted, it may request an urgent opinion of the European Data Protection Board, giving reasons for requesting such opinion, including for the urgency of final measures.

Or. en

Justification

This amendment is consistent with the amendment to Article 51.2.

Amendment 87

Proposal for a regulation

Article 63 – paragraph 1

Text proposed by the Commission

Amendment

1. For the purposes of this Regulation, an enforceable measure of the supervisory authority of one Member State shall be enforced in all Member States concerned.

1. For the purposes of this Regulation, an enforceable measure of the **competent** supervisory authority of one Member State shall be enforced in all Member States concerned.

Or. en

Justification

This amendment is consistent with the amendment to Article 51.2.

Amendment 88

Proposal for a regulation

Article 63 – paragraph 2

Text proposed by the Commission

Amendment

2. Where **a** supervisory authority does not submit a draft measure to the consistency mechanism in breach of Article 58(1) to (5), the measure of the supervisory authority shall not be legally valid and enforceable.

2. Where **the competent** supervisory authority does not submit a draft measure to the consistency mechanism in breach of Article 58(1) to (5), the measure of the supervisory authority shall not be legally valid and enforceable.

Or. en

Justification

This amendment is consistent with the amendment to Article 51.2.

Amendment 89

Proposal for a regulation

Article 66 – paragraph 1

Text proposed by the Commission

Amendment

1. The European Data Protection Board shall ensure the consistent application of this Regulation. To this effect, the European Data Protection Board shall, on its own initiative **or** at the request of the Commission, in particular:

1. The European Data Protection Board shall ensure the consistent application of this Regulation. To this effect, the European Data Protection Board shall, on its own initiative, at the request of the Commission **or other interested parties**, in particular:

Or. en

Justification

Interested parties should have the possibility to access the European Data Protection Board and submit to it data protection related matters of concern in terms of consistent EU-wide application.

Amendment 90

Proposal for a regulation

Article 66 – paragraph 1 – point b

Text proposed by the Commission

Amendment

(b) examine, on its own initiative or on request of one of its members or on request of the Commission, any question covering the application of this Regulation and issue guidelines, recommendations and best practices addressed to the supervisory authorities in order to encourage consistent application of this Regulation;

(b) examine, on its own initiative or on request of one of its members or on request of the Commission **or other interested parties**, any question covering the application of this Regulation and issue guidelines, recommendations and best practices addressed to the supervisory authorities in order to encourage consistent application of this Regulation;

Or. en

Justification

This amendment is in line with amendment to Article 66.1.

Amendment 91

Proposal for a regulation

Article 66 – paragraph 4 (new)

Text proposed by the Commission

Amendment

4a. Where appropriate, the European Data Protection Board shall, in its execution of the tasks as outlined in this Article, consult interested parties and give them the opportunity to comment within a reasonable period. The European Data Protection Board shall, without prejudice to Article 72, make the results of the consultation procedure publicly available.

Or. en

Justification

This amendment intends to provide interested parties the opportunity to be consulted and provide comments within a reasonable timeframe before the European Data Protection Board adopts opinions or reports. The possibility for industry to be consulted also exists in other regulatory domains (e.g. the European Regulators Group BEREC in the context of the EU's telecoms regulatory framework).

Amendment 92

Proposal for a regulation

Article 77 – paragraph 1

Text proposed by the Commission

Amendment

1. Any person who has suffered damage as a result of an unlawful processing operation or of an action incompatible with this Regulation shall have the right to receive compensation from the controller **or the processor** for the damage suffered.

1. Any person who has suffered damage as a result of an unlawful processing operation or of an action incompatible with this Regulation shall have the right to receive compensation from the controller for the damage suffered.

Or. en

Justification

This amendment is consistent with the amendments to Article 26.

Amendment 93

Proposal for a regulation

Article 77 – paragraph 2

Text proposed by the Commission

Amendment

2. Where more than one controller **or processor** is involved in the processing, each controller **or processor** shall be jointly and severally liable for the entire amount of the damage.

2. Where more than one controller is involved in the processing, each controller shall be jointly and severally liable for the entire amount of the damage, **to the extent that liability has not already been established in the determination of responsibilities envisaged in Article 24.**

Or. en

Justification

This amendment is consistent with the amendments to Article 26.

Amendment 94

Proposal for a regulation

Article 77 – paragraph 3

Text proposed by the Commission

Amendment

3. The controller **or the processor** may be exempted from **this** liability, in whole or in part, if the controller **or the processor** proves that **they are** not responsible for the event giving rise to the damage.

3. The controller may be exempted from liability **under paragraph 2**, in whole or in part, if the **respective** controller proves that **it is** not responsible for the event giving rise to the damage.

Justification

This amendment is consistent with the amendments to Article 26.

Amendment 95

Proposal for a regulation

Article 77 – paragraph 3a (new)

Text proposed by the Commission

Amendment

3a. If a processor processes personal data other than as instructed by the controller, he may be held liable should any person suffer damage as a result of such processing.

Justification

This amendment is consistent with the amendments to Article 26.

General Data Protection Regulation

BT's amendments to the proposed Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) - COM (2012) 11/4

November 2012

Overview

BT suggests amendments to cover eight key areas:

1. The need for a general proportionality principle
2. The need for clarity on key concepts, rights and definitions, in particular the definitions of 'personal data', 'data subject', 'consent'
3. Burgeoning operational costs resulting from Article 5(f)
4. Privacy by design and privacy by default
5. Electronic data subject access requests
6. Transfers of personal data to third countries
7. The impact of the right of data portability
8. The impact of the right to be forgotten

BT's proposed changes are marked in ***bold italics***.

1. General proportionality principle

EC Proposal	Proposed BT's amendments
<p>Article 22 Responsibility of the controller</p> <p>1. The controller shall adopt policies and implement appropriate measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation.</p> <p>2. The measures provided for in paragraph 1 shall in particular include:</p> <p>(a) keeping the documentation pursuant to Article 28;</p> <p>(b) implementing the data security requirements laid down in Article 30;</p> <p>(c) performing a data protection impact assessment pursuant to Article 33;</p> <p>(d) complying with the requirements for prior authorisation or prior consultation of the supervisory authority pursuant to Article 34(1) and (2); [...]</p> <p>3. The controller shall implement mechanisms to ensure the verification of the effectiveness of the measures referred to in paragraphs 1 and 2. If proportionate, this verification shall be carried out by independent internal or external auditors.</p> <p>4. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures referred to in paragraph 1 other than those already referred to in paragraph 2, the conditions for the verification and auditing mechanisms referred to in paragraph 3 and as regards the criteria for proportionality under paragraph 3, and considering specific measures for micro, small and medium-sized-enterprises.</p>	<p>Article 22 Responsibility of the controller</p> <p>1. (a) The controller shall adopt policies and implement appropriate measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation.</p> <p>(b) <i>The policies to be adopted and measures to be implemented by the controller in accordance with sub-paragraph (a) above shall be proportionate to the risks of the processing to the rights of the data subject and to the burdens on and infringement of the rights of the data controller.</i></p> <p>2. The measures provided for in paragraph 1 shall in particular include:</p> <p>(a) keeping the documentation pursuant to Article 28;</p> <p>(b) implementing the data security requirements laid down in Article 30;</p> <p>(c) performing a data protection impact assessment pursuant to Article 33;</p> <p>(d) complying with the requirements for prior authorisation or prior consultation of the supervisory authority pursuant to Article 34(1) and (2); [...]</p> <p>3. The controller shall implement mechanisms to ensure the verification of the effectiveness of the measures referred to in paragraphs 1 and 2. <i>[deleted]</i></p>

Justification

The Regulation is intended to protect the fundamental rights of individuals particularly their right to the protection of personal data. A broad and inclusive definition of personal data has consequently been adopted. The scope of the Regulation, therefore, extends from the processing in commonly accepted ways of data of little significance to the processing of highly sensitive information in perhaps surprising ways. The Regulation should recognise this breadth of application and also the need to reconcile the rights protected by the Regulation with other fundamental rights assured by the Treaty on the Functioning of the European Union. Accordingly, the application of the principles and procedures of the Regulation and the duties of data controllers should be expressly adjusted to this range of sensitivity by a clear proportionality principle. It would also be excessive to require mandatory verification by an auditor of the measures taken by a data controller in all circumstances, even where that requirement is expressed to be 'if proportionate'. It is sufficient for the controller to implement verification mechanisms and the choice of mechanism should be left to the controller's discretion.

We have also removed the reference to mandatory data protection officers from Article 22 given the concept of the main establishment of the data controller has not yet been clarified, and the extent of the obligation not yet certain,

2. Definitions of data subject, personal data and data subject's consent

EC Proposal	Proposed BT's amendments
<p>Article 4 Definitions</p> <p>(1) 'data subject' means an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;</p> <p>(2) 'personal data' means any information relating to a data subject;</p> <p>[...]</p> <p>(8) 'the data subject's consent' means any freely given specific, informed and explicit indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed;</p>	<p>[In Article 4 for paragraphs (1) and (2), substitute the following:]</p> <p><i>(1)'personal data' shall mean any information relating to an identified or identifiable living natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, by the data controller in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;</i></p> <p>[And renumber the subsequent paragraphs include:]</p> <p><i>(7) 'the data subject's consent' means any freely given specific, and informed [delete] indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed and which indication is capable of being demonstrated by the data controller,</i></p>

Justification

The existing definition of 'personal data' is proposed on the basis that it must be clear it should only include within its scope that which relates to a living individual. It should not be so widely cast so as to include any information relating to a data subject as to do so would include within the scope of the definition data which is of so little significance it is of no use to anyone including the data subject. This is particularly of concern in relation to the online world. Data controllers must have certainty around this definition and where to draw the line between that which is relevant to a data subject and that which is not, in terms of building systems to comply with the Regulation and operation of its obligations in respect thereof.

Whilst consent is an important element of data protection particularly in relation to the processing of sensitive data, the Regulation is too prescriptive about the form of consent. To require 'explicit' consent in all data processing circumstances is excessive, and removes the opportunity for consent to be implied by a course of conduct as a lawful option. 'Implied' consent is a necessary and accepted concept and essential to verify and complete a number of customer transactions. The word 'explicit' has therefore been removed. The essential elements are that the data subject has knowingly agreed to the processing of data and for procedural purposes that agreement can later be demonstrated. The proposed amendment seeks to implement those essentials.

3. Principles relating to personal data processing

EC Proposal	Proposed BT's amendments
<p>Article 5 Principles relating to personal data processing</p> <p>Personal data must be:</p> <p>(a) processed lawfully, fairly and in a transparent manner in relation to the data subject;</p> <p>(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;</p> <p>(c) adequate, relevant, and limited to the minimum necessary in relation to the purposes for which they are processed; they shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data;</p> <p>(d) accurate and kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;</p> <p>(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the data will be processed solely for historical, statistical or scientific research purposes in accordance with the rules and conditions of Article 83 and if a periodic review is carried out to assess the necessity to continue the storage;</p> <p>(f) processed under the responsibility and liability of the controller, who shall ensure and demonstrate for each processing operation the compliance with the provisions of this Regulation.</p>	<p>Article 5 Principles relating to personal data processing</p> <p>Personal data must be:</p> <p>(a) processed lawfully, fairly and in a transparent manner in relation to the data subject;</p> <p>(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;</p> <p>(c) adequate, relevant, and limited to the minimum necessary in relation to the purposes for which they are processed; they shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data;</p> <p>(d) accurate and kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;</p> <p>(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the data will be processed solely for historical, statistical or scientific research purposes in accordance with the rules and conditions of Article 83 and if a periodic review is carried out to assess the necessity to continue the storage;</p> <p>(f) processed under the responsibility and liability of the controller, who shall ensure and <i>if required to do so demonstrate compliance of the controller's processing with the provisions of this Regulation to the supervisory authority having competence under paragraph 2 of Article 51.</i></p>

Justification

Article 5(f) runs the risk of imposing on data controllers unnecessarily burdensome logging and auditing requirements for *each* processing of personal data, which would provide no proportionate benefit to individuals by securing their rights.

'Each processing operation' is an ambiguous expression. The potential size of data storage requirements, which are needed to demonstrate compliance as required by this proposed Regulation, would directly contradict those requirements in the proposed text, which relate to data minimisation.

Article 5f contains no time limit in terms of data retention for the ability to demonstrate compliance for each processing operation, which would inevitably add to the cost and uncertainty of the proposal. We have therefore suggest a general duty to ensure compliance and to demonstrate it to the supervisory authority on an inspection would be a) more acceptable and b) more efficient for data controllers to implement without prejudicing the rights of data subjects.

4. Privacy by Design and by Default

EC Proposal	Proposed BT's amendments
<p>Article 23 Data protection by design and by default</p> <p>1. Having regard to the state of the art and the cost of implementation, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.</p> <p>2. The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals.</p> <p>3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures and mechanisms referred to in paragraph 1 and 2, in particular for data protection by design requirements applicable across sectors, products and services.</p> <p>4. The Commission may lay down technical standards for the requirements laid down in paragraph 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>	<p>Article 23 Data protection by design and by default</p> <p>1. Having regard to the state of the art and the cost of implementation, the controller shall design [deleted] and implement appropriate technical and organisational measures and procedures with the objective of the processing meeting the requirements of this Regulation [deleted].</p> <p>2. [Deleted and replaced with:] The controller shall be accountable in accordance with article 5 for the effectiveness of the design and implementation of the measures and procedures referred to in paragraph 1 of this article.</p> <p>3.</p> <p>4. [Deleted]</p>

Justification

The objective of privacy by design is laudable, but legislation needs to be flexible to permit innovative design which accommodates itself to developing technology and the variety of circumstances confronting a controller. The article should be expressed in terms of its broad objective; that is that the initial design phase should take account of the requirements of the Regulation, rather than adding them as an afterthought. It should not be dependent on detailed technical implementing measures and should refer to the accountability of the controller for achieving that objective. There is no need to repeat any detailed aspects of the Regulation, such as data minimisation or data subject access rights, as they are a given due to the reference to meeting the requirements of the Regulation. Nor is it appropriate for the European Commission to lay down technical standards in this area as these could add substantially to the cost of compliance, and uncertainty to data controllers' obligations in this area.

5. Right of access for the data subject

EC Proposal	Proposed BT's amendments
<p>Article 15 Right of access for the data subject</p> <p>1. The data subject shall have the right to obtain from the controller at any time, on request, confirmation as to whether or not personal data relating to the data subject are being processed. Where such personal data are being processed, the controller shall provide the following information: (a) the purposes of the processing; [...]</p> <p>2. The data subject shall have the right to obtain from the controller communication of the personal data undergoing processing. Where the data subject makes the request in electronic form, the information shall be provided in electronic form, unless otherwise requested by the data subject.</p> <p>3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the communication to the data subject of the content of the personal data referred to in point (g) of paragraph 1.</p> <p>4. The Commission may specify standard forms and procedures for requesting and granting access to the information referred to in paragraph 1, including for verification of the identity of the data subject and communicating the personal data to the data subject, taking into account the specific features and necessities of various sectors and data processing situations. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>	<p>Article 15 Right of access for the data subject</p> <p>1. The data subject shall have the right to obtain from the controller at any time, on request, confirmation as to whether or not personal data relating to the data subject are being processed. Where such personal data are being processed, the controller shall provide the following information: (a) the purposes of the processing; [...]</p> <p>2. The data subject shall have the right to obtain from the controller communication of the personal data undergoing processing. [deleted] Where so requested by the data subject the information shall be provided in electronic form unless that is not reasonably practical.</p> <p>3. Where a data controller— (a) reasonably requires further information in order to satisfy himself as to the identity of the person making a request under this article and to locate the information which that person seeks, and (b) has informed that person of that requirement, the data controller is not obliged to comply with the request unless he is supplied with that further information.</p> <p>4. Where a data controller cannot comply with the request without disclosing information relating to another individual who can be identified from that information, he is not obliged to comply with the request unless— (a) the other individual has consented to the disclosure of the information to the person making the request, or (b) it is reasonable in all the circumstances to comply with the request without the consent of the other individual.</p> <p>5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the communication to the data subject of the content of the personal data referred to in point (g) of paragraph 1.</p> <p>6. The Commission may specify standard forms and procedures for requesting and granting access to the information referred to in paragraph 1, including for verification of the identity of the data subject and communicating the personal data to the data subject, taking into account the specific features and necessities of various sectors and data processing situations. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>

Justification

First, there is no reason to restrict to cases where the request has been made electronically, an electronic response to a subject access request. Subject to the method being practical in the circumstances of the case, it should be up to the data subject to choose whether an electronic response is acceptable.

Secondly, the right of subject access needs elaboration and qualification particularly to ensure that the request is from the person whose data are being requested and in order to protect the data protection and privacy rights of third parties. In cases of complex data systems and extensive data records it is also reasonable for the controller to be able to seek help from the data subject to track down the information required. The right of subject access has also to be qualified by other exemptions to protect the public interest, the interests of the data subject and the fundamental rights of third parties. The European Commission and the co-legislators are urged to develop further amendments to this article in order to provide for those essential protections.

6. Transfer of Personal Data to Third Countries

EC Proposal	Proposed BT's amendments
<p>Article 43 Transfers by way of binding corporate rules</p> <p>1. A supervisory authority shall in accordance with the consistency mechanism set out in Article 58 approve binding corporate rules, provided that they:</p> <p>(a) are legally binding and apply to and are enforced by every member within the controller's or processor's group of undertakings, and include their employees;</p> <p>(b) expressly confer enforceable rights on data subjects;</p> <p>(c) fulfil the requirements laid down in paragraph 2.</p> <p>2. The binding corporate rules shall at least specify:</p> <p>(a) the structure and contact details of the group of undertakings and its members;</p> <p>[...]</p> <p>3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for binding corporate rules within the meaning of this Article, in particular as regards the criteria for their approval, the application of points (b), (d), (e) and (f) of paragraph 2 to binding corporate rules adhered to by processors and on further necessary requirements to ensure the protection of personal data of the data subjects concerned.</p> <p>4. The Commission may specify the format and procedures for the exchange of information by electronic means between controllers, processors and supervisory authorities for binding corporate rules within the meaning of this Article. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).</p> <p>Article 58 (2)(f) Opinion by the European Data Protection Board: 'aims to approve binding corporate rules within the meaning of Article 43. '</p>	<p>Article 43 Transfers by way of binding corporate rules</p> <p>1. A supervisory authority <i>shall in accordance with the procedure set out in paragraph 3 below</i> approve binding corporate rules, provided that they:</p> <p>(a) are legally binding and apply to and are enforced by every member within the controller's or processor's group of undertakings, and include their employees;</p> <p>(b) expressly confer enforceable rights on data subjects;</p> <p>(c) fulfil the requirements laid down in paragraph 2.</p> <p>2. The binding corporate rules shall at least specify:</p> <p>(a) the structure and contact details of the group of undertakings and its members;</p> <p>[...]</p> <p><i>3. A data controller or processor may request the supervisory authority having competence under Article 51 to approve binding corporate rules for that data controller or processor. The competent supervisory authority shall nominate two further supervisory authorities to assist in the examination and approval of the binding corporate rules. The unanimous approval of the three authorities is sufficient to authorise the binding corporate rules without their being communicated in accordance with Article 58. In the absence of unanimity, the competent supervisory authority may implement the consistency mechanism in accordance with Article 58.</i></p> <p>4. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for binding corporate rules within the meaning of this Article, in particular as regards the criteria for their approval, the application of points (b), (d), (e) and (f) of paragraph 2 to binding corporate rules adhered to by processors and on further necessary requirements to ensure the protection of personal data of the data subjects concerned.</p> <p>5. The Commission may specify the format and procedures for the exchange of information by electronic means between controllers, processors and supervisory authorities for binding corporate rules within the meaning of this Article. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).</p> <p>[Article 58 (2)(f) shall be amended to read as follows:] <i>'aims to approve binding corporate rules within the meaning of Article 43 on which the competent supervisory authority and the two other nominated supervisory authorities are unable to reach unanimous agreement.'</i></p>

Justification

The binding corporate rules process needs to be as efficient as possible. There is a severe risk for the European Data Protection Board and for the Commission to be overloaded with applications, many of which will on further examination prove to be acceptable.

The data protection authorities have themselves developed a mutual recognition system by which a lead authority with the assistance of two others examine and agree binding corporate rules on behalf of those authorities – the majority – who have been able to agree to the mutual recognition procedure.

In the interests of efficiency and without any prejudice to the substance of data protection, that procedure should be incorporated into the new arrangements.

7. Data Portability

EC Proposal	Proposed BT's amendments
<p>Article 18 - Right to data portability</p> <p>1. The data subject shall have the right, where personal data are processed by electronic means and in a structured and commonly used format, to obtain from the controller a copy of data undergoing processing in an electronic and structured format which is commonly used and allows for further use by the data subject.</p> <p>2. Where the data subject has provided the personal data and the processing is based on consent or on a contract, the data subject shall have the right to transmit those personal data and any other information provided by the data subject and retained by an automated processing system, into another one, in an electronic format which is commonly used, without hindrance from the controller from whom the personal data are withdrawn.</p> <p>3. The Commission may specify the electronic format referred to in paragraph 1 and the technical standards, modalities and procedures for the transmission of personal data pursuant to paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>	<p>Article 18 - Right to data portability</p> <p>1 Where the data subject has provided the personal data and the processing is based on consent or on a contract:</p> <p>a. the data subject shall have the right, where personal data are processed by electronic means and in a structured and commonly used format, to obtain from the controller in an electronic and structured format which is commonly used and allows for further use by the data subject, a copy of those data provided by the data subject and undergoing processing;</p> <p>b. the data subject shall have the right to transmit those personal data and any other information provided by the data subject and retained by an automated processing system, into another one, in an electronic format which is commonly used, without hindrance from the controller from whom the personal data are withdrawn.</p> <p>2. The rights of the data subject set out in paragraph 1 above:</p> <p>(a) are subject to:</p> <p>(i) the right of the data controller to retain and not disclose data which are commercially confidential;</p> <p>(ii) any legal duties imposed on the controller to retain the data;</p> <p>(iii) the right of the controller to retain data to protect or assert its own interests; and</p> <p>(b) in any event may not be exercised until the expiry or other termination of a contract for the purposes of which the data were provided.</p> <p>3. The Commission may specify the electronic format referred to in paragraph 1 and the technical standards, modalities and procedures for the transmission of personal data pursuant to paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>

Justification

The right of data portability was conceived in the context of social networking sites in order to allow individuals to carry to another similar site the data which they have provided. The current version of Article 18 is drawn so widely that it is capable of prejudicing routine consumer contractual arrangements and depriving data controllers of their special and commercially confidential data. The amended text addresses both problems whilst still allowing individuals to transport data provided by them to other sites on the termination of any consumer contractually agreed period.

8. Right to be forgotten

EC Proposal	Proposed BT's amendments
<p>Article 17 Right to be forgotten and to erasure</p> <p>1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child, where one of the following grounds applies:</p> <p>(a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;</p> <p>(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data;</p> <p>(c) the data subject objects to the processing of personal data pursuant to Article 19;</p> <p>(d) the processing of the data does not comply with this Regulation for other reasons.</p> <p>...</p> <p>3. The controller shall carry out the erasure without delay, except to the extent that the retention of the personal data is necessary:</p> <p>(a) for exercising the right of freedom of expression in accordance with Article 80;</p> <p>(b) for reasons of public interest in the area of public health in accordance with Article 81;</p> <p>(c) for historical, statistical and scientific research purposes in accordance with Article 83;</p> <p>(d) for compliance with a legal obligation to retain the personal data by Union or Member State law to which the controller is subject; Member State laws shall meet an objective of public interest, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued;</p> <p>(e) in the cases referred to in paragraph 4.</p> <p>...</p>	<p>Article 17 Right to be forgotten and to erasure</p> <p>1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child, where one of the following grounds applies:</p> <p>(a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;</p> <p>(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data;</p> <p>(c) the data subject objects to the processing of personal data pursuant to Article 19;</p> <p>(d) [deleted]</p> <p>....</p> <p>3. The controller shall carry out the erasure without delay, except to the extent that the retention of the personal data is necessary:</p> <p>(a) for exercising the right of freedom of expression in accordance with Article 80;</p> <p>(b) for reasons of public interest in the area of public health in accordance with Article 81;</p> <p>(c) for historical, statistical and scientific research purposes in accordance with Article 83;</p> <p>(d) for compliance with a legal obligation to retain the personal data by Union or Member State law to which the controller is subject; Member State laws shall meet an objective of public interest, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued;</p> <p>(e) for the protection of the data subject rights and freedoms of third parties;</p> <p>(f) for the protection or assertion of the rights of the data controller, or</p> <p>(g) in the cases referred to in paragraph 4.</p> <p>...</p>

Justification

Traditional data protection rules already require that, subject to limited exceptions, data be kept for no longer than is necessary for the purpose for they were obtained. The conversion of the duty to delete data into a right to be forgotten has been provoked by several notorious cases relating to the use of information on social network sites.

Whilst the objective of the new right is laudable, it must be carefully drawn so as not to prejudice the rights of data controllers and third parties operating in other industry sectors. Article 17(1) (d) is drawn so widely as to be unpredictable in its consequences and lacking legal certainty in its effect. Paragraph 3 of the article does not seem to make adequate provision for the protection of the rights of the data controller and others. Indeed, it is entirely likely in some cases – e.g. those relating to mental health – that data should be retained for the protection of the data subject. Data controllers should also have the flexibility to retain data to protect their own interests, such as proving the existence of a contract entered into by a data subject, and to comply with legal requirements.

For further information please contact:

tilmann.kupfer@bt.com

or

cecile.plaidy@bt.com

in Brussels

© British Telecommunications plc
Registered office: 81 Newgate Street, London
EC1A 7AJ
Registered in England No: 1800000



Proposed Amendment 1

Article 4 Definitions	
Commission Proposal	Telefónica Proposal (proposed new text in blue)
<p>(5) 'controller' means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes, conditions and means of the processing of personal data; where the purposes, conditions and means of processing are determined by Union law or Member State law, the controller or the specific criteria for his nomination may be designated by Union law or by Member State law;</p>	<p>(5) 'controller' means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes, conditions and means of the processing of personal data; where the purposes, conditions and means of processing are determined by Union law or Member State law, the controller or the specific criteria for his nomination may be designated by Union law or by Member State law;</p>

Justification:

The definition of controller should be based on the decision of the purposes for which personal data are processed (i.e. “why” the data are processed) rather than the conditions or means by which this is achieved (i.e. “how” the data are processed).

The control over the reason/purpose for processing is the logical basis for allocating different responsibilities between controllers who are responsible for what and why data is processed and processing parties who deal with how data is processed”.

A clear divide between controller and processor and their roles and responsibilities is key in a Cloud environment. More and more data processing is outsourced by the controller to a service provider (processor). Controllers often rely on their service providers to determine the most effective technological solutions to deliver outsourced processing. In fact, service providers sell themselves to their customers on the basis of their technical expertise, and necessarily exercise a certain, but limited, autonomy over the means and conditions by which they process data **on their customers’ behalf**. However, by doing so, service providers risk exposure under the current Proposal to the full compliance requirements of the Directive, a disproportionate burden when considering that the purposes for which they process data are entirely mandated by their customer. It is also not in alignment with the typical practice of sharing responsibilities of the service providers and their customers in commercial agreements regarding such data processing services.

Proposed Amendment 2

Article 18 Right to data portability	
Commission Proposal	Telefónica Proposal (proposed new text in blue)
<ol style="list-style-type: none">1. The data subject shall have the right, where personal data are processed by electronic means and in a structured and [...].2. Where the data subject has provided the personal data and the processing is based on consent or on a contract, [...].3. The Commission may specify the electronic format referred to in paragraph 1 and the technical standards, [...].	<ol style="list-style-type: none">1. The data subject shall have the right, where personal data are processed by electronic means and in a structured and [...].2. Where the data subject has provided the personal data and the processing is based on consent or on a contract, [...].3. The Commission may specify the electronic format referred to in paragraph 1 and the technical standards, [...].

Justification:

Data portability is fraught with technical and competition issues and therefore easier said than done. But apart from this enforcement difficulties, Telefónica would like to make a more important point: in essence, it is a competition or market organisation measure to be addressed in the proper regulation, but not related to data protection or privacy.

Transparency as a whole will be of further more importance to obtain confidence from our customers, therefore the market will provide for the most suitable forms of Data Subjects Access Rights. Some of our Operating Businesses are already today providing answers to customer requests for data in an electronic form and the customers are free to use it however they want. This will evolve in the future due to increasing amounts of data and the necessary process development going along with it.

We would, therefore, suggest striking it from this Regulation and strengthening and make easier the right to access to data. In other words to reinforce the data Subject Access Rights.

Competition issues around Cloud services are not solved by providing a general data portability right. Cloud provides different services with different technical, business and competition implications with different portability possibilities, the data is not the same and the services are not the same, except that we would aim at building "uniform" cloud based services in Europe (which is not really the idea of the European Cloud Strategy). We cannot provide a blank slate regarding portability for all the services around cloud business without considering the service provided and the competition constraints in each business proposition based on Cloud: hosting, IaaS, processing, SaaS, etc.

It is not so easy to move data from one provider to another, especially if the cloud provider provides value added services and not only infrastructure. And this will not be solved by a generic data portability right.

Service costs and prices will clearly increase without not clear benefit in most of the cases, innovation will be constrained by European formats, standards and rules, and the European cloud services will be still less competitive from the end user perspective although implement user's data portability rights.

- MEP Kelly's Draft Opinion tries to introduce some improvements in the wording of Art.18, but at the end there seems to be no difference between Art. 18 as amended by MEP Kelly and Art. 15 on right of access for the data subjects. Having a sound right of access (art. 15) would solve the problems the new right to Data Portability is willing to address, without any negative effects as identified above.

Proposed Amendment 3

Article 26 Processor	
Commission Proposal	Telefónica Proposal (proposed new text in blue)
<p>1. Where a processing operation is to be carried out on behalf of a controller, the controller shall choose a processor providing sufficient guarantees to implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject, in particular in respect of the technical security measures and organizational measures governing the processing to be carried out and shall ensure compliance with those measures.</p> <p>2. The carrying out of processing by a processor shall be governed by a contract or other legal act binding the processor to the controller and stipulating in particular that the processor shall:</p> <p>(a) act only on instructions from the controller, in particular, where the transfer of the personal data used is prohibited;</p> <p>(b) employ only staff who have committed themselves to confidentiality or are under a statutory obligation of</p>	<p>1. Where a processing operation is to be carried out on behalf of a controller, the controller shall choose a processor providing sufficient guarantees to implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject, in particular in respect of the technical security measures and organizational measures governing the processing to be carried out and shall ensure compliance with those measures.</p> <p>2. The carrying out of processing by a processor shall be governed by a contract or other legal act binding the processor to the controller and stipulating in particular that the processor shall:</p> <p>(a) act only on instructions from the controller, in particular, where the transfer of the personal data used is prohibited;</p> <p>(b) employ only staff who have committed themselves to confidentiality or are under a statutory obligation of</p>

<p>confidentiality;</p> <p>(c) take all required measures pursuant to Article 30;</p> <p>(d) only enlist another further processors only with the prior permission of the controller that enable the requirements of this Regulation to be met;</p> <p>(e) insofar as this is possible given the nature of the processing, create in agreement with the controller the necessary technical and organisational requirements for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;</p> <p>(f) assist the controller in ensuring compliance with the obligations pursuant to Articles 30 to 34;</p> <p>(g) hand over all results to the controller after the end of the processing and not process the personal data further after the end of the agreed processing otherwise;</p> <p>(h) upon request make available to the controller and the supervisory authority all relevant and permissible information necessary to control compliance with the obligations laid down in this Article.</p> <p>3. The controller and the processor shall document in writing the controller's instructions and the processor's obligations referred to in paragraph 2.</p>	<p>confidentiality;</p> <p>(c) take all required measures pursuant to Article 30;</p> <p>(d) only enlist another further processors only with the prior permission of the controller that enable the requirements of this Regulation to be met;</p> <p>(e) insofar as this is possible given the nature of the processing, create in agreement with the controller the necessary technical and organisational requirements for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;</p> <p>(f) assist the controller in ensuring compliance with the obligations pursuant to Articles 30 to 34;</p> <p>(g) hand over all results to the controller after the end of the processing and not process the personal data further after the end of the agreed processing otherwise;</p> <p>(h) upon request make available to the controller and the supervisory authority all relevant and permissible information necessary to control compliance with the obligations laid down in this Article.</p> <p>3. The controller and the processor shall document in writing the controller's instructions and the processor's obligations referred to in paragraph 2.</p>
--	--

4. If a processor processes personal data other than as instructed by the controller, the processor shall be considered to be a controller in respect of that processing and shall be subject to the rules on joint controllers laid down in Article 24.

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the responsibilities, duties and tasks in relation to a processor in line with paragraph 1, and conditions which allow facilitating the processing of personal data within a group of undertakings, in particular for the purposes of control and reporting.

~~4. If a processor processes personal data other than as instructed by the controller, the processor shall be considered to be a controller in respect of that processing and shall be subject to the rules on joint controllers laid down in Article 24.~~

~~5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the responsibilities, duties and tasks in relation to a processor in line with paragraph 1, and conditions which allow facilitating the processing of personal data within a group of undertakings, in particular for the purposes of control and reporting.~~

Justification:

This article introduces many new obligations on processors that should preferably be set in the contractual agreements between controllers and processors.

Furthermore, we suggest to delete the possibility for the Commission to adopt delegated.

Proposed Amendment 4

Article 28 Documentation	
Commission Proposal	Proposal (proposed new text in blue)
<p>1. Each controller and processor and, if any, the controller's representative, shall maintain documentation of all processing operations under its responsibility.</p> <p>2. The documentation shall contain at least the following information:</p> <p>(a) the name and contact details of the controller, or any joint controller or processor, and of the representative, if any;</p> <p>(b) the name and contact details of the data protection officer, if any;</p> <p>(c) the purposes of the processing, including the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);</p> <p>(d) a description of categories of data subjects and of the categories of personal data relating to them;</p> <p>(e) the recipients or categories of recipients of the personal data, including the controllers to whom personal data are disclosed for the legitimate interest pursued by them;</p> <p>(f) where applicable, transfers of data to a third country or an international organisation, including the identification of that third country or international</p>	<p>1. Each controller and processor and, if any, the controller's representative, shall maintain documentation of all processing operations under its responsibility.</p> <p>2. The documentation shall contain at least the following information:</p> <p>(a) the name and contact details of the controller, or any joint controller or processor, and of the representative, if any;</p> <p>(b) the name and contact details of the data protection officer, if any;</p> <p>(c) the purposes of the processing, including the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);</p> <p>(d) a description of categories of data subjects and of the categories of personal data relating to them;</p> <p>(e) the recipients or categories of recipients of the personal data, including the controllers to whom personal data are disclosed for the legitimate interest pursued by them;</p> <p>(f) where applicable, transfers of data to a third country or an international organisation, including the identification of that third country or international</p>

organisation and, in case of transfers referred to in point (h) of Article 44(1),
the documentation of appropriate safeguards;
(g) a general indication of the time limits for erasure of the different categories of data;
(h) the description of the mechanisms referred to in Article 22(3).

3. The controller and the processor and, if any, the controller's representative, shall make the documentation available, on request, to the supervisory authority.

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the documentation referred to in paragraph 1, to take account of in particular the responsibilities of the controller and the processor and, if any, the controller's representative.

6. The Commission may lay down standard forms for the documentation referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

~~organisation and, in case of transfers referred to in point (h) of Article 44(1),
the documentation of appropriate safeguards;
(g) a general indication of the time limits for erasure of the different categories of data;
(h) the description of the mechanisms referred to in Article 22(3).~~

~~3. The controller and the processor and, if any, the controller's representative, shall make the documentation available, on request, to the supervisory authority.~~

~~5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the documentation referred to in paragraph 1, to take account of in particular the responsibilities of the controller and the processor and, if any, the controller's representative.~~

~~6. The Commission may lay down standard forms for the documentation referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).~~

Justification:

With the aim to reduce administrative burden on controllers, Art. 28 replaces the general obligation to notify individual processing operations to the supervisory authority under Articles 18(1) and 19 of Directive 95/46/EC. However, we believe this new obligation to maintain documentation of all processing operations will involve heavy bureaucratic requirements and therefore seriously risk increasing rather than reducing the administrative burden, compared to the current rules.

We are also concerned that identical obligations apply to data controllers and data processors (which currently are not subject to any notification obligation). This poses a particular problem in the area of cloud computing. Indeed, imposing disproportionate documentation obligations on data processors -identical to the controllers' obligations- risks severely slowing the development and roll out of new cloud computing offerings and services in Europe.

Finally, we firmly believe Article 28 conflicts with the principles of accountability and efficiency that are set out in Article 22 of the GDPR, therefore it should be simplified in order to become effective and proportionate. Only Article 28.2.a. and 28.2.b. should be maintained, combined with a general duty to keep an inventory and description of the way the controller ensures that processing operations comply with data protection rules.

Finally, we suggest to delete the possibility for the Commission to adopt delegated and implementing acts.

Proposed Amendment 5

Article 33 Data Protection Impact Assessment	
Commission Proposal	Proposal (proposed new text in blue)
(1) Where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller or the processor acting on the controller's	(1) Where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller or the processor acting on the controller's

behalf shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

(2) The following processing operations in particular present specific risks referred to in paragraph 1:

(a) a systematic and extensive evaluation of personal aspects relating to a natural person or for analysing or predicting in particular the natural person's economic situation, location, health, personal preferences, reliability or behaviour, which is based on automated processing and on which measures are based that produce legal effects concerning the individual or significantly affect the individual; [...]

(4) The controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations.

~~behalf~~ shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

~~(2) The following processing operations in particular present specific risks referred to in paragraph 1:~~

~~(a) a systematic and extensive evaluation of personal aspects relating to a natural person or for analysing or predicting in particular the natural person's economic situation, location, health, personal preferences, reliability or behaviour, which is based on automated processing and on which measures are based that produce legal effects concerning the individual or significantly affect the individual; [...]~~

~~(4) The controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations.~~

Justification:

Data controllers should have flexibility in determining risks under the principle of accountability. Data controllers know the particularities of their products, services or sectors and can better adapt DPIAs to their needs.

A PIA is naturally a duty of the controllers, therefore, imposing this obligation also on processors should be questioned as it could be even more counterproductive, diluting the liabilities between the data controller and the data processor. This poses a particular problem in the area of cloud, where more than ever the responsibilities and roles of the data controller and the data processor shall be clearly differentiated.

We call for the removal of the obligation to conduct a PIA of a processing based on profiling, as we do not agree with the fact that profiling per se presents “specific risks”.

Article 33 (4) obliges data controllers to seek the views of data subjects or their representatives (e.g., consumer organisations) on the intended processing of their personal data. This obligation is disproportionate and would create commercial concern for companies developing new products and services in highly competitive markets. Therefore, we suggest its deletion.

Proposed Amendment 6

Article 77 Right to compensation and liability	
Commission Proposal	Telefónica Proposal (proposed new text in blue)
<p>1. Any person who has suffered damage as a result of an unlawful processing operation or of an action incompatible with this Regulation shall have the right to receive compensation from the controller or the processor for the damage suffered.</p> <p>2. Where more than one controller or processor is involved in the processing, each controller or processor shall be jointly and severally liable for the entire amount of the damage, to the extent that liability has not already been established in the determination of responsibilities envisaged in Article 24.</p> <p>3. The controller or the processor may be exempted from this liability, in whole or in part, if the controller or the processor proves that they are not responsible for the event giving rise to the damage.</p>	<p>1. Any person who has suffered damage as a result of an unlawful processing operation or of an action incompatible with this Regulation shall have the right to receive compensation from the controller or the processor for the damage suffered.</p> <p>2. Where more than one controller or processor is involved in the processing, each controller or processor shall be jointly and severally liable for the entire amount of the damage, to the extent that liability has not already been established in the determination of responsibilities envisaged in Article 24.</p> <p>3. The controller or the processor may be exempted from this liability, in whole or in part, if the controller or the processor proves that they are it is not responsible for the event giving rise to the damage.</p>

Justification:

Liability should be maintained on the data controller as it is currently the case further to the Directive 1995/46/EC. The controller is the one who has the direct link with the data subject and is the one responsible vis-à-vis the data subject. If the controller considers any eventual damage was due to the processor's incorrect processing, the data controller will ask compensation from the processor. Furthermore, the controller and the processor normally establish the liability relationship in the contractual arrangements, for cases where the processor does not act as requested by the data controller.

This article instead of helping data subjects creates confusion for controllers, processors and even more importantly for data subjects.



Amendments proposed by COCIR on the General Data Protection Regulation¹

Please find below amendments proposed by COCIR on the General Data Protection Regulation.

Article 4: Definitions

(12) 'data concerning health' means any **information personal data** which relates to the physical or mental health of ~~an individual a data subject~~, or to the provision of health services to the ~~individual data subject~~.

Data not directly associated with the data subject, data associated to a medical equipment (e.g. serial number of a medical device), is not 'data concerning health'. Anonymised and pseudonymised data are not 'data concerning health'.

(13) 'anonymised data' means previously identifiable data that have been de-identified and for which a code or other link no longer exists. An investigator would not be able to link anonymized information back to a specific data subject.

(14) 'pseudonymised data' means previously identifiable data where Personally Identifiable Information (PII) – such as name, date of birth, address or account number – has been replaced with a code (pseudonyms or symbol). The link between the code and the PII is kept separately. An investigator would not be able to link anonymized information back to a specific data subject.

+ new recital: 'technical data' or any data associated to a piece of equipment used to process data (e.g. serial number, etc) but which is not directly associated with the data subject, and does not allow the identification of the data subject, should not be considered 'personal data'.

Justification:

The Regulation should recognise that data that do not relate to a data subject or cannot be linked to a data subject through various data protection mechanisms (e.g. anonymisation or pseudonymisation) are not 'personal data', nor 'data concerning health'.

¹ http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf



Article 14: Information to the data subject

7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria ~~for categories of recipients referred to in point (f) of paragraph 1~~, for the requirements for the notice of potential access referred to in point (g) of paragraph 1, the criteria for the further information necessary referred to in point (h) of paragraph 1 for specific sectors and situations, and the conditions and appropriate safeguards for the exceptions laid down in point (b) of paragraph 5. In doing so, the Commission shall take the appropriate measures for micro, small and medium-sized-enterprises.

Justification:

In a healthcare environment, categories of recipients of data vary on healthcare providers' or eHealth service provider practices, organizations, and workflows. It should remain under the power of these actors considering the case reference as required. The European Commission adopting prescriptive delegated acts (Art. 14(7)) is not the right approach as it will delay the process and reduce flexibility in healthcare settings.

Article 17: Right to be forgotten and to erasure

(3) The controller shall carry out the erasure without delay, except to the extent that the retention of the personal data is necessary:

(a) for exercising the right of freedom of expression in accordance with Article 80;

(b) for reasons of public interest in the area of public health in accordance with Article 81;

(c) for maintaining medical records for prevention, medical diagnosis, treatment, palliative care, clinical trials, patient registries, and other health research and medical innovation purposes.

~~(e d)~~ for historical, statistical and scientific research purposes in accordance with Article 83;

~~(d e)~~ for compliance with a legal obligation to retain the personal data by Union or Member State law to which the controller is subject; Member State laws shall meet an objective of public interest, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued;

~~(e-f)~~ in the cases referred to in paragraph 4.

Justification:

Implementing the right to be forgotten and to erasure in healthcare requires careful consideration of the consequences. Deleting data from electronic health records does not effectively protect individual privacy, and can run counter to patient safety, public interest, health research, and eHealth deployment. For instance, deleting all or parts of the information contained in an electronic health record would undermine the ability of medical professionals to treat the patient effectively. Statistical analyses will be "depowered" if data is deleted, particularly in the case of orphan diseases or conditions with difficult inclusion and exclusion criteria, such as pediatric.



Article 20: Measures based on profiling²

Delete

Justification:

Profiling techniques per se do not need special regulatory treatment given the many safeguards introduced in the draft Regulation especially when incentives are provided for companies to anonymize and/or pseudonymize data. The current text of Article 20 might render legitimate use of data for health research impossible with great consequences for the social benefits in this area.

Article 23: Data protection by design and by default

Delete

Alternatively:

(1) Having regard to the state of the art and the cost of implementation, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

2. The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals.

~~3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures and mechanisms referred to in paragraph 1 and 2, in particular for data protection by design requirements applicable across sectors, products and services.~~

~~4. The Commission may lay down technical standards for the requirements laid down in paragraph 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).~~

Recital (61)

Delete

Justification:

The concepts of 'Privacy by Design' and 'Privacy by Default' are subject to interpretation and lack clear definition. These ideas are probably more effective as reflecting organisational policy or for use as marketing concepts, rather than as a framework for compliance with legal requirements. In addition, the underlying elements of PBD and PBD are already reflected in the Regulation through new requirements: data protection impact assessment, data minimisation, etc. These concepts are therefore superfluous at best, and would introduce legal uncertainty at worse.

² This amendment falls if anonymised data are not subject to the Regulation.



Article 26: Processor

1. Where a processing operation is to be carried out on behalf of a controller, the controller shall choose a processor providing sufficient guarantees to implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject, in particular in respect of the technical security measures and organizational measures governing the processing to be carried out and shall ensure compliance with those measures.

2. The carrying out of processing by a processor shall be governed by a contract or other legal act binding the processor to the controller and stipulating in particular that the processor shall:

(a) act only on instructions from the controller, in particular, where the transfer of the personal data used is prohibited;

(b) employ only staff who have committed themselves to confidentiality or are under a statutory obligation of confidentiality;

(c) take all required measures pursuant to Article 30;

~~(d) enlist another processor only with the prior permission of the controller;~~

~~(d-e)~~ insofar as this is possible given the nature of the processing, create in agreement with the controller the necessary technical and organisational requirements for the fulfillment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;

~~(e f)~~ assist the controller in ensuring compliance with the obligations pursuant to Articles 30 to 34;

~~(f g) hand over all results to the controller after the end of the processing and not process the personal data further after the end of the agreed processing otherwise;~~

~~(g h) upon request~~ make available to the controller ~~and the supervisory authority~~ all **relevant and permissible** information necessary to control compliance with the obligations laid down in this Article.

3. The controller and the processor shall document in writing the controller's instructions and the processor's obligations referred to in paragraph 2.

4. If a processor processes personal data other than as instructed by the controller, the processor shall be considered to be a controller in respect of that processing and shall be subject to the rules on joint controllers laid down in Article 24.

~~5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the responsibilities, duties and tasks in relation to a processor in line with paragraph 1, and conditions which allow facilitating the processing of personal data within a group of undertakings, in particular for the purposes of control and reporting.~~

Justification:

The proposed text introduces a host of new requirements for data processors and states how these should be included in the contractual arrangements. Some of these additions are unworkable in practice. For example, a controller may want to ensure that additional sub-processors - which may be numerous - apply effective data protection but this does not mean they are able or willing, to assess each in turn prior to their employment. As the processor has the closer relationship, they are better placed to make such a judgment. In relation to handing over results at the end of processing, there may be no results as such to hand over if the data minimisation principle has been effectively applied. Making data available to the supervisory authority should be handled by the controller. Certain information may be subject to a confidentiality obligation under law



or contract and hence a processor may not be at liberty to disclose such information to a supervisory authority. Moreover, such data should not be required to be transmitted on a regular basis as this would overburden authorities and further increase the administrative burden.

Requiring each Data Controller (e.g. hospital) to agree, individually, to each sub-processor enlisted by a Data Processor would introduce excessive administrative burden and increase costs to both the data controller and data processor.

Article 28: Documentation

1. Each controller ~~and processor~~ and, if any, the controller's representative, shall maintain documentation of all processing operations under its responsibility.
2. The documentation shall contain at least the following information:
 - (a) the name and contact details of the controller, or any joint controller or processor, and of the representative, if any;
 - (b) the name and contact details of the data protection officer, if any;
 - (c) the purposes of the processing, including the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);
 - (d) a description of categories of data subjects and of the categories of personal data relating to them;
 - (e) the recipients or categories of recipients of the personal data, including the controllers to whom personal data are disclosed for the legitimate interest pursued by them;
 - (f) where applicable, transfers of data to a third country or an international organisation, including the identification of that third country or international organisation and, in case of transfers referred to in point (h) of Article 44(1), the documentation of appropriate safeguards;
 - (g) a general indication of the time limits for erasure of the different categories of data;
 - (h) the description of the mechanisms referred to in Article 22(3).
3. The controller ~~and the processor~~ and, if any, the controller's representative, shall make the documentation available, on request, to the supervisory authority.
4. The obligations referred to in paragraphs 1 and 2 shall not apply to the following controllers ~~and processors~~:
 - (a) a natural person processing personal data without a commercial interest; or
 - (b) an enterprise or an organisation employing fewer than 250 persons that is processing personal data only as an activity ancillary to its main activities.
5. ~~The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the documentation referred to in paragraph 1, to take account of in particular the responsibilities of the controller and the processor and, if any, the controller's representative.~~
6. The Commission may lay down standard forms for the documentation referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Justification:

Requiring both controllers and processors to maintain the same documentation for the same processing operation in an unnecessary burden that does not enhance the protection of data subjects or facilitate enforcement by the authorities. Controllers are in the best position to determine the purposes of processing and provide associated documentation that supports the basis and details of processing. Furthermore, given the



required level of detail already demanded in the documentation, it does not make sense for the Commission to have powers to adopt even more requirements or criteria.

Recital (65)

In order to demonstrate compliance with this Regulation, the controller ~~or processor~~ should document each processing operation. Each controller ~~and processor~~ should be obliged to co-operate with the supervisory authority and make this documentation, on request, available to it, so that it might serve for monitoring those processing operations.

Justification:

In line with proposed amendments to Article 28.

Article 30: Security of Processing

1. The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected, having regard to the state of the art and the costs of their implementation.
 2. The controller and the processor shall, following an evaluation of the risks, take the measures referred to in paragraph 1 to protect personal data against accidental or unlawful destruction or accidental loss and to prevent any unlawful forms of processing, in particular any unauthorised disclosure, dissemination or access, or alteration of personal data.
- ~~(3) The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the technical and organisational measures referred to in paragraphs 1 and 2, including the determinations of what constitutes the state of the art, for specific sectors and in specific data processing situations, in particular taking account of developments in technology and solutions for privacy by design and data protection by default, unless paragraph 4 applies.~~
- ~~(4) The Commission may adopt, where necessary, implementing acts for specifying the requirements laid down in paragraphs 1 and 2 to various situations, in particular to:~~
- ~~(a) prevent any unauthorised access to personal data;~~
 - ~~(b) prevent any unauthorised disclosure, reading, copying, modification, erasure or removal of personal data;~~
 - ~~(c) ensure the verification of the lawfulness of processing operations.~~
- ~~Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).~~

Justification:

Any specifications pertaining the security requirements for processing personal data should be technologically neutral, flexible, scalable and applicable to the type of data being processed, the context for the data processing, and the potential implications to the processing activities. In the healthcare context, highly secure transmission and storage of data is desirable, however, access controls must be respectful of the need to access data in the provision of care, serviceability of medical devices and healthcare technology, etc.



Article 33: Data protection impact assessment

1. Where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller ~~or the processor acting on the controller's behalf~~ shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.
2. The following processing operations in particular present specific risks referred to in paragraph 1:
 - (a) a systematic and extensive evaluation of personal aspects relating to a natural person or for analysing or predicting in particular the natural person's economic situation, location, health, personal preferences, reliability or behaviour, which is based on automated processing and on which *decisions* are based that produce legal effects *that gravely and adversely affect the individual's fundamental rights*
 - (b) information on sex life, health, race and ethnic origin or for the provision of health care, epidemiological researches, or surveys of mental or infectious diseases, where the data are processed for taking measures or decisions regarding specific individuals on a large scale;
 - (c) monitoring publicly accessible areas, especially when using optic-electronic devices (video surveillance) on a large scale;
 - (d) personal data in large scale filing systems on children, genetic data or biometric data;
 - ~~(e) other processing operations for which the consultation of the supervisory authority is required pursuant to point (b) of Article 34(2).~~
 - (e) Impact assessment should be carried out if the processing differs significantly from existing practices of the controller and the new approach in itself presents specific risks and this creates doubts with the compliance of this Regulation.**
- ~~3. The assessment shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned.~~
- ~~4. The controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations.~~
- ~~3.-5.~~ Where the controller is a public authority or body and where the processing results from a legal obligation pursuant to point (c) of Article 6(1) providing for rules and procedures pertaining to the processing operations and regulated by Union law, paragraphs 1 to 4 shall not apply, unless Member States deem it necessary to carry out such assessment prior to the processing activities.
- ~~4.-6. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the processing operations likely to present specific risks referred to in paragraphs 1 and 2 and the requirements for the assessment referred to in paragraph 3, including conditions for scalability, verification and auditability. In doing so, the Commission shall consider specific measures for micro, small and medium sized enterprises.~~
- ~~5.-7. The Commission may specify standards and procedures for carrying out and verifying and auditing the assessment referred to in paragraph 3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).~~



Justification:

With the view to ensure legal certainty and enable better enforcement by supervisory authorities and in accordance with Recital 62 which requires "a clear attribution of the responsibilities under this Regulation", privacy impact assessments should be carried out by the controller. Notably, the controller is in the best position to assess the impact of any processing. The controller, and not the processor, has ready access to all relevant information, including risks and benefits of processing the personal data. Furthermore, the requirement to seek the views of data subjects is impractical.

Specific risks should be clarified. The notion of harm or 'grave or adverse impact' on the individual's rights could be an element to determine 'specific risks'.

The obligation to carry out impact assessment should not apply to every single existing routine processing, but only to new processings which differ significantly to the current practices of the Data Controller. Given the fact that according to Art. 14 data subjects need to be informed of the data processing, an obligation to consult data subjects as part of the assessment appears misplaced and unnecessary.

Furthermore, impact assessments should not be standardised. Different types of organisations may have equally effective means of performing such assessments, and unnecessary constraints may hinder improvements in the process, as technologies emerge, and contexts change.

Article 34: Prior authorisation and prior consultation

Delete

Alternatively

1. The controller ~~or the processor as the case may be~~ shall obtain an authorisation from the supervisory authority prior to the processing of personal data, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where a controller or processor adopts contractual clauses as provided for in point (d) of Article 42(2) or does not provide for the appropriate safeguards in a legally binding instrument as referred to in Article 42(5) for the transfer of personal data to a third country or an international organisation.
2. **The authorisation process by the supervisory authority should be limited in time, with a maximum timeline of 15 days to respond, or request additional information, where deemed necessary.**
- ~~2. The controller or processor acting on the controller's behalf shall consult the supervisory authority prior to the processing of personal data in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where:~~
 - ~~(a) a data protection impact assessment as provided for in Article 33 indicates that processing operations are by virtue of their nature, their scope or their purposes, likely to present a high degree of specific risks; or~~
 - ~~(b) the supervisory authority deems it necessary to carry out a prior consultation on processing operations that are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope and/or their purposes, and specified according to paragraph 4.~~
3. Where the supervisory authority is of the opinion that the intended processing does not comply with this Regulation, in particular where risks are insufficiently identified



or mitigated, it shall prohibit the intended processing and make appropriate proposals to remedy such non-compliance.

- ~~4. The supervisory authority shall establish and make public a list of the processing operations which are subject to prior consultation pursuant to point (b) of paragraph 2. The supervisory authority shall communicate those lists to the European Data Protection Board.~~
- ~~5. Where the list provided for in paragraph 4 involves processing activities which are related to the offering of goods or services to data subjects in several Member States, or to the monitoring of their behaviour, or may substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57 prior to the adoption of the list.~~
- ~~6. The controller or processor shall provide the supervisory authority with the data protection impact assessment provided for in Article 33 and, on request, with any other information to allow the supervisory authority to make an assessment of the compliance of the processing and in particular of the risks for the protection of personal data of the data subject and of the related safeguards.~~
4. ~~7.~~ Member States shall consult the supervisory authority in the preparation of a legislative measure to be adopted by the national parliament or of a measure based on such a legislative measure, which defines the nature of the processing, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects.
- ~~8. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for determining the high degree of specific risk referred to in point (a) of paragraph 2.~~
5. ~~9.~~ The Commission may set out standard forms and procedures for prior authorisations ~~and consultations~~ referred to in paragraphs 1 ~~and 2~~, ~~and standard forms and procedures for informing the supervisory authorities pursuant to paragraph 6.~~ Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Justification:

Requiring prior consultation in the case of the wide range of processing operations that may qualify for a 'high degree of specific risks', in accordance with the long list in Article 33, is likely to be a serious impediment to innovation in Europe. DPAs could face a deluge of cases that quickly back-up. Even if the DPAs had the resources to handle the case-load, conducting a thorough investigation is likely to be a case of months, not days. An ex-post system is far more fitting to a regime of effective and accountable data protection which does not impede growth and innovation. In addition, it is essential to set a time limit for the assessment by the supervisory authority in order to avoid unreasonable delays.

Recital (74)

~~Where a data protection impact assessment indicates that processing operations involve a high degree of specific risks to the rights and freedoms of data subjects, such as excluding individuals from their right, or by the use of specific new technologies, the supervisory authority should be consulted, prior to the start of operations, on a risky processing which might not be in compliance with this Regulation, and to make proposals to remedy such situation. Such consultation should equally take place in the course of the preparation either of a measure by the national parliament or of a measure~~



~~based on such legislative measure which defines the nature of the processing and lays down appropriate safeguards.~~

Justification:

In line with changes to Article 34.

Article 39: Certification

1. The Member States and the Commission shall encourage, in particular at European level, the establishment of data protection certification mechanisms and of data protection seals and marks, allowing data subjects to quickly assess the level of data protection provided by controllers and processors. The data protection certifications mechanisms **shall be voluntary, capable of global application and affordable. These mechanisms shall also be technology neutral and shall** contribute to the proper application of this Regulation, taking account of the specific features of the various sectors and different processing operations.

~~2. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the data protection certification mechanisms referred to in paragraph 1, including conditions for granting and withdrawal, and requirements for recognition within the Union and in third countries.~~

~~3. The Commission may lay down technical standards for certification mechanisms and data protection seals and marks and mechanisms to promote and recognize certification mechanisms and data protection seals and marks. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).~~

Justification:

The amendment proposed to Article 39(1) would introduce important conditions on certification schemes that would ensure they are widely usable by controllers and processors large and small. Specifically, certification schemes would need to: be voluntary, affordable, be capable of being rolled-out and recognised globally, be neutral as to system, service or technology.

The adoption of delegated and implementing acts for the purposes of data protection certification would create regulatory uncertainty (Article 39 (2) and (3)). Moreover, the express provision regarding the possibility for the Commission to lay down technical standards in this area is too broad and risks endangering the principle of technology neutrality.

By contrast, the view supported by Directive 2002/58/EC, that "no mandatory requirements for specific technical features [should be] imposed on products and services, including terminal or other electronic communications equipment, which could impede the placing of equipment on the market and the free circulation of such equipment in and between Member States", should be maintained.



Article 41: Transfers with an adequacy decision

1. A transfer may take place where the Commission has decided that the third country, or a territory or a processing sector within that third country, or the international organisation in question ensures an adequate level of protection. Such transfer shall not require any further authorisation.
 2. When assessing the adequacy of the level of protection, the Commission shall give consideration to the following elements:
 - (a) the rule of law, relevant legislation in force, both general and sectoral, including concerning public security, defense, national security and criminal law, the professional rules and security measures which are complied with in that country or by that international organisation, as well as effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects residing in the Union whose personal data are being transferred;
 - (b) the existence and effective functioning of one or more independent supervisory authorities in the third country or international organisation in question responsible for ensuring compliance with the data protection rules, for assisting and advising the data subjects in exercising their rights and for co-operation with the supervisory authorities of the Union and of Member States; and
 - (c) the international commitments the third country or international organisation in question has entered into.
 - (3) The Commission may decide that a third country, or a territory or a processing sector within that third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).
- (4) Transfers to the United States of America under HIPAA rules are deemed adequate safeguards.**

Justification:

Many global or European companies have a strong presence in third countries (e.g. in the USA), and have invested in processing capabilities there. Transfer of health data to the USA should be allowed under the HIPAA rules which establish adequate safeguards for privacy. In addition the transfer of anonymized / pseudonymised data should not require further authorization or consultation where the recipient does not reasonably have access to the key and contractual or legal restrictions prohibit re-identification of the data subjects.

Article 44: Derogations

1. In the absence of an adequacy decision pursuant to Article 41 or of appropriate safeguards pursuant to Article 42, a transfer or a set of transfers of personal data to a third country or an international organisation may take place only on condition that:
 - (a) the data subject has consented to the proposed transfer, after having been informed of the risks of such transfers due to the absence of an adequacy decision and appropriate safeguards; or
 - (b) The personal data has been anonymised or pseudonymised, and the key is kept separately from the data.**



- (~~b~~ c) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; or
 - (~~e~~-d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person; or
 - (~~d~~-e) the transfer is necessary for important grounds of public interest; or
 - (e f) the transfer is necessary for the establishment, exercise or defence of legal claims; or
 - (~~f~~-g) the transfer is necessary in order to protect the vital interests of the data subject or of another person, where the data subject is physically or legally incapable of giving consent; or
 - (~~g~~-h) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in Union or Member State law for consultation are fulfilled in the particular case; or
 - (h i) the transfer is necessary for the purposes of the legitimate interests pursued by the controller or the processor, which cannot be qualified as frequent or massive, and where the controller or processor has assessed all the circumstances surrounding the data transfer operation or the set of data transfer operations and based on this assessment adduced appropriate safeguards with respect to the protection of personal data, where necessary.
2. A transfer pursuant to point (g) of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. When the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.
 3. Where the processing is based on point (h) of paragraph 1, the controller or processor shall give particular consideration to the nature of the data, the purpose and duration of the proposed processing operation or operations, as well as the situation in the country of origin, the third country and the country of final destination, and adduced appropriate safeguards with respect to the protection of personal data, where necessary.
 4. Points (b), (c) and (h) of paragraph 1 shall not apply to activities carried out by public authorities in the exercise of their public powers.
 5. The public interest referred to in point (d) of paragraph 1 must be recognised in Union law or in the law of the Member State to which the controller is subject.
 6. The controller or processor shall document the assessment as well as the appropriate safeguards adduced referred to in point (h) of paragraph 1 of this Article in the documentation referred to in Article 28 and shall inform the supervisory authority of the transfer.
 7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying 'important grounds of public interest' within the meaning of point (d) of paragraph 1 as well as the criteria and requirements for appropriate safeguards referred to in point (h) of paragraph 1.

Justification:

As per article 44



Article 64: European Data Protection Board

1. A European Data Protection Board is hereby set up.
2. The European Data Protection Board shall be composed of the head of one supervisory authority of each Member State and of the European Data Protection Supervisor.
3. Where in a Member State more than one supervisory authority is responsible for monitoring the application of the provisions pursuant to this Regulation, they shall nominate the head of one of those supervisory authorities as joint representative.
4. The Commission shall have the right to participate in the activities and meetings of the European Data Protection Board and shall designate a representative. The chair of the European Data Protection Board shall, without delay, inform the Commission on all activities of the European Data Protection Board.
- 5. The Industry shall have the right to participate in the activities and meetings of the European Data Protection Board and shall designate a representative. Industry should provide technologically neutral guidance regarding safeguards for personal data processing.**

Justification:

Industry participation in the Board will provide guidance to develop scalable, technologically neutral guidance regarding safeguards for personal data processing.

Article 77: Right to compensation and liability

1. Any person who has suffered damage as a result of an unlawful processing operation or of an action incompatible with this Regulation shall have the right to receive compensation from the controller ~~or the processor~~ for the damage suffered.
2. Where more than one controller ~~or processor~~ is involved in the processing, each controller ~~or processor~~ shall be jointly and severally liable for the entire amount of the damage, **to the extent that liability has not already been established in the determination of responsibilities envisaged in Article 24.**
- 3. If a processor processes personal data other than as instructed by the controller, they may be held liable should any person suffer damage as a result of such processing.**
- 4. In case of joint controllers,** one controller ~~or the processor~~ may be exempted from this liability, in whole or in part, if the controller ~~or the processor~~ proves that they are not responsible for the event giving rise to the damage.

Justification:

Under the current Directive, liability is correctly attributed to the data controller. Essentially, they direct the data processor and if the processor does not act on those orders then contractual arrangements apply to address the circumstances. Introducing a vague liability clause does not clarify the current situation but creates confusion for controllers, processors and data subjects alike.

Article 81: Processing of personal data concerning health

1. Within the limits of this Regulation and in accordance with point (h) of Article 9(2), processing of personal data concerning health must be on the basis of Union law ~~or Member State law~~ which shall provide for suitable and specific measures to safeguard the data subject's legitimate interests, and be necessary for:



- (a) the purposes of preventive or occupational medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject to the obligation of professional secrecy or another person also subject to an equivalent obligation of confidentiality under Member State law or rules established by national competent bodies; or 'or another person who has committed to confidentiality by contract with his employer'.
 - (b) reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety, inter alia for medicinal products or medical devices; or
 - (c) other reasons of public interest in areas such as social protection, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system **and the provision of health services.**
2. Processing of personal data concerning health which is necessary for historical, statistical or scientific research purposes, such as patient registries set up for improving diagnoses and differentiating between similar types of diseases and preparing studies for therapies, is subject to the conditions and safeguards referred to in Article 83.
 3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying other reasons of public interest in the area of public health as referred to in point (b) of paragraph 1, as well as criteria and requirements for the safeguards for the processing of personal data for the purposes referred to in paragraph 1.

+ new recital:

The principles of data protection should take context into consideration and should recognise the need for medical equipment manufacturers to maintain medical systems and devices with the support of technicians or engineers, provided they have been trained on the confidentiality of 'data concerning health', have signed a commitment of confidentiality by contract with their employer and third parties and remote maintenance security rules are in place. Manufacturers are also consulted by healthcare providers to advice on radiation dose for medical images on the basis of the patient age, weight, medical condition, etc. The Regulation should facilitate such scenarios. The principles of data protection should also take obligations under other legal frameworks into consideration and should recognize the obligation for medical equipment manufacturers to collect clinical data to evaluate the performance of said medical equipment/devices³.

Justification:

Processing of personal data should be based on Union law only. The reference to Member States in 81.1 laws undermines the harmonisation brought by the Regulation and could impose additional or conflicting requirements in the context of "safeguarding the data subject's legitimate interests".

The proposed exemption for processing data concerning health of Article 81 does not take into account registry studies for the improvement of medical devices or medical services, like eHealth services, effectively making it impossible for companies to meet regulatory requirements under the medical devices regulation. The analysis of health data should be authorized for professionals who are not healthcare professionals, but have been trained to privacy and have a signed a commitment to secrecy (e.g. laboratory agents, workers in a telemedicine service, etc). The same logic applies for the

³This last statement falls is anonymised data are not covered by the Regulation.



technical maintenance (remote or onsite) of medical devices, which is carried out by technicians (not by healthcare professionals).

Article 83: Processing for historical, statistical and scientific research purposes

1. Within the limits of this Regulation, personal data may be processed for historical, statistical or scientific research purposes only if:
 - (a) these purposes cannot be otherwise fulfilled by processing data which does not permit or not any longer permit the identification of the data subject;
 - (b) data enabling the attribution of information to an identified or identifiable data subject is kept separately from the other information as long as these purposes can be fulfilled in this manner.
- 2. *Within the limits of this Regulation, personal data may be processed for the purposes of manufacturer's regulatory pre- and post-market obligations with respect to clinical evaluation of medical devices*⁴.**
- 3. ~~2.~~** Bodies conducting historical, statistical or scientific research may publish or otherwise publicly disclose personal data only if:
 - (a) the data subject has given consent, subject to the conditions laid down in Article 7;
 - (b) the publication of personal data is necessary to present research findings or to facilitate research insofar as the interests or the fundamental rights or freedoms of the data subject do not override these interests; or
 - (c) the data subject has made the data public.
- 4. ~~3.~~** The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the processing of personal data for the purposes referred to in paragraph 1 and ~~2~~ **3** as well as any necessary limitations on the rights of information to and access by the data subject and detailing the conditions and safeguards for the rights of the data subject under these circumstances.

Justification:

The regulation should take into account the obligations for manufacturers under the medical devices Regulation to perform registry studies and post-marketing follow-up studies with respect to medical devices.

⁴ *This amendment falls is anonymised data are not subject to the Regulation.*



COCIR Contribution to the General Data Protection Regulation¹ ***To the attention of Members of the European Parliament and Representatives of EU Member States***

COCIR represents the European Medical Diagnostic Imaging, Electromedical and Healthcare ICT Industry. Our members offer many technologies that support the safe, fast and seamless transfer of medical data to support quality healthcare.

COCIR supports an effective, clear and reliable data protection framework and welcomes the attempt to harmonise the legal framework through the adoption of a regulation. COCIR also recognises considerable improvements in the provisions for data concerning health. However COCIR recalls that quality healthcare depends on the availability of comprehensive health data at the point of care and throughout the healthcare cycle. COCIR feels some provisions could restrict the availability of health data, delay innovation, create legal uncertainty and increase compliance costs. We therefore recommend that the following aspects of the regulation be considered:

COCIR main recommendations:

1. Recognise that data which does not identify a data subject is not personal data (Art. 4)
2. Keep obligations of controllers and processors separate as per current regime (Art. 24-26-77)
3. Reduce administrative burden between Data Controller and Data Processor (Art. 26)
4. Allow processing of data concerning health by technicians and engineers for technical maintenance and equipment performance evaluation under adequate conditions (Art. 81-83)

COCIR secondary recommendations:

1. Extend the exemption to the right to be forgotten to healthcare data (Art. 17)
2. Allow the secondary use of anonymised and pseudonymised data for health purposes (Art. 20)
3. Delete privacy by design and privacy by default obligations (Art. 23)
4. Consider context and feasibility for Data Breach notifications (Art. 31-32)
5. Ensure data protection impact assessments and pre-authorisation obligations for 'high-risk' processings take account of the context and are not 'one size fits all' (Art. 33 - 34)
6. Keep certification industry led and voluntary for more efficiency (Art. 39)
7. Recognise compliance with non-EU frameworks, e.g. HIPAA Privacy and Security Rules, in the U.S., as adequate safeguard for transferring data beyond EU borders (Art. 42)
8. Allow the transfer of anonymised, pseudonymised and encrypted data to a third country, without further regulatory authorisation, where re-identification is not possible either via restrictive contractual obligation(s) or via technical means (e.g. no key accessible to re-identify data) (Chapter V)
9. Introduce proportionality to Administrative Sanctions (Art. 79)
10. Limit the number and scope of delegated acts for more legal certainty:
 - a. Ensure technical neutrality of delegated acts
 - b. Provide for industry consultation or direct participation in the drafting of delegated acts
 - c. Provide timeline for the adoption of remaining delegated acts

¹ http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf



DETAILED BRIEFING

I. The sharing of health data increases patient safety, allows innovation and advancement in healthcare technologies, and facilitates medical research

- **Facilitating access to information and timely, collaborative decision-making:** Healthcare delivery in modern hospitals is a highly complex, labour-intensive activity. A large institution will have over 10,000 medical devices, each collecting different identifiable data elements contributing to the medical record. Behind every episode of care, there could be twenty to fifty persons who come into contact with one or more element of the medical record (nurse, laboratory specimen transport, laboratory technician, pathologist, pathology resident, clinical physician, intern, medical student, resident, primary care physician, physician office, physician practice administrator, etc.) - all with the common goal of improving patient health. Within and beyond the hospital environment, the electronic health record is fast becoming an essential requirement for modern, efficient and safe healthcare systems, linking all parts of the system to the patient. Appropriately controlled access to the health record is essential for primary and secondary care providers, pharmacies, some social care providers and the rapidly expanding area of home-healthcare where patients can be managed and monitored in their own homes.
- **Serving public health interests and leveraging the value of patient registries:** Patient registries are today's primary tool to systematically identify statistical correlations that indicate potential approaches to new ways of therapy. Patient registries are therefore invaluable for improving diagnoses, differentiating between similar types of diseases and preparing studies for therapies. High quality record capture procedures ensure comparability of findings. Studies with large numbers of patients ensure repeatability of findings. Both are cornerstones of scientific work in modern medicine. It has to be noted, that for certain diseases and for certain types of healthcare facilities, the use of clinical registries is already required by national legislation and with the growing use of Electronic Health Record, the future ability of countries to introduce large-scale, population-level data analysis for medical and health trends will increase.
- **Benefits of advancements in Telemedicine:** There is a major shift underway in the practice of medicine and healthcare enabled by technologies that allow remote patient management. Video and computer enabled consultations and diagnosis, in-home patient monitoring, referral of diagnostic images and laboratory reports, etc., for remote examination and expert analysis are increasing, globally. Use of these innovations cuts unnecessary patient travel, best utilizes limited professional resources and drives efficiencies in healthcare delivery-and all rely on the exchange of patient data, including transfer of relevant data outside of the country of origin.



II. Expected Impact of the Proposed General Data Protection Regulation on the Healthcare Sector

The Commission's goal of enhancing the single market by increasing harmonisation of data protection rules across the 27 Member States is to be welcomed. However the benefits of harmonisation are at risk of being outweighed by a number of measures that would result in delaying innovation, creating legal uncertainty, increasing compliance cost for industry and imposing significant burdens on healthcare providers. For eHealth and related domains that seek to innovate and continue to increase quality of care, challenges remain and new ones have emerged. While not an exhaustive list of the healthcare industry's concerns, COCIR seeks to address a select few issues, as follows:

A – COCIR main recommendations

1. Recognise that data which do not identify a data subject are not personal data (Art. 4)

The proposed definitions of Personal Data and Data Concerning Health are too broad and may result in overly-burdensome requirements.

The proposed Regulation defines "personal data" very broadly, as "any information relating to a data subject," including "an identification number, location data, online identifier." This definition fails to provide legal clarity and should explicitly require that context be taken into account in determining whether data identifies a data subject. Indeed, recitals 23 and 24 already recognise that context is a relevant factor, and that data which do not identify a data subject (e.g. the serial number of a device for the provision of telemonitoring in the home) are not personal data; this should be reflected explicitly in the definitions.

Article 4(12), on the other hand, defines "data concerning health" as "any information which relates to the physical or mental health of an individual, or to the provision of health services to the individual." The inconsistent reference to "an individual," a concept that is not defined in the Regulation, as opposed to a "data subject," should be removed. This inconsistency would turn data that relate to "an individual" but do not personally identify a data subject into sensitive data requiring heightened protection under Article 81.

For instance, a telemedicine service provider may decide to outsource the maintenance of its medical devices to an external company. This company would need select information on the devices, such as serial numbers, in order to monitor their status, even though said information does not per se identify the individual. Considering the serial number of a device as personal data, or data related to the provision of health services to an individual, would bring additional burdens without improving patient privacy.

Moreover, following from Recital 23, the Regulation should expressly recognise in the definitions the category of "anonymised data." Anonymised data would be defined as personal data processed so as to render natural persons no longer identifiable. When personal data are processed with the sole purpose of rendering them anonymous and/or pseudonymous, the provisions of the proposed Regulation should not apply, with the exception of section 2 relating to data security.



Recommendations:

- In the definition of "personal data," recognise the importance of context in determining whether data identify a data subject.
- In the definition of "data concerning health," replace "individual" with "data subject".
- Add a definition for "anonymised" and "pseudonymised" data.
- Article 4 should explicitly recognise that data which cannot link to the data subject (e.g. anonymised data), data which are not directly associated to a data subject (e.g. technical data) or data which require unreasonable time and effort to identify a data subject (e.g. pseudonymised data) are not personal data and are not subject to the Regulation.

2. Keep obligations of controllers and processors separate as per current regime (Art. 24-26-77, etc)

New independent obligations on processors, which would create confusion as to obligations and responsibility between controllers and processors, should be reconsidered in favour of better applying existing requirements.

If independent obligations are placed on processors they will have a duty to better understand the information they process as opposed to relying on representation by the controller. That defeats the concept of data minimization as more entities will need to know more detail about data subjects. Furthermore uncertainty is increased if processors have to determine whether instructions of controllers are compatible with their interpretation of individual requirements. The relation with data subjects is established and maintained by controllers and this is why the existing legal framework foresees direct responsibilities for controllers whilst the responsibilities of processors are left to be determined bilaterally between controllers and processors depending on the circumstances.

Recommendation:

- Maintain the approach of the existing legal framework in Directive 95/46/EC. This would promote clarity as well as better enforcement from the point of view of the relationship with supervisory authorities.



3. Reduce administrative burden between Data Controller and Data Processor (Art. 26 - d)

Requiring each Data Controller (healthcare provider organisation) to agree, individually, to each sub-processor enlisted by a Data Processor (eHealth service provider) would introduce excessive administrative burden and increase costs to both the data controller and data processor.

Article 26 (d) provides that a *data processor* may enlist a *sub-processor* only with prior permission of the *data controller*. A Medical device manufacturer/service provider seeking to enlist a third-party processor to engage in, for example, data mining, data destruction or data storage services acts as *data processor*. Based on the text of the Proposed Regulation, each *data controller* (healthcare provider) would have to agree to such sub-processing. This would introduce excessive administrative burden to both the data controller and data processor, including, significant additional costs. The better approach would be a set of pre-determined conditions within a contract under which the *controller* agrees to allow the *data processor* to enlist the services of a *sub-processor*, this would also preclude inefficiencies caused by disparate opinions where more than one data controller is involved (e.g. data processor B provides services to many data controllers, and may enlist the services of a sub-processor).

Recommendation:

- Maintain the approach of the existing legal framework in Directive 95/46/EC.

4. Allow processing of data concerning health by technicians and engineers for technical maintenance and equipment performance evaluation under adequate conditions. (Art. 81 and 83)

The proposed exemption for processing data concerning health of Article 81 and 83 does not take into account maintenance of medical equipment by manufacturers and registry studies for the improvement of medical devices or medical services, like eHealth services effectively making it impossible for companies to meet regulatory requirements under the medical devices regulation.

Article 81.1(a) provides that data concerning health may be processed by a healthcare professional or a professional with an equivalent obligation of professional secrecy. It is not clear whether this provision covers technicians and engineers employed by manufacturers, who may have access to data concerning health when maintaining medical systems, either onsite or remotely. The regulation should clarify that professionals who have signed a commitment of confidentiality by contract with their employer qualify as '*professionals with an equivalent obligation of professional secrecy*'.

The current envisaged regulation that will replace the Active Implantable Medical Devices Directive and the Medical Devices Directive will put emphasis on manufacturer obligations to perform registry studies and post-marketing follow-up studies with respect to medical devices. It is unclear whether the exemption in Article 81(1) can facilitate such studies, as all data processing would need to take place by healthcare professionals. This presents



obstacles for healthcare industry relying on contractual obligations to meet the heightened confidentiality obligations imposed by the Regulation².

Article 81(b) and (c) only apply in cases of 'public interest', of which it is unclear that these would apply in the case of a manufacturer seeking to meet its regulatory obligations to improve its medical device.

The exemption in Article 81 (1) will also prevent the rapid roll out of e/mHealth services in Europe as it requires data acquired in "preventive or occupational medicine, medical diagnosis, the provision of care or treatment or the management of health-care services" to be processed by healthcare practitioners (HCPs). Manufacturers and eHealth providers implement security measures at HCPs request and follow highest standards in their commercial practices. The result of requiring the additional HCP secrecy criterion, on top of existing security obligations, would impede the provision of quality m/eHealth services or to analyze health data without involving an HCP in the process.

Examples from other regions, e.g. U.S. HIPAA rules, could ease the reflection.

Recommendations:

- Extend article 81.1 (a) to professionals who have signed a commitment of confidentiality by contract to enable the maintenance on medical equipment by manufacturers.
- Extend to Article 81 (c) to "and services in the health insurance system and the provision of health services."
- Provide guidance/clarification on "public interest."
- Clarify that the processing "for historical, statistical or scientific research purposes" in the meaning of Article 83 includes processing for the purposes of the manufacturer's regulatory pre- and post-market obligations with respect to clinical evaluation of a medical device, by clear guidance.

² This concern falls if anonymised data are not subject to the Regulation.



B – COCIR secondary recommendations

1. Extend the exemption to the right to be forgotten to healthcare (Art. 17)

Implementing the right to be forgotten and to erasure in healthcare requires careful consideration of the consequences. Deleting data from an electronic health record does not effectively protect individual privacy, and furthermore, can run counter to patient safety, public interest, health research, and eHealth deployment.

Under the proposed Regulation, Article 17, a patient can ask for the deletion of data in his electronic health record. Article 17.3(b) sets forth an exception to the “right to be forgotten” where retention of personal data is necessary for “reasons of public interest in the area of public health in accordance with Article 81” and for “historical, scientific research purposes, in accordance with Article 83.” But it remains unclear to what extent this exception applies. Clarifying the scope for the exception is crucial, as deleting data from electronic health records poses a number of problems:

- Patient safety: Deleting all or parts of the information contained in an electronic health record would undermine the ability of medical professionals to treat the patient effectively. In Germany the ‘Lipobay’ episode revealed that many serious drug interactions could have been avoided if general practitioners had had access to information on drugs prescribed by specialists (e.g. interactions between Viagra and lowering blood pressure drugs). The Regulation should foresee at minima a mechanism to inform patients on the potential consequences of blocking access to or deleting data in their electronic health record.
- Medical professionals’ liability: Clinicians might object to the deletion of data for liability issues: in case of investigation clinicians need to refer to the electronic health record to justify their decisions and treatment delivered. For example German doctors are obliged to keep records for thirty years.
- Risks to health research: Statistical analyses will be “depowered” if data is deleted (particularly in the case of orphan diseases or conditions with difficult inclusion and exclusion criteria, such as paediatric). Further, this may mean that clinical trials and clinical investigations will be conducted outside Europe to avoid any such risk.
- Technical feasibility: Deleting data from an electronic health record may be technically challenging and costly:
 - Medical records are traced in logs. Logs might contain patient information. Browsing through logs to delete information elements could be a very lengthy and costly procedure.
 - Information elements are regularly extracted from the health record for various clinical activities. Each of these derived information elements constitutes distributed traces that take a variety of forms given the clinical activities performed. Thus they are difficult and sometimes impossible to track electronically.
 - The health record or parts of the record may be copied by a medical professional, or by the patient himself. Depending on the number of copies and the location of the copied information, tracking each copies of the record and deleting all copies automatically is almost impossible. For instance, a



patient may have copied his medical file on the Cloud or on his personal computer without the Data Controller knowing or having access to these systems for erasure. In addition, Article 17 requires that the controller have full control over all kind of installed (third party) subsystems. This is not realistic in a healthcare environment.

- Organisational feasibility: The regulation lacks clarity as to which healthcare provider/professional involved in the patient's care—where each contributes in some fashion to the EHR—is ultimately responsible for deleting the data.
- Contradiction with national eHealth programmes: Deleting data from electronic health records runs counter to the foundations of national eHealth platforms and health information exchange infrastructures in which governments are investing large amounts of public money in many European countries. Ministries of health leading eHealth programmes should be consulted and informed of the potential consequences of the right to be forgotten in an EHR context.

Recommendation:

- Clarify Article 17.3(b) exception to the erasure of personal data in the case of healthcare, or specify such exception with respect to electronic health records.

2. Allow the secondary use of anonymised and pseudonymised data for health purposes (Art. 20)

As formulated now Article 20 will become an obstacle to many existing practises with respect to secondary use of data in the health environment.

Health research, particularly in the areas of health services, population and public health, critically depends on the availability of existing data about people. However, most of this data can be anonymised and/or pseudonymised to serve the purpose.

COCIR is concerned about Article 20 not providing a distinction between data processing that identifies an individual and data processing that does not. As currently drafted, Article 20 - which uses the term "natural person" rather than "data subject," seems to broaden the overall scope of the regulation even further by not focusing on personal information and what would constitute a risk for the data subject. We believe profiling techniques per se do not need special regulatory treatment given the many safeguards introduced in the draft Regulation especially when incentives are provided for companies to anonymise and/or pseudonymise data. The current text of Article 20 might render legitimate use of data for health research impossible with great consequences for the social benefits in this area.

Recommendation:

- Delete Article 20 or, alternatively, revert to the language currently in force under Article 15 of the Directive 95/46/EC.

3. Delete privacy by design and privacy by default obligations (Art. 23)



The introduction of the concepts of 'privacy by design' and 'privacy by default' in the Regulation lack legal clarity and runs counter the principle of technology – neutrality.

COCIR believes the usefulness of introducing the concepts of “privacy by design” and “privacy by default” into legislation is dubious. These concepts are still being discussed internationally, and mean different things to different people – they are probably more effective as a policy or marketing, rather than legal, tool.

It is certainly true that organizations should consider the privacy implications of their products and services, both to meet users’ expectations and needs and to comply with the relevant legislation. But the actual way it does so should remain flexible and leave room for adaptation based on each organization’s business model, size and interaction with personal data. Industry-led innovation in this area will create trust and allow for innovative solutions, services and technologies.

Introducing a separate legal obligation, by contrast, would be superfluous. In particular, it would seriously risk running counter to the principle of technology neutrality, notably if technical standards are mandated as proposed in the draft text. General-purpose legislation such as the proposed data protection Regulation should be strictly technology-neutral – it should not introduce specific technology or operational mandates, nor contribute to a differentiation between ICT and other economic sectors

Recommendation:

- Remove the concepts of “privacy by design” and “privacy by default” (Article 23) from the Regulation, together with the corresponding recitals (61). Alternatively, remove paragraphs 3 and 4 on delegated and implementing acts from Article 23 and allow for fully industry owned and led measures.

4. Consider context and feasibility for data breach notifications (Art. 31 & 32)

The scope of definition of breach and associated notification requirements, especially the concepts of reasonable timeframe and mitigating effects of safeguards (encryption etc) and potential for harm/adverse impact pose issues of practicability and undue burden. Specific problems in the breach notification requirements include the over-inclusive definition which includes inadvertent access to information within the organization by organization staff as well as the contemplated 24 hours for response/reporting. Breach notification requirements should be risk-based so that they apply only to sectors and/or data types where individuals face a real risk of harm in the event of a breach.

Recommendation:

- Recognise that 24 hours is not sufficient to acknowledge a data breach, analyse it and be able to notify it.
- Adopt a two step approach: require initial breach notification within a reasonable time frame, but allow additional time as necessary to submit the requested information as per current requirements for medical devices. This will allow more time for a qualitative impact assessment, and efficient corrective and mitigation actions.



5. Ensure data protection impact assessments and pre-authorisation obligations for 'high-risk' processings take account of the context and are not 'one size fits all' (Art. 33 – 34)

Impact Assessments should not be standardized. Different types of organizations may have equally effective means of performing such assessments, and unnecessary constraints may hinder improvements in the process, as technologies emerge, and contexts change. Further, consultation with authorities will prove overly burdensome in the context of healthcare, unless the Data Protection Officer has some decision-making authority based on the level of risk involved in the processing activity. This level of risk should be further defined, and a threshold set for when consultation with authorities is required.

Article 33 requires that the processing of personal data relating to health as well as processing of genetic data is subject to the data protection impact assessment requirement. The criteria for impact assessments are not yet clear (as the Commission may clarify them by implementing act under Article 33 (6)). While clarity is crucial to understanding under precisely what circumstances assessments are required, it is equally important that the processes used by varying types or organizations (medical device manufacturers, IT service providers, eHealth service providers, healthcare provider organizations, etc.) are not constrained by specifications under implementing acts. Industry notes that Data Protection Impact Assessments are already implemented by industry in varying forms.

Given that processing activities are often different, impact assessments should not be "one-size-fits-all," rather they should be relative to the scope of processing, volume and type of data, and organizational aspects of those entities performing the assessments.

In addition, while Article 34 provides for a prohibition to start the data processing before approval of the impact assessment, it does not specify timelines for processing of requests by national authorities. Legal certainty as to when a decision can be expected on the adequacy of impact assessment is crucial for stakeholders. Divergence between practices and procedure in this regard between member states will cause forum shopping and the divergences that were amongst the important reasons for the drafting of the Proposed Regulation (see Recitals 7 and 8).

Recommendations:

- Data Protection Impact Assessment should not be mandatory, but should be part of the accountability scheme which can be audited, for instance as part of a certification.
- The regime should allow organizations to construct their own assessment, based on their specific type of organization, legal requirements, contractual obligations, and, where appropriate, internal policies. These assessments should be relative to the scope and types of processing activities, and performed based on a more well-defined category of "high-risk" activity.
- Prior consultation should not be needed when processing is based on consent or contract. Where approval is required (Article 34), a clear time line for the approval should be clarified prior to effective dates.



6. Keep certification industry led and voluntary for more efficiency for more efficiency (Art. 39)

Certification mechanisms, data protection seals and marks, and similar frameworks developed and managed by industry should be favoured. They should remain industry-led as per current practice, and not via delegated acts, implementing acts and technical standards.

The certification process generally applicable in the EU should not be altered in the case of data protection. The current conformity mark procedure provides for full industry participation and the necessary legal certainty for companies both inside and outside the EEA³ to be able to operate in the EU. A certification mechanism developed and managed by industry, with regulators having backstop regulatory authority, helps to improve trust while reducing compliance burdens and fostering competitiveness.

An alteration of the said framework through the adoption of delegated and implementing acts for the purposes of data protection certification, as proposed by the draft Regulation, would create regulatory imbalance and uncertainty. Moreover, the express provision regarding the possibility for the Commission to lay down technical standards in this area is too broad and risks endangering the principle of technology neutrality.

By contrast, COCIR strongly supports the view, incorporated in Directive 2002/58/EC, that “no mandatory requirements for specific technical features [should be] imposed on products and services, including terminal or other electronic communications equipment, which could impede the placing of equipment on the market and the free circulation of such equipment in and between Member States.”

Recommendation:

- Remove paragraphs 2 and 3 on delegated and implementing acts in Article 39.
- Rather than creating yet another certification scheme, authorities should consider promotion and adoption of existing and established frameworks (e.g. ISO/IEC 27001) which have proven efficient.
- The legal framework should provide for mutual recognition of national seals/certification schemes in the healthcare sector.

7. Recognise compliance with non-EU regulatory frameworks, e.g. HIPAA Privacy and Security Rules in the U.S., as adequate safeguard for transferring data beyond EU borders (Art. 42)

Consider HIPAA rules as adequate safeguard for transfer of health data to the USA.

Medical devices companies and companies providing eHealth services are often not only active in the EU and may need to process personal data of EU data subjects in third countries that may or may not have an adequacy finding in order to avoid to have to

³ European Economic Area



duplicate processing means that are already available outside the EU. Many of COCIR's members, for example, have a strong presence in the US and may have invested in processing capabilities there. In this context, it should be noted that HIPAA is a tested and validated set of rules for the processing of health data in the US. HIPAA compliance could provide a mechanism similar to the adequacy findings for the current DOC Safe Harbour Certification as an adequacy finding for the export of personal data in the health field.

Recommendation:

- Recognize HIPAA compliance as "a processing sector within that third country [which] ensures an adequate level of protection within the meaning of [EU rules on adequacy finding for export of personal data]" in Article 41 (3).

8. Allow the transfer of anonymised, pseudonymised and encrypted data to a third country, without further regulatory authorisation, where re-identification is not possible either via restrictive contractual obligation(s) or via technical means (e.g. no key accessible to re-identify data) (Chapter V).

The transfer of anonymised data should not require any further authorisation or consultation where the recipient does not reasonably have access to the key and contractual or legal restrictions prohibit re-identification of the data subjects.

Anonymised⁴ and pseudonymised⁵ data which do not reasonably permit re-identification of a data subject, and encrypted data⁶ which do not permit understanding of the information, are central to many data processing operations. Responsible data controllers and processors have invested heavily in a raft of data processing techniques to prevent the identification of data subjects and protect user privacy. These efforts should be recognised and encouraged.

Recommendation:

- Add anonymisation and pseudonymisation as recognised means for appropriately safeguarding personal data prior to transferring it to a recipient located in a third country. A transfer of anonymised data, while the key stays within the EU, should not require any further regulatory authorisation.

⁴ Previously identifiable data that have been de-identified and for which a code or other link no longer exists. An investigator would not be able to link anonymised information back to a specific individual.

⁵ Pseudonymisation, a Privacy Enhancing Technology (PET), is essentially the replacement of Personally Identifiable Information (PII) – such as name, address or account number – with pseudonyms. Key-coded data are a classical example of pseudonymisation. Personally Identifiable Information (PII) is earmarked by codes, while the link between the code and the PII (like name, date of birth, address, etc.) is kept separately.

⁶ Encrypted data is information that has been transformed and made unreadable by the use of algorithms. Only those with the key can decrypt the data.



9. Introduce proportionality to administrative sanctions (Art. 79)

While there is a general recognition of the need to enhance credible enforcement mechanisms, specifically sanctions and fines, the current proposal lacks proportionality and measurable criteria for legal clarity to prevent primarily a controller and if established secondly the processor as its representative.

This may result in making the EU less competitive in attracting investment in facilities or services. Furthermore the mandatory nature of the fine may not allow mitigating safeguards and the context of the acts to be properly taken into account.

The proposed regulation text currently lacks clarity and remains vague: A few concepts require clarification e.g. 'negligently', 'incomplete information', 'sufficiently transparent manner', 'does not take all necessary steps'.

Furthermore it is not clear who has the burden of proof for the following new obligations.

- Article 79/5 (b) refers to data subject's right of access (Article 15). Who has the burden of proof that a data subject obtained access or received information from the controller? (E.g. in case the request sent by email did not reach the controller.)
- Article 79/5 (c) refers to the right to be forgotten and to erasure (Article 17) and implies that all third parties are known to the Data Controller, which is not always the case (see comments on Article 17). In the context of electronic health records, whose obligation is it to make sure that all "known" data are erased? How to ensure that all third parties publication is known?
- Article 79/5 (d) refers to the right to data portability (Article 18) but does not consider security aspects in controller/processor systems.

Recommendations:

- Propose administrative fines that are reasonable and proportional to the harm caused. Administrative fines should not be purely punitive but should encourage organisations to take all necessary steps to avoid repetition of similar situations.
- Add further clarity in the regulation text or provide guidance to clarify those terms to avoid disproportionate imposition of fines.

10. Limit the number and scope of delegated acts for more legal certainty

The number and scope of delegated acts in the proposed Regulation may undermine legal certainty of existing provisions and introduce too much specificity in requirements or implementation methodologies. Guidance on principle or framework level is useful, but limitations on choice of standards and additional certification mechanisms and processes will needlessly constrain cost-effective, scalable implementation of technological and organizational solutions. The number of delegated acts should be reduced, and clear timelines should be introduced for those delegated acts that remain.

A few examples:



11. Article 14(7) empowers the European Commission to adopt delegated acts to specify the criteria for categories of recipients of personal data. In a healthcare environment, categories of recipients of data vary, depending on healthcare provider or eHealth service provider practices, organizations, and workflows. It should remain under the power of these actors considering the case reference as required. The European Commission adopting prescriptive delegated acts (Article 14(7)) is not the right approach as it will delay the process and reduce flexibility in healthcare settings.
12. Article 30(4) – Security of Processing, allows the Commission to adopt implementing acts for specifying the requirements to prevent unauthorized access, disclosure, reading, copying, modification, erasure or removal of personal data. Care must be taken that any specifications pertaining the security requirements for processing personal data are technologically neutral, flexible, scalable and most important, applicable to the type of data being processed, the context for the data processing, and the potential implications to the processing activities. In the healthcare context, highly secure transmission and storage of data is desirable, however, access controls must be respectful of the need to access data in the provision of care, serviceability of medical devices and healthcare technology, etc.
13. Article 81–Processing of personal data concerning health—provides that the processing must be on the basis of Union *or* Member State Law—laws that could impose additional or conflicting requirements in the context of “safeguarding the data subject’s legitimate interests.” It is imperative that appropriate care be taken to ensure that those measures, criteria, requirements, etc., provided for either by Commission adoption of delegated acts (per 81.3) or by Member State law (81.1) be technology, service and business model neutral, industry-based, flexible, and appropriate to support innovation and technological advancement in the healthcare industry. In addition, additional or supplemental requirements must not impede the fulfilment of regulatory obligations under other EU legislation, such as the Medical Devices Directive.

Recommendations:

- Modify Article 14(7) to ensure that the identification of categories of recipients of data remains under the control and the responsibility of healthcare providers and/or eHealth service providers in a healthcare environment.
- Modify Article 81.1 as follows:
81.1 – ...must be on the basis of Union law ~~or Member State law~~ which shall provide for suitable and specific measures to safeguard the data subject’s legitimate interests (...).
- Seek healthcare industry input via direct inclusion of industry on the Board per Article 64(3), or at a minimum via regular consultation to develop scalable, technologically neutral guidance regarding safeguards for personal data processing. Consider industry-specific approach, taking into account the individuals’ interest in safe, secure, timely and quality care.



COCIR Position Paper on the General Data Protection Regulation¹

COCIR represents the European Medical Diagnostic Imaging, Electromedical and Healthcare ICT Industry. Our industry offers many technologies that support the safe, fast and seamless transfer of medical data to support quality healthcare.

COCIR supports an effective, clear and reliable data protection framework and welcomes the intent to harmonise the legal framework at European level through the adoption of an EU regulation. COCIR also recognises considerable improvements in the provisions for data concerning health. However COCIR recalls that quality healthcare depends on the availability of comprehensive health data at the point of care and throughout the healthcare cycle. COCIR feels some provisions could restrict the availability of health data, delay innovation, create legal uncertainty and increase compliance costs. We therefore recommend that the following aspects of the regulation be considered:

COCIR's main recommendations to improve the General Data Protection Regulation:

1. **Clarify definitions** (Art. 4): The use of anonymised, pseudonymised or key-coded data by the healthcare and research sectors should be facilitated by the Regulation. Article 4 should recognise that data which cannot identify the data subject (e.g. anonymised data); data which are not directly associated to the data subject (e.g. technical data) or data which require unreasonable time and effort to identify the data subject (e.g. pseudonymised data) are not personal data and are not subject to the Regulation.
2. **Maintain clear and separate responsibilities between the healthcare provider and the medical technology provider**, as per the current regime (Art. 28- 33- 34- 77). The relationship between the healthcare provider and the medical technology provider should be managed by contract, not by law.
3. **Reduce administrative burden** (Art. 26): In an environment where outsourcing is part of the business model and care delivery, seeking approval of the healthcare provider before enlisting other medical technology providers generates administrative burden on both sides, without bringing benefits to privacy.
4. **Allow processing of data concerning health by medical technology manufacturers for maintenance and equipment performance evaluation purposes** (Art. 81 - 83): Professionals employed by medical technology manufacturers (technicians, engineers, medical professionals), should be able to access data concerning health for technical maintenance and equipment performance evaluation.

¹ http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf



DETAILED BRIEFING

COCIR believes the following provisions could be improved to add legal clarity, legal certainty and ensure feasibility in a healthcare environment.

The following detailed briefing includes additional information substantiating the four critical recommendations (Part A) articulated above as well as secondary recommendations (part B).

A - COCIR main recommendations

1. Clarify definitions (Art. 4)

The proposed definitions for '*Personal Data*' and '*Data Concerning Health*' are too broad. The Regulation should cover only data that can lead to the identification of a data subject. For instance the serial number of a medical device may be considered 'data concerning health' although it is associated to a medical equipment and not to a data subject.

- **Anonymised** data cannot be linked to the data subject and should be explicitly excluded from the scope of the Regulation.
- Other data that are not directly associated to the data subject, and that cannot identify the data subject without unreasonable time and effort should also be explicitly excluded from the scope of the Regulation:
 - **Pseudonymised** data are data where personally identifiable information (PII) - such as name, date of birth, address or account number - has been replaced with a code. An investigator would not be able to link anonymised information back to a specific data subject provided the link between the code and the PII is kept separately.
 - **Technical data** are data directly associated to medical equipment (e.g. serial number of a medical device) but are not directly associated to a data subject. An investigator would not be able to link technical information back to a specific data subject without unreasonable time and effort.

2. Maintain clear and separate responsibilities between the healthcare provider (data controller) and the medical technology provider (data processor) (Art. 24-26-77)

The new obligations on processors create confusion around responsibility between healthcare provider (data controllers) and medical technology provider (data processors). Responsibilities and liabilities between the controller and the processor need to be handled through contractual arrangements, not through law.

COCIR recommends keeping the approach of the existing legal framework in Directive 95/46/EC. This would promote clarity as well as better enforcement from the point of view of the relationship with supervisory authorities.



COCIR

SUSTAINABLE COMPETENCE IN ADVANCING HEALTHCARE

European Coordination Committee of the Radiological, Electromedical and Healthcare IT Industry

3. Reduce administrative burden when enlisting a sub-processor (Art. 26)

Requiring each Data Controller (e.g. a hospital) to agree to each sub-processor enlisted by a Data Processor (e.g. eHealth service provider) introduces an excessive administrative burden and increases costs for both the Data Controller and Data Processor. COCIR recommends keeping the existing legal framework in Directive 95/46/EC. Responsibilities and liabilities between the controller and the processor should be handled through contractual arrangements, not through law.

4. Allow processing of Data Concerning Health by technicians for technical maintenance and equipment performance evaluation (Art. 81-83)

Article 81 provides that data concerning health may be processed by a healthcare professional or a professional with an equivalent obligation of professional secrecy.

It is not clear whether this provision covers technicians and engineers employed by manufacturers, who may have access to Data Concerning Health when maintaining medical systems, either onsite or remotely. The regulation should clarify that professionals who have signed a commitment of secrecy by contract with their employer qualify as *'professionals with an equivalent obligation of professional secrecy'*.

The proposed exemption for processing data concerning health in article 83 does not seem to take into account registry studies for the improvement of medical devices or medical services effectively making it impossible for companies to meet regulatory requirements under the medical devices Regulation. The regulation should clarify that the processing "*for historical, statistical or scientific research purposes*" in the meaning of Article 83 includes processing for the purposes of the manufacturer's regulatory pre- and post-market obligations with respect to clinical evaluation of a medical device, by clear guidance².

B- COCIR secondary recommendations

1. Extend the exemption to the right to be forgotten to healthcare (Art. 17)

Implementing the right to be forgotten in healthcare requires careful consideration of the consequences. Deleting data from an electronic health record can run counter to patient safety, public interest, healthcare research and eHealth deployment. Medical records, patient registries and other clinical databases should be exempted from the right to be forgotten.

2. Allow the secondary use of anonymised and pseudonymised data for health purposes (Art. 20)

The text of Article 20 might render legitimate use of data for health research impossible or extremely difficult, with great consequences for the social benefits in this area. COCIR

² This concern falls if anonymised data are not subject to the Regulation.



recommends deleting Article 20 or reverting to the language currently used in Article 15 of Directive 95/46/EC.³

3. Delete 'privacy by design' and 'privacy by default' obligations (Art. 23)

Although COCIR supports imbedding privacy and data protection features in products and services from the onset, we are concerned that 'Privacy by Design' and 'Privacy by Default' mean different things for different people. The intent of both is already reflected in the Regulation through new requirements: data protection impact assessment, data minimisation, etc. COCIR feels these concepts are superfluous and should be deleted.

4. Consider context and feasibility for Data Breach Notifications (Art. 31 - 32)

The definition of 'breach' and associated notification requirements, especially the concepts of 'reasonable timeframe' and 'mitigating effects of safeguards' and 'potential for harm/adverse impact' pose issues of practicability in a real world environment. Industry would greatly benefit from a more pragmatic and proportional approach. A two-step approach could be considered for the notification of the breach, and the submission of the requested documentation within a longer time frame. This would allow more time for a qualitative impact assessment, and efficient corrective and mitigation actions.

5. Ensure data protection impact assessments and pre-authorisation obligations take account the context and are not 'one size fits all' (Art. 33-34)

Data Protection Impact Assessment should not be mandatory, and should be relative to the scope and types of processing activities, and based on a well-defined category of "high-risk" activity. Organisations should be able to construct their own assessment, based on their specific type of organisation, legal requirements, contractual obligations, and, where appropriate, internal policies.

Prior consultation should not be needed when processing is based on consent or contract. Where approval is required (Article 34), a clear time line for the approval should be clarified prior to effective dates.

6. Keep certification industry led and voluntary for more efficiency (Art. 39)

Certification mechanisms and data protection seals and marks developed and managed by industry should be favoured. They should remain voluntary rather than mandatory and COCIR recommends the adoption of existing internationally recognised standards (e.g. ISO/IEC 27001) rather than developing new certification mechanisms. COCIR also recommends removing paragraphs 2 and 3 on delegated and implementing acts in Article 39.

³ *This concern falls if anonymised data are not subject to the Regulation.*



7. Recognise compliance with non-EU frameworks, e.g. HIPAA Privacy and Security Rules in the U.S., as adequate safeguard for transferring data beyond EU borders (Art. 42)

Many COCIR members have a strong presence outside of Europe (e.g. in the USA), and have invested in processing capabilities there. Transfer of health data to the USA should be allowed under the HIPAA rules which provide safeguards for privacy. The transfer of anonymised / pseudonymised data should not require further authorization or consultation where the recipient does not reasonably have access to the key, and contractual or legal restrictions prohibit re-identification of the data subjects.

8. Allow the transfer of anonymised, pseudonymised and encrypted data to a third country, without further regulatory authorisation, where re-identification is not possible (Chapter V)

The transfer of anonymised data should not require any further authorisation or consultation where the recipient does not reasonably have access to the key and contractual or legal restrictions prohibit re-identification of the data subjects. Anonymised⁴ and pseudonymised⁵ data which do not reasonably permit re-identification of a data subject, and encrypted data⁶ which do not permit understanding of the information, are central to many data processing operations. Responsible data controllers and processors have invested heavily in a raft of data processing techniques to prevent the identification of data subjects and protect user privacy. These efforts should be recognised and encouraged.

9. To introduce proportionality to Administrative Sanctions (Art. 79)

COCIR recognises the need for credible enforcement mechanisms, specifically sanctions and fines, but notes that the current proposal lacks proportionality. This may result in making the EU less competitive in attracting investment in facilities or services. Furthermore some terms would need a clear definition to be implementable, e.g. *'incomplete information'*, *'insufficiently transparent'*, etc.

⁴ *Previously identifiable data that have been de-identified and for which a code or other link no longer exists. An investigator would not be able to link anonymised information back to a specific data subject.*

⁵ *Pseudonymisation, a Privacy Enhancing Technology (PET), is the replacement of Personally Identifiable Information (PII) – such as name, address or account number – with pseudonyms. Key-coded data are a classical example of pseudonymisation. Personally Identifiable Information (PII) is earmarked by codes, while the link between the code and the PII (like name, date of birth, address, etc.) is kept separately.*

⁶ *Encrypted data are information that has been transformed and made unreadable by the use of algorithms. Only those with the key can decrypt the data.*



10. Limit the number and scope of delegated acts for more legal certainty

The number and scope of delegated acts undermines the legal certainty of the Regulation. The number should be reduced and clear timelines introduced for those remaining.

- The categories of recipients of health data should not be determined by delegated acts, but by healthcare organisations (Art. 14.7).
- The legal framework should be fully harmonised to avoid conflicting provisions between the Regulation, delegated acts and national law (Art. 81.1).
- Measures, criteria, requirements, etc., provided for by delegated acts (Art.81.3) should be technology, service and business model neutral and industry-based.

EUROPEAN BANKING FEDERATION PROPOSED AMENDMENTS TO THE EUROPEAN COMMISSION PROPOSAL FOR A REGULATION ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA AND THE FREE MOVEMENT OF SUCH DATA

The European Banking Federation (EBF) supports the objectives of the current review. However, the European Commission's proposal aims to clarify some broad and complex issues for which the EBF identified concerns for European banks in regard to fulfilling their data protection obligations. Please find below a summary of the EBF key priorities (I) and the amendments proposed on the Regulation (II).

I. EBF KEY PRIORITIES

A. Data breach notification

- **Introducing an obligation to notify personal data breaches in 24 hours for other sectors than the telecommunications sectors appears disproportionate to the EBF.**
- At present, banks already notify their customers for instance if their credit card has been skimmed (i.e. information about a card and the associated PIN-code is copied for the purpose of manufacturing a fake card). It is also in the bank's interest to protect their customers against fraud and sustain a very high level of security. The banks can also be held liable for damages when their customers may suffer due to deficiencies in Banks IT- security systems. The banks test and update their systems and security solutions regularly to make sure that the information in the bank's system is always well-protected and secure. The transfer of information between the customer's computer and the online banking system is always encrypted. The customer must also make sure that his/her computer, codes and personal information are protected to prevent the possibility of fraud. **To avoid "data breaches" the EBF strongly believes that it would be more effective to inform customers on how to protect their own computers, never disclose their bank account details to unknown persons etc.**
- A mandatory personal data breach notification system could first give rise to organisational concerns since the implementation of such a system of notification could burden and delay the process of information to the customers.
- Attention should be paid to the criteria which trigger the obligation to notify: **The notification requirement should be limited to serious breaches affecting more than one individual.** Otherwise there is a danger of triggering an avalanche of notifications with the potential to confuse and unnecessarily alarm individuals or desensitise affected data subjects (where notifications are so commonplace they are to a large extent ignored by the recipient, thereby rendering the notification worthless).

- **Exemptions from data breach provisions should be awarded where sophisticated encryption is used.** This will encourage the practice of encrypting personal data, especially prior to their transmission. It should also be possible to dispense with notification if measures are taken to adequately compensate those affected, e.g. by issuing new credit cards to replace cards whose details have been compromised.

A framework where notification is made in the most expedient time possible would achieve the goal of ensuring regulators and data subjects are well informed without causing unnecessary burden for regulators or alarm to victims of breaches. In addition, especially for the banking sector, notification to data subjects at all times may enable certain forms of fraud.

B. Consent

- **Consent given by consumers in a tacit way should be allowed. The word “explicit” should indeed be deleted** as we believe that certain conditions (e.g. definition of certain period of time to opt-out) should be set to constitute a framework to allow for the practice of tacit consent as is already the case in some jurisdictions (e.g. Spain, Austria).
- A typical consent situation within the banking industry is the transfer of data to credit agencies. This consent may under the regulation not be deemed as freely given as almost all banks require customers to sign credit agency consent. However, it is in the interest of the financial marketplace, the various financial institutions and the data subject (prevent excessive indebtedness, insolvency) to have a working credit information system.
- Often customers may be perceived as being in a situation of imbalance with respect to companies that process personal data. It will be difficult to ascertain what “significant imbalance” may mean.

C. Right to data portability - Article 18

- **The portability principle seems to be designed for new technology / information society industry.** Therefore **the EBF would like to limit the scope of Article 18 to storage of data in online-databases.** Indeed, the extension of such a right to the financial sector seems inappropriate considering the nature of the data kept in bank servers, their sensitiveness and their variety. Should the scope of this provision not be limited, we are indeed concerned that the right to data portability increases the risk of disclosure of personal data to third parties.
- The EBF also would like to stress that the exercise of this right could require organisations to disclose information on trade secrets or information on other customers. The banking industry has to comply with retention requirements deriving from commercial and tax law. The obligation to bank secrecy should be taken into account.
- If we take the example of a customer with a real estate loan, the data held about this customer including his financial credit worthiness represents at the same time intellectual property of the various financial institutions, which is protected by constitutional rights as well.
- This principle cannot lead to a completely imbalanced between claimant and defendant in case of a civil litigation as the data subject may be in the position to extract all data from the affected company or extract at least information which would have to be provided under the very civil procedure rules.

D. Profiling - Article 20

- Profiling is a typical technique used in the area of Anti Money Laundering to identify unusual financial transactions which might not fit in the financial profile of the customer. This is required by the Anti Money Laundering laws and it is also in the interest of the various financial institutions not to be misused by criminal actions. It is therefore based on the balance of interests.
- It is important to stress that it might be an information overload for the customers if this information have to be given in advance of an e.g. current account contract.
- In addition, as not all requirements regarding Anti Money Laundering derive from the law itself but from supervisory authority circulars we believe that it is imperative to resolve the relationship of draft regulation and the Anti Money Laundering Directive, local implementations and deduced circulars.

E. Fraud - Notably Article 6, 9, 20 and Lawfulness of processing - Article 6.1

- The EBF suggests adding particular cases of lawful processing of data. The EBF considers that detecting and preventing fraud in consumer lending is of significant importance, not only to financial institutions, but can help to protect consumers from identity theft. Therefore, fraud prevention and detection should be explicitly recognised as a legitimate purpose for data processing.
- Banks are entitled to process fraud data in order to prevent frauds and minimise risks related to the granting of credits and undertakings. The processing of this kind of sensitive data is currently possible if data protection authorities issue permission for reason for pertaining to an important public interest. **The EBF wonders whether the restrictions of Article 9 of the proposed regulation will still allow the maintenance of such databases in the future.**
- The EBF thinks that Article 6.1.c should be widened-up to include orders, recommendations of competent organisations as well as the requirements of supervisory authorities. In an on-line world and a global economy, international standards of supervisory bodies should indeed be recognised.

II. EBF AMENDMENTS

- **Explicit consent**

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
1.	Recital 25	(25) Consent should be given explicitly by any appropriate method enabling a freely given specific and informed indication of the data subject's wishes, either by a statement or by a clear affirmative action by the data subject, ensuring that individuals are aware that they give their consent to the processing of personal data, including by ticking a box when visiting an Internet website or by any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data. Silence or inactivity should therefore not constitute consent.	(25) Consent should be given explicitly by any appropriate method enabling a freely given specific and informed indication of the data subject's wishes, either by a statement or by a clear affirmative action by the data subject, ensuring that individuals are aware that they give their consent to the processing of personal data, including by ticking a box when visiting an Internet website or by any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data. Silence or inactivity should therefore not constitute consent.
<p>Justification</p> <ul style="list-style-type: none"> • With the current requirements, the definition of consent seems to obviate the changes in technique, especially to on-line media. • Consent given by consumers in a tacit way should be allowed. The word “explicit” should indeed be deleted as we believe that certain conditions (e.g. definition of certain period of time to opt-out) should be set to constitute a framework to allow for the practice of tacit consent as is already the case in some jurisdictions (e.g. Spain, Austria). • A typical consent situation within the banking industry is the transfer of data to credit agencies. This consent may under the regulation not be deemed as freely given as almost all banks require customers to sign credit agency consent. However, it is in the interest of the financial marketplace, the various financial institutions and the data subject (prevent excessive indebtedness, insolvency) that there is a working credit information system. 			

- Consent in the case of “imbalance between the controller and the data subject”

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
2.	Recital 34	<p>Consent should not provide a valid legal ground for the processing of personal data, where there is a clear imbalance between the data subject and the controller. This is especially the case where the data subject is in a situation of dependence from the controller, among others, where personal data are processed by the employer of employees' personal data in the employment context. Where the controller is a public authority, there would be an imbalance only in the specific data processing operations where the public authority can impose an obligation by virtue of its relevant public powers and the consent cannot be deemed as freely given, taking into account the interest of the data subject.</p>	<p>Consent should not provide a valid legal ground for the processing of personal data, where there is a clear imbalance between the data subject and the controller. This is especially the case where the data subject is in a situation of dependence from the controller, among others, where personal data are processed by the employer of employees' personal data in the employment context. Where the controller is a public authority, there would be an imbalance only in the specific data processing operations where the public authority can impose an obligation by virtue of its relevant public powers and the consent cannot be deemed as freely given, taking into account the interest of the data subject.</p> <p>However, imbalance between the controller and the data subject is not a problem where Union or Member State law has made the data subject's consent a specific condition for a specific type of processing of the personal data or set of processing operations or where the purpose or purposes of the processing of the personal data is in the interest of the data subject.</p>
<p>Justification</p> <p>The imbalance should not be a problem in case the processing is required by Union or Member State law as a specific condition for the processing (other than article 6.1). E.g., the Dutch Medical Examinations Act requires employee consent for the disclosure of a medical report prepared by the company doctor to the employer.</p> <p>Furthermore, consent should be possible where the purpose of the processing is in the interest of the data subject. E.g., an employer should be allowed to ask the consent of an expat to disclose his personal data to a tax advisor or moving company, paid for by the employer. In this example, the tax advisor or moving company are controllers of the personal data as they render their services directly to the employee. This means that the disclosure needs a basis in article 6.1 of this Regulation. Because the use of such services cannot be made a condition of the expat contract under labour law and the disclosure cannot be based on any other processing basis as mentioned in article 6.1 except consent, the expat's consent would be required in such case.</p>			

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
3.	Recital 86	Provisions should be made for the possibility for transfers in certain circumstances where the data subject has given his consent, where the transfer is necessary in relation to a contract or a legal claim, where important grounds of public interest laid down by Union or Member State law so require or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest. In this latter case such a transfer should not involve the entirety of the data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or if they are to be the recipients.	Provisions should be made for the possibility for transfers in certain circumstances where the data subject has given his consent, where the transfer is necessary in relation to a contract or a legal claim, where important grounds of public interest laid down by Union or Member State law so require or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest. In this latter case such a transfer should not involve the entirety of the data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or if they are to be the recipients. An important public interest may be recognised by Union or Member State Law or the law of a third country to which the data controller may also be subject.
<p style="text-align: center;">Justification</p> <p>The banking sector believes that such public interest should also be a public interest recognised abroad. The enacting of laws abroad that provide for the disclosure of detailed banking related information responds to very specific needs of public interest [and are the product of a democratic process]. In such circumstances, banks should be able to assess the circumstances of an obligation to disclose based on the powers of a foreign regulator and weigh the privacy rights of the data subjects against the public interest at hand. The banking sector believes that the decision of disclosing such data should not be lightly made and as counterweigh, additional measures should be put in place to make such disclosure in line with the principles of the Regulation, as it should occur prior to any data processing. Any request for disclosure should be first tested against the principles of necessity, subsidiarity and proportionality. In addition and where necessary, special arrangements with the receiving party concerning the confidentiality of the data could be made.</p>			

- **Collective redress**

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
4.	Recital 112	(112) Any body, organisation or association which aims to protects the rights and interests of data subjects in relation to the protection of their data and is constituted according to the law of a Member State should have the right to lodge a complaint with a supervisory authority or exercise the right to a judicial remedy on behalf of data subjects, or to lodge, independently of a data subject's complaint, an own complaint where it considers that a personal data breach has occurred.	(112) Any body, organisation or association which aims to protects the rights and interests of data subjects in relation to the protection of their data and is constituted according to the law of a Member State should have the right to lodge a own complaint with a supervisory authority or exercise the right to a judicial remedy on behalf of data subjects, or to lodge, and independently of a data subject's complaint, an own complaint where it considers that a personal data breach has occurred.

Justification

The EBF would like to stress that the introduction of EU collective actions are still under discussion, therefore it would be more appropriate to wait for the outcome before including any such provisions in EU legislation, especially in the data protection Regulation.

The ability for individuals to bring class actions against entities in case of negligence could have negative unintended consequences. The EBF is therefore not in favor of class actions with regard to such individual rights as privacy and data protection. The current system containing a relevant oversight regime is sufficient according to the EBF.

A one-size-fits-all approach to penalties could leave businesses facing sanctions that are too severe for the incidence in question and could hurt business in Europe in an environment that is already squeezed.

Should nevertheless class actions be accepted, the EBF believes that the representative body should evidence an interest by referring to its statutory purpose and the membership of the data subject(s), e.g. consumer organisations.

- Scope

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
5.	Article 2	<ol style="list-style-type: none"> 1. This Regulation applies to the processing of personal data wholly or partly by automated means, and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system. 2. This Regulation does not apply to the processing of personal data: <ol style="list-style-type: none"> (a) in the course of an activity which falls outside the scope of Union law, in particular concerning national security; (b) by the Union institutions, bodies, offices and agencies; (c) by the Member States when carrying out activities which fall within the scope of Chapter 2 of the Treaty on European Union; (d) by a natural person without any gainful interest in the course of its own exclusively personal or household activity; (e) by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. 	<ol style="list-style-type: none"> 1. This Regulation applies to the processing of personal data wholly or partly by automated means, and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system. 2. This Regulation does not apply to the processing of personal data: <ol style="list-style-type: none"> (a) in the course of an activity which falls outside the scope of Union law, in particular concerning national security; (b) by the Union institutions, bodies, offices and agencies; (c) by the Member States when carrying out activities which fall within the scope of Chapter 2 of the Treaty on European Union; (d) by a natural person without any gainful interest in the course of its own exclusively personal or household activity; (e) by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

Justification

- The EBF considers that the application of the new data protection rules to EU institutions, bodies, offices and agencies should be consistent with the other legal instruments and therefore Regulation (EC) No 45/2001¹ should be fully in line with the general Data Protection Regulation. The EBF considers that the Union institutions, bodies, offices and agencies should be in the scope of the Data protection Regulation.
- The EBF believes that sufficient administrative safeguards need to be put in place to make sure that banks' clients can rest assured that the information will not be disclosed to third parties or be abused in any other way.
- The EBF would like to stress that the type of data that banks will be required to transmit to their prudential authorities (i.e. European Central bank, the Financial Stability Board located in Basel) will evolve in the future. The main objective is no longer to collect data on banks' activities in an aggregate form but also to become aware of the main bilateral links and relationships between the major financial institutions and their principal counterparties on both the assets and liability side of the balance sheet (i.e. credit exposures and funding providers). In this perspective, this means that supervisory authorities will become aware of information broken down at a contract level: top 50 individual counterparties and funding providers (single names, not aggregates) will need to be reported.

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
6.	Article 4, paragraph 3	(3) 'processing' means any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation , use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, erasure or destruction;	(3) 'processing' means any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation , use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, erasure or destruction;

Justification

This definition is the same as in the 95/46/EC Directive.

The definition of “processing” includes the “consultation” of personal data. It seems there was no particular problem with the inclusion of the word “consultation” under the current 95/46/EC Directive. However, under the new Regulation, this means that each time a consultation is made, it is a processing in itself, thus all the requirements of the Regulation are applicable, in particular the consent of the person concerned if no other lawfulness conditions of the processing can apply. This is a problem now because tacit consent is not any longer allowed (if the name of a person is included in a database, this means normally that a previous treatment has been made, and one can rely on the fact that the person had previously been informed, or had given his consent, or the processing had been made in accordance with the applicable law...).

¹ Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data

Under the proposed Regulation, this means that, each time a consultation is made (such as a consultation of a bank's client name on the Internet, consultation of World Check database, consultation of the Commission's database of persons, groups and entities subject to EU financial sanctions,...), the consent of the data subject is required and he/she should also be informed of the processing. In conclusion, the word "consultation" should be deleted in the definition of "processing".

• **Definition of data subject's consent**

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
7.	Article 4, paragraph 8	(8) 'the data subject's consent' means any freely given specific, informed and explicit indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed;	(8) 'the data subject's consent' means any freely given specific, isolated [separate – one off] and informed expression of will, either by a statement or an action, which, in view of the context and circumstances at the time consent is required, signifies the data subject's agreement to the processing of the personal data ;

Justification

- Distinction must be made between isolated statements or statements as part of a contractual arrangement.
- The EBF believes that the current definition of the data subject's consent requires more clarification. With the current requirements, the definition of consent seems to obviate the changes in technique, especially to on-line media. More specifically (see Recital 25), it is our opinion that the word "explicit" should be deleted as we believe that certain conditions (e.g. definition of certain period of time to opt-out) should be set to constitute a framework to allow for the practice of tacit consent as is already the case in some jurisdictions (e.g. Spain, Austria).

• **Definition of personal data breach**

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
8.	Article 4 paragraph 9	(9) ' personal data breach ' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of,	(9) 'personal data breach' means a substantial breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised

	or access to, personal data transmitted, stored or otherwise processed;	disclosure of, or access to, personal data transmitted, stored or otherwise processed;
Justification		
Only substantial breaches of security should be notified in order not to represent an unnecessary burden on data protection authorities and individuals.		

• **Definition of groups of undertakings**

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
9.	Article 4, paragraph 16	(16) 'group of undertakings' means a controlling undertaking and its controlled undertakings;	(16) 'group of undertakings' means a controlling undertaking and its controlled undertakings; the controlling undertaking should be the undertaking which can exercise a dominant influence over the other undertakings by virtue, for example, of ownership, financial participation or the rules which govern it or the power to have personal data protection rules implemented.
Justification			
The EBF believes that the definition of “group of undertakings” should be clarified and include the definition proposed under Recital 28 in order to have an objective criterion for the control.			

• **Principles relating to personal data processing**

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
10.	Article 5 paragraph c	1. Personal data must be: (...) (c) adequate, relevant, and limited to the minimum necessary in relation to the purposes for which they are processed; they shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does	1. Personal data must be: (...) (c) adequate, relevant, and limited to the minimum necessary not excessive in relation to the purposes for which they are processed; they shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that

		<p>not involve personal data; (...)</p>	<p>does not involve personal data; (...)</p> <p>2. In order to assess whether the processing of personal data for other purposes than for which the personal data was collected, is incompatible with such purposes, as referred to under paragraph 1(b), the controller shall take into account:</p> <p>(a) the relationship between the purpose of the intended processing and the purpose for which the data were obtained;</p> <p>(b) the nature of the data concerned;</p> <p>(c) the consequences of the intended processing for the data subject;</p> <p>(d) the extent to which appropriate guarantees have been put in place to protect the interests of the data subject.</p> <p>(e) the information that has been given to the data subject.</p>
--	--	--	---

Justification

- **It should be noted that article 5.c may be in conflict with other obligations of the banking sector**, for example the proposed Directive of the European Parliament and the Council on credit agreements relating to residential property, which requires creditors to conduct “thorough” assessment of the consumer’s creditworthiness based notably on the “necessary” information (Article 14); the Consumer Credit Directive (Article 8) which requires creditors to assess a consumer’s creditworthiness on the basis of “sufficient information” before the conclusion of a credit agreement or the Anti-Money Laundering legislation. Overlap should be avoided in this regard. The EBF believes that personal data should be proportionate to the processing purposes.
- In addition, the EBF considers that the **limitation of the possibility to process the personal data only if the purpose cannot be fulfilled otherwise creates the risk of litigation for banks**, either on the basis that the bank requested personal data where it is deemed unnecessary, or on the basis of not having requested all the relevant information to fully fulfill their legal obligations, be it related to Anti-Money Laundering or creditworthiness assessment.

- Lawfulness of processing

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
11.	Article 6	<p>1. Processing of personal data shall be lawful only if and to the extent that at least one of the following applies:</p> <ul style="list-style-type: none"> (a) the data subject has given consent to the processing of their personal data for one or more specific purposes; (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; (c) processing is necessary for compliance with a legal obligation to which the controller is subject; (d) processing is necessary in order to protect the vital interests of the data subject; (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (f) processing is necessary for the purposes of the legitimate interests pursued by a 	<p>1. Processing of personal data shall be lawful only if and to the extent that at least one of the following applies:</p> <ul style="list-style-type: none"> (a) the data subject has given consent to the processing of their personal data for one or more specific purposes; (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; (c) processing is necessary for compliance with a EU or national legal obligation or legal right to which the controller is subject notably processing carried out on the basis of orders, recommendations of competent organizations as well as the requirements of supervisory authorities including the performance of a task carried out for assessing creditworthiness or for fraud prevention and detection purposes. (d) processing is necessary in order to protect the vital interests of the data subject (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or for the performance of a task carried out for assessing creditworthiness or for fraud prevention and detection purposes; (f) processing is necessary for the purposes of the legitimate interests pursued by a controller, or

		<p>controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks.</p> <p>4. Where the purpose of further processing is not compatible with the one for which the personal data have been collected, the processing must have a legal basis at least in one of the grounds referred to in points (a) to (e) of paragraph 1. This shall in particular apply to any change of terms and general conditions of a contract.</p> <p>5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the conditions referred to in point (f) of paragraph 1 for various sectors and data processing situations, including as regards the processing of personal data related to a child.</p>	<p>by the third party or parties to whom the data are disclosed except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks.(g) The data are collected from public registers, lists or documents accessible by everyone;</p> <p>(g) The processing is necessary to defend an interest, collecting evidences as judicial proofs or file an action.</p> <p>4. Where the purpose of further processing is not compatible with the one for which the personal data have been collected, the processing must have a legal basis at least in one of the grounds referred to in points (a) to (e) of paragraph 1. This shall in particular apply to any change of terms and general conditions of a contract.</p> <p>5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the conditions referred to in point (f) of paragraph 1 for various sectors and data processing situations, including as regards the processing of personal data related to a child.</p>
--	--	--	---

Justification

- The EBF suggests adding particular cases of lawful processing of data. The EBF considers that detecting and preventing fraud in consumer lending is of significant importance, not only to financial institutions, but can help to protect consumers from identity theft. Therefore, fraud prevention and detection should be explicitly recognised as a legitimate purpose for data processing.
- The EBF thinks that Article 6.1.c should be widened-up to include orders, recommendations of competent organisations as well as the requirements of supervisory authorities. In an on-line world and a global economy, international standards of supervisory bodies should indeed

be recognised.

- In addition, the current formulation of article 6.1 f is too vague to be usable.
- Furthermore, the EBF regrets to note that Article 6.4 restricts the range of compatible purposes and suggests its deletion.
- Finally, the power of the Commission to adopt delegated acts (Article 6.5) for this specific article creates legal uncertainty.

- **Conditions for consent**

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
12.	Article 7, paragraph 4	<ol style="list-style-type: none"> 1. The controller shall bear the burden of proof for the data subject's consent to the processing of their personal data for specified purposes. 2. If the data subject's consent is to be given in the context of a written declaration which also concerns another matter, the requirement to give consent must be presented distinguishable in its appearance from this other matter. 3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. 4. Consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller. 	<ol style="list-style-type: none"> 1. The controller shall bear the burden of proof for the data subject's consent to the processing of their personal data for specified purposes. 2. If the data subject's consent is to be given in the context of a written declaration which also concerns another matter, the requirement to give consent must be presented distinguishable in its appearance from this other matter. 3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal or in cases where a minimum mandatory term of storage is provided by a European or national law, or data are processed according to European and national regulatory provisions, or for anti-fraud or legal purposes. The data subject has to communicate his willingness to withdraw his or her consent to the processor. The withdrawal of the consent is effective 30 days after the receipt of the declaration. 4. Consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller.

Justification

- Often customers may be perceived as being in a situation of imbalance with respect to companies that process personal data. It will be difficult to ascertain what “significant imbalance” may mean. If one argues that customers are often in a situation of imbalance with respect to companies, consent will never be a legitimate ground to base data processing. This collides with the principle that there are six legitimate grounds for the processing of data in Article 6.1 of the draft Regulation, consent being one of them.
In addition, there are situations where data subjects will be confronted with the choice of granting or not consent with negative consequences if they do not provide it. In these situations such choice will bring data subjects in a situation of imbalance. This provision is likely to negatively affect the banking sector. Some may argue for instance **that banks and their customers may be in a situation of imbalance. This may lead banks not being able to rely on consent.**

The banking sector is subject to worldwide heavy regulators’ controls, which may require the processing of personal data for numerous specific situations to meet legal and regulatory obligations. In certain circumstances, well informed consent may be the sole adequate ground for processing data in order to meet the privacy rights of data Subjects. If article 7.4 remains, the banking sector will be detrimentally affected and will be indirectly put in a situation of inequality with respect to other sectors.

The EBF would therefore suggest deleting the entire paragraph 4 of Article 7.

- The right of data subject to withdraw their consent at any time can actually prevent the performance of legal requirements such as those of responsible lending. It may become very difficult for financial institutions to find appropriate information in clients’ databases (collecting either negative or positive information) to assess their creditworthiness when the clients may withdraw their consent whenever they feel like (for example at their very moment when their debts become overdue). The compliance with the Consumer Credit Directive Requirements (and future Mortgage Credit Directive as well) can hardly be assured and the effectiveness of creditworthiness assessment diminished.
- In the employment context, it may be appropriate that the employer can process health information concerning the employee's sick leave or data of employees covered by the collective agreements social chapters. It is also very uncertain whether an employer can process personal data concerning health at all, when the nature of art. 7, 9 and 81 is compared. If the employer cannot process health information it will complicate efforts to maintain the employee's relationship with the company and the labour market. It would also be extremely intrusive, if the employers no longer can process criminal records in employment. In the financial sector, it is very important that the employer is able to do so. For example, it is not reassuring that employers in connection with employment, of employees that handle the customers' money transactions, does not have the possibility to determine whether, the employee previously has been convicted of financial crimes. This process is also here governed by the general principles of treatment in Article 5 which is sufficient.
- The continued processing should be permitted in order to continue the contractual relationship that may exist between the controller and the data subject, or to allow the fulfillment of any obligation of the controller, or to respect legal basis.

- **Exception to Article 7 paragraph 4**

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
13.	New Article 7, paragraph 5	-	<p>5. Paragraph 4 shall not apply where the data subject's consent is required:</p> <p>(a) by law, or</p> <p>(b) where the purpose of processing is likely to serve the interest of the data subject.</p>
Justification			
<p>No consent is required in case of a processing that is necessary for the purposes of the legitimate interest pursued by the controller or the processor which cannot be qualified as frequent or massive and where the controller or processor has assessed all the circumstances surrounding the data transfer operation or the set of data transfer operations and based on this assessment adduced appropriate safeguards with respect to the protection of personal data.</p>			

- **Special categories of personal data**

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
14.	Article 9	<p>1. The processing of personal data, revealing race or ethnic origin, political opinions, religion or beliefs, trade-union membership, and the processing of genetic data or data concerning health or sex life or criminal convictions or related security measures shall be prohibited.</p>	<p>1. The processing of personal data concerning health by financial institutions shall be allowed if it is used as part of an acceptance procedure or in exercising the duty of care.</p> <p>2. The processing of personal data, revealing race or ethnic origin, political opinions, religion or beliefs, trade-union membership, and the processing of genetic data or data concerning health or sex life or criminal convictions or related security measures shall be prohibited.</p> <p>(a) The prohibition as described in paragraph 2 shall not apply with respect of processing of personal data concerning criminal convictions</p>

			<p>or related security measures in the context of databases which contain data on fraud committed against the credit institutions or members of other financial groups regulated by EU or national legislation and set up by financial institutions to prevent fraud.</p> <p>The restrictions on the processing of data relating to criminal convictions should not apply to data relating to criminal offences.</p> <p>(b) The processing of personal data concerning health by financial institutions shall be allowed if it is used as a key factor in the assessment of risk or consumer's creditworthiness based on relevant and accurate actuarial or statistical data in the context of the provision of financial services to consumers.</p> <p>(ba) processing of data relating to criminal offences or related security measures is carried out either under the control of official authority or when the processing is necessary for compliance with a legal or regulatory obligation or right to which a controller is subject, or for the performance of a task carried out for important public interest reasons, and in so far as authorised by Union law or Member State law providing for adequate safeguards. A complete register of criminal convictions shall be kept only under the control of official authority.</p> <p>(bb) The prohibition to the processing of data relating to criminal convictions does not apply to responsible parties who process these data for their own purposes with a view to:</p>
--	--	--	---

		<p>2. Paragraph 1 shall not apply where:</p> <p>(a) the data subject has given consent to the processing of those personal data, subject to the conditions laid down in Articles 7 and 8, except where Union law or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject; or</p> <p>(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller in the field of employment law in so far as it is authorised by Union law or Member State law providing for adequate safeguards; or</p> <p>(...)</p>	<p>(bba) assessing an application by data subjects in order to take a decision about them or provide a service to them, or</p> <p>(bbb) protecting their interests, provided that this concerns criminal offences which have been or, as indicated by certain facts and circumstances, can be expected to be committed against them or against persons in their service.</p> <p>The prohibition does not apply where these data are processed for the account of third parties where these third parties are legal persons forming part of the same group,</p> <p>3. Paragraph 2 shall not apply where:</p> <p>(a) the data subject has given consent to the processing of those personal data, subject to the conditions laid down in Articles 7 and 8, except where Union law or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject; or</p> <p>(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller in the field of employment law in so far as it is authorised by Union law or Member State law providing for adequate safeguards; or</p> <p>(...)</p>
--	--	---	--

Justification

- Under the current Directive, banks are allowed to maintain special defaulters and fraudsters databases, for which national data protection authorities may grant exemptions. These databases are used to record any frauds committed against the banks' operations. The exemption order also permits banks to disclose fraud data to other banks that are within the scope of the permission.

- Banks are entitled to process fraud data in order to prevent frauds and minimize risks related to the granting of credits and undertakings. The processing of this kind of sensitive data is currently possible if data protection authorities issue permission for reason for pertaining to an important public interest. **The EBF wonders whether the restrictions of Article 9 of the proposed regulation will still allow the maintenance of such databases in the future.**
- We would welcome **a clear distinction between data relating to criminal convictions and data relating to criminal offenses. At least the restrictions on the processing of data relating to criminal convictions should not apply to data relating to criminal offences** as such restriction hampers the prevention, detection and handling of such offences.
- As regards to health data, the EBF would support the inclusion of derogation for these specific sectors since banks and insurance companies need to process health related data in the acceptance process of some banking and insurance products. We fear that financial institutions would not be able to simply rely on the consent of the data subjects present in Article 7 when processing health/medical data because of the potential “situation of imbalance” between data subjects and financial institutions.

• **Definition of personal data concerning criminal convictions**

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
15.	Proposal for a new Article (12a)	-	(12a) ‘personal data concerning criminal convictions’ means any personal data relating to the application of the criminal justice system;

Justification

Controllers that are victim of criminal offences should have the right to process data of such offences committed against them or their organisations.

• **Procedures and mechanisms for exercising the rights of the data subject**

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
16.	Article 12	1. The controller shall establish procedures for providing the information referred to in Article 14 and for the exercise of the rights of data subjects referred to in Article 13 and Articles 15 to 19. The controller shall provide in particular mechanisms	1. The controller shall establish procedures for providing the information referred to in Article 14 and for the exercise of the rights of data subjects referred to in Article 13 and Articles 15 to 19. The controller shall provide in particular mechanisms

		<p>for facilitating the request for the actions referred to in Article 13 and Articles 15 to 19. Where personal data are processed by automated means, the controller shall also provide means for requests to be made electronically.</p> <p>2. The controller shall inform the data subject without delay and, at the latest within one month of receipt of the request, whether or not any action has been taken pursuant to Article 13 and Articles 15 to 19 and shall provide the requested information. This period may be prolonged for a further month, if several data subjects exercise their rights and their cooperation is necessary to a reasonable extent to prevent an unnecessary and disproportionate effort on the part of the controller. The information shall be given in writing. Where the data subject makes the request in electronic form, the information shall be provided in electronic form, unless otherwise requested by the data subject.</p> <p>3. If the controller refuses to take action on the request of the data subject, the controller shall inform the data subject of the reasons for the refusal and on the possibilities of lodging a complaint to the supervisory authority and seeking a judicial remedy.</p> <p>4. The information and the actions taken on requests referred to in paragraph 1 shall be free of charge. Where requests are manifestly excessive, in particular because of their repetitive character, the controller may charge a fee for providing the information or taking the action requested, or the controller may not take the action requested. In that case, the controller shall bear the</p>	<p>for facilitating the request for the actions referred to in Article 13 and Articles 15 to 19. Where personal data are processed by automated means, the controller shall may also provide means for requests to be made electronically.</p> <p>2. The controller shall inform the data subject without delay and, at the latest within two months of receipt of the request, whether or not any action has been taken pursuant to Article 13 and Articles 15 to 19 and shall provide the requested information. This period may be prolonged for a further month, if several data subjects exercise their rights and their cooperation is necessary to a reasonable extent to prevent an unnecessary and disproportionate effort on the part of the controller. The information shall be given in writing. Where the data subject makes the request in electronic form, the information shall be provided in electronic form through a secure procedure, unless otherwise requested by the data subject. Before providing any data and in order to prevent any data breach possibilities, a proper identification of the data subject is needed.</p> <p>3. If the controller refuses to take action on the request of the data subject, the controller shall inform the data subject of the reasons for the refusal and on the possibilities of lodging a complaint to the supervisory authority and seeking a judicial remedy.</p> <p>4. The information and the actions taken on requests referred to in paragraph 1 shall be free of charge once a year. Where requests are manifestly excessive, in particular because of their repetitive character, the controller may charge a fee for providing the information or taking the action requested, or the controller may not take the action requested. In that case, the controller shall bear the</p>
--	--	--	---

		<p>burden of proving the manifestly excessive character of the request.</p> <p>5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the manifestly excessive requests and the fees referred to in paragraph 4.</p> <p>6. The Commission may lay down standard forms and specifying standard procedures for the communication referred to in paragraph 2, including the electronic format. In doing so, the Commission shall take the appropriate measures for micro, small and medium-sized enterprises. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>	<p>burden of proving the manifestly excessive character of the request.</p> <p>5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the manifestly excessive requests and the fees referred to in paragraph 4.</p> <p>6. The Commission may lay down standard forms and specifying standard procedures for the communication referred to in paragraph 2, including the electronic format. In doing so, the Commission shall take the appropriate measures for micro, small and medium-sized enterprises. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>
--	--	--	--

Justification

- The delay to inform the data subject is too short.
- The EBF considers that the controller should remain free to provide means to individuals for exercising their rights. We acknowledge the fact that data subjects may request information electronically. However, the EBF believes that a secure way is needed to be able to provide the said data. **A proper identification of the subject is needed before providing any data and to prevent any data breach possibilities. Furthermore the data subject has to support a secure procedure for the transmission of the data via Internet, e.g. encryption mechanism.**
- Providing the required information implies administrative expenses (not for profit) for European banks. Therefore, **the EBF considers that data controllers should be permitted to request an appropriate (not for profit) contribution in order to cover the administrative costs of providing that information.** In case the Commission considers this opportunity of paramount importance the EBF would **suggest limiting the free of charge only if the access is exercised once a year.**
- The EBF objects to the idea of giving the Commission the mandate to lay down standard forms and standard procedures for the communication, including the electronic format. It should be up to the bank and the customer to decide on how to communicate.

- Information to the data subject

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
17.	Article 14	<p>1. Where personal data relating to a data subject are collected, the controller shall provide the data subject with at least the following information:</p> <ul style="list-style-type: none"> (a) the identity and the contact details of the controller and, if any, of the controller's representative and of the data protection officer; (b) the purposes of the processing for which the personal data are intended, including the contract terms and general conditions where the processing is based on point (b) of Article 6(1) and the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1); (c) the period for which the personal data will be stored; (...) <p>5. Paragraphs 1 to 4 shall not apply, where:</p> <ul style="list-style-type: none"> (a) the data subject has already the information referred to in paragraphs 1, 2 and 3; or (b) the data are not collected from the data subject and the provision of such information proves impossible or would involve a disproportionate effort; or (c) the data are not collected from the data subject and recording or disclosure is expressly laid down by law; or 	<p>1. Where personal data relating to a data subject are collected, the controller shall provide the data subject with at least the following information:</p> <ul style="list-style-type: none"> (a) the identity and the contact details of the controller and, if any, of the controller's representative and of the data protection officer; (b) the purposes of the processing for which the personal data are intended, including the contract terms and general conditions where the processing is based on point (b) of Article 6(1) and the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1); (c) the period for which the personal data will be stored; (...) <p>5. Paragraphs 1 to 4 shall not apply, where:</p> <ul style="list-style-type: none"> (a) the data subject has already the information referred to in paragraphs 1, 2 and 3; or (b) the data are not collected from the data subject and the provision of such information proves impossible or would involve a disproportionate effort difficulties; or (c) the data are not collected from the data subject and recording or disclosure is expressly laid down by

		(d) the data are not collected from the data subject and the provision of such information will impair the rights and freedoms of others, as defined in Union law or Member State law in accordance with Article 21.	law; or (d) the data are not collected from the data subject and the provision of such information will impair the rights and freedoms of others, as defined in Union law or Member State law in accordance with Article 21.
--	--	--	---

Justification

- It is suggested that the data subject addresses his/her request to the service in charge (a delegate to the data protection in the company) but not to a natural person (Mr. or Ms. X) responsible for this particular function. A change in the name of the person in charge would indeed imply a change in all the contractual documentation containing his/her name.
- It should be noted that the period for which the personal data is stored can be changed during customer relationship. Instead of emphasising the requirement to inform the customer on the time period for which the data will be stored, the regulation should highlight the principle of accountability and the obligation to erase the erroneous, unnecessary, incomplete or obsolete personal data.
- The EBF considers the term “disproportionate effort” opens to various interpretations and should be clarified.
- The proposed Regulation requires the provision of a specific explanation of the justification for processing data (under Art 14, b, Art 15, h). Given that the rationale behind the processing of data is usually very clear to customers, (e.g. when applying for a mortgage or a bank account), the benefits associated with justification of processing in all circumstances are questionable. We would suggest the deletion of the above words in Article 14(1) (b

• **Right of access for the data subject**

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
18.	Article 15	<p>1. The data subject shall have the right to obtain from the controller at any time, on request, confirmation as to whether or not personal data relating to the data subject are being processed. Where such personal data are being processed, the controller shall provide the following information:</p> <p>(a) the purposes of the processing;</p>	<p>1. The data subject shall have the right to obtain from the controller at any time, on request, confirmation as to whether or not personal data relating to the data subject are being processed in order to be aware and verify the lawfulness of the processing. Where such personal data are being processed, the controller shall provide the following information:</p> <p>(a) the purposes of the processing;</p>

	<p>(b) the categories of personal data concerned;</p> <p>(c) the recipients or categories of recipients to whom the personal data are to be or have been disclosed, in particular to recipients in third countries;</p> <p>(d) the period for which the personal data will be stored;</p> <p>(e) the existence of the right to request from the controller rectification or erasure of personal data concerning the data subject or to object to the processing of such personal data;</p> <p>(f) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority;</p> <p>(g) communication of the personal data undergoing processing and of any available information as to their source;</p> <p>(h) the significance and envisaged consequences of such processing, at least in the case of measures referred to in Article 20.</p> <p>2. The data subject shall have the right to obtain from the controller communication of the personal data undergoing processing. Where the data subject makes the request in electronic form, the information shall be provided in electronic form, unless otherwise requested by the data subject.</p>	<p>(b) the categories of personal data concerned;</p> <p>(c) the recipients or categories of recipients to whom the personal data are to be or have been disclosed, in particular to recipients in third countries;</p> <p>(d) the period for which the personal data will be stored;—A general indication of the period of time for which the personal data will be stored. The data controller must provide more detailed retention periods if requested by the data subject.</p> <p>(e) the existence of the right to request from the controller rectification or erasure of personal data concerning the data subject or to object to the processing of such personal data;</p> <p>(f) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority;</p> <p>(g) communication of the personal data undergoing processing and of any available information as to their source if the request is specified with clear criteria such as the time or the category of data;</p> <p>(h) the significance and envisaged consequences of such processing, at least in the case of measures referred to in Article 20.</p> <p>2. The data subject shall have the right to obtain from the controller communication of the personal data undergoing processing in order to be aware and verify the lawfulness of the processing. Where the data subject makes the request in electronic form, the information shall be provided in electronic form, through a secure procedure, unless otherwise requested by the data subject. Before providing any data and in order to prevent any data breach possibilities, a proper identification of the subject is needed.</p>
--	---	---

		<p>3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the communication to the data subject of the content of the personal data referred to in point (g) of paragraph 1.</p> <p>4. The Commission may specify standard forms and procedures for requesting and granting access to the information referred to in paragraph 1, including for verification of the identity of the data subject and communicating the personal data to the data subject, taking into account the specific features and necessities of various sectors and data processing situations. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>	<p>3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the communication to the data subject of the content of the personal data referred to in point (g) of paragraph 1.</p> <p>4. The Commission may specify standard forms and procedures for requesting and granting access to the information referred to in paragraph 1, including for verification of the identity of the data subject and communicating the personal data to the data subject, taking into account the specific features and necessities of various sectors and data processing situations. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>
--	--	--	--

Justification

The EBF would welcome the restriction of the right of access for the data subject to the lawfulness of processing. We believe that recital 51 on competence is not sufficient to ensure that the said right of access should not be used for vexatious purposes or as part of a fishing expedition in the preparation of a law suit, but only for the establishment of the lawfulness of the access to data. More concrete conditions for the right of access in the recitals would be welcome. We would also welcome that the concrete condition: *“be aware and verify the lawfulness of the processing”* included in Recital 51 be added to the wording of Article 15 of the draft Regulation.

- Article 15, 1, g: The EBF believes that in order to ensure legal certainty of the scope, the communication of the personal data needs to be limited. Consumers need to specify their request (time or category of data etc.) and the answer needs to be consequently proportionate.
- Article 15, paragraph 2, last sentence of paragraph 2: as mentioned previously (see remarks under Article 12, paragraph 2), the EBF believes that a secure way is needed to be able to provide the said data. A proper identification of the subject is needed before providing any data and to prevent any data breach possibilities.
- The proposed Regulation requires the specific period for the retention of personal data to be relayed to the customer (Art 15, d). Given that different data will have different retention periods, it may be challenging for customers to view this information on a privacy notice. Provided that the business complies with existing obligations to retain data for as long as is necessary, this should satisfy the data protection requirements. It is therefore difficult to see how specifying a retention period for different types of data would necessarily benefit the customer.

- **Right to be forgotten and to erasure**

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
19.	Article 17, paragraph 1(a)	<p>1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child, where one of the following grounds applies:</p> <p>(a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; (...)</p>	<p>1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child, where one of the following grounds applies:</p> <p>(a) the data are no longer necessary in relation to the purposes for which they were collected or further processed and the legally mandatory minimum retention period has expired (...)</p>

Justification

The EBF is convinced that this article designed to protect internet social media users, may be extremely difficult to execute in the banking sector. Banks are obliged to store some data. For instance, for statistics purposes to process credit applications and assess objectively the creditworthiness of customers. As identified in others amendments the right to be forgotten and erasure should be limited in particular taking in consideration the data held by credit reference bureau. It should be paid attention to the misuse of this right in the field of credit.

Meeting the obligations the 3rd EU Anti-Money Laundering (AML) Directive also implies the storage of data for a long period of time. Article 30 of the 3rd AML Directive provides for instance that in the case of the customer due diligence the record keeping of documents and information is required for a period of **at least five years** after the business relationship with their customer has ended.

In the majority of cases, banks shall therefore not be able to erase all the data processed – on request of the data subject.

The term ‘further processed’ strikes a better balance regarding the Articles 6.4 and 5 b.

- **Right to data portability**

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
20.	Article 18	<ol style="list-style-type: none"> 1. The data subject shall have the right, where personal data are processed by electronic means and in a structured and commonly used format, to obtain from the controller a copy of data undergoing processing in an electronic and structured format which is commonly used and allows for further use by the data subject. 2. Where the data subject has provided the personal data and the processing is based on consent or on a contract, the data subject shall have the right to transmit those personal data and any other information provided by the data subject and retained by an automated processing system, into another one, in an electronic format which is commonly used, without hindrance from the controller from whom the personal data are withdrawn. 3. The Commission may specify the electronic format referred to in paragraph 1 and the technical standards, modalities and procedures for the transmission of personal data pursuant to paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2). 	<ol style="list-style-type: none"> 1. In cases of data stored in internet platforms of social networks, the data subject shall have the right, where personal data are processed by electronic means and in a structured and commonly used format, to obtain from the controller a copy of data undergoing processing in an electronic and structured format which is commonly used and allows for further use by the data subject. 2. Where the data subject has provided the personal data and the processing is based on consent or on a contract, the data subject shall have the right to transmit those personal data and any other information provided by the data subject and retained by an automated processing system, into another one, in an electronic format which is commonly used, without hindrance from the controller from whom the personal data are withdrawn. 3. The Commission may specify the electronic format referred to in paragraph 1 and the technical standards, modalities and procedures for the transmission of personal data pursuant to paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).
Justification <ul style="list-style-type: none"> • Only applicable to user generated content. • Article 18 applies to social networks and online-databases, where the data subject stores his personal data in an online-platform. The provision does not fit for processing of personal data in companies in their internal databases. Therefore EBF would like to limit the scope of Article 18 			

to storage of data in online-databases. Indeed, the extension of such a right to the financial sector seems inappropriate considering the nature of the data kept in bank servers, their sensitiveness and their variety. Should the scope of this provision not be limited, we are indeed concerned that the right to data portability increases the risk of disclosure of personal data to third parties.

- The EBF also would like to stress that the exercise of this right could require organizations to disclose information on trade secrets or information on other customers. The obligation to bank secrecy should be taken into account.
- If we take the example of a customer with a real estate loan. The data held about this customer including his financial credit worthiness represents at the same time intellectual property of the various financial institutions, which is protected by constitutional rights as well.
- This principle cannot lead to a completely imbalanced between claimant and defendant in case of a civil litigation as the data subject may be in the position to extract all data from the affected company or extract at least information which would have to be provided under the very civil procedure rules.

- **Measures based on profiling**

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
21.	Article 20	<ol style="list-style-type: none"> 1. Every natural person shall have the right not to be subject to a measure which produces legal effects concerning this natural person or significantly affects this natural person, and which is based solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour. 2. Subject to the other provisions of this Regulation, a person may be subjected to a measure of the kind referred to in paragraph 1 only if the processing: <ol style="list-style-type: none"> (a) is carried out in the course of the entering into, or performance of, a contract, where the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or where 	<ol style="list-style-type: none"> 1. Every natural person shall have the right not to be subject to a measure decision which produces legal effects concerning this natural person or significantly affects this natural person, and which is based solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour. 2. Subject to the other provisions of this Regulation, a person may be subjected to a measure of the kind referred to in paragraph 1 only if the processing: <ol style="list-style-type: none"> (a) is carried out in the course of the entering into, or performance of, a contract, where the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or where

		<p>suitable measures to safeguard the data subject's legitimate interests have been adduced, such as the right to obtain human intervention; or</p> <p>(b) is expressly authorized by a Union or Member State law which also lays down suitable measures to safeguard the data subject's legitimate interests; or</p> <p>(c) is based on the data subject's consent, subject to the conditions laid down in Article 7 and to suitable safeguards.</p> <p>3. Automated processing of personal data intended to evaluate certain personal aspects relating to a natural person shall not be based solely on the special categories of personal data referred to in Article 9.</p> <p>4. In the cases referred to in paragraph 2, the information to be provided by the controller under Article 14 shall include information as to the existence of processing for a measure of the kind referred to in paragraph 1 and the envisaged effects of such processing on the data subject.</p> <p>5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for suitable measures to safeguard the data subject's legitimate interests referred to in paragraph 2.</p>	<p>suitable measures to safeguard the data subject's legitimate interests have been adduced, such as the right to obtain human intervention; or</p> <p>(b) is necessary to comply with expressly authorized by a Union or Member State law which also lays down suitable measures to safeguard the data subject's legitimate interests; or</p> <p>(c) is based on the data subject's consent, subject to the conditions laid down in Article 7 and to suitable safeguards.</p> <p>3. Automated processing of personal data intended to evaluate certain personal aspects relating to a natural person shall not be based solely on the special categories of personal data referred to in Article 9.</p> <p>4. In the cases referred to in paragraph 2, the information to be provided by the controller under Article 14 shall include information as to the existence of processing for a measure of the kind referred to in paragraph 1 and the envisaged effects of such processing on the data subject.</p> <p>5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for suitable measures to safeguard the data subject's legitimate interests referred to in paragraph 2.</p>
--	--	---	--

Justification

- The EBF is concerned on the impact of the provisions concerning profiling to the European banking industry. The definition being too broad should be adapted as only decision having legal effect can be taken into consideration.
- Profiling is a typical technique used in the area of Anti Money Laundering to identify unusual financial transactions which might not fit in the financial profile of the customer. This is required by the Anti Money Laundering laws and it is also in the interest of the various financial

institutions not to be misused by criminal actions. It is therefore based on the balance of interests.

- It is important to stress that it might be an information overload for the customers if this information have to be given in advance of an e.g. current account contract.
- In addition, as not all requirements regarding Anti Money Laundering (AML) derive from the law itself but from supervisory authority circulars we believe that it is imperative to resolve the relationship of draft regulation and the AML Directive, local implementations and deduced circulars.
- Furthermore, the rules on profiling should not prohibit or restrict risk assessment as part of lending practices as foreseen for example in the EU Consumer Credit Directive and in banking supervisory law (risk-based approach by “Basel II”). The draft Regulation extends the restrictions of Directive 95/46 to practices that do not necessarily have a negative effect for people if they are intended to make information more relevant and more useful for the individual. By encompassing all forms of personalisation, whatever the possible impact on users, the new rules could compromise the effort made by companies to offer their customers "customised" products and services and degrade the quality of services offered to European citizens.
- Delegated acts for this purpose are not necessary: paragraph 2 is sufficient.

• **Responsibility of the controller**

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
22.	Article 22	<ol style="list-style-type: none"> 1. The controller shall adopt policies and implement appropriate measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation. 2. The measures provided for in paragraph 1 shall in particular include: <ol style="list-style-type: none"> (a) keeping the documentation pursuant to Article 28; (b) implementing the data security requirements laid down in Article 30; (c) performing a data protection impact assessment pursuant to Article 33; (d) complying with the requirements for prior authorisation or prior consultation of the supervisory authority pursuant to Article 	<ol style="list-style-type: none"> 1. The controller shall adopt policies and implement appropriate measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation. 2. The measures provided for in paragraph 1 shall in particular include: <ol style="list-style-type: none"> (a) keeping the documentation pursuant to Article 28; (b) implementing the data security requirements laid down in Article 30; (c) performing a data protection impact assessment pursuant to Article 33; (d) complying with the requirements for prior authorisation or prior consultation of the supervisory authority pursuant to Article 34(1)

		<p>34(1) and (2);</p> <p>(e) designating a data protection officer pursuant to Article 35(1).</p> <p>3. The controller shall implement mechanisms to ensure the verification of the effectiveness of the measures referred to in paragraphs 1 and 2. If proportionate, this verification shall be carried out by independent internal or external auditors.</p> <p>4. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures referred to in paragraph 1 other than those already referred to in paragraph 2, the conditions for the verification and auditing mechanisms referred to in paragraph 3 and as regards the criteria for proportionality under paragraph 3, and considering specific measures for micro, small and medium-sized-enterprises.</p>	<p>and (2);</p> <p>(e) designating a data protection officer pursuant to Article 35(1).</p> <p>3. The controller shall implement mechanisms to ensure the verification of the effectiveness of the measures referred to in paragraphs 1 and 2. If proportionate, this verification shall be carried out by independent internal or external auditors.</p> <p>4. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures referred to in paragraph 1 other than those already referred to in paragraph 2, the conditions for the verification and auditing mechanisms referred to in paragraph 3 and as regards the criteria for proportionality under paragraph 3, and considering specific measures for micro, small and medium sized enterprises.</p>
--	--	--	--

Justification

- **The proposed definitions of controller and processor lead to a difficult distinction of both concepts. The EBF members feel that the suggested provisions add a layer of bureaucracy that goes beyond what is necessary and will not lead to improved protection for individuals** (who may summon one or the other party and in the end still come to the conclusion that he/she summoned the wrong one). We would like to invite the European Commission to rethink the concepts of controller and processor. Leaving the definitions as they are, perpetuates the difficulties that in practice companies are facing when trying to comply with the data protection principles adequately.

For example in the banking sector, a financial institution can be seen as controller and processor at the same time when effecting payments on behalf of their customers. Additionally, the confusion is caused by the fact that the payer partially acts as controller in respect of the payment order.

Service providers in the different sectors are traditionally viewed as “simple” processors, but in reality they have the *de facto* control on the processing of the data, not the controller. The consequence of them being considered as “mere” processors is that it is not them upon whom the main privacy obligations fall, but still on the controller. It is therefore nor realistic nor fair that the controller primarily carries the weight of abiding by the data protection principles.

A solution would be to give sufficient freedom to such parties on how to best protect the privacy rights of individuals in a well established legal framework where an adequate balance between the privacy rights of individuals and the freedom to conduct a business (Article 16 of the EU Charter of Fundamental Rights) is sought.

- **Current banking supervision requirements combined with the proposed requirements may overlap. Duplication of burdens should be avoided.**
- **Furthermore, the duplication of burdens will lead to an increase of costs.**
- The EBF would suggest deleting the provision offering the possibility for the Commission to adopt delegated act as it is up to the controller to determine the measures required to meet its obligations.

- **Sector specific supervision: new article 22b**

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
23.	Proposal for a new Article 22b	-	Articles 23, 26, 27, 28, 29, 30, 31, 32, 33 do not apply if and insofar as the controller is subject to a similar obligation by virtue of sector specific Union law and under supervision of an independent sectorial Supervisory Authority.

Justification

By virtue of Article 22 of Directive 2006/48/EC the national legislator may designate the Banking Supervisory Authority as the competent authority to deal with security related issues in the financial sector.

- **Data protection by design and by default**

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
24.	Article 23	1. Having regard to the state of the art and the cost of implementation, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and	1. Having regard to the state of the art and the cost of implementation, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures

		<p>organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.</p> <p>2. The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals.</p> <p>3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures and mechanisms referred to in paragraph 1 and 2, in particular for data protection by design requirements applicable across sectors, products and services.</p> <p>4. The Commission may lay down technical standards for the requirements laid down in paragraph 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>	<p>and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.</p> <p>2. The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals.</p> <p>3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures and mechanisms referred to in paragraph 1 and 2, in particular for data protection by design requirements applicable across sectors, products and services.</p> <p>4. The Commission may lay down technical standards for the requirements laid down in paragraph 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>
--	--	--	--

Justification

- The EBF would suggest deleting the provision offering the possibility for the Commission to adopt delegated act as it is up to the controller to determine the measures required to meet its obligations.
- However, should the Commission adopt delegated acts, the European banking sector would strongly favour the opt-out option (default consent for data processing) in the “appropriate measures and mechanisms” to be designed by the European Commission in its delegated acts, according to paragraphs 3 and 4. This may be extremely helpful for cross-selling in banking sector.

• **Representatives of controllers not established in the Union**

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
25.	Article 25	<p>1. In the situation referred to in Article 3(2), the controller shall designate a representative in the Union.</p> <p>2. This obligation shall not apply to:</p> <p>(a) a controller established in a third country where the Commission has decided that the third country ensures an adequate level of protection in accordance with Article 41; or</p> <p>(b) an enterprise employing fewer than 250 persons; or</p> <p>(c) a public authority or body; or</p> <p>(d) a controller offering only occasionally goods or services to data subjects residing in the Union.</p> <p>3. The representative shall be established in one of those Member States where the data subjects whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, reside.</p> <p>4. The designation of a representative by the controller shall be without prejudice to legal actions which could be initiated against the controller itself.</p>	<p>1. In the situation referred to in Article 3(2), the controller shall designate a representative in the Union.</p> <p>2. This obligation shall not apply to:</p> <p>(a) a controller established in a third country where the Commission has decided that the third country ensures an adequate level of protection in accordance with Article 41; or</p> <p>(b) an enterprise employing fewer than 250 persons; or</p> <p>(c) a public authority or body; or</p> <p>(d) a controller offering only occasionally goods or services to data subjects residing in the Union.</p> <p>3. The representative shall be established in one of those Member States where the data subjects whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, reside.</p> <p>4. The designation of a representative by the controller shall be without prejudice to legal actions which could be initiated against the controller itself as the controller remains fully liable.</p>
<p>Justification</p> <p>Article 25 (4) implies that the representative can be held liable, while the representative should not be liable but the controller.</p>			

• Processor

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
26.	Article 26	<p>1. Where a processing operation is to be carried out on behalf of a controller, the controller shall choose a processor providing sufficient guarantees to implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject, in particular in respect of the technical security measures and organizational measures governing the processing to be carried out and shall ensure compliance with those measures.</p> <p>2. The carrying out of processing by a processor shall be governed by a contract or other legal act binding the processor to the controller and stipulating in particular that the processor shall:</p> <p>(a) act only on instructions from the controller, in particular, where the transfer of the personal data used is prohibited;</p> <p>(b) employ only staff who have committed themselves to confidentiality or are under a statutory obligation of confidentiality;</p> <p>(c) take all required measures pursuant to Article 30;</p> <p>(d) enlist another processor only with the prior permission of the controller;</p> <p>(e) insofar as this is possible given the nature of the processing, create in agreement with the controller the necessary technical and organisational requirements for the fulfilment of the controller's obligation to respond to requests</p>	<p>1. Where a processing operation is to be carried out on behalf of a controller, the controller shall choose a processor providing sufficient guarantees to implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject, in particular in respect of the technical security measures and organizational measures governing the processing to be carried out and shall ensure compliance with those measures.</p> <p>2. The carrying out of processing by a processor shall be governed by a contract or other legal act binding the processor to the controller and stipulating in particular that the processor shall:</p> <p>(a) act only on instructions from the controller, in particular, where the transfer of the personal data used is prohibited;</p> <p>(b) employ only staff who have committed themselves to confidentiality or are under a statutory obligation of confidentiality;</p> <p>(c) take all required measures pursuant to Article 30;</p> <p>(d) enlist another processor only with the prior permission of the controller;</p> <p>(e) insofar as this is possible given the nature of the processing, create in agreement with the controller the necessary technical and organisational requirements for the fulfilment of the controller's obligation to respond to requests</p>

		<p>for exercising the data subject's rights laid down in Chapter III;</p> <p>(f) assist the controller in ensuring compliance with the obligations pursuant to Articles 30 to 34;</p> <p>(g) hand over all results to the controller after the end of the processing and not process the personal data otherwise;</p> <p>(h) make available to the controller and the supervisory authority all information necessary to control compliance with the obligations laid down in this Article.</p> <p>3. The controller and the processor shall document in writing the controller's instructions and the processor's obligations referred to in paragraph 2.</p> <p>4. If a processor processes personal data other than as instructed by the controller, the processor shall be considered to be a controller in respect of that processing and shall be subject to the rules on joint controllers laid down in Article 24.</p> <p>5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the responsibilities, duties and tasks in relation to a processor in line with paragraph 1, and conditions which allow facilitating the processing of personal data within a group of undertakings, in particular for the purposes of control and reporting.</p>	<p>for exercising the data subject's rights laid down in Chapter III;</p> <p>(f) assist the controller in ensuring compliance with the obligations pursuant to Articles 30 to 34;</p> <p>(g) hand over all results to the controller after the end of the processing and not process the personal data otherwise;</p> <p>(h) make available to the controller and the supervisory authority all information necessary to control compliance with the obligations laid down in this Article.</p> <p>3. The controller and the processor shall document in writing the controller's instructions and the processor's obligations referred to in paragraph 2.</p> <p>4. If a processor processes personal data other than as instructed by the controller, the processor shall be considered to be a controller in respect of that processing and shall be subject to the rules on joint controllers laid down in Article 24.</p> <p>5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the responsibilities, duties and tasks in relation to a processor in line with paragraph 1, and conditions which allow facilitating the processing of personal data within a group of undertakings, in particular for the purposes of control and reporting.</p>
--	--	---	---

Justification

It is the controller that instructs the processor. If the processor processes personal data other than instructed by the controller, the processor violates the agreement. Considering the processor to be a joint controller would be conflicting with the duties, responsibilities and liability of both parties and the contractual relationship between both parties.

• Documentation

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
27.	Article 28	<p>1. Each controller and processor and, if any, the controller's representative, shall maintain documentation of all processing operations under its responsibility.</p> <p>2. The documentation shall contain at least the following information:</p> <ul style="list-style-type: none"> (a) the name and contact details of the controller, or any joint controller or processor, and of the representative, if any; (b) the name and contact details of the data protection officer, if any; (c) the purposes of the processing, including the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1); (d) a description of categories of data subjects and of the categories of personal data relating to them; (e) the recipients or categories of recipients of the personal data, including the controllers to whom personal data are disclosed for the legitimate interest pursued by them; (f) where applicable, transfers of data to a third country or an international organisation, including the identification of that third country or international organisation and, in case of transfers referred to in point (h) of Article 44(1), the documentation of appropriate safeguards; 	<p>1. Each controller and processor and, if any, the controller's representative, shall maintain an overview of all processing operations under its responsibility.</p> <p>2. The overview shall contain at least the following information:</p> <ul style="list-style-type: none"> (a) the name and contact details of the controller, or any joint controller or processor, and of the representative, if any; (b) the name and contact details of the data protection officer, if any; (c) the purposes of the processing, including the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1); (d) a description of categories of data subjects and of the categories of personal data relating to them; (e) the recipients or categories of recipients of the personal data, including the controllers to whom personal data are disclosed for the legitimate interest pursued by them; (f) where applicable, transfers of data to a third country or an international organisation, including the identification of that third country or international organisation and, in case of transfers referred to in point (h) of Article 44(1), the documentation of appropriate safeguards;

		<p>(g) a general indication of the time limits for erasure of the different categories of data;</p> <p>(h) the description of the mechanisms referred to in Article 22(3).</p> <p>3. The controller and the processor and, if any, the controller's representative, shall make the documentation available, on request, to the supervisory authority.</p> <p>4. The obligations referred to in paragraphs 1 and 2 shall not apply to the following controllers and processors:</p> <p>(a) a natural person processing personal data without a commercial interest; or</p> <p>(b) an enterprise or an organisation employing fewer than 250 persons that is processing personal data only as an activity ancillary to its main activities.</p> <p>5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the documentation referred to in paragraph 1, to take account of in particular the responsibilities of the controller and the processor and, if any, the controller's representative.</p> <p>6. The Commission may lay down standard forms for the documentation referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>	<p>(g) a general indication of the time limits for erasure of the different categories of data;</p> <p>(h) the description of the mechanisms referred to in Article 22(3).</p> <p>3. The controller and the processor and, if any, the controller's representative, shall make the documentation available, on request, to the supervisory authority.</p> <p>4. The obligations referred to in paragraphs 1 and 2 shall not apply to the following controllers and processors:</p> <p>(a) a natural person processing personal data without a commercial interest; or</p> <p>(b) an enterprise or an organisation employing fewer than 250 persons that is processing personal data only as an activity ancillary to its main activities.</p> <p>5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the documentation referred to in paragraph 1, to take account of in particular the responsibilities of the controller and the processor and, if any, the controller's representative.</p> <p>6. The Commission may lay down standard forms for the documentation referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>
--	--	--	--

Justification

One of the negative consequences of the draft Regulation is the administrative burden it could imply on businesses. Article 28 introduces an obligation for controllers and processors to maintain documentation of the processing operations for which they are responsible. As stated by the

EDPS in his opinion (sections 187-189) of 7th March, the EBF doubts whether the proposed provision will lower the administrative burden.

The EBF suggests therefore deleting the word “at least” to define clearly the information that the documentation shall contain.

It is not feasible to maintain documentation of all processing operations. Within the banking activities there are many processing operations. Processing of transactions alone would be impossible to document, it would mean an enormous burden on administration and archiving. It is, however, possible to maintain an overview of all the categories of processing operations.

- **Security of processing**

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
28.	Article 30	<p>1. The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected, having regard to the state of the art and the costs of their implementation.</p> <p>2. The controller and the processor shall, following an evaluation of the risks, take the measures referred to in paragraph 1 to protect personal data against accidental or unlawful destruction or accidental loss and to prevent any unlawful forms of processing, in particular any unauthorised disclosure, dissemination or access, or alteration of personal data.</p> <p>3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the technical and organisational measures referred to in paragraphs 1 and 2, including the determinations of what constitutes the state of the art, for specific sectors and in specific data processing situations, in particular taking account of developments in technology and solutions for privacy by design and data protection</p>	<p>1. The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected, having regard to the state of the art and the costs of their implementation.</p> <p>2. The controller and the processor shall, following an evaluation of the risks, take the measures referred to in paragraph 1 to protect personal data against accidental or unlawful destruction or accidental loss and to prevent any unlawful forms of processing, in particular any unauthorised disclosure, dissemination or access, or alteration of personal data.</p> <p>3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the technical and organisational measures referred to in paragraphs 1 and 2, including the determinations of what constitutes the state of the art, for specific sectors and in specific data processing situations, in particular taking account of developments in technology and solutions for privacy by design and data protection by default,</p>

	<p>by default, unless paragraph 4 applies.</p> <p>4. The Commission may adopt, where necessary, implementing acts for specifying the requirements laid down in paragraphs 1 and 2 to various situations, in particular to:</p> <ul style="list-style-type: none"> (a) prevent any unauthorised access to personal data; (b) prevent any unauthorised disclosure, reading, copying, modification, erasure or removal of personal data; (c) ensure the verification of the lawfulness of processing operations. <p>Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>	<p>unless paragraph 4 applies.</p> <p>4. The Commission may, where necessary, provide guidelines for specifying the requirements laid down in paragraphs 1 and 2 to various situations, in particular to:</p> <ul style="list-style-type: none"> (a) prevent any unauthorised access to personal data; (b) prevent any unauthorised disclosure, reading, copying, modification, erasure or removal of personal data; (c) ensure the verification of the lawfulness of processing operations. <p>Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>
--	--	---

Justification

Depending on the type of business of the controller and the assignment to the processor appropriate technical and organizational measures may differ. It is therefore up to controller and processor to determine these measures. Guidelines may be provided by the Commission.

• **Notification of a personal data breach to the supervisory authority**

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
29.	Article 31	<p>1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 24 hours after having become aware of it, notify the personal data breach to the supervisory authority. The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within 24 hours.</p>	<p>1. In the case of any significantly harmful a-personal data breach the controller shall without undue delay and, where feasible, not later than 24 hours after having become aware of it, notify the personal data breach to the supervisory authority within a reasonable time. The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within 24 hours.</p> <p>A significantly harmful personal data breach</p>

		<p>2. Pursuant to point (f) of Article 26(2), the processor shall alert and inform the controller immediately after the establishment of a personal data breach.</p> <p>3. The notification referred to in paragraph 1 must at least:</p> <ul style="list-style-type: none"> (a) describe the nature of the personal data breach including the categories and number of data subjects concerned and the categories and number of data records concerned; (b) communicate the identity and contact details of the data protection officer or other contact point where more information can be obtained; (c) recommend measures to mitigate the possible adverse effects of the personal data breach; (d) describe the consequences of the personal data breach; (e) describe the measures proposed or taken by the controller to address the personal data breach. <p>4. The controller shall document any personal data breaches, comprising the facts surrounding the</p>	<p>shall be determined by the controller, who can be assisted by the data protection officer, based on factors including the assessment of whether a personal data breach has created serious breaches for a significant number of data subjects.</p> <p>Exemptions from data breach provisions should be awarded where sophisticated encryption is used or if measures are taken to adequately compensate those affected.</p> <p>2. Pursuant to point (f) of Article 26(2), the processor shall alert and inform the controller immediately after the establishment of a personal data breach.</p> <p>3. The notification referred to in paragraph 1 must at least:</p> <ul style="list-style-type: none"> (a) describe the nature of the personal data breach including the categories and number of data subjects concerned and the categories and number of data records concerned; (b) communicate the identity and contact details of the data protection officer or other contact point where more information can be obtained; (c) recommend measures to mitigate the possible adverse effects of the personal data breach; (d) describe the consequences of the personal data breach; (e) describe the measures proposed or taken by the controller to address the personal data breach. <p>4. The controller shall document any personal data breaches, comprising the facts surrounding the</p>
--	--	--	---

		<p>breach, its effects and the remedial action taken. This documentation must enable the supervisory authority to verify compliance with this Article. The documentation shall only include the information necessary for that purpose.</p> <p>5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for establishing the data breach referred to in paragraphs 1 and 2 and for the particular circumstances in which a controller and a processor is required to notify the personal data breach.</p> <p>6. The Commission may lay down the standard format of such notification to the supervisory authority, the procedures applicable to the notification requirement and the form and the modalities for the documentation referred to in paragraph 4, including the time limits for erasure of the information contained therein. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>	<p>breach, its effects and the remedial action taken. This documentation must enable the supervisory authority to verify compliance with this Article. The documentation shall only include the information necessary for that purpose.</p> <p>5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for establishing the data breach referred to in paragraphs 1 and 2 and for the particular circumstances in which a controller and a processor is required to notify the personal data breach.</p> <p>6. The Commission may lay down the standard format of such notification to the supervisory authority, the procedures applicable to the notification requirement and the form and the modalities for the documentation referred to in paragraph 4, including the time limits for erasure of the information contained therein. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>
--	--	--	--

Justification

Financing institutions fully understand that there are circumstances that require notification to a financial and or data protection regulator in the event of a breach.

Introducing an obligation to notify personal data breaches in 24 hours for other sectors than the telecommunications sectors appears however quite disproportionate to the EBF.

Furthermore, this obligation might even conflict with national financial law and regulation.

At present, banks already notify their customers for instance if their credit card has been skimmed (i.e. information about a card and the associated PIN-code is copied for the purpose of manufacturing a fake card). It is also in the bank’s interest to protect their customers against fraud and sustain a very high level of security. The banks can also be held liable for damages their customers may suffer due to deficiencies in banks IT- security systems. The banks test and update their systems and security solutions regularly to make sure that the information in the bank’s system is always well-protected and secure. The transfer of information between the customer’s computer and the online banking system is always encrypted. The customer must also make sure that his/her computer, codes and personal information are protected to prevent the possibility of fraud. **To avoid**

“data breaches” it would be more effective to inform customers on how to protect their own computers, never disclose their bank account details to unknown persons etc.

- A mandatory personal data breach notification system could first give rise to organizational concerns since the implementation of such a system of notification could burden and delay the process of information to the customers.
- Attention should be paid to the criteria which trigger the obligation to notify: **The notification requirement should be limited to serious breaches affecting more than one individual.** There is otherwise a danger of triggering an avalanche of notifications with the potential to confuse and unnecessarily alarm individuals or desensitise affected data subjects (where notifications are so commonplace they are to a large extent ignored by the recipient, thereby rendering the notification worthless).
- **Exemptions from data breach provisions should be awarded where sophisticated encryption is used.** This will encourage the practice of encrypting personal data, especially prior to their transmission. It should also be possible to dispense with notification if measures are taken to adequately compensate those affected, e.g. by issuing new credit cards to replace cards whose details have been compromised.

A framework where notification is made in the most expedient time possible would achieve the goal of ensuring regulators and data subjects are well informed without causing unnecessary burden for regulators or alarm to victims of breaches.

In addition, especially for the banking sector, notification to data subjects at all times may enable certain forms of fraud.

- The obligation to notify the supervisory authority negatively affects certain sectors. The banking, insurance and telecoms sector have already specific obligations entailing the notification of such breaches (substantial disruptions in service provided to the customers and in payment and IT system) to the relevant competent authorities. **This would result in an unnecessary double process/reporting.**
- It is unlikely that delegated acts will be adopted at the moment when the Regulation will start to apply. Therefore the new obligations cannot effectively be implemented in the sense that, if no delegated act is in place, every single data breach will have to be notified to the national supervisory authority.

In the absence of clear provisions ensuring legal certainty, the national supervisory authorities’ practices might be highly inconsistent. Therefore, EBF is of the view that the rules regarding data breach notifications constitute essential elements of the proposal within the meaning of Article 290 of the Treaty on the Functioning of the European Union (TFEU) (Opinion shared by the EDPS and the Working Party Article 29) and should not be left to be regulated by means of delegated acts.

• **Communication of a personal data breach to the data subject**

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
30.	Article 32	1. When the personal data breach is likely to adversely affect the protection of the personal data or privacy of the data subject, the controller	1. In the case of any significantly harmful personal data breach , when the personal data breach is likely to adversely affect the protection of the

		<p>shall, after the notification referred to in Article 31, communicate the personal data breach to the data subject without undue delay.</p> <ol style="list-style-type: none"> 2. The communication to the data subject referred to in paragraph 1 shall describe the nature of the personal data breach and contain at least the information and the recommendations provided for in points (b) and (c) of Article 31(3). 3. The communication of a personal data breach to the data subject shall not be required if the controller demonstrates to the satisfaction of the supervisory authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the personal data breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it. 4. Without prejudice to the controller's obligation to communicate the personal data breach to the data subject, if the controller has not already communicated the personal data breach to the data subject of the personal data breach, the 	<p>personal data or privacy of the data subject, the controller shall, after the notification referred to in Article 31, communicate the personal data breach to the data subject without undue delay.</p> <p>A significantly harmful personal data breach shall be determined by the controller based on factors including the assessment of whether a personal data breach has created serious breaches for a significant number of data subjects.</p> <p>Exemptions from data breach provisions should be awarded where sophisticated encryption is used or if measures are taken to adequately compensate those affected.</p> <ol style="list-style-type: none"> 2. The communication to the data subject referred to in paragraph 1 shall describe the nature of the personal data breach and contain at least the information and the recommendations provided for in points (b) and (c) of Article 31(3). 3. The communication of a personal data breach to the data subject shall not be required if the controller demonstrates to the satisfaction of the supervisory authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the personal data breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it. 4. Without prejudice to the controller's obligation to communicate the personal data breach to the data subject, if the controller has not already communicated the personal data breach to the data subject of the personal data breach, the supervisory
--	--	---	---

		<p>supervisory authority, having considered the likely adverse effects of the breach, may require it to do so.</p> <p>5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements as to the circumstances in which a personal data breach is likely to adversely affect the personal data referred to in paragraph 1.</p> <p>6. The Commission may lay down the format of the communication to the data subject referred to in paragraph 1 and the procedures applicable to that communication. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>	<p>authority, having considered the likely adverse effects of the breach, may require it to do so.</p> <p>5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements as to the circumstances in which a personal data breach is likely to adversely affect the personal data referred to in paragraph 1.</p> <p>6. The Commission may lay down the format of the communication to the data subject referred to in paragraph 1 and the procedures applicable to that communication. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>
--	--	---	---

Justification

- A wide mandatory personal data breach notification system could give rise to organisational concerns since the implementation of such a system of notification would lead to an administrative burden and in fact risk delaying the process of contacting customers when it is really necessary (i.e. when the breach is significantly harmful)
- Attention should be paid to the criteria which trigger the obligation to notify: **The notification requirement should be limited to serious breaches affecting more than one individual.** There is otherwise a danger of triggering an avalanche of notifications with the potential to confuse and unnecessarily alarm individuals or desensitise affected data subjects (where notifications are so commonplace they are to a large extent ignored by the recipient, thereby rendering the notification worthless).
- **Exemptions from data breach provisions should be awarded where sophisticated encryption is used.** This will encourage the practice of encrypting personal data, especially prior to their transmission. It should also be possible to dispense with notification if measures are taken to adequately compensate those affected, e.g. by issuing new credit cards to replace cards whose details have been compromised.

A framework where notification is made in the most expedient time possible would achieve the goal of ensuring regulators and data subjects are well informed without causing unnecessary burden for regulators or alarm to victims of breaches.

In addition, especially for the banking sector, notification to Data Subjects at all times, may enable certain forms of fraud

- What is more worrying, an attempt to **clarify what should constitute ‘adversely affect’** exists currently only in Recital 66, notably a breach should be considered as adversely affecting the personal data or privacy of a data subject where it could result in, for example, identity theft or fraud, physical harm, significant humiliation or damage to reputation.

- Both Articles 31 and 32 empower the Commission to adopt delegated acts to further specify the criteria and the requirements for establishing the data breach and the circumstances in which a personal data breach is likely to adversely affect the personal data. It is unlikely that delegated acts will be adopted at the moment when the Regulation will start to apply. Therefore the new obligations cannot effectively be implemented in the sense that, if no delegated act is in place, every single data breach will have to be notified to the national supervisory authority/communicated to the data subject.

EBF is of the view that the rules regarding data breach notifications constitute essential elements of the proposal within the meaning of Article 290 of the Treaty on the Functioning of the European Union (TFEU) (Opinion shared by the EDPS and the Working Party Article 29) and should not be left to be regulated by means of delegated acts.

- Restrictions from the application of Article 32 are possible only if laid down in Union or Member State law under Article 21 of the draft Regulation (Restrictions).

- Sectorial Supervisory Authority: New Article 32b**

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
31.	New Article 32b	-	Articles 31 and 32 do not apply if and insofar as the controller is subject to an obligation to notify an independent sectorial Supervisory Authority by virtue of legislation based on sector specific Union law.

Justification

By virtue of Article 22 of Directive 2006/48/EC, the national legislator may designate the Banking Supervisory Authority as the competent authority to deal with security breaches in the financial sector.

- Data protection impact assessment**

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
32.	Article 33	1. Where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes,	1. Where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes,

		<p>the controller or the processor acting on the controller's behalf shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.</p> <p>2. The following processing operations in particular present specific risks referred to in paragraph 1:</p> <p>(a) a systematic and extensive evaluation of personal aspects relating to a natural person or for analysing or predicting in particular the natural person's economic situation, location, health, personal preferences, reliability or behaviour, which is based on automated processing and on which measures are based that produce legal effects concerning the individual or significantly affect the individual;</p> <p>(b) information on sex life, health, race and ethnic origin or for the provision of health care, epidemiological researches, or surveys of mental or infectious diseases, where the data are processed for taking measures or decisions regarding specific individuals on a large scale;</p> <p>(c) monitoring publicly accessible areas, especially when using optic-electronic devices (video surveillance) on a large scale;</p> <p>(d) personal data in large scale filing systems on children, genetic data or biometric data;</p> <p>(e) other processing operations for which the consultation of the supervisory authority is required pursuant to point (b) of Article 34(2).</p>	<p>the controller or the processor acting on the controller's behalf shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.</p> <p>2. The following processing operations in particular present specific risks referred to in paragraph 1:</p> <p>(a) a systematic and extensive evaluation of personal aspects relating to a natural person or for analysing or predicting in particular the natural person's economic situation, location, health, personal preferences, reliability or behaviour, which is based on automated processing and on which measures are based that produce legal effects concerning the individual or significantly affect the individual;</p> <p>(b) information on sex life, health, race and ethnic origin or for the provision of health care, epidemiological researches, or surveys of mental or infectious diseases, where the data are processed for taking measures or decisions regarding specific individuals on a large scale;</p> <p>(c) monitoring publicly accessible areas, with the exception of the banking devices especially when using optic-electronic devices (video surveillance) on a large scale;</p> <p>(d) personal data in large scale filing systems on children, genetic data or biometric data;</p> <p>(e) other processing operations for which the consultation of the supervisory authority is required pursuant to point (b) of Article 34(2).</p>
--	--	---	---

	<p>3. The assessment shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned.</p> <p>4. The controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations.</p> <p>5. Where the controller is a public authority or body and where the processing results from a legal obligation pursuant to point (c) of Article 6(1) providing for rules and procedures pertaining to the processing operations and regulated by Union law, paragraphs 1 to 4 shall not apply, unless Member States deem it necessary to carry out such assessment prior to the processing activities.</p> <p>6. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the processing operations likely to present specific risks referred to in paragraphs 1 and 2 and the requirements for the assessment referred to in paragraph 3, including conditions for scalability, verification and auditability. In doing so, the Commission shall consider specific measures for micro, small and medium-sized enterprises.</p> <p>7. The Commission may specify standards and procedures for carrying out and verifying and</p>	<p>3. The assessment shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned.</p> <p>4. The controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations.</p> <p>5. Where the controller is a public authority or body and where the processing results from a legal obligation pursuant to point (c) of Article 6(1) providing for rules and procedures pertaining to the processing operations and regulated by Union law, paragraphs 1 to 4 shall not apply, unless Member States deem it necessary to carry out such assessment prior to the processing activities.</p> <p>6. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the processing operations likely to present specific risks referred to in paragraphs 1 and 2 and the requirements for the assessment referred to in paragraph 3, including conditions for scalability, verification and auditability. In doing so, the Commission shall consider specific measures for micro, small and medium-sized enterprises.</p> <p>7. The Commission may specify standards and procedures for carrying out and verifying and</p>
--	---	---

		auditing the assessment referred to in paragraph 3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	auditing the assessment referred to in paragraph 3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).
--	--	---	---

Justification

Data protection impact assessments cause unwanted burden and costs on business with little benefit as well as an unwanted administrative burden on individuals in question. In order to lessen the burden, consultation with data subjects should be eliminated.

- In the draft Regulation, the requirement for an impact assessment can be sanctioned by a fine of € 1,000,000 or 2% of the company's annual worldwide turnover. Considering that the wording "specific risk" is too vague and could be interpreted as limiting the requirement to only treatments listed in Article 33, deleting the word "in particular", would ensure more legal certainty.
- Processing operations' specific risks listed in 2. (a) are already mentioned and controlled by the Article 20 of this draft Regulation, it is therefore not necessary to add any additional conditions by submitting them to an impact assessment as profiling does not present any particular risks. The deletion of paragraph 2. (a) is therefore necessary.
- In order to ensure the public, the customers and the employees' security, banking activities require using optic-electronic devices (video surveillance. In these circumstances and given the specific need for the banking sector, the banking devices should be exempted from this requirement.
- In line with the justification mentioned above, the EBF suggests deleting article 33.4 as obtaining the consent of the data subject for all the processing operations requiring an impact assessment would be unrealistic leading to unreasonable charges, especially for large-scale processing operations.
- The criteria and conditions applicable to processing operations that may present specific risks, the contents of the impact assessment and the conditions of modularity, of the verification and of the auditability are key elements to be included in the regulation itself. It is therefore necessary to delete paragraph 6 related to delegated acts.

• **Designation of the data protection officer**

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
33.	Article 35	1. The controller and the processor shall designate a data protection officer in any case where: <ul style="list-style-type: none"> (a) the processing is carried out by a public authority or body; or (b) the processing is carried out by an enterprise 	1. The controller and the processor may shall designate a data protection officer in some any case where: <ul style="list-style-type: none"> (a) the processing is carried out by a public authority or body; or

		<p>employing 250 persons or more; or</p> <p>(c) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects.</p> <p>2. In the case referred to in point (b) of paragraph 1, a group of undertakings may appoint a single data protection officer.</p> <p>3. Where the controller or the processor is a public authority or body, the data protection officer may be designated for several of its entities, taking account of the organisational structure of the public authority or body.</p> <p>4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may designate a data protection officer.</p> <p>5. The controller or processor shall designate the data protection officer on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and ability to fulfil the tasks referred to in Article 37. The necessary level of expert knowledge shall be determined in particular according to the data processing carried out and the protection required for the personal data processed by the controller or the processor.</p> <p>6. The controller or the processor shall ensure that any other professional duties of the data protection</p>	<p>(b) the processing is carried out by an enterprise employing 250 persons or more; or</p> <p>(c) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects.</p> <p>2. In the case referred to in point (b) of paragraph 1, a group of undertakings may appoint a single data protection officer. A group of undertakings may designate a single data protection officer to deal with one or several issues implemented by several entities of the group.</p> <p>3. Where the controller or the processor is a public authority or body, the data protection officer may be designated for several of its entities, taking account of the organisational structure of the public authority or body.</p> <p>4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may designate a data protection officer.</p> <p>5. The controller or processor shall designate the data protection officer on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and ability to fulfil the tasks referred to in Article 37. The necessary level of expert knowledge shall be determined in particular according to the data processing carried out and the protection required for the personal data processed by the controller or the processor.</p> <p>6. The controller or the processor shall ensure that any other professional duties of the data protection officer are compatible with the person's tasks and</p>
--	--	---	---

		<p>officer are compatible with the person's tasks and duties as data protection officer and do not result in a conflict of interests.</p> <p>7. The controller or the processor shall designate a data protection officer for a period of at least two years. The data protection officer may be reappointed for further terms. During their term of office, the data protection officer may only be dismissed, if the data protection officer no longer fulfils the conditions required for the performance of their duties.</p> <p>8. The data protection officer may be employed by the controller or processor, or fulfil his or her tasks on the basis of a service contract.</p> <p>9. The controller or the processor shall communicate the name and contact details of the data protection officer to the supervisory authority and to the public.</p> <p>10. Data subjects shall have the right to contact the data protection officer on all issues related to the processing of the data subject's data and to request exercising the rights under this Regulation.</p> <p>11. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the core activities of the controller or the processor referred to in point (c) of paragraph 1 and the criteria for the professional qualities of the data protection officer referred to in paragraph 5.</p>	<p>duties as data protection officer and do not result in a conflict of interests.</p> <p>7. The controller or the processor shall designate a data protection officer for a period of at least two years. The data protection officer shall have a level of management autonomy and may be reappointed for further terms. During their term of office, the data protection officer may only be dismissed, if the data protection officer no longer fulfils the conditions required for the performance of their duties.</p> <p>8. The data protection officer may be employed by the controller or processor, or fulfil his or her tasks on the basis of a service contract.</p> <p>9. The controller or the processor shall communicate the name and contact details of the data protection officer to the supervisory authority and to the public.</p> <p>10. Data subjects shall have the right to contact the data protection officer or any delegated officer on all issues related to the processing of the data subject's data and to request exercising the rights under this Regulation.</p> <p>11. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the core activities of the controller or the processor referred to in point (c) of paragraph 1 and the criteria for the professional qualities of the data protection officer referred to in paragraph 5.</p>
--	--	--	---

Justification

The designation of a data protection officer (DPO) as well as the working procedures of the DPO shall be subject to more flexibility than in the current EC proposal.

- The EBF is aware of good experiences with data protection officers in some EU Member States. Nevertheless, the EBF questions the added value of a EU-wide mandatory implementation of a data protection officer. Good knowledge of data protection issues within an organisation as well as a good complaints resolution procedure is sufficient. Such a mandatory introduction could indeed lead to further administrative expenditures and not bring any added value.
- The EBF considers that in some group of undertakings some treatments may be common to different companies for transversal issues such as human resources, anti-money laundering and fight against terrorist financing, etc. In this perspective, the EBF believes that a group of undertakings might designate a single data protection officer to deal with one or several issues implemented by several entities of the group, for the group of undertakings to designate one data protection officer.
- In the EBF views, to ensure the independence of the DPO, it has to have a functional independence.
- The EBF considers the provision mentioning that “During their term of office, the data protection officer may only be dismissed, if the data protection officer no longer fulfils the conditions required for the performance of their duties” could be disproportionate and conflict with some provisions related to labour law. It may even mean, quite illogically, that for an employer there will be no chance of contract termination with a DPO for any other breach of their duties based on provision of law or contract, except for the reason stipulated above.
- The EBF believes that the contact details of the DPO should not be communicated to the public (otherwise personal data of a DPO will not be protected the same way as the data of other employees). Indeed, the EBF considers that the public have the possibility to contact the controller who will decide of the necessity to contact or not the DPO.

- **Transfers by way of binding corporate rules**

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
34.	Article 43	<p>1. A supervisory authority shall in accordance with the consistency mechanism set out in Article 58 approve binding corporate rules, provided that they:</p> <p>(a) are legally binding and apply to and are enforced by every member within the controller’s or processor’s group of undertakings, and include their employees;</p> <p>(b) expressly confer enforceable rights on data subjects;</p>	<p>1. A supervisory authority shall in accordance with the consistency mechanism set out in Article 58 approve binding corporate rules, provided that they:</p> <p>(a) are legally binding and apply to and are enforced by every member within the controller’s or processor’s group of undertakings, cooperating financial companies, and include their employees;</p> <p>(b) expressly confer enforceable rights on data subjects;</p>

		<p>(c) fulfil the requirements laid down in paragraph 2.</p> <p>2. The binding corporate rules shall at least specify:</p> <p>(a) the structure and contact details of the group of undertakings and its members;</p> <p>(b) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;</p> <p>(c) their legally binding nature, both internally and externally;</p>	<p>(c) fulfil the requirements laid down in paragraph 2.</p> <p>2. The binding corporate rules shall at least specify:</p> <p>(a) the structure and contact details of the group of undertakings and its members;</p> <p>(b) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;</p> <p>(c) their legally binding nature, both internally and externally;</p>
--	--	---	--

Justification

It is important for the EBF that not only “controller’s or processor’s group of undertaking” can use binding corporate rules (BCRs) but also cooperating financial companies, e.g. cooperation between banks and insurance companies or mortgage companies. It is indeed essential that a level playing field applies concerning the exchange of information within group companies and exchange of information between cooperating companies.

Currently organisations can rely on internal policies to make BCRs binding. However, Article 43 explicitly requires that BCRs are legally binding. Our members suggest removing this requirement to ensure that already approved BCRs remain valid. This would also ensure that BCRs can become an effective and efficient measure for transfers or personal data and thus gain momentum as it would give organisations the flexibility how they ensure the binding nature of BCRs within their group.

Article 43.2 b establishes that among other aspects BCRs should specify the data transfers or set of transfers, “including the categories of personal data” and the “type of processing”. Categories of personal data and the types of processing should not be referred to in the BCRs. Making a list of these items may be contra-productive. What if new data categories of data are processed by the data controller or new types of processing are carried out with regard to the data subjects that are covered by the BCRs? Would then such data not fall within the scope of the BCRs? Would this mean that new BCRs need to be approved?

- Derogations

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
35.	Article 44	<p>1. In the absence of an adequacy decision pursuant to Article 41 or of appropriate safeguards pursuant to Article 42, a transfer or a set of transfers of personal data to a third country or an international organisation may take place only on condition that:</p> <p>(...)</p> <p>(e) the transfer is necessary for the establishment, exercise or defence of legal claims; or</p> <p>(...)</p> <p>(h) the transfer is necessary for the purposes of the legitimate interests pursued by the controller or the processor, which cannot be qualified as frequent or massive, and where the controller or processor has assessed all the circumstances surrounding the data transfer operation or the set of data transfer operations and based on this assessment adduced appropriate safeguards with respect to the protection of personal data, where necessary.</p> <p>4. Points (b), (c) and (h) of paragraph 1 shall not apply to activities carried out by public authorities in the exercise of their public powers.</p> <p>5. The public interest referred to in point (d) of</p>	<p>1. In the absence of an adequacy decision pursuant to Article 41 or of appropriate safeguards pursuant to Article 42, a transfer or a set of transfers of personal data to a third country or an international organisation may place only on condition that:</p> <p>(...)</p> <p>(e) the transfer is necessary for the establishment, exercise or defence of legal claims; or to comply with requirements of competent governmental or regulatory authorities of such third countries to which the data controller or processor is subject.</p> <p>(...)</p> <p>(h) the transfer is necessary for the purposes of the legitimate interests pursued by the controller or the processor, which cannot be qualified as frequent or massive, and where the controller or processor has assessed all the circumstances surrounding the data transfer operation or the set of data transfer operations and based on this assessment adduced appropriate safeguards with respect to the protection of personal data, where necessary.</p> <p>4. Points (b), (c) and (h) of paragraph 1 shall not apply to activities carried out by public authorities in the exercise of their public powers.</p> <p>5. The public interest referred to in point (d) of paragraph 1 must be recognised in Union law or</p>

		<p>paragraph 1 must be recognised in Union law or in the law of the Member State to which the controller is subject.</p> <p>6. The controller or processor shall document the assessment as well as the appropriate safeguards adduced referred to in point (h) of paragraph 1 of this Article in the documentation referred to in Article 28 and shall inform the supervisory authority of the transfer.</p>	<p>in the law of the Member State to which the controller is subject.</p> <p>6. Where a transfer is based on Article 44. 1 h and the nature of the transfer or set of transfers is such that the privacy rights of the data subjects need to be adequately protected, the controller or processor shall document the assessment as well as the appropriate safeguards adduced referred to in point (h) of paragraph 1 of this Article in the documentation referred to in Article 28 and shall consider informing the supervisory authority of the transfer.</p>
--	--	---	--

Justification

- It is the view of the banking sector that an exception for the disclosure of personal data to regulators or authorities of third countries to which data controllers are also subject should be explicitly referred to in the Regulation.
- **The “legitimate interest” exception**
 1. The banking sector welcomes this exception, however a further analysis of this provision reveals that data controllers will hardly be able to rely on it as it is currently drafted.
 2. The banking sector understands that where a data transfer is not massive or frequent such transfer is less likely to infringe the privacy rights of data subjects. To be able to rely on this ground, the banking sector proposes stipulating that any transfer based on this ground should be subject to a weighing of interests: the legitimate interest of the data controller to disclose on the one hand and on the other, the privacy rights of the data subjects. In doing so, banks should observe the principles of necessity, subsidiarity and proportionality, and adduce necessary safeguards for the transfer. These safeguards should be in syntony with the nature of such a data transfer. The banking sector is aware of the fact that documenting the steps that may lead to the disclosure contributes to making an adequate assessment of the situation. However, transfers that are less likely to affect the privacy rights of data subjects it should not be necessary to document the steps or to inform the supervisory authorities of the transfer.
 3. This would cover the situation that a regulator in a third country requires once or twice (hence not frequently) specific information that could affect clients or employees of European banks, but also other possible transfers that would not be covered by the other options set out in Chapter V of the regulation. This would also cover certain disclosures to their parties in complex banking transactions where it cannot be said that the disclosure is for the benefit of the data subject and where the infringement of the privacy rights of the data subjects are unlikely to be affected, such as in securitisations or in the transfer of certain titles or claims.
 4. However, it can be that due to specific legislation to which branches or subsidiaries in third countries of EU based financial institutions requires those branches or subsidiaries to provide for “frequent” disclosure of information of the EU subsidiary including individuals’ related data.
 5. The banking sector understands that most “massive” and “frequent” disclosures to third countries can take place either because the transfer is

effected to a country where an adequacy decision as per section 41 of the draft regulation exists, adequate safeguards as per section 42 of the draft regulation have been adopted, or where BCRs are in place as per article 43. However requests of regulators that could be qualified as “frequent” do not find a justification in the current draft Chapter V, while it would still be justified to state that a legitimate interest of the bank would exist for such “frequent” or “massive” disclosure.

6. It is the view of the banking sector that a final ground for transfers which are massive or frequent should be allowed under the Regulation. Of course, since this type of transfers are likely to infringe the privacy rights of the data subjects, the banking sector understands that adequate measures should be in place. Since banks understand the nature of the requests for disclosure, they can also assess which measures are most appropriate to respond to the protection of the individuals’ right to privacy as recognised in the Regulation.

7. The Regulation’s accountability principle should guarantee that the financial sector is able to decide which measures are the most appropriate when a data transfer would take place based on a “legitimate interest”.

8. The most efficient way to address this is deleting the words “frequent” and “massive” and leave financial institutions with the burden of assessing themselves whether such transfer would be allowed. Financial institutions should do so based on the general principles of the Regulation such as necessity, subsidiarity and proportionality and the obligation to consider the adoption of additional adequate safeguards. These may include – depending on the nature of the transfer- informing the privacy regulator.

9. Data controllers should first assess whether the transfer can be made based on other grounds. Secondly, when it has been established that this is not the case, the principles of the Regulation should be applied and an assessment should be made as to which additional measures should be taken to ensure that the privacy rights of the data subjects are adequately addressed.

- **The “public interest” exception**

1. This derogation is to be read in conjunction with Article 44.4 and 44.7 of the draft Regulation. Article 44.5 limits this derogation to the extent that it only applies where the public interest is recognised in Union law or in the law of the Member State to which the data controller is subject.

2. The banking sector believes that such public interest should also be a public interest recognised abroad. The enacting of laws abroad that provide for the disclosure of detailed banking related information responds to very specific needs of public interest [and are the product of a democratic process]. In such circumstances, banks should be able to assess the circumstances of an obligation to disclose based on the powers of a foreign regulator and weigh the privacy rights of the data subjects against the public interest at hand. The banking sector believes that the decision of disclosing such data should not be lightly made and as counterweigh, additional measures should be put in place to make such disclosure in line with the principles of the Regulation, as it should occur prior to any data processing. Any request for disclosure should be first tested against the principles of necessity, subsidiarity and proportionality. In addition and where necessary, special arrangements with the receiving party concerning the confidentiality of the data could be made.

- Supervisory authority

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
36.	Article 46	<ol style="list-style-type: none"> 1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application of this Regulation and for contributing to its consistent application throughout the Union, in order to protect the fundamental rights and freedoms of natural persons in relation to the processing of their personal data and to facilitate the free flow of personal data within the Union. For these purposes, the supervisory authorities shall co-operate with each other and the Commission. 2. Where in a Member State more than one supervisory authority are established, that Member State shall designate the supervisory authority which functions as a single contact point for the effective participation of those authorities in the European Data Protection Board and shall set out the mechanism to ensure compliance by the other authorities with the rules relating to the consistency mechanism referred to in Article 57. 3. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to this Chapter, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them. 	<ol style="list-style-type: none"> 1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application of this Regulation and for contributing to its consistent application throughout the Union, in order to protect the fundamental rights and freedoms of natural persons in relation to the processing of their personal data and to facilitate the free flow of personal data within the Union. For these purposes, the supervisory authorities shall co-operate with each other and the Commission. 2. Where in a Member State more than one supervisory authority are established, that Member State shall designate the supervisory authority which functions as a single contact point for the effective participation of those authorities in the European Data Protection Board and shall set out the mechanism to ensure compliance by the other authorities with the rules relating to the consistency mechanism referred to in Article 57. Controllers pertaining to regulated sector should have the possibility to be subject to the supervision of such sector specific regulators for the observance of the Regulation. 3. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to this Chapter, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.

Justification

Certain sectors are already subject to the supervision of sector specific regulators. Including a reference to the possibility for controllers pertaining to regulated sectors (such as the financial and insurance industry) to choose to be subject to the supervision of such sector specific regulators for the observance of the Regulation, would avoid double supervision.

Indeed, the EBF believes that the current definition requires more clarification to avoid overlap between supervision of privacy and financial services supervision which could lead to a doubling of the administrative burden, conflicts with enforcement, problems with delineation of responsibilities, notably as regards the establishment of the fine by the competent authority.

• Confidentiality

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
37.	Article 72	<ol style="list-style-type: none"> 1. The discussions of the European Data Protection Board shall be confidential. 2. Documents submitted to members of the European Data Protection Board, experts and representatives of third parties shall be confidential, unless access is granted to those documents in accordance with Regulation (EC) No 1049/2001 or the European Data Protection Board otherwise makes them public. 3. The members of the European Data Protection Board, as well as experts and representatives of third parties, shall be required to respect the confidentiality obligations set out in this Article. The chair shall ensure that experts and representatives of third parties are made aware of the confidentiality requirements imposed upon them. 	<ol style="list-style-type: none"> 1. The discussions of the European Data Protection Board shall be confidential. The European Data Protection Board shall make accessible its opinions, guidelines, recommendations and best practices. 2. Documents submitted to members of the European Data Protection Board, experts and representatives of third parties shall be confidential, unless access is granted to those documents in accordance with Regulation (EC) No 1049/2001 or the European Data Protection Board otherwise makes them public. 3. The members of the European Data Protection Board, as well as experts and representatives of third parties, shall be required to respect the confidentiality obligations set out in this Article. The chair shall ensure that experts and representatives of third parties are made aware of the confidentiality requirements imposed upon them.

Justification

Article 66.3 requires the European Data Protection Board to publicly issue opinions, guidelines recommendations and best practices. However, Article 72 provides that the discussion of the European Data Protection Board should be kept confidential.

The current Article 29 Working Party publishes minutes of the meeting it holds. We find them very useful and would like to obtain the same transparency of the European Data Protection Board.

- **Right to lodge a complaint with a supervisory authority**

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
38.	Article 73	<ol style="list-style-type: none"> 1. Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority in any Member State if they consider that the processing of personal data relating to them does not comply with this Regulation. 2. Any body, organisation or association which aims to protect data subjects' rights and interests concerning the protection of their personal data and has been properly constituted according to the law of a Member State shall have the right to lodge a complaint with a supervisory authority in any Member State on behalf of one or more data subjects if it considers that a data subject's rights under this Regulation have been infringed as a result of the processing of personal data. 3. Independently of a data subject's complaint, any body, organisation or association referred to in paragraph 2 shall have the right to lodge a complaint with a supervisory authority in any Member State, if it considers that a personal data breach has occurred. 	<ol style="list-style-type: none"> 1. Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority in any Member State if they consider that the processing of personal data relating to them does not comply with this Regulation. 2. Any body, organisation or association which aims to protect data subjects' rights and interests concerning the protection of their personal data and has been properly constituted according to the law of a Member State shall have the right to lodge a complaint with a supervisory authority in any Member State on behalf of one or more data subjects if it considers that a data subject's rights under this Regulation have been infringed as a result of the processing of personal data. 3. Independently of a data subject's complaint, any body, organisation or association referred to in paragraph 2 shall have the right to lodge a complaint with a supervisory authority in any Member State, if it considers that a personal data breach has occurred.

Justification

- **The EBF would like to stress that the introduction of EU collective actions are still under discussion, therefore it would be more appropriate to wait for the outcome before including any such provisions in EU legislation, especially in the data protection Regulation.**

The ability for individuals to bring class actions against entities in case of negligence could have negative unintended consequences. The EBF is therefore not in favor of class actions with regard to such individual rights as privacy and data protection. The current system containing a relevant oversight regime is sufficient according to the EBF. A one-size-fits-all approach to penalties could leave businesses facing sanctions that are too severe for the incidence in question and could hurt business in Europe in an environment that is already squeezed.

- Should nevertheless class actions be accepted, the EBF believes that the representative body should evidence an interest by referring to its statutory purpose and the membership of the data subject(s), e.g. consumer organisations.

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
39.	Article 76	<p>1. Any body, organisation or association referred to in Article 73(2) shall have the right to exercise the rights referred to in Articles 74 and 75 on behalf of one or more data subjects.</p> <p>2. Each supervisory authority shall have the right to engage in legal proceedings and bring an action to court, in order to enforce the provisions of this Regulation or to ensure consistency of the protection of personal data within the Union.</p> <p>(...)</p>	<p>1. Any body, organisation or association referred to in Article 73(2) shall have the right to exercise the rights referred to in Articles 74 and 75 on behalf of one or more data subjects.</p> <p>2. Each supervisory authority shall have the right to engage in legal proceedings and bring an action to court, in order to enforce the provisions of this Regulation or to ensure consistency of the protection of personal data within the Union.</p> <p>(...)</p>

Justification

In line with the arguments developed above, the EBF would like to stress that the introduction of EU collective actions are still under discussion, therefore it would be more appropriate to wait for the outcome before including any such provisions in EU legislation, especially in the data protection Regulation. (see justifications concerning the amendment to article 73- EBF amendment 38).

• Administrative sanctions

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
40.	Article 79	<p>2. The administrative sanction shall be in each individual case effective, proportionate and dissuasive. The amount of the administrative fine shall be fixed with due regard to the nature, gravity and duration of the breach, the intentional or negligent character of the infringement, the degree of responsibility of the natural or legal person and of previous breaches by this person, the technical and organizational measures and procedures implemented pursuant to Article 23 and the degree of cooperation with the supervisory authority in order to remedy the breach.</p> <p>(...)</p> <p>4. The supervisory authority shall impose a fine up to 250 000 EUR, or in case of an enterprise up to 0,5 % of its annual worldwide turnover, to anyone who, intentionally or negligently:</p> <p>(a) does not provide the mechanisms for requests by data subjects or does not respond promptly or not in the required format to data subjects pursuant to Articles 12(1) and (2);</p> <p>(b) charges a fee for the information or for responses to the requests of data subjects in violation of Article 12(4).</p> <p>5. The supervisory authority shall impose a fine up to 500 000 EUR, or in case of an enterprise up to 1 % of its annual worldwide turnover, to anyone who, intentionally or negligently:</p>	<p>1. Where the supervisory authority decides to impose an administrative sanction, this sanction shall The administrative sanction shall be in each individual case be effective, proportionate and dissuasive. The amount of the administrative fine shall be fixed with due regard to the nature, gravity and duration of the breach, the intentional or negligent character of the infringement, the degree of responsibility of the natural or legal person and of previous breaches by this person, the technical and organizational measures and procedures implemented pursuant to Article 23 and the degree of cooperation with the supervisory authority in order to remedy the breach.</p> <p>(...)</p> <p>4. The supervisory authority may impose a fine up to 250 000 EUR, or in case of an enterprise up to 0,5 % of its annual worldwide turnover, to anyone who, intentionally or negligently:</p> <p>(a) does not provide the mechanisms for requests by data subjects or does not respond promptly or not in the required format to data subjects pursuant to Articles 12(1) and (2);</p> <p>(b) charges a fee for the information or for responses to the requests of data subjects in violation of Article 12(4).</p> <p>5. The supervisory authority may impose a fine up to 500 000 EUR, or in case of an enterprise up to 1 % of its annual worldwide turnover, to anyone who, intentionally or negligently:</p>

		<p>(a) does not provide the information, or does provide incomplete information, or does not provide the information in a sufficiently transparent manner, to the data subject pursuant to Article 11, Article 12(3) and Article 14;</p> <p>(...)</p> <p>6. The supervisory authority shall impose a fine up to 1 000 000 EUR or, in case of an enterprise up to 2 % of its annual worldwide turnover, to anyone who, intentionally or negligently:</p> <p>(a) processes personal data without any or sufficient legal basis for the processing or does not comply with the conditions for consent pursuant to Articles 6, 7 and 8;</p> <p>(b) processes special categories of data in violation of Articles 9 and 81;</p> <p>(...)</p> <p>7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of updating the amounts of the administrative fines referred to in paragraphs 4, 5 and 6, taking into account the criteria referred to in paragraph 2.</p>	<p>(a) does not provide the information, or does provide incomplete information, or does not provide the information in a sufficiently transparent manner, to the data subject pursuant to Article 11, Article 12(3) and Article 14;</p> <p>(...)</p> <p>6. The supervisory authority may impose a fine up to 1 000 000 EUR or, in case of an enterprise up to 2 % of its annual worldwide turnover, to anyone who, intentionally or negligently:</p> <p>(a) processes personal data without any or sufficient legal basis for the processing or does not comply with the conditions for consent pursuant to Articles 6, 7 and 8;</p> <p>(b) processes special categories of data in violation of Articles 9 and 81;</p> <p>(...)</p> <p>7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of updating the amounts of the administrative fines referred to in paragraphs 4, 5 and 6, taking into account the criteria referred to in paragraph 2.</p>
--	--	--	---

Justification

- Article 79 use a mandatory language and states that supervisory authorities “shall impose a fine” in the situations described. This leads to a situation where very little margin of appreciation is left to the supervisory authorities. In this regard, EBF would like to stress, at the outset, the importance of the clarity and certainty of the obligations set out in the proposed Regulation (see EBF comments regarding ‘consent’ and ‘data breach’).

The EBF members believes that generally sanctions should not be systematically imposed and a margin of discretion in deciding when to impose a fine should be left to the supervisory authority since many factors influence the nature of the infringement (EDPS opinion, paragraph 266; Working Party Article 29 opinion, page 23).

- In addition, the EBF would like to stress that according to the subsidiarity principle usually regulation in the area of administrative proceedings and the imposition of administrative fines fall within the competences of the Member States.
- **The EBF considers that the sole criteria of the annual worldwide turnover of enterprises could lead to very disproportionate amounts of fines; therefore the administrative sanctions should be limited to a fixed amount.**

- **Processing of national identification number**

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
41.	Article 80a	-	The private sector processing of a national identification number or any other identifier of general application shall not be subject to additional regulation by Member States.

Justification

Article 8.7 of the Directive 95/46/EC provides that: “Member States shall determine the conditions under which a national identification number or any other identifier of general application may be processed”. The EBF would indeed like to stress that the social security number (SSN) is well spread throughout society. The SSN must be available for the purpose of structuring and organisation of large enterprise administration, increasing data quality, the faultless exchange of data between organisations en the avoidance of false hits in queries. There is therefore no justification for the current differences of approach taken by the Member States.

- **Processing in the employment context**

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
42.	Article 82	1. Within the limits of this Regulation, Member States may adopt by law specific rules regulating the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, health and	1. Within the limits of this Regulation, and in particular, in accordance with the principles relating to personal data processing as set out in Article 5 and in addition to the provisions of Article 6 it shall be lawful for employers to: (a) process employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance

		<p>safety at work, and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.</p> <p>2. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.</p>	<p>of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, health and safety at work, and for the purposes of the exercise and enjoyment, on an individual or collective basis, or rights and benefits related to employment, and for the purpose of the termination of the employment relationship; and or</p> <p>(b) install, upgrade, revise or change employee data processing systems including information technology security systems designed to protect employment data from unauthorised access by third parties, such as viruses and malware without the approval of any supervisory authority.</p> <p>2. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.</p> <p>2. It shall be lawful for employers to transfer employee personal data referred to in paragraph 1(a) to third countries providing: the Commission has issued an adequacy decision with regard to said third country or the employer shall have in place the appropriate safeguards referred to and described in Articles 42.1 & 42.2 (b) and (c) but, in the case of employee personal data only, without any prior approval of any supervisory authority. Employers shall keep appropriate records as will enable the appropriate supervisory authorities to subsequently audit such data transfers should the need arise.</p>
--	--	---	---

		<p>3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the safeguards for the processing of personal data for the purposes referred to in paragraph 1.</p>	<p>3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the safeguards for the processing of personal data for the purposes referred to in paragraph 1</p> <p>3. Where appropriate, employers will inform employees and employees' representatives, at the relevant level, as provided for by national law and/or practice about employment related data processing activities.</p> <p>4. If an employer is found to be in breach of paragraph 2 by a supervisory authority then any enforcement notice issued against the employer by the supervisory authority shall provide the employer with days in which to remedy such breach. Any failure to remedy such breach within the required time provided in the enforcement notice will result in penalties and/or administrative fines as provided for in Articles 78 and 79.</p>
--	--	---	--

Justification

The EBF believes that current Article 82 undermines the concept of a Regulation by allowing Member States to adopt rules additional to those already spelt out in the Regulation as regards employees' personal data. For financial institutions operating across Europe this may lead to being required to eventually comply with the Regulation and 27 different sets of domestic employment related data protection laws. Such complexity already places the EU at a competitive disadvantage in attracting employers and encouraging job growth and economic development against those world areas without such difficult and complex laws. We therefore believe that the article proposed by the EBF on the processing of employment-related personal data should replace current Article 82.

- **Exercise of the delegation**

EBF Amendment n°	Article	Text proposed by the European Commission	Amendment proposed
------------------	---------	--	--------------------

43.	Article 86	2. The delegation of power referred to in Article 6(5), Article 8(3), Article 9(3), Article 12(5), Article 14(7), Article 15(3), Article 17(9), Article 20(6), Article 22(4), Article 23(3), Article 26(5), Article 28(5), Article 30(3), Article 31(5), Article 32(5), Article 33(6), Article 34(8), Article 35(11), Article 37(2), Article 39(2), Article 43(3), Article 44(7), Article 79(6), Article 81(3), Article 82(3) and Article 83(3) shall be conferred on the Commission for an indeterminate period of time from the date of entry into force of this Regulation.	Deletion
-----	-------------------	--	-----------------

Justification

- The present draft Regulation establishes a framework of principles. In addition to these principles, no fewer than 26 of the 91 Articles of the draft regulation give the European Commission the power to effectively adopt delegated or implementing acts. **The EBF sees this technique as problematic since it leaves too much uncertainty with regard to the actual implementation of the Regulation. The effective and consistent application of the Regulation can indeed be endangered if the delegated or implementing acts are not yet adopted when the Regulation applies.**
- A delegated act may not cover an essential subject (Article 290 of the Treaty on the functioning of the European Union) with regard to the subject of the regulation. This is the case of the acts specified in articles 6, 8, 17, 18 paragraph 3, 26, 33. Also, a delegated act does not appear necessary when draft regulation measures are of a general nature: it is for those responsible for processing to demonstrate responsibility and to determine the appropriate resources to comply with these measures. The regulations are not intended to interfere in the organisation of companies. This is particularly the case concerning Articles 22, 23 and 31 paragraph 6 of the draft Regulation.
- In their opinions, the European Data Protection Supervisor (EDPS) (section 71-72) and the Article 29 Working Party (section ‘Role of the Commission’, page 7) recognise also this point. Both opinions also question whether the delegated acts foreseen in the proposed Regulation are all restricted to non-essential elements as required by Article 290(1) TFEU. More specifically, essential elements should be inserted in the Regulation itself and should not be made subject to delegated acts.
- Finally, the EBF would like to invite the European Commission to consult stakeholders not appointed by EU governments, including representatives of the banking sector when adopting these acts.

Contact persons:

Séverine Anciberro: s.anciberro@ebf-fbe.eu;

Fanny Derouck: f.derouck@ebf-fbe.eu;

Noémie Papp : noemie.papp@ebf-fbe.eu

Proposal for a Data Protection Regulation

BEUC analysis of consumer benefits versus administrative burden of key provisions

BEUC welcomes the proposal for a Regulation on Data Protection as a major improvement for individuals, particularly in light of the ever-increasing use of personal data in the internet environment. The proposal strikes the right balance between, on one hand the need for an effective system of data protection, and on the other for businesses not to be confronted with excessive administrative burdens.

And yet, lesser administrative burden should not result in weaker protection of personal data nor limit the liability of companies *vis-à-vis* data subjects. On this theme, the draft regulation has abolished the burdensome notification procedure while establishing the principle of accountability according to which the data controller will adopt policies and implement appropriate measures to ensure and be able to demonstrate compliance with the Regulation.

The new provisions will allow controllers to adopt the measures most appropriate to the nature of their activities, thus providing a high degree of flexibility. In parallel, the proposal will help restore consumer control over personal data and enhance consumer trust. Therefore BEUC urges you not to overestimate the impact on businesses, but instead ensure the adoption of a user-centric approach by placing the data subject at the forefront of your considerations.

Consumer confidence is essential to economic recovery. According to the Eurobarometer survey (No. 390), a lack of consumer trust acts as a significant barrier to the development of e-commerce and the digital economy. A solid framework for data protection would help boost consumer confidence, especially in the complex online environment. Innovation will only be able to be rolled out on a large scale if people trust the way their data is being handled.

The present paper has looked at a set of provisions in the draft Regulation, providing a comparative assessment of the impact on the protection of individuals' personal data and the impact on businesses. It becomes obvious that businesses will benefit significantly from the new rules, both in terms of legal harmonisation and reduction of administrative burden.

If further action is deemed necessary to mitigate the risk of legal uncertainty and administrative burden, this should focus on minimising the provisions subject to the adoption of delegated and implementing acts, thus allowing data controllers more flexibility in the choice of measures and subject to guidance by the European Data Protection Board.

-Overall assessment-

Impact on consumers	Impact on businesses
<p>Strengthening and clarification of key data protection principles, including data minimisation and purpose limitation. Strengthening of the rights of data subjects to access their data.</p> <p>More transparency about how your data is handled, with easy-to-understand information, putting an end to privacy notices full of legal jargon.</p> <p>Notification about breaches of their personal data without undue delay.</p> <p>Improved administrative and judicial remedies in cases of violation of data protection rights.</p> <p>Increased responsibility and accountability for those processing personal data – including through the principles of 'privacy by design' and 'privacy by default'.</p>	<p>A level playing field for businesses through one single law applicable to any business across the EU. This harmonisation is expected to save businesses up to €2.3 billion per year.</p> <p>A 'one-stop-shop' – companies in the EU will be answerable to a single data protection authority (DPA), no matter how many EU countries they do business in.</p> <p>Abolition of the current obligation to notify data processing, which costs businesses about €130 million per year.</p> <p>The accountability principle grants businesses the flexibility to adopt appropriate measures in order to comply with the obligations set by the draft Regulation (Article 22).</p>

Right of access

Article 15

"The data subject shall have the right to obtain from the controller at any time, on request, confirmation as to whether or not personal data relating to the data subject are being processed. Where such personal data are being processed, the controller shall provide the following information."

Impact on consumers	Impact on businesses
<p>The proposal deletes the possibility for data controllers to charge consumers a fee for accessing their personal data that has been processed.</p> <p>The right of (free) access of data subjects to their personal data underpins the right to retain the ownership and the control of the data by the data subject at all times.</p> <p>Consumers have a right to know what data a company or organisation holds about them and should not have to pay to access their personal data.</p> <p>In a survey commissioned by the UK consumer organisation Which? 76% of consumers said that they found it unacceptable or completely unacceptable that companies can charge £10 to provide the information held about them.</p>	<p>Businesses claim that the obligation to give free access will lead to unscrupulous requests to access that would be costly for them.</p> <p>The Commission's proposal already includes an exception for requests which are manifestly excessive, in particular because of their repetitive character.</p> <p>However there is no valid reason or data that demonstrates that this would be the case. For instance, in those countries where the fee has been abolished, this did <u>not</u> result in any increase of requests.</p>

Data portability

Article 18

“The data subject shall have the right, where personal data are processed by electronic means and in a structured and commonly used format, to obtain from the controller a copy of data undergoing processing in an electronic and structured format which is commonly used and allows for further use by the data subject.”

Impact on consumers	Impact on businesses
<p>The right to Data Portability will ensure consumers are not 'locked in' to services and are able to easily retrieve their data and change provider.</p> <p>The right to data portability will enable people to recover and/or to shift their own data from one platform/cloud to another.</p> <p>However, for this right to be effective, interoperability between services and promotion of open standards is required.</p>	<p>An effective right to data portability will help promote competition.</p> <p>It will help reduce monopolisations of market power and improve competition in the market, so that new services can innovate and attract consumers away from the original service.</p> <p>The right to data portability already exists under EU law, including number portability for telecommunications operators.</p>

Responsibility of the data controller

Article 22

“The controller shall adopt policies and implement appropriate measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation.

“The controller shall implement mechanisms to ensure the verification of the effectiveness of the measures referred to in paragraphs 1 and 2. If proportionate, this verification shall be carried out by independent internal or external auditors.”

Impact on consumers	Impact on businesses
<p>Accountability shifts the primary responsibility for data protection from the individual to the organisation collecting and using data.</p> <p>Accountability does not displace the individual’s ability to assert his rights, but relieves him of much of the burden of policing the marketplace for enterprises using data irresponsibly.</p> <p>The new Regulation will enhance data protection efficiency by allowing regulators to focus their resources on activities which pose the greatest risk to individuals.</p>	<p>Only the abolition of the notification requirement saves businesses €130 million per year. The average cost for each notification is estimated to be €200.</p> <p>Businesses will enjoy sufficient flexibility in the choice of the means to adopt in order to comply with the obligations set in the Regulation.</p> <p>Businesses will be able to more effectively conserve scarce resources allocated to data protection.</p> <p>Accountability directs scarce resources towards mechanisms which most effectively provide protection for data. Organisations will adopt the tools best suited to guaranteeing protections focus on reaching substantive privacy outcomes (measurable information protection goals) and to demonstrate their ability to achieve them.</p>

Data Protection by Design

Article 23:

“The controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.”

Impact on consumers	Impact on businesses
<p>Data Protection by Design will help limit the collection of personal data and consumers trust that their personal data is protected.</p> <p>Data Protection by Default will ensure that even non-digital consumers, who are unfamiliar with privacy settings of services and products will have protection.</p> <p>These two principles will help empower data subjects’ control and enhance enforcement of data protection legislation.</p> <p>Consumers’ personal data will be respected throughout the lifecycle of products and services.</p>	<p>Organisations who collect, use and disclose personal information should proactively accommodate the privacy interests and rights of individuals throughout their operations.</p> <p>The “payoff” to organisations would come in many ways, including: improved customer satisfaction and trust; enhanced reputation; commercial and enduring competitive advantage.</p> <p>77% of the security industry believes that it should be a mandatory obligation.</p> <p>More than 13 EU projects related to privacy enabling technologies are currently funded by the EU budget. An additional call for projects related to security and privacy has been published in July 2011 with a budget of €80 million. These measures would provide support to the application of the principle of Privacy by Design in the industry.</p> <p>Privacy by Design rules are already included in the national legislation of many EU Member States.</p>

Article 28 Documentation	
Impact on consumers	Impact on businesses
<p>The documentation obligations will facilitate the task of Data Protection Authorities when monitoring the compliance of data processing operations with the principles and rules set in the Regulation.</p> <p>The documentation obligations will facilitate the enforcement of the Regulation by both data subjects and the data protection authorities.</p>	<p>The obligation to maintain documentation about the processing operations partly replaces the cumbersome notification obligation.</p> <p>The current obligation to notify data processing costs businesses approximately €130 million per year.</p> <p>The documentation items in Article 28 refer mostly to the information that the consumer should receive when their data is processed and therefore the extra burden from the documentation obligation is zero.</p> <p>The documentation obligations refer to the minimum information that any responsible and accountable business needs to keep records of in particular in the context of the obligation to carry out an impact assessment.</p>

Data Breach Notification Obligation

Article 31:

"In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 24 hours after having become aware of it, notify the personal data breach to the supervisory authority. The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within 24 hours."

Article 32:

"When the personal data breach is likely to adversely affect the protection of the personal data or privacy of the data subject, the controller shall, after the notification referred to in Article 31, communicate the personal data breach to the data subject without undue delay."

Impact on consumers	Impact on businesses
<p>Data breaches can lead to significant harm to consumers, ranging from undesired spam to identity theft. 88% of Europeans want to be informed when their personal data is lost, stolen or compromised (Eurobarometer).</p> <p>74% of UK consumers would always wish to be notified of a data breach (Which? survey).</p> <p>A data breach notification will also include information about measures to be taken by the individual in order to mitigate the impact of the breach.</p>	<p>The cost will be minimal: according to the Impact Assessment of the European Commission 7.1% of EU companies have experienced a breach, of which:</p> <ul style="list-style-type: none">- 55% actually informed the individual whose data was affected and- indicated a cost of less than €500 for the notification.

Data Protection Impact Assessment

Article 33

“Where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller or the processor acting on the controller’s behalf shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.”

Impact on consumers	Impact on businesses
<p>Consumers can trust that a business has implemented a thorough assessment of the potential risks related to the protection of personal data and has taken measures to mitigate them.</p> <p>Consumers have the opportunity to provide their views within the framework of the DPIA.</p> <p>A DPIA provides consumers with enhanced transparency on the processing operations carried out by businesses.</p>	<p>A DPIA is an early warning system. It provides a way to detect potential privacy problems, take precautions and build tailored safeguards before, not after, the organisation makes heavy investments.</p> <p>A DPIA enables an organisation to demonstrate its compliance with privacy legislation in the context of a subsequent complaint, privacy audit or compliance investigation.</p> <p>A company that undertakes a DPIA and engages with data subjects and their representatives will earn trust from consumers and maintain a competitive advantage over competitors.</p> <p>If an organisation has engaged with stakeholders from an early stage, it will be very difficult for stakeholders to claim negligibility of the business at a later stage.</p>

1 November 2012

Draft DIGITALEUROPE amendments

Amendment 1

Recital 23 (Data Subject)	
Commission proposal	Proposed DIGITALEUROPE amendment
<p>The principles of protection should apply to any information concerning an identified or identifiable person. To determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the individual. The principles of data protection should not apply to data rendered anonymous in such a way that the data subject is no longer identifiable.</p>	<p>The principles of protection should apply only to any <i>specific</i> information concerning an identified or identifiable person. To determine whether a person is identifiable, account should be taken: of all the (i) only of those means likely reasonably to be used either by the controller or by any other natural or legal person to identify the individual, and (ii) of the reasonable likeliness of a person being identified. The principles of data protection should not apply to data rendered anonymous or made unreadable in such a way that the data subject is no longer or not yet identifiable from the data.</p> <p><i>Serial numbers of products, IP addresses, International Mobile Equipment Identity codes or other such identifiers should not be regarded as personal data before a link to a natural person can be established. Such identifiers should still not be regarded as personal data even after establishment of such link when they remain standalone in the possession of a controller or processor, i.e. when they are not combined with additional data in order to identify or target activities at a natural person.</i></p> <p><i>Where business contact information, such as names, surnames, professional addresses, emails, phone, fax numbers, is solely used or processed in a clearly defined business context, relating to a company and not an individual, this Regulation will not apply.</i></p>

Justification

Whether or not a person is identifiable should not be determined on the basis of a third party’s means to identify the individual. Furthermore it should be made clear that the theoretical possibility to identify an individual is in itself not sufficient for considering an individual as identifiable. An overly broad definition of ‘data subject’ encompassing those identifiers (such as serial numbers etc.) which are not connected to a natural person does not lead to a better protection; on the contrary it takes away incentives to make data anonymous or to refrain from linking it to a natural person.

In line with an approach of the Spanish Data Privacy Authority, business contact information should be excluded from the Regulation's scope in certain cases. However, it is essential that the processing of contact information fulfils two requirements in order to be exempt from the scope. Firstly that the data processed is limited to what is merely necessary to identify the person within the company and secondly that the inclusion of contact information must be purely accidental or incidental regarding the real aim sought by the data processing, which is related not to the individual, but to the company where the person works.

Amendment 2

Recital 24 (Definition of Personal Data)	
Commission proposal	Proposed DIGITALEUROPE amendment
<p>When using online services, individuals may be associated with online identifiers provided by their devices, applications, tools and protocols, such as Internet Protocol addresses or cookie identifiers. This may leave traces which, combined with unique identifiers and other information received by the servers, may be used to create profiles of the individuals and identify them. It follows that identification numbers, location data, online identifiers or other specific factors as such need not necessarily be considered as personal data in all circumstances.</p>	<p>When using online services, individuals may be associated with online identifiers provided by their devices, applications, tools and protocols, such as Internet Protocol addresses or cookie identifiers. This may leave traces which, combined with unique identifiers and other information received by the servers, may be used to create profiles of the individuals and identify them. It follows that identification numbers, location data, online identifiers or other specific factors as such need not necessarily be considered as personal data in all circumstances.</p>

Justification

Online identifiers and location data on their own cannot identify individuals and cannot be considered as being personal data. Deleting “as such” indicates that online identifiers and location data can be considered as personal data when combined with other relevant information.

Amendment 3

Recital 25 (Consent)	
Commission proposal	Proposed DIGITALEUROPE amendment
<p>1. Consent should be given explicitly by any appropriate method enabling a freely given specific and informed indication of the data subject's wishes, either by a statement or by a clear affirmative action by the data subject, ensuring that individuals are aware that they give their consent to the processing of personal data, including by ticking a box when visiting an Internet website or by any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data. Silence or inactivity should therefore not constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. If the data subject's consent is to be given following an electronic request, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.</p>	<p>1. Consent should be given—<i>explicitly unambiguously</i> by any appropriate method <i>within the context of the product or service being offered</i> enabling a freely given specific and informed indication of the data subject's wishes, either by a statement or by a clear affirmative action by the data subject, ensuring that individuals are aware that they give their consent to the processing of personal data, including by ticking a box when visiting an Internet website or by any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data. Silence or inactivity should therefore not constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. If the data subject's consent is to be given following an electronic request, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.</p>

Justification

The term 'unambiguous' is better suited as it does not lower but rather increases the requirements of 'consent' compared to 'explicit' (because of the combination with the requirement of 'affirmative action') and it has a much better chance to be understood in a consistent way in all the Member States.

Amendment 4

Recital 27 (Main Establishment)	
Commission proposal	Proposed DIGITALEUROPE amendment
<p>The main establishment of a controller in the Union should be determined according to objective criteria and should imply the effective and real exercise of management activities determining the main decisions as to the purposes, conditions and means of processing through stable arrangements. This criterion should not depend whether the processing of personal data is actually carried out at that location; the presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute such main establishment and are therefore no determining criteria for a main establishment. The main establishment of the processor should be the place of its central administration in the Union.</p>	<p>The main establishment of a controller <i>and of a processor</i> in the Union should be determined <i>by the data controller and data processor respectively. Such determination should be made and evaluated</i> according to <i>the following</i> objective criteria: <i>the location of the group's European headquarters, the location of the company within the group with delegated data protection responsibilities, the location of the company which is best placed (in terms of management function, administrative burden etc) to deal with and enforce the rules as set out in this Regulation, the place where</i> and should imply the effective and real exercise of management activities determining the main-most decisions as to the purposes <i>or</i> conditions and means of processing <i>are taken</i> through stable arrangements. This criterion should not depend whether the processing of personal data is actually carried out at that location; The presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute such main establishment and are therefore no determining criteria for a main establishment. The main establishment of the processor should be the place of its central administration in the Union.</p>

Justification

The determination of the main establishment should be done on the basis of various criteria to ensure organisations have enough guidance to determine their main establishment and provide objective measures by which to judge their decision in the event of a dispute. Already there are such criteria to determine the lead DPA in the context of Binding Corporate Rules (BCRs) which have a proven track record. We think inserting the same criteria as outlined in Art 29 WP opinion 108 would provide more clarity and options that would not be covered under the current proposal. Moreover, as many entities are both controllers and processors,

we believe that they should be subject to the same set of criteria in determining their main establishment to avoid potentially conflicting results. For the same reason, we have changed “main” decisions to “most” as this would bring it in line with the BCR guidance.

Amendment 5

Recital 28 (Main Establishment)	
Commission proposal	Proposed DIGITALEUROPE amendment
<p>A group of undertakings should cover a controlling undertaking and its controlled undertakings, whereby the controlling undertaking should be the undertaking which can exercise a dominant influence over the other undertakings by virtue, for example, of ownership, financial participation or the rules which govern it or the power to have personal data protection rules implemented.</p>	<p>A group of undertakings should cover a controlling undertaking and its controlled undertakings, whereby the controlling undertaking should be the undertaking which can exercise a dominant influence over the other undertakings by virtue, for example, of ownership, financial participation or the rules which govern it or the power to have personal data protection rules implemented. <i>A group of undertakings may nominate a single main establishment in the Union.</i></p>

Justification

The amendment clarifies that a group of undertakings can be viewed as a single entity responsible to a single supervisory authority. The simplification achieved by nominating a single point of contact should not be undermined by various supervisory authorities viewing individual controlled undertakings as separate data controllers or processors.

Amendment 6

Recital 34 (Consent)	
Commission proposal	Proposed DIGITALEUROPE amendment
<p>Consent should not provide a valid legal ground for the processing of personal data, where there is a clear imbalance between the data subject and the controller. This is especially the case where the data subject is in a situation of dependence from the controller, among others, where personal data are processed by the employer of employees' personal data in the employment</p>	<p>Consent should not provide a valid legal ground for the processing of personal data, where there is a clear imbalance between the data subject and the controller, <i>resulting in the data subject not having a true option of refusal without being subject to harmful consequences, taking into account the interest of the data subject. Such situations may exist, among others, in relation to</i></p>



<p>context. Where the controller is a public authority, there would be an imbalance only in the specific data processing operations where the public authority can impose an obligation by virtue of its relevant public powers and the consent cannot be deemed as freely given, taking into account the interest of the data subject.</p>	<p><i>certain aspects of employment relationship, in context of essential services or when dealing with public authorities. This is especially the case where the data subject is in a situation of dependence from the controller, among others, where personal data are processed by the employer of employees' personal data in the employment context. Where the controller is a public authority, there would be an imbalance only in the specific data processing operations where the public authority can impose an obligation by virtue of its relevant public powers and the consent cannot be deemed as freely given, taking into account the interest of the data subject.</i></p>
---	---

Justification

Only when a data subject would suffer harmful consequences, taking into account the interest of the data subject, should consent be excluded as a valid legal ground for processing. There will be instances where in an employer – employee relationship, consent should be deemed a valid ground as a refusal by the employee would not have any harmful consequences.

Amendment 7

Recital 39 (Processing of Data for Network Security Purposes)	
Commission proposal	Proposed DIGITALEUROPE amendment
<p>The processing of data to the extent strictly necessary for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data, and the security of the related services offered by, or accessible via, these networks and systems, by public authorities, Computer Emergency Response Teams – CERTs, Computer Security Incident Response Teams – CSIRTs, providers of electronic communications networks and</p>	<p>The processing of data to the extent strictly necessary for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data, and the security of the related services offered by, or accessible via, these networks and systems, by public authorities, Computer Emergency Response Teams – CERTs, Computer Security Incident Response Teams – CSIRTs, providers of <i>public or private</i> electronic communications</p>



<p>services and by providers of security technologies and services, constitutes a legitimate interest of the concerned data controller. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping ‘denial of service’ attacks and damage to computer and electronic communication systems.</p>	<p>networks and services and by providers of security technologies and services, constitutes a legitimate interest of the concerned data controller and vital interest of the data subject. This could, for example, include preventing unauthorised access to public or private electronic communications networks and malicious code distribution and stopping ‘denial of service’ attacks and damage to computers and-or electronic communication systems.</p>
---	--

Justification

To maintain network and information security and protect the users’ terminals, it may be so that in specific cases personal data needs to be processed. Such processing is in the legitimate interest of the data controller and vital interest of the data subject and should be perceived as grounds for lawful processing under Article 6.1 (d) and 6.1 (f). We welcome the clarification and we support the intent of recital 39.

Amendment 8

Recital 49 (Processing of Data for Network Security Purposes)	
Commission proposal	Proposed DIGITALEUROPE amendment
<p>The information in relation to the processing of personal data relating to the data subject should be given to them at the time of collection, or, where the data are not collected from the data subject, within a reasonable period, depending on the circumstances of the case. Where data can be legitimately disclosed to another recipient, the data subject should be informed when the data are first disclosed to the recipient.</p>	<p>The information in relation to the processing of personal data relating to the data subject should be given to them at the time of collection, or, where the data are not collected from the data subject, within a reasonable period, depending on the circumstances of the case. <i>Except when processing data strictly necessary for the purposes of ensuring network and information security, where</i> data can be legitimately disclosed to another recipient, the data subject should be informed when the data are first disclosed to the recipient.</p> <p><i>In cases of threats to network and information security, a reasonable period for the obligation to explicitly inform the data subject on the legitimate interests pursued would be after the conclusion of the investigation at hand or once effective</i></p>

	<p><i>security is restored and the data subject can be identified, taking into account article 10. Should the investigation involve competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences, the responsibility for exercising the rights of the data subject will pass to the authorities in question.</i></p>
--	--

Justification

In certain situations in networking and information security processing where it is possible to identify the data subject (for example, an ISP which has a direct relationship with their subscribers and can map IP addresses to individuals), it is preferable to undertake certain processing without informing the data subject at the time, such as when there is a compromised machine sending spam and other circumstances where one is using the data to track the control traffic and identify the real malicious actors further up the chain. Hence a reasonable time period for informing the data subject that their personal data has been processed (in accordance with Article 14.4(b)) is after the conclusion of such investigations.

If the data subject in question is a suspected malicious actor and the suspected offence is criminal, you may not want to prejudice investigations by law enforcement authorities, and hence the responsibility to exercise the data subjects' rights in such situations should pass over to the authorities in question.

Furthermore, given that security companies may need to cooperate during investigations (e.g. a network security company and an ISP), the proposed requirement to inform the data subject at the point another recipient is informed could lead to data subjects being informed too early in the process and hence it should be deleted or an exception made when data is processed for network and information security purposes.

Amendment 9

Recital 51 (Right of access for the data subject)	
Commission proposal	Proposed DIGITALEUROPE amendment
<p>Any person should have the right of access to data which has been collected concerning them, and to exercise this right easily, in order to be aware and verify the lawfulness of the processing. Every data subject should therefore have the right to know and obtain</p>	<p>Any person should have the right of access to personal data which has been collected concerning them, and to exercise this right easily, in order to be aware and verify the lawfulness of the processing. Every data subject should therefore have the right to</p>

<p>communication in particular for what purposes the data are processed, for what period, which recipients receive the data, what is the logic of the data that are undergoing the processing and what might be, at least when based on profiling, the consequences of such processing. This right should not adversely affect the rights and freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of these considerations should not be that all information is refused to the data subject.</p>	<p>know and obtain communication in particular for what purposes the <i>personal</i> data are processed, for what period, which recipients receive the <i>personal</i> data, what is the logic of the <i>personal</i> data that are undergoing the processing and what might be, at least when based on profiling, the consequences of such processing. This right should not adversely affect the rights and freedoms of others, including <i>for example</i> trade secrets <i>such as algorithms used, protection of network and information security</i>, or intellectual property and in particular the copyright protecting the software. However, the result of these considerations should not be that all information is refused to the data subject.</p>
--	---

Justification

The above clarifications would allow for the data subjects to exercise their legitimate rights of access but also recognizes that in some cases, such requirements need to be qualified as it should not be used to gain access to specific trade secrets such as algorithms, nor impede with legitimate interests such as protecting users' terminals. Malicious actors should not be given the ability to block the work of CERTs, CSIRTs, providers of electronic communications networks and services and providers of security technologies and services.

In line with proposed amendments to Article 20, no specific additional requirement for "profiling" is required.

Amendment 10

Recital 52 (Right of access for the data subject)	
Commission proposal	Proposed DIGITALEUROPE amendment
<p>The controller should use all reasonable measures to verify the identity of a data subject that requests access, in particular in the context of online services and online identifiers. A controller should not retain personal data for the unique purpose of being able to react to potential requests.</p>	<p>The controller should use all—reasonable measures <i>within the context of the product or service being provided, or otherwise within the context of the relationship between the controller and the data subject, and the sensitivity of the personal data being processed</i> to verify the identity of a data subject that requests access, in particular in the context of online services and online identifiers. A controller should not retain <i>nor</i></p>

	<i>be forced to gather</i> personal data for the unique purpose of being able to react to potential requests.
--	---

Justification

In some cases, complying with a right of access requirement will have as a consequence that the data controller will need to gather (more) personal data from the data subject in order to comply with the request. For example, data such as an IP address or an online identifier, that based on the context of the specific processing isn't personal data if the data controller can't by all means likely reasonably identify the data subject, would now become personal data as the data controller would need to collect more personal information as to verify the identity of the data subject, including gathering his IP address or online identifier and connecting as to authenticate that the person who is requesting access is actually the legitimate person. In line with the principle of data minimization, the Regulation should strive to avoid any additional requirements which impose on the data subject the obligation to do so. In addition, requiring "all" reasonable measures be used to verify identity would require multiple types of identity verification which may not be reasonable or practical, especially in cases where the sensitivity of the personal data being processed is low.

Amendment 11

Recital 58 (Profiling)	
Commission proposal	Proposed DIGITALEUROPE amendment
<p>Every natural person should have the right not to be subject to a measure which is based on profiling by means of automated processing. However, such measure should be allowed when expressly authorised by law, carried out in the course of entering or performance of a contract, or when the data subject has given his consent. In any case, such processing should be subject to suitable safeguards, including specific information of the data subject and the right to obtain human intervention and that such measure should not concern a child.</p>	<p>Every natural person A data subject should have the right not to be subject to a measure which is based on profiling by means of automated processing, <i>which produces legal effects that gravely and adversely affect his fundamental rights. Depending on the context this may include processing aimed at evaluating, analysing or predicting a natural person's performance at work, economic situation, health, personal preferences, reliability or behaviour.</i> However, such measures should be allowed when expressly authorised by law, carried out in the course of entering or performance of a contract, <i>when necessary in a democratic society for the purposes of Article 21 or for the purposes of the</i></p>

	<p><i>legitimate interests pursued by a controller or when the data subject has given his consent. In any case, such processing should be subject to suitable safeguards as outlined in this Regulation. including specific information of the data subject and the right to obtain human intervention and that such measure should not concern a child.</i></p>
--	---

Justification

In line with proposed amendments to Article 20.

The prohibition of profiling of a child was deleted in the final adopted Commission proposal as it was recognized that particularly in the online world, data subjects and their identity and consequently age, are not always identifiable by the controller.

Amendment 12

Recital 61 (Data Protection by Design/Default)	
Commission proposal	Proposed DIGITALEUROPE amendment
<p>The protection of the rights and freedoms of data subjects with regard to the processing of personal data require that appropriate technical and organisational measures are taken, both at the time of the design of the processing and at the time of the processing itself, to ensure that the requirements of this Regulation are met. In order to ensure and demonstrate compliance with this Regulation, the controller should adopt internal policies and implement appropriate measures, which meet in particular the principles of data protection by design and data protection by default.</p>	<p><i>To meet consumer and business expectations around the protection of the rights and freedoms of data subjects with regard to the processing of personal data require that appropriate technical and organisational measures are may be taken, both at the time of the design of the processing and at the time of the processing itself, to ensure that the requirements of this Regulation are met. In order to ensure and demonstrate compliance with this Regulation, the controller should adopt internal policies and implement appropriate measures. which meet in particular the principles of data protection by design and data protection by default. Measures having as an objective the increase of consumer information and ease of choice shall be encouraged, based on industry cooperation and favouring innovative solutions, products and services.</i></p>

Justification

Privacy by Design/Default (PbD/D) are concepts currently being discussed internationally, relates to internal privacy and data protection processes of organizations and are based on a number of factors including their business models, size and interaction with personal data. Although every organization should strive to integrate privacy and data protection into its internal processes, the actual way it does so should remain flexible and leave room for adaptation based on the factors above. This is to say that there is no one right way, which is especially true in the case of SMEs and for entities that are far removed from processing identifiable personal data. It is essential that any PbD concept be technology-neutral and not introduce specific technology or operational mandates, or contribute to a differentiation between ICT and other economic sectors.

To avoid lack of consistency throughout the proposed text, it is important to streamline the proposed language for Art. 23 with other Data Protection by Design/Default-type obligations, which cover to large extends the proposed text, e.g. Art. 22 and Art. 5 c), Art. 26 (processor agreements), Art. 28 (documentation), Art. 30 (security), Art. 33 (data protection impact assessment) and Art. 35 (data protection officer).

The PbD/D concepts should therefore focus on designing privacy into processes and organizations and should maintain as a key objective providing consumers with appropriate tools to make an informed choice, but avoid creating additional uncertainties via unclear obligations, definitions and terms. Industry-led innovation in this area will create trust and allow for innovative solutions, services and technologies to flourish in the spirit of the European Digital Agenda. Finally, there is a clear need to look into the issue with a global perspective to avoid further fragmentation, taking stock of industry’s own efforts and taking technology developments into account.

Amendment 13

Recital 62 (Controller/Processor)	
Commission proposal	Proposed DIGITALEUROPE amendment
<p>The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processor, also in relation to the monitoring by and measures of supervisory authorities, requires a clear attribution of the responsibilities under this Regulation, including where a controller determines the purposes, conditions and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller.</p>	<p>The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processor, also in relation to the monitoring by and measures of supervisory authorities, requires a clear attribution of the responsibilities under this Regulation, including where a controller determines the purposes, conditions and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller.</p>

Justification

In line with proposed amendments to Art 24.

Amendment 14

Recital 65 (Controller/Processor)	
Commission proposal	Proposed DIGITALEUROPE amendment
In order to demonstrate compliance with this Regulation, the controller or processor should document each processing operation. Each controller and processor should be obliged to co-operate with the supervisory authority and make this documentation, on request, available to it, so that it might serve for monitoring those processing operations.	In order to demonstrate compliance with this Regulation, the controller or processor should document <i>different categories of each</i> processing operation under its responsibility . Each controller and processor should be obliged to co-operate with the supervisory authority and make this documentation, on request, available to it, so that it might serve for monitoring those processing operations.

Justification

In line with proposed amendments to Article 28.

Amendment 15

Recital 66 (Security of Processing)	
Commission proposal	Proposed DIGITALEUROPE amendment
In order to maintain security and to prevent processing in breach of this Regulation, the controller or processor should evaluate the risks inherent to the processing and implement measures to mitigate those risks. These measures should ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks and the nature of the personal data to be protected. When establishing technical standards and organisational measures to ensure security of	In order to maintain security and to prevent processing in breach of this Regulation, the controller or processor should evaluate the risks inherent to the processing and implement measures to mitigate those risks. These measures should ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks and the nature of the personal data to be protected. <i>The implementation by the controller and the processor of such measures and the execution</i>

<p>processing, the Commission should promote technological neutrality, interoperability and innovation, and, where appropriate, cooperate with third countries.</p>	<p><i>thereof which would require processing of certain data to increase network and information security, is in the legitimate interests of the data controller, the processor and, where applicable, a third party providing support in its implementation.</i> When establishing technical standards and organisational measures to ensure security of processing, the Commission should promote technological neutrality, interoperability and innovation, and, where appropriate, cooperate with third countries.</p>
---	--

Justification

Data controllers and processors should ensure that they have the right organizational measures in place to ensure security of processing and hence, enhancing overall network and information security. Such measures could, for example, be targeted at preventing unauthorized access to electronic communications networks, malicious code distribution and stopping of attacks and damage to computer and electronic communication systems. Where the implementation and execution of such measures would require the processing of data to the extent necessary for purposes of ensuring network and information security by the data controller, processor or a third party, such processing should be deemed to be a legitimate interest for processing. Such processing would need to provide the necessary safeguards as outlined in the regulation where possible.

Amendment 16

Recital 67 (Breach Notification)	
Commission proposal	Proposed DIGITALEUROPE amendment
<p>A personal data breach may, if not addressed in an adequate and timely manner, result in substantial economic loss and social harm, including identity fraud, to the individual concerned. Therefore, as soon as the controller becomes aware that such a breach has occurred, the controller should notify the breach to the supervisory authority without undue delay and, where feasible, within 24 hours. Where this cannot achieved within 24 hours, an explanation of the reasons for the delay should accompany the notification. The</p>	<p>A personal data breach may, if not addressed in an adequate and timely manner, result in substantial economic loss and social harm, including identity fraud, to the individual concerned. Therefore, as soon as the controller becomes aware that such a material breach has occurred, the controller should notify the breach to the supervisory authority without undue delay. and, where feasible, within 24 hours. Where this cannot achieved within 24 hours, an explanation of the reasons for the delay should accompany</p>

<p>individuals whose personal data could be adversely affected by the breach should be notified without undue delay in order to allow them to take the necessary precautions. A breach should be considered as adversely affecting the personal data or privacy of a data subject where it could result in, for example, identity theft or fraud, physical harm, significant humiliation or damage to reputation. The notification should describe the nature of the personal data breach as well as recommendations as well as recommendations for the individual concerned to mitigate potential adverse effects. Notifications to data subjects should be made as soon as reasonably feasible, and in close cooperation with the supervisory authority and respecting guidance provided by it or other relevant authorities (e.g. law enforcement authorities). For example, the chance for data subjects to mitigate an immediate risk of harm would call for a prompt notification of data subjects whereas the need to implement appropriate measures against continuing or similar data breaches may justify a longer delay.</p>	<p>the notification. The individuals whose personal data could be adversely affected by the breach should be notified without undue delay in order to allow them to take the necessary precautions. A breach should be considered as adversely affecting the personal data or privacy of a data subject where it could result in, for example, identity theft or fraud, physical harm, significant humiliation or damage to reputation. The notification should describe the nature of the personal data breach as well as recommendations for the individual concerned to mitigate potential adverse effects. Notifications to data subjects should be made as soon as reasonably feasible, and in close cooperation with the supervisory authority and respecting guidance provided by the supervisory authority where applicable by it or other relevant authorities (e.g. law enforcement authorities). For example, the chance for data subjects to mitigate an immediate risk of harm would call for a prompt notification of data subjects whereas the need to implement appropriate measures against continuing or similar data breaches may justify a longer delay.</p>
---	---

Justification

In line with proposed language to Art 31.

Amendment 17

Recital 70 (Privacy Impact Assessment)	
Commission proposal	Proposed DIGITALEUROPE amendment
<p>Directive 95/46/EC provided for a general obligation to notify processing of personal data to the supervisory authorities. While this obligation produces administrative and financial burdens, it did not in all cases contribute to improving the protection of personal data. Therefore such indiscriminate</p>	<p>Directive 95/46/EC provided for a general obligation to notify processing of personal data to the supervisory authorities. While this obligation produces administrative and financial burdens, it did not in all cases contribute to improving the protection of personal data. Therefore such indiscriminate</p>

<p>general notification obligation should be abolished, and replaced by effective procedures and mechanism which focus instead on those processing operations which are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes. In such cases, a data protection impact assessment should be carried out by the controller or processor prior to the processing, which should include in particular the envisaged measures, safeguards and mechanisms for ensuring the protection of personal data and for demonstrating the compliance with this Regulation.</p>	<p>general notification obligation should be abolished, and replaced by effective procedures and mechanism which focus instead on those processing operations which are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes. In such cases, a data protection impact assessment should be carried out by the controller or processor prior to the processing, which should include in particular the envisaged measures, safeguards and mechanisms for ensuring the protection of personal data and for demonstrating the compliance with this Regulation.</p>
--	---

Justification

It should be up to the data controllers to assess the impact to privacy as they will determine the purposes of the processing.

Amendment 18

Recital 74 (Privacy Impact Assessment)	
Commission proposal	Proposed DIGITALEUROPE amendment
<p>Where a data protection impact assessment indicates that processing operations involve a high degree of specific risks to the rights and freedoms of data subjects, such as excluding individuals from their right, or by the use of specific new technologies, the supervisory authority should be consulted, prior to the start of operations, on a risky processing which might not be in compliance with this Regulation, and to make proposals to remedy such situation. Such consultation should equally take place in the course of the preparation either of a measure by the national parliament or of a measure based on such legislative measure</p>	<p>Where a data protection impact assessment indicates that processing operations involve a high degree of specific risks to the rights and freedoms of data subjects, such as excluding individuals from their right, or by the use of specific new technologies, the supervisory authority should be consulted, prior to the start of operations, on a risky processing which might not be in compliance with this Regulation. and to make proposals to remedy such situation. Such consultation should equally take place in the course of the preparation either of a measure by the national parliament or of a measure based on such legislative measure which defines</p>



which defines the nature of the processing and lays down appropriate safeguards.	the nature of the processing and lays down appropriate safeguards.
--	---

Justification

Consultation should take place between supervisory authorities and data controllers and processors where there is an indication that processing operations involve a high degree of specific risks to the rights and freedom of data subjects and the risky processing might not be in compliance with this Regulation. Requiring prior consultation in other instances within the framework of this legislation will go against the goals of achieving a more flexible system.

Amendment 19

Recital 129 (Delegated Acts)	
Commission proposal	Proposed DIGITALEUROPE amendment
In order to fulfil the objectives of this Regulation, namely to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data and to ensure the free movement of personal data within the Union, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the Commission. In particular, delegated acts should be adopted in respect of lawfulness of processing; specifying the criteria and conditions in relation to the consent of a child; processing of special categories of data; specifying the criteria and conditions for manifestly excessive requests and fees for exercising the rights of the data subject; criteria and requirements for the information to the data subject and in relation to the right of access; the right to be forgotten and to erasure; measures based on profiling; criteria and requirements in relation to the responsibility of the controller and to data	In order to fulfil the objectives of this Regulation, namely to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data and to ensure the free movement of personal data within the Union, the power to adopt acts <i>in specific cases and</i> in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the Commission. In particular, delegated acts should be adopted in respect of lawfulness of processing; specifying the criteria and conditions in relation to the consent of a child; processing of special categories of data; specifying the criteria and conditions for manifestly excessive requests and fees for exercising the rights of the data subject; criteria and requirements for the information to the data subject and in relation to the right of access; the right to be forgotten and to erasure; measures based on profiling; criteria and requirements in relation to the responsibility

protection by design and by default; a processor; criteria and requirements for the documentation and the security of processing; criteria and requirements for establishing a personal data breach and for its notification to the supervisory authority, and on the circumstances where a personal data breach is likely to adversely affect the data subject; the criteria and conditions for processing operations requiring a data protection impact assessment; the criteria and requirements for determining a high degree of specific risks which require prior consultation; designation and tasks of the data protection officer; codes of conduct; criteria and requirements for certification mechanisms; criteria and requirements for transfers by way of binding corporate rules; transfer derogations; administrative sanctions; processing for health purposes; processing in the employment context and processing for historical, statistical and scientific research purposes. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level. The Commission, when preparing and drawing-up delegated acts, should ensure a simultaneous, timely and appropriate transmission of relevant documents to the European Parliament and Council.

~~of the controller and to data protection by design and by default; a processor; criteria and requirements for the documentation and the security of processing; criteria and requirements for establishing a personal data breach and for its notification to the supervisory authority, and on the circumstances where a personal data breach is likely to adversely affect the data subject; the criteria and conditions for processing operations requiring a data protection impact assessment; the criteria and requirements for determining a high degree of specific risks which require prior consultation; designation and tasks of the data protection officer; codes of conduct; criteria and requirements for certification mechanisms; criteria and requirements for transfers by way of binding corporate rules; transfer derogations; administrative sanctions; processing for health purposes; processing in the employment context and processing for historical, statistical and scientific research purposes. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level. The Commission, when preparing and drawing up delegated acts, should ensure a simultaneous, timely and appropriate transmission of relevant documents to the European Parliament and Council.~~

Appropriate industry-led measures and policies shall take due account of the principles of technology, service and business model neutrality so as to favour the free movement of personal data within the Union.

Justification

Same justification as amendment 63

The recitals need not lay down an exhaustive list of delegated acts and we therefore propose to delete and refer to the individual articles. The present Data Protection Reform package aims at building a strong, consistent and modern data protection framework at EU level that

can withstand the test of time and new technological developments. To achieve this goal, the language of the Regulation should remain technology neutral, and future proof for the decades to come.

Amendment 20

Recital 130 (Implementing Acts)	
Commission proposal	Proposed DIGITALEUROPE amendment
<p>In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission for: specifying standard forms in relation to the processing of personal data of a child; standard procedures and forms for exercising the rights of data subjects; standard forms for the information to the data subject; standard forms and procedures in relation to the right of access; the right to data portability; standard forms in relation to the responsibility of the controller to data protection by design and by default and to the documentation; specific requirements for the security of processing; the standard format and the procedures for the notification of a personal data breach to the supervisory authority and the communication of a personal data breach to the data subject; standards and procedures for a data protection impact assessment; forms and procedures for prior authorisation and prior consultation; technical standards and mechanisms for certification; the adequate level of protection afforded by a third country or a territory or a processing sector within that third</p>	<p>In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission. for: specifying standard forms in relation to the processing of personal data of a child; standard procedures and forms for exercising the rights of data subjects; standard forms for the information to the data subject; standard forms and procedures in relation to the right of access; the right to data portability; standard forms in relation to the responsibility of the controller to data protection by design and by default and to the documentation; specific requirements for the security of processing; the standard format and the procedures for the notification of a personal data breach to the supervisory authority and the communication of a personal data breach to the data subject; standards and procedures for a data protection impact assessment; forms and procedures for prior authorisation and prior consultation; technical standards and mechanisms for certification; the adequate level of protection afforded by a third country or a territory or a</p>



country or an international organisation; disclosures not authorized by Union law; mutual assistance; joint operations; decisions under the consistency mechanism. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers. In this context, the Commission should consider specific measures for micro, small and medium-sized enterprises.

~~processing sector within that third country or an international organisation; disclosures not authorized by Union law; mutual assistance; joint operations; decisions under the consistency mechanism. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers. In this context, the Commission should consider specific measures for micro, small and medium sized enterprises.~~

In implementing the provisions of this Regulation, it shall be ensured that no mandatory requirements for specific technical features are imposed on products and services, including terminal or other electronic communications equipment, which could impede the placing of equipment on the market and the free circulation of such equipment in and between Member States.

Justification

The recitals need not lay down an exhaustive list of implementing acts and we therefore propose to delete and refer to the individual articles. The present Data Protection Reform package aims at building a strong, consistent and modern data protection framework at EU level that can withstand the test of time and new technological developments. To achieve this goal, the language of the Regulation should remain technology neutral, and future proof for the decades to come.

Amendment 21

Article 2.1 (Material Scope)	
Commission proposal	Proposed DIGITALEUROPE amendment
1. This Regulation applies to the processing of personal data wholly or partly by automated means, and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.	1. This Regulation applies to the processing of personal data wholly or partly by automated means, <i>without discrimination between such processing means</i> , and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

Justification

The present Data Protection Reform package aims at building a strong, consistent and modern data protection framework at EU level that can withstand the test of time and new technological developments. To achieve this goal, the language of the Regulation should remain technology neutral, and future proof for the decades to come.

Amendment 22

Article 4.1 (Definitions)	
Commission proposal	Proposed DIGITALEUROPE amendment
'data subject' means an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;	'data subject' means an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person-, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;

Justification

Online identifiers and location data on their own cannot identify individuals and need to be removed from this list. Also, in view of the fact that the draft Regulation places new burdens

on data controllers and processors, it is important to have a clear definition for 'personal data'.

Amendment 23

Article 4.2(a) (NEW) (Definitions)	
Commission proposal	Proposed DIGITALEUROPE amendment
	<i>'identification number' means any numeric, alphanumeric or similar code typically used in the online space, excluding codes assigned by a public or state controlled authority to identify a natural person as an individual.</i>

Justification

The definition of the term 'identification number' would help avoid confusion and increase legal certainty of article 4.1.

Amendment 24

Article 4 (5) (Definitions)	
Commission proposal	Proposed DIGITALEUROPE amendment
'controller' means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes, conditions and means of the processing of personal data; where the purposes, conditions and means of processing are determined by Union law or Member State law, the controller or the specific criteria for his nomination may be designated by Union law or by Member State law;	'controller' means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes, conditions and means of the processing of personal data; where the purposes, conditions and means of processing are determined by Union law or Member State law, the controller or the specific criteria for his nomination may be designated by Union law or by Member State law;

Justification

The essential character of a controller is that they decide why data is being processed in the first place and retain overall responsibility for activities undertaken. How exactly this is done in practice, e.g. whether one set of equipment or processing method is used over another, is

not a prerequisite for such a role. Focusing on the determination of the purposes as the primary factor brings greater clarity to the distinction between controllers and processors.

Amendment 25

Article 4 (8) (definitions: consent)	
Commission proposal	Proposed DIGITALEUROPE amendment
'the data subject's consent' means any freely given specific, informed and explicit indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed;	'the data subject's consent' means any freely given specific, informed and <i>unambiguous</i> <i>explicit</i> indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed;

Justification

The term 'unambiguous' is better suited as it does not lower but rather increases the requirements of 'consent' compared to 'explicit' (in combination with the requirement of 'affirmative action') and it has a much better chance to be understood in a consistent way in all the Member States.

Amendment 26

Article 4 (13) (Definitions)	
Commission proposal	Proposed DIGITALEUROPE amendment
'main establishment' means as regards the controller, the place of its establishment in the Union where the main decisions as to the purposes, conditions and means of the processing of personal data are taken; if no decisions as to the purposes, conditions and means of the processing of personal data are taken in the Union, the main establishment is the place where the main processing activities in the context of the activities of an establishment of a controller in the Union	'main establishment' means <i>as regards the controller, the place of its establishment in the Union</i> <i>the location as determined by the data controller or data processor on the basis of the following objective criteria: the location of the group's European headquarters, the location of the company within the group with delegated data protection responsibilities, the location of the company which is best placed (in terms of management function, administrative</i>



<p>take place. As regards the processor, 'main establishment' means the place of its central administration in the Union;</p>	<p><i>burden etc) to address and enforce the rules as set out in this Regulation, the place where the main most decisions as to the purposes or conditions and means of the processing of personal data are taken. if no decisions as to the purposes, conditions and means of the processing of personal data are taken in the Union, the main establishment is the place where the main processing activities in the context of the activities of an establishment of a controller in the Union take place. As regards the processor, 'main establishment' means the place of its central administration in the Union;</i></p>
---	--

Justification

The determination of the main establishment should be done on the basis of various criteria to ensure organisations have enough guidance to determine their main establishment and provide objective measures by which to judge their decision in the event of a dispute. Already there are such criteria to determine the lead DPA in the context of Binding Corporate Rules (BCRs) which have a proven track record. We think inserting the same criteria as outlined in Art 29 WP opinion 108 would provide more clarity and options that would not be covered under the current proposal. Moreover, as many entities are both controllers and processors, we believe that they should be subject to the same set of criteria in determining their main establishment to avoid potentially conflicting results. For the same reason, we have changed “main” decisions to “most” as this would bring it in line with the BCR guidance.

Amendment 27

Article 5 (Principles relating to personal data processing)	
Commission proposal	Proposed DIGITALEUROPE amendment
<p>Personal data must be:</p> <p>(a) processed lawfully, fairly and in a transparent manner in relation to the data subject;</p> <p>(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;</p>	<p>Personal data must be:</p> <p>(a) processed lawfully, fairly and in a transparent manner in relation to the data subject;</p> <p>b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes; <i>in particular, those mechanisms shall ensure that by default personal data are not made accessible</i></p>



<p>(c) adequate, relevant, and limited to the minimum necessary in relation to the purposes for which they are processed; they shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data;</p> <p>(d) accurate and kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;</p> <p>(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the data will be processed solely for historical, statistical or scientific research purposes in accordance with the rules and conditions of Article 83 and if a periodic review is carried out to assess the necessity to continue the storage;</p> <p>(f) processed under the responsibility and liability of the controller, who shall ensure and demonstrate for each processing operation the compliance with the provisions of this Regulation.</p>	<p><i>to an indefinite number of individuals.</i></p> <p>(c) adequate, relevant, and limited to the minimum necessary in relation to the purposes for which they are processed; they shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data;</p> <p>(d) accurate and kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;</p> <p>(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the data will be processed solely for historical, statistical or scientific research purposes in accordance with the rules and conditions of Article 83 and if a periodic review is carried out to assess the necessity to continue the storage;</p> <p>(f) processed under the responsibility and liability of the controller, who shall ensure and demonstrate for each processing operation the compliance with the provisions of this Regulation.</p>
---	---

Justification

The principle added by this proposed amendment is taken from Article 23. From a structural point of view and to preserve the specific principle of Art 23 (2), we propose to move the language into Art 5, establishing the “principles relating to personal data processing”.

Amendment 28

Article 6 (1) (Lawfulness of processing)	
Commission proposal	Proposed DIGITALEUROPE amendment
<p>1. Processing of personal data shall be lawful only if and to the extent that at least one of the following applies:</p> <p>(a) the data subject has given consent to the processing of their personal data for one or more specific purposes;</p> <p>(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;</p> <p>(c) processing is necessary for compliance with a legal obligation to which the controller is subject;</p> <p>(d) processing is necessary in order to protect the vital interests of the data subject;</p> <p>(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;</p> <p>(f) processing is necessary for the purposes of the legitimate interests pursued by a controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks.</p> <p>2. Processing of personal data which is necessary for the purposes of historical, statistical or scientific research shall be lawful subject to the conditions and</p>	<p>1. Processing of personal data shall be lawful only if and to the extent that at least one of the following applies:</p> <p>(a) the data subject has given consent to the processing of their personal data for one or more specific purposes;</p> <p>(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; <i>or as otherwise appropriate to manage or effectuate the relationship between the controller and data subject;</i></p> <p>(c) processing is necessary for compliance with a legal obligation to which the controller is subject;</p> <p>(d) processing is necessary in order to protect the vital interests of the data subject;</p> <p>(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;</p> <p>(f) processing is necessary for the purposes of the legitimate interests pursued by a controller <i>or by a third party</i>, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks.</p> <p>2. Processing of personal data which is necessary for the purposes of historical, statistical or scientific research shall be lawful subject to the conditions and</p>

<p>safeguards referred to in Article 83.</p> <p>3. The basis of the processing referred to in points (c) and (e) of paragraph 1 must be provided for in:</p> <p>(a) Union law, or</p> <p>(b) the law of the Member State to which the controller is subject.</p> <p>The law of the Member State must meet an objective of public interest or must be necessary to protect the rights and freedoms of others, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued.</p> <p>4. Where the purpose of further processing is not compatible with the one for which the personal data have been collected, the processing must have a legal basis at least in one of the grounds referred to in points (a) to (e) of paragraph 1. This shall in particular apply to any change of terms and general conditions of a contract.</p> <p>5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the conditions referred to in point (f) of paragraph 1 for various sectors and data processing situations, including as regards the processing of personal data related to a child.</p>	<p>safeguards referred to in Article 83.</p> <p>3. The basis of the processing referred to in points (c) and (e) of paragraph 1 must be provided for in:</p> <p>(a) Union law, or</p> <p>(b) the law of the Member State to which the controller is subject.</p> <p>The law of the Member State must meet an objective of public interest or must be necessary to protect the rights and freedoms of others, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued.</p> <p>4. Where the purpose of further processing is not compatible with the one for which the personal data have been collected, the processing must have a legal basis at least in one of the grounds referred to in points (a) to (e) of paragraph 1. This shall in particular apply to any change of terms and general conditions of a contract.</p> <p>5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the conditions referred to in point (f) of paragraph 1 for various sectors and data processing situations, including as regards the processing of personal data related to a child.</p>
---	---

Justification

The processing of personal data in the legitimate interest of third parties should be deemed lawful, provided that the interests or the rights and freedoms of the data subject are not overriding. Such provision was already a substantial part of Directive 95/46/EC and is still necessary, among others, for legitimate business purposes of credit or collection agencies.

Amendment 29

Article 7 (Conditions for consent)	
Commission proposal	Proposed DIGITALEUROPE amendment
<p>1. The controller shall bear the burden of proof for the data subject's consent to the processing of their personal data for specified purposes.</p> <p>2. If the data subject's consent is to be given in the context of a written declaration which also concerns another matter, the requirement to give consent must be presented distinguishable in its appearance from this other matter.</p> <p>3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.</p> <p>4. Consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller.</p>	<p>1. The controller shall bear the burden of proof for the data subject's consent to the processing of their personal data for specified purposes.</p> <p>2. If the data subject's consent is to be given in the context of a written declaration which also concerns another matter, the requirement to give consent must be presented distinguishable in its appearance from this other matter.</p> <p>3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.</p> <p>4. Consent shall not provide a legal basis for the processing, where there is when, due to a significant imbalance between the position of the data subject and the controller, the data subject could not refuse his consent without suffering harmful consequences of a material nature attributable to the controller.</p>

Justification

The proposed deletion will simplify the Regulation without diminishing the requirements necessary to obtain consent and therefore the protection of data subjects. Article 4.8 already specifies that consent needs to be given unambiguously on an informed basis. This regulates in a crystal clear way that the consumer needs to be fully aware of what he/she gives his/her consent to.

'Consent' should continue to be an important justification allowing the procession of personal data. The proposal of the Commission risks to devalue the consent requirement to an empty shell as in practice in a vast majority of cases there will be a significant imbalance between the controller and the data subject (quasi all employer/employee and business/consumer relationships). It is therefore important to specify that consent is not a basis for data processing only when the imbalance is such that the data subject would suffer material harm as a consequence of not providing consent.

Amendment 30

Article 10 (Processing not allowing identification)	
Commission proposal	Proposed DIGITALEUROPE amendment
If the data processed by a controller do not permit the controller to identify a natural person, the controller shall not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation.	If the data processed by a controller do not permit the controller, <i>through means used by the controller</i> , to identify a natural person, the controller shall not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation.

Justification

The proposed insertion would further clarify Article 10 that a controller does not have to collect additional information about data subjects in order to identify them for the sole purpose of complying with any provision of the regulation.

Amendment 31

Article 14 (Information to the data subject)	
Commission proposal	Proposed DIGITALEUROPE amendment
<p>1. Where personal data relating to a data subject are collected, the controller shall provide the data subject with at least the following information:</p> <p>(a) the identity and the contact details of the controller and, if any, of the controller's representative and of the data protection officer;</p> <p>(b) the purposes of the processing for which the personal data are intended, including the contract terms and general conditions where the processing is based on point (b) of Article 6(1) and the legitimate interests pursued by the controller where the processing is based on point (f) of Article</p>	<p>1. Where personal data relating to a data subject are collected, the controller shall provide the data subject with at least the following information:</p> <p>(a) the identity and the contact details of the controller and, if any, of the controller's representative and of the data protection officer;</p> <p>(b) the purposes of the processing for which the personal data are intended, including the contract terms and general conditions where the processing is based on point (b) of Article 6(1) and the legitimate interests pursued by the controller where the processing is based on point (f) of Article</p>

<p>6(1);</p> <p>(c) the period for which the personal data will be stored;</p> <p>(d) the existence of the right to request from the controller access to and rectification or erasure of the personal data concerning the data subject or to object to the processing of such personal data;</p> <p>(e) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority;</p> <p>(f) the recipients or categories of recipients of the personal data;</p> <p>(g) where applicable, that the controller intends to transfer to a third country or international organisation and on the level of protection afforded by that third country or international organisation by reference to an adequacy decision by the Commission;</p> <p>(h) any further information necessary to guarantee fair processing in respect of the data subject, having regard to the specific circumstances in which the personal data are collected.</p> <p>2. Where the personal data are collected from the data subject, the controller shall inform the data subject, in addition to the information referred to in paragraph 1, whether the provision of personal data is obligatory or voluntary, as well as the possible consequences of failure to provide such data.</p> <p>3. Where the personal data are not collected from the data subject, the controller shall inform the data subject, in addition to the information referred to in paragraph 1, from which source the personal data originate.</p> <p>4. The controller shall provide the information referred to in paragraphs 1, 2 and 3:</p> <p>(a) at the time when the personal data are</p>	<p>6(1);</p> <p>(c) the period for which the personal data will be stored;</p> <p>(d) the existence of the right to request from the controller access to and rectification or erasure of the personal data concerning the data subject or to object to the processing of such personal data;</p> <p>(e) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority;</p> <p>(f) the recipients or categories of recipients of the personal data;</p> <p>(g) where applicable, that the controller intends to transfer to a third country or international organisation and on the level of protection afforded by that third country or international organisation by reference to an adequacy decision by the Commission;</p> <p>(h) any further information necessary to guarantee fair processing in respect of the data subject, having regard to the specific circumstances in which the personal data are collected.</p> <p>2. Where the personal data are collected from the data subject, the controller shall inform the data subject, in addition to the information referred to in paragraph 1, whether the provision of personal data is obligatory or voluntary, as well as the possible consequences of failure to provide such data.</p> <p>3. Where the personal data are not collected from the data subject, the controller shall inform the data subject, in addition to the information referred to in paragraph 1, from which source the personal data originate.</p> <p>4. The controller shall provide the information referred to in paragraphs 1, 2 and 3:</p> <p>(a) at the time when the personal data are</p>
---	---

<p>obtained from the data subject; or</p> <p>(b) where the personal data are not collected from the data subject, at the time of the recording or within a reasonable period after the collection, having regard to the specific circumstances in which the data are collected or otherwise processed, or, if a disclosure to another recipient is envisaged, and at the latest when the data are first disclosed.</p> <p>5. Paragraphs 1 to 4 shall not apply, where:</p> <p>(a) the data subject has already the information referred to in paragraphs 1, 2 and 3; or</p> <p>(b) the data are not collected from the data subject and the provision of such information proves impossible or would involve a disproportionate effort; or</p> <p>(c) the data are not collected from the data subject and recording or disclosure is expressly laid down by law; or</p> <p>(d) the data are not collected from the data subject and the provision of such information will impair the rights and freedoms of others, as defined in Union law or Member State law in accordance with Article 21.</p> <p>6. In the case referred to in point (b) of paragraph 5, the controller shall provide appropriate measures to protect the data subject's legitimate interests.</p> <p>7. The Commission shall be empowered to adopt delegated acts in accordance with</p>	<p>obtained from the data subject; or</p> <p>(b) where the personal data are not collected from the data subject, at the time of the recording or within a reasonable period after the collection, having regard to the specific circumstances in which the data are collected or otherwise processed, or, <i>except when processing data strictly necessary for the purposes of ensuring network and information security, including fraud prevention</i> if a disclosure to another recipient is envisaged, and at the latest when the data are first disclosed.</p> <p>5. Paragraphs 1 to 4 shall not apply, where:</p> <p>(a) the data subject has already the information referred to in paragraphs 1, 2 and 3; or</p> <p>(b) the data are not collected from the data subject and the provision of such information proves impossible, <i>impractical, or</i> or would involve a disproportionate effort <i>or would impair other legitimate interests of the controller or vital interests of the data subject;</i> or</p> <p>(c) the data are not collected from the data subject and recording or disclosure is expressly laid down by law; or</p> <p>(d) the data are not collected from the data subject and the provision of such information will impair the rights and freedoms of others, as defined in Union law or Member State law in accordance with Article 21.</p> <p>6. In the case referred to in point (b) of paragraph 5, the controller shall provide appropriate measures to protect the data subject's legitimate interests.</p> <p>7. The Commission shall be empowered to</p>
--	--



<p>Article 86 for the purpose of further specifying the criteria for categories of recipients referred to in point (f) of paragraph 1, the requirements for the notice of potential access referred to in point (g) of paragraph 1, the criteria for the further information necessary referred to in point (h) of paragraph 1 for specific sectors and situations, and the conditions and appropriate safeguards for the exceptions laid down in point (b) of paragraph 5. In doing so, the Commission shall take the appropriate measures for micro, small and medium-sized-enterprises.</p> <p>8. The Commission may lay down standard forms for providing the information referred to in paragraphs 1 to 3, taking into account the specific characteristics and needs of various sectors and data processing situations where necessary. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>	<p>adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria for categories of recipients referred to in point (f) of paragraph 1, the requirements for the notice of potential access referred to in point (g) of paragraph 1, the criteria for the further information necessary referred to in point (h) of paragraph 1 for specific sectors and situations, and the conditions and appropriate safeguards for the exceptions laid down in point (b) of paragraph 5. In doing so, the Commission shall take the appropriate measures for micro, small and medium-sized-enterprises.</p> <p>8. The Commission may lay down standard forms for providing the information referred to in paragraphs 1 to 3, taking into account the specific characteristics and needs of various sectors and data processing situations where necessary. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>
---	---

Justification

Having established that personal data may be processed for network and information security purposes based on the provisions in article 6 (1) d, e and f, the data controller must abide by the conditions to inform the data subject on the legitimate interests pursued and on the right to object (as well as being compliant with further rights such as the right of access). In situations in networking and information security processing where it is possible to identify the data subject (for example, an ISP which has a direct relationship with their subscribers and can map IP addresses to individuals), it is preferable to undertake certain processing without informing the data subject at the time, such as when there is a compromised machine sending spam and other circumstances where one is using the data to track the control traffic and identify the real malicious actors further up the chain. Hence a reasonable time period for informing the data subject that their personal data has been processed (in accordance with Article 14.4(b)) is after the conclusion of such investigations.

If the data subject in question is a suspected malicious actor and the suspected offence is criminal, you may not want to prejudice investigations by law enforcement authorities, and hence the responsibility to exercise the data subjects' rights in such situations should pass over to the authorities in question.

Article 14.4(b) also envisages the informing of data subjects at the latest at first point of contact with a further recipient of the data. Given security companies may need to cooperate during investigations (e.g. a network security company and an ISP), this clause could lead to data subjects being informed too early in the process and hence it should be deleted or an exception made when data is processed for network and information security purposes.

Amendment 32

Article 15 (Right of access for the data subject)	
Commission proposal	Proposed DIGITALEUROPE amendment
<p>1. The data subject shall have the right to obtain from the controller at any time, on request, confirmation as to whether or not personal data relating to the data subject are being processed. Where such personal data are being processed, the controller shall provide the following information:</p> <p>(a) the purposes of the processing;</p> <p>(b) the categories of personal data concerned;</p> <p>(c) the recipients or categories of recipients to whom the personal data are to be or have been disclosed, in particular to recipients in third countries;</p> <p>(d) the period for which the personal data will be stored;</p> <p>(e) the existence of the right to request from the controller rectification or erasure of personal data concerning the data subject or to object to the processing of such personal data;</p> <p>(f) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority;</p> <p>(g) communication of the personal data undergoing processing and of any</p>	<p>1. The data subject shall have the right to obtain from the controller at any time, on request, confirmation as to whether or not personal data relating to the data subject are being processed. Where such personal data are being processed and the controller can reply to this request without gathering additional personal data, the controller shall provide the following information:</p> <p>(a) the purposes of the processing;</p> <p>(b) the categories of personal data concerned;</p> <p>(c) the recipients or categories of recipients to whom the personal data are to be or have been disclosed, in particular to recipients in third countries;</p> <p>(d) the period for which the personal data will be stored;</p> <p>(e) the existence of the right to request from the controller rectification or erasure of personal data concerning the data subject or to object to the processing of such personal data;</p> <p>(f) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority;</p> <p>(g) communication of the personal data undergoing processing and of any</p>



<p>available information as to their source;</p> <p>(h) the significance and envisaged consequences of such processing, at least in the case of measures referred to in Article 20.</p> <p>2. The data subject shall have the right to obtain from the controller communication of the personal data undergoing processing. Where the data subject makes the request in electronic form, the information shall be provided in electronic form, unless otherwise requested by the data subject.</p> <p>3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the communication to the data subject of the content of the personal data referred to in point (g) of paragraph 1.</p> <p>4. The Commission may specify standard forms and procedures for requesting and granting access to the information referred to in paragraph 1, including for verification of the identity of the data subject and communicating the personal data to the data subject, taking into account the specific features and necessities of various sectors and data processing situations. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>	<p>available information as to their source;</p> <p>(h) the significance and envisaged consequences of such processing, at least in the case of measures referred to in Article 20.</p> <p>2. The data subject shall have the right to obtain from the controller communication of the personal data undergoing processing. Where the data subject makes the request in electronic form, the information shall be provided in electronic form, unless otherwise requested by the data subject.</p> <p>3. <i>(NEW) The right of access shall exclude any information whose disclosure could prejudice the securing, protecting and maintaining the resiliency of one or more information systems, for example the algorithms used in the processing.</i></p> <p>3. 4. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria, and requirements and exceptions for the communication to the data subject of the content of the personal data referred to in point (g) of paragraph 1.</p> <p>4. 5. The Commission may specify standard forms and procedures for requesting and granting access to the information referred to in paragraph 1, including for verification of the identity of the data subject and communicating the personal data to the data subject, taking into account the specific features and necessities of various sectors and data processing situations. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>
---	---

Justification

In some cases, complying with a right of access requirement will have as a consequence that the data controller will need to gather (more) personal data from the data subject in order to comply with the request. For example, data such as an IP address, that is based on the context of the specific processing isn't personal data if the data controller can't by all means likely reasonably identify the data subject, would now become personal data as the data controller would need to collect more personal information as to verify the identity of the data subject, including gathering his IP address as to authenticate that the person who is requesting access is actually the legitimate person. In line with the principle of data minimization, the Regulation should strive to avoid any additional requirements which impose on the data subject the obligation to do so. The above clarifications would allow for the data subjects to exercise their legitimate rights of access but also recognizes that in some cases, such requirements need to be qualified as it should not be used to gain access to specific trade secrets such as algorithms, nor impede with legitimate interests such as protecting users' terminals. Malicious actors should not be given the ability to block the work of CERTs, CSIRTs, providers of electronic communications networks and services and providers of security technologies and services. Furthermore the reference to Art. 20 has been deleted for consistency with proposed amendment to Art 20.

Amendment 33

Article 17 (Right to be Forgotten and to erasure)	
Commission proposal	Proposed DIGITALEUROPE amendment
<p>1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child, where one of the following grounds applies:</p> <p>(a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;</p> <p>(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data;</p> <p>(c) the data subject objects to the processing of personal data pursuant to Article 19;</p>	<p>1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child, where one of the following grounds applies:</p> <p>(a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;</p> <p>(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data;</p> <p>(c) the data subject objects to the processing of personal data pursuant to Article 19;</p>

<p>(d) the processing of the data does not comply with this Regulation for other reasons.</p> <p>2. Where the controller referred to in paragraph 1 has made the personal data public, it shall take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible, to inform third parties which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data. Where the controller has authorised a third party publication of personal data, the controller shall be considered responsible for that publication.</p> <p>3. The controller shall carry out the erasure without delay, except to the extent that the retention of the personal data is necessary:</p> <p>(a) for exercising the right of freedom of expression in accordance with Article 80;</p> <p>(b) for reasons of public interest in the area of public health in accordance with Article 81;</p> <p>(c) for historical, statistical and scientific research purposes in accordance with Article 83;</p> <p>(d) for compliance with a legal obligation to retain the personal data by Union or Member State law to which the controller is subject; Member State laws shall meet an objective of public interest, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued;</p> <p>(e) in the cases referred to in paragraph 4.</p> <p>4. Instead of erasure, the controller shall restrict processing of personal data where:</p> <p>(a) their accuracy is contested by the data subject, for a period enabling the controller to verify the accuracy of the data;</p> <p>(b) the controller no longer needs the personal</p>	<p>(d) the processing of the data does not comply with this Regulation for other reasons.</p> <p>2. Where the controller referred to in paragraph 1 has made the personal data public, it shall take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible, to inform third parties which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data. Where the controller has authorised a third party publication of personal data, the controller shall be considered responsible for that publication.</p> <p>3. The controller shall carry out the erasure without delay, except to the extent that the retention of the personal data is necessary:</p> <p>(a) for exercising the right of freedom of expression in accordance with Article 80;</p> <p>(b) for reasons of public interest in the area of public health in accordance with Article 81;</p> <p>(c) for historical, statistical and scientific research purposes in accordance with Article 83;</p> <p>(d) for compliance with a legal obligation to retain the personal data by Union or Member State law to which the controller is subject; Member State laws shall meet an objective of public interest, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued;</p> <p>(e) in the cases referred to in paragraph 4.</p> <p>4. Instead of erasure, the controller shall restrict processing of personal data where:</p> <p>(a) their accuracy is contested by the data subject, for a period enabling the controller to verify the accuracy of the</p>
--	---

<p>data for the accomplishment of its task but they have to be maintained for purposes of proof;</p> <p>(c) the processing is unlawful and the data subject opposes their erasure and requests the restriction of their use instead;</p> <p>(d) the data subject requests to transmit the personal data into another automated processing system in accordance with Article 18(2).</p> <p>5. Personal data referred to in paragraph 4 may, with the exception of storage, only be processed for purposes of proof, or with the data subject's consent, or for the protection of the rights of another natural or legal person or for an objective of public interest.</p> <p>6. Where processing of personal data is restricted pursuant to paragraph 4, the controller shall inform the data subject before lifting the restriction on processing.</p> <p>7. The controller shall implement mechanisms to ensure that the time limits established for the erasure of personal data and/or for a periodic review of the need for the storage of the data are observed.</p> <p>8. Where the erasure is carried out, the controller shall not otherwise process such</p>	<p>data;</p> <p>(b) the controller no longer needs the personal data for the accomplishment of its task but they have to be maintained for purposes of proof;</p> <p>(c) the processing is unlawful and the data subject opposes their erasure and requests the restriction of their use instead;</p> <p>(d) the data subject requests to transmit the personal data into another automated processing system in accordance with Article 18(2).</p> <p>5. Personal data referred to in paragraph 4 may, with the exception of storage, only be processed for purposes of proof, or with the data subject's consent, or for the protection of the rights of another natural or legal person or for an objective of public interest.</p> <p>6. Where processing of personal data is restricted pursuant to paragraph 4, the controller shall inform the data subject before lifting the restriction on processing.</p> <p>7. <i>(NEW) Requests for the rectification, erasure or blocking of data shall not prejudice processing that is necessary to secure, protect and maintain the resiliency of one or more information systems. In addition, the right of rectification and/or erasure or personal data shall not apply to any personal data that is required to be maintained by legal obligation or to protect the rights of the controller, processor, or third parties.</i></p> <p>7.8 The controller shall implement mechanisms to ensure that the time limits established for the erasure of personal data and/or for a periodic review of the need for the storage of the data are observed.</p>
--	---

<p>personal data.</p> <p>9. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying:</p> <ul style="list-style-type: none"> (a) the criteria and requirements for the application of paragraph 1 for specific sectors and in specific data processing situations; (b) the conditions for deleting links, copies or replications of personal data from publicly available communication services as referred to in paragraph 2; (c) the criteria and conditions for restricting the processing of personal data referred to in paragraph 4. 	<p>8.9 Where the erasure is carried out, the controller shall not otherwise process such personal data.</p> <p>9.10 The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying:</p> <ul style="list-style-type: none"> (a) the criteria and requirements for the application of paragraph 1 for specific sectors and in specific data processing situations; (b) the conditions for deleting links, copies or replications of personal data from publicly available communication services as referred to in paragraph 2; (c) the criteria and conditions for restricting the processing of personal data referred to in paragraph 4.
---	---

Justification

In addition, there are circumstances where the right of the data subject to rectify or erase personal data should not apply – for example, in compliance with EU member states laws and other jurisdictions requiring maintenance of certain types of personal data for national security reasons, or for investigations of potential wrongdoing.

Amendment 34

Article 18 (Right to data portability)	
Commission proposal	Proposed DIGITALEUROPE amendment
<p>1. The data subject shall have the right, where personal data are processed by electronic means and in a structured and commonly used format, to obtain from the controller a copy of data undergoing processing in an electronic and structured format which is commonly used and allows for further use by the data subject.</p>	<p>1. The data subject shall have the right, where personal data are processed by electronic means and in a structured and commonly used format, to obtain from the controller a copy of their data undergoing processing in an electronic and structured format which is commonly used and allows for further use by the data subject.</p>
<p>2. Where the data subject has provided the</p>	<p>2. Where the data subject has provided the personal data and the processing is based on</p>



<p>personal data and the processing is based on consent or on a contract, the data subject shall have the right to transmit those personal data and any other information provided by the data subject and retained by an automated processing system, into another one, in an electronic format which is commonly used, without hindrance from the controller from whom the personal data are withdrawn.</p> <p>3. The Commission may specify the electronic format referred to in paragraph 1 and the technical standards, modalities and procedures for the transmission of personal data pursuant to paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>	<p>consent or on a contract, the data subject shall have the right to transmit those personal data, <i>which are processed by electronic means and in a structured and commonly used format</i> and any other information provided by the data subject and retained by an automated processing system, into another one, in an electronic format which is commonly used, without hindrance from the controller from whom the personal data are withdrawn.</p> <p>3. The Commission may specify the electronic format referred to in paragraph 1 and the technical standards, modalities and procedures for the transmission of personal data pursuant to paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>
---	--

Justification

Users should own their data and ask for it when they no longer wish to use it. It should be clear that portability refers to the data provided by the subject which is in a commonly used format. Standardizing the format of data risks storing more or less data than is required for the service in question, and also poses a risk to the security of that data – common keys become easier to break. Standardizing data formats would also hinder innovation, as current uses of data may not reflect future needs and practices.

Amendment 35

Article 20 (Measures based on profiling)	
Commission proposal	Proposed DIGITALEUROPE amendment
<p>1. Every natural person shall have the right not to be subject to a measure which produces legal effects concerning this natural person or significantly affects this natural person, and which is based solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work,</p>	<p>1. Every natural person data subject shall have the right not to be subject to a measure which produces legal effects <i>that gravely and adversely affect his fundamental rights concerning this natural person or significantly affects this natural person</i>, and which is based solely on automated processing intended to evaluate, certain personal aspects relating to this natural</p>



economic situation, location, health, personal preferences, reliability or behaviour.	person or to analyse or predict the natural person's performance at work, economic situation, location , health, personal preferences, reliability or behaviour.
---	--

Justification

Additional, distinct measures for processing of personal data through automated means are only justified for cases where the measure produces legal effects; any other profiling that constitutes processing of personal data is normal processing and already subject to all the provisions of the Regulation. The list in article 20 needs to be a closed one.

Amendment 36

Article 22 (Responsibility of the controller)	
Commission proposal	Proposed DIGITALEUROPE amendment
1. The controller shall adopt policies and implement appropriate measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation.	1. The controller shall adopt policies and implement appropriate measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation.
2. The measures provided for in paragraph 1 shall in particular include:	2. The measures provided for in paragraph 1 shall in particular include:
(a) keeping the documentation pursuant to Article 28;	(a) keeping the documentation pursuant to Article 28;
(b) implementing the data security requirements laid down in Article 30;	(b) implementing the data security requirements laid down in Article 30;
(c) performing a data protection impact assessment pursuant to Article 33;	(c) performing a data protection impact assessment pursuant to Article 33;
(d) complying with the requirements for prior authorisation or prior consultation of the supervisory authority pursuant to Article 34(1) and (2);	(d) complying with the requirements for prior authorisation or prior consultation of the supervisory authority pursuant to Article 34(1) and (2);



<p>(e) designating a data protection officer pursuant to Article 35(1).</p> <p>3. The controller shall implement mechanisms to ensure the verification of the effectiveness of the measures referred to in paragraphs 1 and 2. If proportionate, this verification shall be carried out by independent internal or external auditors.</p> <p>4. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures referred to in paragraph 1 other than those already referred to in paragraph 2, the conditions for the verification and auditing mechanisms referred to in paragraph 3 and as regards the criteria for proportionality under paragraph 3, and considering specific measures for micro, small and medium-sized-enterprises.</p>	<p>(e) designating a data protection officer pursuant to Article 35(1), if any.</p> <p>3. The controller shall implement mechanisms to ensure the verification of the effectiveness of the measures referred to in paragraphs 1 and 2. If proportionate, this verification shall be carried out by independent internal or external auditors.</p> <p>4. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures referred to in paragraph 1 other than those already referred to in paragraph 2, the conditions for the verification and auditing mechanisms referred to in paragraph 3 and as regards the criteria for proportionality under paragraph 3, and considering specific measures for micro, small and medium-sized enterprises.</p> <p><i>Having regard to the state of the art, the nature of personal data processing and the type of the organization, both at the time of the determination of the means for processing and at the time of the processing itself, appropriate and demonstrable technical and organizational measures should be implemented in such a way that the processing will meet the requirements of this Regulation and ensures the protection of the rights of the data subject by design.</i></p> <p><i>Such measures include, without limitation:</i></p> <p>a) <i>Sufficiently independent management oversight of processing of personal data to ensure the existence and effectiveness of the technical and organizational measures;</i></p>
---	--



- b) Existence of proper policies, instructions or other guidelines to guide data processing needed to comply with the Regulation as well as procedures and enforcement to make such guidelines effective;*
- c) Existence of proper planning procedures to ensure compliance and to address potentially risky processing of personal data prior to the commencement of the processing;*
- d) Existence of appropriate documentation of data processing to enable compliance with the obligations arising from the Regulation;*
- e) Existence of adequately skilled data protection organization or data protection officer or other staff supported with adequate resources to oversee implementation of measures defined in this article and to monitor compliance with this Regulation, having particular regard to ensuring sufficient organizational independence of such data protection officer or other staff to prevent inappropriate conflicts of interest. Such a function may be fulfilled by way of a service contract;*
- f) Existence of proper awareness and training of the staff participating in data processing and decisions thereto of the obligations arising from this Regulation;*

Upon request by the competent data protection authority, the controller or processor shall demonstrate the existence of technical and organizational measures.

Group of undertakings may apply joint technical and organizational measures to meet its obligations arising from the Regulation.

This article does not apply to a natural person processing personal data without

	<i>commercial interest.</i>
--	-----------------------------

Justification

We believe all organizations engaged in the processing of personal data, including controllers and processors irrespective of their size, should be held accountable for implementing appropriate, demonstrable and effective technical and organizational measures to ensure compliance with the Regulation.

However, to avoid new types of burdens and modalities on organizations and data protection authorities alike resulting from the detailed and prescriptive proposal, a simpler, and outcomes based organizational accountability obligation should be introduced. To ensure optimal data protection, the Regulation should provide enough flexibility to allow different organizations to implement the most effective technical and organizational measures, fit for the nature and structure of each respective organization.

Accountability is a well-established principle of data protection, found in existing guidance such as the OECD Guidelines¹ and APEC Privacy Framework² and in the laws of for example Canada and Mexico. Regulators, industry and advocacy groups have further defined the essential elements of accountability³.

Essential elements of effective privacy programs include sufficient management oversight, policies, processes and practices to make the policies effective, risk assessment and mitigation planning procedures, adequately skilled data protection staff, awareness and training of staff, internal enforcement, issue response and remedies to those whose privacy has been put at risk. Such program should be tailored having regard to the type of the organization, the nature of the processed personal data and the state of the art of technologies and available methodologies, for example to carry out a data protection impact assessment. Implementing such Accountability concept in the Data Protection Regulation instead of opting for the antiquated prescriptive and straight-jacked set of compliance requirements as currently proposed would in practice lead to improved data protection and avoid unnecessary burden for controllers, processors and DPAs.

Amendment 37

Art 23 (Data Protection by Design/Default)

¹ http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html

² http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx

³ http://www.informationpolicycentre.com/accountability-based_privacy_governance/



Commission proposal	Proposed DIGITALEUROPE amendment
<p>1. Having regard to the state of the art and the cost of implementation, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.</p> <p>2. The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals.</p>	<p>1. Having regard to the state of the art and, the cost of implementation <i>and international best practices, appropriate measures and procedures may be implemented to extend technically feasible and effective to ensure the processing operation meets the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures and procedures in such a way that the processing will meet</i> the requirements of this Regulation and ensures the protection of the rights of the data subject.</p> <p>2. The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals.</p> <p><i>Such measures and procedures shall:</i></p> <ul style="list-style-type: none"> (a) <i>follow the principle of technology, service and business model neutrality</i> (b) <i>be based on global industry-led efforts and best practices</i> (c) <i>be flexible based on an entities' business model, size, and level of interaction with personal data</i> (d) <i>take due account of existing internationally recognised technical standards and regulations in the area of public safety and security</i>



<p>3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures and mechanisms referred to in paragraph 1 and 2, in particular for data protection by design requirements applicable across sectors, products and services.</p> <p>4. The Commission may lay down technical standards for the requirements laid down in paragraph 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>	<p>(e) <i>take due account of international developments</i></p> <p>3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures and mechanisms referred to in paragraph 1 and 2, in particular for data protection by design requirements applicable across sectors, products and services.</p> <p><i>In implementing the provisions of this Regulation, it shall be ensured that no mandatory requirements for specific technical features are imposed on products and services, including terminal or other electronic communications equipment, which could impede the placing of equipment on the market and the free circulation of such equipment in and between Member States.</i></p> <p>4. The Commission may lay down technical standards for the requirements laid down in paragraph 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>
---	--

Justification

Privacy by Design/Default (PbD/D) are concepts currently being discussed internationally, relates to internal privacy and data protection processes of organizations and are based on a number of factors including their business models, size and interaction with personal data. Although every organization should strive to integrate privacy and data protection into its internal processes, the actual way it does so should remain flexible and leave room for adaptation based on the factors above. This is to say that there is no one right way, which is especially true in the case of SMEs and for entities that are far removed from processing identifiable personal data. It is essential that any PbD concept be technology-neutral and not

introduce specific technology or operational mandates, or contribute to a differentiation between ICT and other economic sectors.

To avoid lack of consistency throughout the proposed text, it is important to streamline the proposed language for Art. 23 with other Data Protection by Design/Default-type obligations, which cover to large extends the proposed text, e.g. Art. 22 and Art. 5 c), Art. 26 (processor agreements), Art. 28 (documentation), Art. 30 (security), Art. 33 (data protection impact assessment) and Art. 35 (data protection officer).

The PbD/D concepts should therefore focus on designing privacy into processes and organizations and should maintain as a key objective providing consumers with appropriate tools to make an informed choice, but avoid creating additional uncertainties via unclear obligations, definitions and terms. Industry-led innovation in this area will create trust and allow for innovative solutions, services and technologies to flourish in the spirit of the European Digital Agenda. Finally, there is a clear need to look into the issue with a global perspective to avoid further fragmentation, taking stock of industry’s own efforts and taking technology developments into account.

Amendment 38

Article 24 (Joint Controllers)	
Commission proposal	Proposed DIGITALEUROPE amendment
<p>Where a controller determines the purposes, conditions and means of the processing of personal data jointly with others, the joint controllers shall determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the procedures and mechanisms for exercising the rights of the data subject, by means of an arrangement between them.</p>	<p>Where a controller determines the purposes, conditions and means of the processing of personal data jointly with others, the joint controllers shall determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the procedures and mechanisms for exercising the rights of the data subject, by means of an arrangement between them.</p>

Justification

Same as justification for Article 4 (5)

(The essential character of a controller is that they decide why data is being processed in the first place and retain overall responsibility for activities undertaken. How exactly this is done in practice, e.g. whether one set of equipment or processing method is used over another, is not a prerequisite for such a role. Focusing on the determination of the purposes as the primary factor brings greater clarity to the distinction between controllers and processors.)

Amendment 39

Article 26 (Processor)	
Commission proposal	Proposed DIGITALEUROPE amendment
<p>1. Where a processing operation is to be carried out on behalf of a controller, the controller shall choose a processor providing sufficient guarantees to implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject, in particular in respect of the technical security measures and organizational measures governing the processing to be carried out and shall ensure compliance with those measures.</p> <p>2. The carrying out of processing by a processor shall be governed by a contract or other legal act binding the processor to the controller and stipulating in particular that the processor shall:</p> <p>(a) act only on instructions from the controller, in particular, where the transfer of the personal data used is prohibited;</p> <p>(b) employ only staff who have committed themselves to confidentiality or are under a statutory obligation of confidentiality;</p> <p>(c) take all required measures pursuant to Article 30;</p> <p>(d) enlist another processor only with the prior permission of the controller;</p> <p>(e) insofar as this is possible given the nature of the processing, create in agreement with</p>	<p>1. Where a-processing operation is to be carried out on behalf of a controller and would involve personal data that would permit the processor to reasonably identify the data subject, the controller shall choose a processor providing sufficient guarantees assurances to implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject, in particular in respect of the technical security measures and organizational measures governing the processing to be carried out and shall ensure compliance with those measures.</p> <p>2. The carrying out of processing by a processor shall be governed by a contract or other legal act binding the processor to the controller and stipulating in particular that the processor shall:</p> <p>(a) act only on instructions from the controller, in particular, where the transfer of the personal data used is prohibited;</p> <p>(b) employ only staff who have committed themselves to confidentiality or are under a statutory obligation of confidentiality;</p> <p>(c) take all required measures pursuant to Article 30;</p> <p>(d) enlist another processor only with the prior permission of the controller</p> <p>(e) insofar as this is possible given the nature of the processing, create in</p>



<p>the controller the necessary technical and organisational requirements for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;</p> <p>(f) assist the controller in ensuring compliance with the obligations pursuant to Articles 30 to 34;</p> <p>(g) hand over all results to the controller after the end of the processing and not process the personal data further after the end of the agreed processing otherwise;</p> <p>(h) make available to the controller and the supervisory authority all information necessary to control compliance with the obligations laid down in this Article.</p> <p>3. The controller and the processor shall document in writing the controller's instructions and the processor's obligations referred to in paragraph 2.</p> <p>4. If a processor processes personal data other than as instructed by the controller, the processor shall be considered to be a controller in respect of that processing and shall be subject to the rules on joint controllers laid down in Article 24.</p> <p>5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the responsibilities, duties and tasks in relation to a processor in line with paragraph 1, and conditions which allow facilitating the processing of personal data within a group of undertakings, in particular for the purposes of control and reporting.</p>	<p>agreement with the controller the necessary technical and organisational requirements for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;</p> <p>(f) assist the controller in ensuring compliance with the obligations pursuant to Articles 30 to 34;</p> <p>(g) hand over all results to the controller after the end of the processing and not process the personal data further after the end of the agreed processing otherwise;</p> <p>(h) make available to the controller and the supervisory authority all information necessary to control compliance with the obligations laid down in this Article.</p> <p>3. The controller and the processor shall document in writing the controller's instructions and the processor's obligations referred to in paragraph 2.</p> <p>4. If a processor processes personal data for purposes other than as instructed by the controller, the processor shall be considered to be a controller in respect of that processing and shall be subject to the rules on joint controllers laid down in Article 24.</p> <p>5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the responsibilities, duties and tasks in relation to a processor in line with paragraph 1, and conditions which allow facilitating the processing of personal data within a group of undertakings, in particular for the purposes of control and</p>
--	---

	reporting.
--	-----------------------

Justification

The proposed text introduces a host of new requirements for data processors and states how these should be included in the contractual arrangements. Some of these additions are unworkable in practice. For example, a controller may want to ensure that additional sub-processors - which may be numerous – apply effective data protection. But it should be clear this does not mean they should assess each in turn prior to their employment. As the processor has the closer relationship, they are better placed to make such a judgment. In relation to handing over results at the end of processing, there may be no results as such to hand over if the data minimisation principle has been effectively applied. Making data available to the supervisory authority should be handled by the controller. Certain information may be subject to a confidentiality obligation under law or contract and hence a processor may not be at liberty to disclose such information to a supervisory authority. Moreover, such data should not be required to be transmitted on a regular basis as this would overburden authorities and further increase the administrative burden. Finally, Art 26(4) implies that the controller would need to provide very detailed instructions as to what personal data the processor shall process. In reality, this is often not the case, yet based on this article the processor would carry the liability for not receiving extremely detailed instructions from the controller. Where a processor does breach such instructions, it is logical that the processor is considered a controller in respect of that processing but there is no reason to include the original data controller as a joint controller in this instance.

Amendment 40

Article 28 (Documentation)	
Commission proposal	Proposed DIGITALEUROPE amendment
<p>1. Each controller and processor and, if any, the controller's representative, shall maintain documentation of all processing operations under its responsibility.</p> <p>2. The documentation shall contain at least the following information:</p> <p>(a) the name and contact details of the controller, or any joint controller or processor, and of the representative, if any;</p>	<p>1. Each controller and processor and, if any, the controller's representative, shall maintain documentation of all the main categories of processing operations under its responsibility.</p> <p>2. Such The documentation shall contain at least the following information:</p> <p>(a) the name and contact details of the controller, or any joint controller or processor, and of the representative, if any;</p>



<p>(b) the name and contact details of the data protection officer, if any;</p> <p>(c) the purposes of the processing, including the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);</p> <p>(d) a description of categories of data subjects and of the categories of personal data relating to them;</p> <p>(e) the recipients or categories of recipients of the personal data, including the controllers to whom personal data are disclosed for the legitimate interest pursued by them;</p> <p>(f) where applicable, transfers of data to a third country or an international organisation, including the identification of that third country or international organisation and, in case of transfers referred to in point (h) of Article 44(1), the documentation of appropriate safeguards;</p> <p>(g) a general indication of the time limits for erasure of the different categories of data;</p> <p>(h) the description of the mechanisms referred to in Article 22(3).</p> <p>3. The controller and the processor and, if any, the controller's representative, shall make the documentation available, on request, to the supervisory authority.</p> <p>4. The obligations referred to in paragraphs 1 and 2 shall not apply to the following</p>	<p>(b) the name and contact details of the data protection organization or data protection officer, if any;</p> <p>(c) the generic purposes of the processing, ,including the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);</p> <p>(d) a description of categories of data subjects and of the categories of personal data relating to them;</p> <p>(e) the recipients or categories of recipients of the personal data. —,including the controllers to whom personal data are disclosed for the legitimate interest pursued by them;</p> <p>(f) where applicable, transfers of personal data to a third country or an international organisation, ,including the identification of that third country or international organisation and, in case of transfers referred to in point (h) of Article 44(1), a reference to the documentation of appropriate safeguards employed;</p> <p>(g) a general indication of the time limits for erasure or data retention policy applicable to of the different categories of data;</p> <p>(h) the description of the mechanisms referred to in Article 22(3).</p> <p>3. The controller and the processor and, if any, the controller's representative, shall make the documentation available, on the basis of a request outlining the reasons for requiring access to the documents, to the supervisory authority.</p> <p>4. The obligations referred to in paragraphs 1 and 2 shall not apply to the following</p>
---	--



<p>controllers and processors:</p> <p>(a) a natural person processing personal data without a commercial interest; or</p> <p>(b) an enterprise or an organisation employing fewer than 250 persons that is processing personal data only as an activity ancillary to its main activities.</p> <p>5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the documentation referred to in paragraph 1, to take account of in particular the responsibilities of the controller and the processor and, if any, the controller's representative.</p> <p>6. The Commission may lay down standard forms for the documentation referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>	<p>controllers and processors:</p> <p>(a) a natural person processing personal data without a commercial interest; or</p> <p>(b) an enterprise or an organisation employing fewer than 250 persons that is processing personal data only as an activity ancillary to its main activities.</p> <p>5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the documentation referred to in paragraph 1, to take account of in particular the responsibilities of the controller and the processor and, if any, the controller's representative.</p> <p>6. <i>To ensure harmonized requirements within Europe,</i> tThe Commission may lay down standard forms for the documentation referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>
--	---

Justification

Effective data protection requires that organisations have sufficiently documented understanding of their data processing activities. The documentation requirement in Art 28.2 remains at rather high level and appears to largely duplicate the notification provisions in Art. 14.

Instead of satisfying bureaucratic needs, the aim of the documentation should be to help controllers and processors meet their obligations. Companies have many ways of documenting their data processing environment and no specific method should be mandated. Often such documentation exists through multiple means. A very detailed documentation procedure would remain an almost instantly outdated snapshot of a constantly changing reality characterized by complex data processing arrangements in a multiparty environment. Controllers cannot maintain detailed documentation of the IT architecture of the processors. Accordingly, processors should have an obligation to maintain such documentation of their processing. It should be left to the controllers and processors – in agreement with the lead DPA - based on the Accountability principle to determine which documentation is adequate and best suited for specific processing activities to comply with this Regulation and achieve the desired protection.

Amendment 41

Article 29 (Co-operation with the supervisory authority)	
Commission proposal	Proposed DIGITALEUROPE amendment
<p>1. The controller and the processor and, if any, the representative of the controller, shall co-operate, on request, with the supervisory authority in the performance of its duties, in particular by providing the information referred to in point (a) of Article 53(2) and by granting access as provided in point (b) of that paragraph.</p>	<p><i>1. The controller and the processor and, if any, the representative of the controller, shall co-operate, on request, with the supervisory authority in the performance of its duties, in particular by providing the information referred to in point (a) of Article 53(2) and by granting access as provided in point (b) of that paragraph. The controller and the processor and, if any, the controller's representative, shall make the documentation available, on the basis of a request outlining the reasons for requiring access to the documents, to the supervisory authority.</i></p>

Justification

The additional paragraph has been taken from Art. 28 (3) as it fits better in this Article that determines the relationship with the supervisory authority.

Amendment 42

Article 30 (Security of Processing)	
Commission proposal	Proposed DIGITALEUROPE amendment



<p>1. The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected, having regard to the state of the art and the costs of their implementation.</p> <p>2. The controller and the processor shall, following an evaluation of the risks, take the measures referred to in paragraph 1 to protect personal data against accidental or unlawful destruction or accidental loss and to prevent any unlawful forms of processing, in particular any unauthorised disclosure, dissemination or access, or alteration of personal data.</p> <p>3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the technical and organisational measures referred to in paragraphs 1 and 2, including the determinations of what constitutes the state of the art, for specific sectors and in specific data processing situations, in particular taking account of developments in technology and solutions for privacy by design and data protection by default, unless paragraph 4 applies.</p> <p>4. The Commission may adopt, where</p>	<p>1. The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected, having regard to the state of the art and the costs of their implementation.</p> <p>2. The controller and the processor shall, following an evaluation of the risks, take the measures referred to in paragraph 1 to protect personal data against accidental or unlawful destruction or accidental loss and to prevent any unlawful forms of processing, in particular any unauthorised disclosure, dissemination or access, or alteration of personal data.</p> <p>3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the technical and organisational measures referred to in paragraphs 1 and 2, including the determinations of what constitutes the state of the art, for specific sectors and in specific data processing situations, in particular taking account of developments in technology and solutions for privacy by design and data protection by default, unless paragraph 4 applies.</p> <p>3. (NEW) <i>The implementation by the controller and the processor of measures, as referred to in paragraphs 1 and 2, and the execution thereof which would require processing of certain data to increase network and information security, falls under Article 6 (1) f.</i></p> <p>4. The Commission may adopt, where necessary, implementing acts for</p>
--	--



<p>necessary, implementing acts for specifying the requirements laid down in paragraphs 1 and 2 to various situations, in particular to:</p> <p>(a) prevent any unauthorised access to personal data;</p> <p>(b) prevent any unauthorised disclosure, reading, copying, modification, erasure or removal of personal data;</p> <p>(c) ensure the verification of the lawfulness of processing operations.</p> <p>Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>	<p>specifying the requirements laid down in paragraphs 1 and 2 to various situations, in particular to:</p> <p>(a) prevent any unauthorised access to personal data;</p> <p>(b) prevent any unauthorised disclosure, reading, copying, modification, erasure or removal of personal data;</p> <p>(c) ensure the verification of the lawfulness of processing operations.</p> <p>Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>
--	--

Justification

Data controllers and processors should ensure that they have the right organizational measures in place to ensure security of processing and hence, enhancing overall network and information security. Such measures could, for example, be targeted at preventing unauthorized access to electronic communications networks, malicious code distribution and stopping of attacks and damage to computer and electronic communication systems. Where the implementation and execution of such measures would require the processing of data to the extent strictly necessary for purposes of ensuring network and information security by the data controller, processor or a third party, such processing should be deemed to be a legitimate interest for processing. Such processing would need to provide the necessary safeguards as outlined in the regulation where possible.

Amendment 43

Article 31 (Notification of a personal data breach to the supervisory authority)	
Commission proposal	Proposed DIGITALEUROPE amendment
<p>Notification of a personal data breach to the supervisory authority</p> <p>1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 24 hours after having become aware of it, notify</p>	<p>Notification of a personal data breach to the supervisory authority</p> <p>1. In the case of a <i>material</i> personal data breach, the controller shall without undue delay, after the establishment of the existence of a personal data breach, and, where feasible, not later than 24</p>

<p>the personal data breach to the supervisory authority. The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within 24 hours.</p> <p>2. Pursuant to point (f) of Article 26(2), the processor shall alert and inform the controller immediately after the establishment of a personal data breach.</p> <p>3. The notification referred to in paragraph 1 must at least:</p> <p>(a) describe the nature of the personal data breach including the categories and number of data subjects concerned and the categories and number of data records concerned;</p> <p>(b) communicate the identity and contact details of the data protection officer or other contact point where more information can be obtained;</p>	<p>hours after having become aware of notify the personal data breach to the supervisory authority. The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within 24 hours. The notification of a personal data breach to the supervisory authority shall not be required if the controller has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the personal data breach. Such technological protection measures may include those that render the data unintelligible, unusable or anonymised to any person who is not authorised to access it.</p> <p>2. Pursuant to point (f) of Article 26(2), the processor shall without undue delay after the establishment of the existence and nature of a personal data breach alert and inform the appropriate controller or controllers. controller immediately after the establishment of a personal data breach.</p> <p>3. To the extent feasible given the timing of the notification and the circumstances of the personal data breach, the notification referred to in paragraph 1 must at least:</p> <p>(a) describe the nature of the personal data breach including the categories and approximate number of data subjects concerned and the categories and number of data records concerned;</p> <p>(b) communicate the identity and contact details of the data protection officer or other contact point where more information can be obtained;</p>
--	---



<p>(c) recommend measures to mitigate the possible adverse effects of the personal data breach;</p> <p>(d) describe the consequences of the personal data breach;</p> <p>(e) describe the measures proposed or taken by the controller to address the personal data breach.</p> <p>4. The controller shall document any personal data breaches, comprising the facts surrounding the breach, its effects and the remedial action taken. This documentation must enable the supervisory authority to verify compliance with this Article. The documentation shall only include the information necessary for that purpose.</p> <p>5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for establishing the data breach referred to in paragraphs 1 and 2 and for the particular circumstances in which a controller and a processor is required to notify the personal data breach.</p> <p>6. The Commission may lay down the standard format of such notification to the supervisory authority, the procedures applicable to the notification requirement and the form and the modalities for the documentation referred to in paragraph 4, including the time limits for erasure of the information contained therein. Those implementing acts shall be adopted in</p>	<p>(c) <i>include any recommended measures for the data subject</i> to mitigate the possible adverse effects of the personal data breach;</p> <p>(d) describe the consequences of the personal data breach;</p> <p>(e) describe the measures <i>proposed or taken that have been or will be implemented</i> by the controller to address the personal data breach <i>and to mitigate its possible adverse effects</i>.</p> <p>4. The controller shall document <i>material any</i> personal data breaches, comprising the facts surrounding the breach, its effects and the remedial action taken. This documentation must <i>be sufficient to</i> enable the supervisory authority to verify compliance with this Article. The documentation shall only include the information necessary for that purpose.</p> <p>5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for establishing the data breach referred to in paragraphs 1 and 2 and for the particular circumstances in which a controller and a processor is required to notify the personal data breach.</p> <p>6. The Commission may lay down the standard format of such notification to the supervisory authority, <i>and</i> the procedures applicable to the <i>filing of reports. notification requirement and the form and the modalities for the documentation referred to in paragraph 4, including the time limits for erasure of the information contained therein.</i></p>
--	--

<p>accordance with the examination procedure referred to in Article 87(2).</p>	<p>Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>
--	--

Justification

Timely notification of only material breaches to DPAs will allow DPAs to prepare themselves, should affected individuals contact the DPA, as well as allow the DPA to better understand the nature and frequency of breaches. An expectation of notification within 24 hours is unreasonable. The timing of reporting material breaches to the DPA should be flexible so as not to interrupt the organization's efforts to deal with a breach event. Organizations are always at liberty to seek guidance from DPAs in the event of a data breach.

We also deleted the reference to art 26 (2) f to bring it in line with our proposed changes in that article.

Amendment 44

Article 32 (Communication of a personal data breach to the data subject)	
Commission proposal	Proposed DIGITALEUROPE amendment
<p>Communication of a personal data breach to the data subject</p> <ol style="list-style-type: none"> 1. When the personal data breach is likely to adversely affect the protection of the personal data or privacy of the data subject, the controller shall, after the notification referred to in Article 31, communicate the personal data breach to the data subject without undue delay. 2. The communication to the data subject referred to in paragraph 1 shall describe the nature of the personal data breach and contain at least the information and the recommendations provided for in points (b) and (c) of Article 31(3). 3. The communication of a personal data 	<p>Communication of a personal data breach to the data subject</p> <ol style="list-style-type: none"> 1. When the personal data breach is likely to adversely affect the protection of the personal data or privacy of the data subject, the controller shall, after the notification referred to in Article 31, communicate the personal data breach to the data subject without undue delay. 2. The communication to the data subject referred to in paragraph 1 shall describe the nature of the personal data breach and contain at least the information and the recommendations provided for in points (b) and (c) of Article 31(3). 3. The communication of a personal data

<p>breach to the data subject shall not be required if the controller demonstrates to the satisfaction of the supervisory authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the personal data breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it.</p> <p>4. Without prejudice to the controller's obligation to communicate the personal data breach to the data subject, if the controller has not already communicated the personal data breach to the data subject of the personal data breach, the supervisory authority, having considered the likely adverse effects of the breach, may require it to do so.</p> <p>5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements as to the circumstances in which a personal data breach is likely to adversely affect the personal data referred to in paragraph 1.</p> <p>6. The Commission may lay down the format of the communication notification to the data subject referred to in paragraph 1 and the procedures applicable to that communication. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>	<p>breach to the data subject shall not be required if the controller demonstrates to the satisfaction of the supervisory authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the personal data breach. Such technological protection measures shall may include those that render the data unintelligible, unusable or anonymised to any person who is not authorised to access it.</p> <p>4. Without prejudice to the controller's obligation to communicate the personal data breach to the data subject, if the controller has not already communicated the personal data breach to the data subject of the personal data breach, the supervisory authority, having considered the likely adverse effects of the breach, may require it to do so.</p> <p>5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements as to the circumstances in which a personal data breach is likely to adversely affect the personal data referred to in paragraph 1.</p> <p>6. The Commission may lay down the format of the communication notification to the data subject referred to in paragraph 1 and the procedures applicable to that communication. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>
--	--

Justification

Data breach notification is an important element in any mitigation strategy. Timely notification to individuals in cases of material breaches can help them prepare and take steps to protect themselves and mitigate against potential future harm resulting from the breach. Organizations are in the best position to determine whether, when and how to notify their customers when a data breach occurs and so flexibility around timing and method of notification is required to reflect different businesses and operations and the types of data breaches that may occur. The organizations will need to keep track of material breaches as part of the overall obligation of organizational measures, so this can be demonstrated to the supervisory authorities upon request.

Amendment 45

NEW Article (after Art 32)	
(Communication of a personal data breach to other organisations)	
Commission proposal	Proposed DIGITALEUROPE amendment
	<i>A controller that communicates a personal data breach to a data subject pursuant to Article 32 may notify another organisation, a government institution or a part of a government institution of the personal data breach if that organisation, government institution or part may be able to reduce the risk of the harm that could result from it or mitigate that harm. Such notifications can be done without informing the data subject if the disclosure is made solely for the purposes of reducing the risk of the harm to the data subject that could result from the breach or mitigating that harm.</i>

Justification

In many cases other organisations or government institutions are in a position to be able to assist in mitigating harm that may result to a data subject following a personal data breach if they are made aware of the breach and the circumstances surrounding the breach. For example, in certain cases a flag may be added to a consumer’s account or a request may be sent to log in and change one’s password.

Amendment 46

Article 33 (Data protection impact assessment)	
Commission proposal	Proposed DIGITALEUROPE amendment
<p>1. Where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller or the processor acting on the controller's behalf shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.</p> <p>2. The following processing operations in particular present specific risks referred to in paragraph 1:</p> <p>(a) a systematic and extensive evaluation of personal aspects relating to a natural person or for analysing or predicting in particular the natural person's economic situation, location, health, personal preferences, reliability or behaviour, which is based on automated processing and on which measures are based that produce legal effects concerning the individual or significantly affect the individual;</p> <p>(b) information on sex life, health, race and ethnic origin or for the provision of health care, epidemiological researches, or surveys of mental or infectious diseases, where the data are processed for taking measures or decisions regarding specific individuals on a large scale;</p> <p>(c) monitoring publicly accessible areas, especially when using optic-electronic devices (video surveillance) on a large scale;</p>	<p>1. Where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller or the processor acting on the controller's behalf shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.</p> <p>2. The following processing operations in particular present specific risks referred to in paragraph 1:</p> <p>(a) a systematic and extensive evaluation of personal aspects relating to a natural person or for analysing or predicting in particular the natural person's economic situation, location, health, personal preferences, reliability or behavior, which is based on automated processing and on which measures are based that produce legal effects concerning the individual or significantly that gravely and adversely affect the individual's fundamental rights;</p> <p>(b) information on sex life, health, race and ethnic origin or for the provision of health care, epidemiological researches, or surveys of mental or infectious diseases, where the data are processed for taking measures or decisions regarding specific individuals on a large scale;</p> <p>(c) monitoring publicly accessible areas, especially when using optic-electronic devices (video surveillance) on a large scale;</p>



<p>(d) personal data in large scale filing systems on children, genetic data or biometric data;</p> <p>(e) other processing operations for which the consultation of the supervisory authority is required pursuant to point (b) of Article 34(2).</p> <p>3. The assessment shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned.</p> <p>4. The controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations.</p> <p>5. Where the controller is a public authority or body and where the processing results from a legal obligation pursuant to point (c) of Article 6(1) providing for rules and procedures pertaining to the processing operations and regulated by Union law, paragraphs 1 to 4 shall not apply, unless Member States deem it necessary to carry out such assessment prior to the processing activities.</p>	<p>scale;</p> <p>(d) personal data in large scale filing systems on children, genetic data or biometric data;</p> <p>(e) other processing operations for which the consultation of the supervisory authority is required pursuant to point (b) of Article 34(2).</p> <p>3. The assessment shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned.</p> <p>4. The controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations.</p> <p>5. Where the controller is a public authority or body and where the processing results from a legal obligation pursuant to point (c) of Article 6(1) providing for rules and procedures pertaining to the processing operations and regulated by Union law, paragraphs 1 to 4 shall not apply, unless Member States deem it necessary to carry out such assessment prior to the processing activities.</p>
--	---

<p>6. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the processing operations likely to present specific risks referred to in paragraphs 1 and 2 and the requirements for the assessment referred to in paragraph 3, including conditions for scalability, verification and auditability. In doing so, the Commission shall consider specific measures for micro, small and medium-sized enterprises.</p> <p>7. The Commission may specify standards and procedures for carrying out and verifying and auditing the assessment referred to in paragraph 3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>	<p>6. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the processing operations likely to present specific risks referred to in paragraphs 1 and 2 and the requirements for the assessment referred to in paragraph 3, including conditions for scalability, verification and auditability. In doing so, the Commission shall consider specific measures for micro, small and medium-sized enterprises.</p> <p>7. The Commission may specify standards and procedures for carrying out and verifying and auditing the assessment referred to in paragraph 3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>
--	--

Justification

The DPIA obligation is problematic as it is currently proposed. The approach to single out types of processing, brand them as risky, and treat them differently from supposedly non-risky processing is dangerous and will not produce the desired results. We believe all processing of personal data should be planned appropriately prior to commencing the processing to ensure compliance with the Regulation. Organizations should be held accountable for applying risk identification and mitigation planning methodologies that are appropriate for the processing at hand. No specific type of DPIA should be mandated nor should the assessment obligation be reserved to any specific type of processing.

DPIA's are one method, among others, to achieve the ultimate objective of ensuring that risks to privacy have been identified and proper mitigations planned in a timely fashion. Today, depending on the size of the organization, tens, hundreds or even thousands of DPIAs of various kinds are made annually to identify risks and to plan mitigations thereof. Different types of assessments are needed to properly assess different activities. Organizations are constantly searching for best methodologies for such risk identification and mitigation planning. Such methodologies constantly evolve, through efforts by practitioners, academia and various standardization bodies, and such incremental improvement should not be hindered by mandating any specific type of assessment.

The proposal suggests that a DPIA would be needed in specific risky situations. Some of the activities listed in article 33 are standard processing for which such an assessment should not need to be submitted to a DPA for prior authorization or consultation. In the current online reality, processing of location data, user segmentation and other such practices, for example, described as potentially risky

in the proposal, are the norm rather than exception and do not necessarily pose any significant risk to individuals. Therefore they should be removed from the list of risky processing and, in accordance with our belief that all processing warrants planning to ensure compliance, we propose that the reference to risky processing should only relate to prior consultation obligations.

Given the fact that, according to art. 14, data subjects need to be informed of the data processing, an obligation to consult data subjects as part of the assessment appears misplaced and unnecessary. It would also likely result in compromising important trade secrets. To ensure appropriate protection for personal data when data subjects cannot be informed of the processing, we propose a limited prior consultation obligation to govern such instances (see below for our comments and proposal for prior consultation).

Amendment 47

Article 34 (Prior authorisation and prior consultation)	
Commission proposal	Proposed DIGITALEUROPE amendment
<p>1. The controller or the processor as the case may be shall obtain an authorisation from the supervisory authority prior to the processing of personal data, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where a controller or processor adopts contractual clauses as provided for in point (d) of Article 42(2) or does not provide for the appropriate safeguards in a legally binding instrument as referred to in Article 42(5) for the transfer of personal data to a third country or an international organisation.</p> <p>2. The controller or processor acting on the controller's behalf shall consult the supervisory authority prior to the processing of personal data in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where:</p>	<p>1. The controller or the processor as the case may be shall obtain an authorisation from the supervisory authority prior to the processing of personal data, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where a controller or processor adopts contractual clauses as provided for in point (d) of Article 42(2) or does not provide for the appropriate safeguards in a legally binding instrument as referred to in Article 42(5) for the transfer of personal data to a third country or an international organisation.</p> <p>2. The controller or processor acting on the controller's behalf shall consult the supervisory authority prior to the processing of personal data in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where:</p>

(a) a data protection impact assessment as provided for in Article 33 indicates that processing operations are by virtue of their nature, their scope or their purposes, likely to present a high degree of specific risks; or

(b) the supervisory authority deems it necessary to carry out a prior consultation on processing operations that are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope and/or their purposes, and specified according to paragraph 4.

3. Where the supervisory authority is of the opinion that the intended processing does not comply with this Regulation, in particular where risks are insufficiently identified or mitigated, it shall prohibit the intended processing and make appropriate proposals to remedy such non-compliance.

4. The supervisory authority shall establish and make public a list of the processing operations which are subject to prior consultation pursuant to point (b) of paragraph 2. The supervisory authority shall communicate those lists to the European Data Protection Board.

5. Where the list provided for in paragraph 4 involves processing activities which are related to the offering of goods or services to data subjects in several Member States, or to the monitoring of their behaviour, or may substantially affect the free movement of personal data within the Union, the

~~(a) a data protection impact assessment as provided for in Article 33 indicates that processing operations are by virtue of their nature, their scope or their purposes, likely to present a high degree of specific risks; or~~

~~(b) the supervisory authority deems it necessary to carry out a prior consultation on processing operations that are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope and/or their purposes, and specified according to paragraph 4.~~

3. Where the supervisory authority is of the opinion that the intended processing does not comply with this Regulation, in particular where risks are insufficiently identified or mitigated, it shall prohibit the intended processing and make appropriate proposals to remedy such non-compliance. **Such a decision shall be subject to appeal in a competent court and it may not be enforceable while being appealed unless the processing results to immediate serious harm suffered by data subjects.**

~~4. The supervisory authority shall establish and make public a list of the processing operations which are subject to prior consultation pursuant to point (b) of paragraph 2. The supervisory authority shall communicate those lists to the European Data Protection Board.~~

~~5. Where the list provided for in paragraph 4 involves processing activities which are related to the offering of goods or services to data subjects in several Member States, or to the monitoring of their behaviour, or may substantially affect the free movement of personal data~~



supervisory authority shall apply the consistency mechanism referred to in Article 57 prior to the adoption of the list.

6. The controller or processor shall provide the supervisory authority with the data protection impact assessment provided for in Article 33 and, on request, with any other information to allow the supervisory authority to make an assessment of the compliance of the processing and in particular of the risks for the protection of personal data of the data subject and of the related safeguards.

7. Member States shall consult the supervisory authority in the preparation of a legislative measure to be adopted by the national parliament or of a measure based on such a legislative measure, which defines the nature of the processing, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects.

8. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for determining the high degree of specific risk referred to in point (a) of paragraph 2.

9. The Commission may set out standard forms and procedures for prior authorisations and consultations referred to in paragraphs 1 and 2, and standard forms and procedures for informing the supervisory authorities pursuant to paragraph 6. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

~~within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57 prior to the adoption of the list.~~

~~6. The controller or processor shall provide the supervisory authority with the data protection impact assessment provided for in Article 33 and, on request, with any other information to allow the supervisory authority to make an assessment of the compliance of the processing and in particular of the risks for the protection of personal data of the data subject and of the related safeguards.~~

7. Member States shall consult the supervisory authority in the preparation of a legislative measure to be adopted by the national parliament or of a measure based on such a legislative measure, which defines the nature of the processing, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects.

~~8. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for determining the high degree of specific risk referred to in point (a) of paragraph 2.~~

9. The Commission may set out **non mandatory** standard forms and procedures for prior authorisations **and consultations** referred to in paragraphs 1 **and 2, and standard forms and procedures for informing the supervisory authorities pursuant to paragraph 6.** Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Justification

A modern data protection law should not require mandatory ex-ante consultation of the authorities by data controllers. The role of data protection authorities should be to focus ‘ex-post’ on the consistent enforcement of the rules. See also the recommendation of the Article 29 Working Party in its Opinion 3/2010 paragraph 63.

Amendment 48

Article 35 (Designation of Data Protection Officer)	
Commission proposal	Proposed DIGITALEUROPE amendment
<p>1. The controller and the processor shall designate a data protection officer in any case where:</p> <p>(a) the processing is carried out by a public authority or body; or</p> <p>(b) the processing is carried out by an enterprise employing 250 persons or more; or</p> <p>(c) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects.</p> <p>2. In the case referred to in point (b) of paragraph 1, a group of undertakings may appoint a single data protection officer.</p> <p>3. Where the controller or the processor is a public authority or body, the data protection officer may be designated for several of its entities, taking account of the organisational structure of the public authority or body.</p> <p>4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may</p>	<p>1. The controller and the processor shall designate a <i>data protection organization or</i> data protection officer in any case where:</p> <p>(a) the processing is carried out by a public authority or body; or</p> <p>(b) the processing is carried out by an enterprise employing 250 persons or more; or</p> <p>(c) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects.</p> <p>2. In the case referred to in point (b) of paragraph 1, a group of undertakings may appoint a single data protection officer.</p> <p>3. Where the controller or the processor is a public authority or body, the data protection <i>organization or data protection</i> officer may be designated for several of its entities, taking account of the organisational structure of the public authority or body.</p> <p>4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies</p>

<p>designate a data protection officer.</p> <p>5. The controller or processor shall designate the data protection officer on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and ability to fulfil the tasks referred to in Article 37. The necessary level of expert knowledge shall be determined in particular according to the data processing carried out and the protection required for the personal data processed by the controller or the processor.</p> <p>6. The controller or the processor shall ensure that any other professional duties of the data protection officer are compatible with the person's tasks and duties as data protection officer and do not result in a conflict of interests.</p> <p>7. The controller or the processor shall designate a data protection officer for a period of at least two years. The data protection officer may be reappointed for further terms. During their term of office, the data protection officer may only be dismissed, if the data protection officer no longer fulfils the conditions required for the performance of their duties.</p> <p>8. The data protection officer may be employed by the controller or processor, or fulfil his or her tasks on the basis of a service contract.</p> <p>9. The controller or the processor shall communicate the name and contact details</p>	<p>representing categories of controllers or processors may designate a data protection officer.</p> <p>5. The controller or processor shall designate the data protection organization or data protection officer on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and ability to fulfil the tasks referred to in Article 37. The necessary level of expert knowledge shall be determined in particular according to the data processing carried out and the protection required for the personal data processed by the controller or the processor.</p> <p>6. The controller or the processor shall ensure that any other professional duties of the data protection organization or data protection officer are compatible with the person's tasks and duties as data protection officer and do not result in a conflict of interests.</p> <p>7. The controller or the processor shall designate a data protection officer for a period of at least two years. The data protection officer may be reappointed for further terms. During their term of office, the data protection officer may only be dismissed, if the data protection officer no longer fulfils the conditions required for the performance of their duties.</p> <p>8. The data protection officer may be employed by the controller or processor, or fulfil his or her tasks on the basis of a service contract.</p> <p>9. The controller or the processor shall communicate the name and contact</p>
--	--

<p>of the data protection officer to the supervisory authority and to the public.</p> <p>10. Data subjects shall have the right to contact the data protection officer on all issues related to the processing of the data subject's data and to request exercising the rights under this Regulation.</p> <p>11. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the core activities of the controller or the processor referred to in point (c) of paragraph 1 and the criteria for the professional qualities of the data protection officer referred to in paragraph 5.</p>	<p>details of the data protection organization or data protection officer to the supervisory authority and to the public.</p> <p>10. Data subjects shall have the right to contact the data protection organization officer on all issues related to the processing of the data subject's data and to request exercising the rights under this Regulation.</p> <p>11. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the core activities of the controller or the processor referred to in point (c) of paragraph 1 and the criteria for the professional qualities of the data protection officer referred to in paragraph 5.</p>
--	---

Justification

There are clear benefits in having in place roles and responsibilities to ensure compliance. The proposal, however, appears overly detailed in describing the tasks of a data protection officer and it also fails to recognize that also other organizational structures may result in equally or even more effective data protection. Here again it will be much more effective to introduce the Accountability principle into the Regulation instead, as proposed by Amendment 30. In larger organizations it is not reasonable to expect that a single data protection officer would be involved in all issues relating to the protection of personal data. Often in larger organizations the data protection roles and responsibilities, ranging from requirements setting, implementation, training and awareness, incident response and oversight and reporting are rightfully decentralized across the organizations, while being bound together by a comprehensive data protection program. Without senior management support and a systematic approach to compliance management it is unlikely that such a mandatory advisory and monitoring role envisaged by the proposal will lead to desired outcomes.

Some requirements for data protection officers in the proposal may even be counterproductive. For example, creating a two year protected term in form of a job guarantee for a data protection officer creates incentives to outsource the role to an external service provider to balance the risk of an unsuccessful recruitment. As in-depth knowledge of the organization is a prerequisite for successful data protection, this could hardly be seen as a desired outcome in all cases. Organizational independence should also include flexibility in organizing the data protection resources in a way that provides sufficient objectivity and independence of oversight and escalation. It seems more likely that a senior executive with accountability for effective organizational measures and who is a member of

organizations senior management leads to more long-term impact on the organization than a data protection officer with more of a procedural role.

Defining the obligation to appoint a data protection officer based on the number of employees seems arbitrary. It would make more sense to base it on the nature of data processing or number of data subjects involved.

Amendment 49

Article 36 (Position of the data protection officer)	
Commission proposal	Proposed DIGITALEUROPE amendment
<p>1. The controller or the processor shall ensure that the data protection officer is properly and in a timely manner involved in all issues which relate to the protection of personal data.</p> <p>2. The controller or processor shall ensure that the data protection officer performs the duties and tasks independently and does not receive any instructions as regards the exercise of the function. The data protection officer shall directly report to the management of the controller or the processor.</p> <p>3. The controller or the processor shall support the data protection officer in performing the tasks and shall provide staff, premises, equipment and any other resources necessary to carry out the duties and tasks referred to in Article 37.</p>	<p>1. The controller or the processor shall ensure that the data protection organization or data protection officer is properly and in a timely manner involved in all significant issues which relate to the protection of personal data.</p> <p>2. The controller or processor shall ensure that t The data protection organization or data protection officer shall performs the his or her duties and tasks independently and does not receive any instructions as regards the exercise of the function. The data protection officer shall directly report to the management of the controller or the processor.</p> <p>3. The controller or the processor shall support the data protection organization or data protection officer in performing the tasks and shall provide staff, premises, equipment and any other resources necessary to carry out the duties and tasks referred to in Article 37.</p>

Justification

It is not possible for a company to ensure that someone act “independently” just as much as it is impossible for a company to ensure that someone act honestly. Instead, this should be an obligation on the DPO.

Amendment 50

Article 37 (Tasks of the data protection organization or data protection officer)	
Commission proposal	Proposed DIGITALEUROPE amendment
<p>1. The controller or the processor shall entrust the data protection officer at least with the following tasks:</p> <p>a) to inform and advise the controller or the processor of their obligations pursuant to this Regulation and to document this activity and the responses received;</p> <p>b) to monitor the implementation and application of the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, the training of staff involved in the processing operations, and the related audits;</p> <p>c) to monitor the implementation and application of this Regulation, in particular as to the requirements related to data protection by design, data protection by default and data security and to the information of data subjects and their requests in exercising their rights under this Regulation;</p> <p>(d) to ensure that the documentation referred to in Article 28 is maintained;</p> <p>(e) to monitor the documentation, notification and communication of</p>	<p>1. The controller or the processor shall entrust the <i>data protection organization or</i> data protection officer at least with the following tasks:</p> <p>a) to inform and advise the controller or the processor of their obligations pursuant to this Regulation and to document this activity and the responses received;</p> <p>b) to <i>develop, support and</i> monitor the implementation <i>of measures referred to in Article 22, and application of the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, the training of staff involved in the processing operations, and the related audits;</i></p> <p>c) to monitor the implementation and application <i>compliance with the Regulation of this, in particular as to the requirements related to data protection by design, data protection by default and data security and to the information of data subjects and their requests in exercising their rights under this Regulation;</i></p> <p>(d) to ensure that the documentation referred to in Article 28 is maintained;</p> <p>(e) to monitor the documentation, notification and communication of</p>

<p>personal data breaches pursuant to Articles 31 and 32;</p> <p>(f) to monitor the performance of the data protection impact assessment by the controller or processor and the application for prior authorisation or prior consultation, if required pursuant Articles 33 and 34;</p> <p>(g) to monitor the response to requests from the supervisory authority, and, within the sphere of the data protection officer's competence, co-operating with the supervisory authority at the latter's request or on the data protection officer's own initiative;</p> <p>(h) to act as the contact point for the supervisory authority on issues related to the processing and consult with the supervisory authority, if appropriate, on his/her own initiative.</p> <p>2. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for tasks, certification, status, powers and resources of the data protection officer referred to in paragraph 1.</p>	<p>personal data breaches pursuant to Articles 31 and 32;</p> <p>(f) to monitor the performance of the data protection impact assessment by the controller or processor and the application for prior authorisation or prior consultation, if required pursuant Articles 33 and 34;</p> <p>(g) to monitor the response to requests from the supervisory authority, and, within the sphere of the data protection officer's competence, co-operating with the supervisory authority at the latter's request or on the data protection officer's own initiative;</p> <p>(h) to act as the contact point for the supervisory authority on issues related to the processing and consult with the supervisory authority, if appropriate, on his/her own initiative.</p> <p>2. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for tasks, certification, status, powers and resources of the data protection officer referred to in paragraph 1.</p>
--	--

Justification

In today's organizational reality a lot of everyday advice is given over the phone, in meetings, through email or instant messaging. Having an obligation to systematically document one's everyday interaction with supported business operations would generate a massive and disproportionate administrative burden. However, actual privacy impact assessments and similarly structured privacy reviews need to be documented.

It should be up to the organization to define how they decide to organize their data protection organization and business in general. The proposed regulation appears to envision a

centralized organization with full and sole control over its resources and organization, which is just one approach to reach compliance.

Amendment 51

Article 38 (NEW) (Codes of conduct)	
Commission proposal	Proposed DIGITALEUROPE amendment
3. Associations and other bodies representing categories of controllers in several Member States may submit draft codes of conduct and amendments or extensions to existing codes of conduct to the Commission.	3. Associations and other bodies representing categories of controllers <i>or processors</i> in several Member States may submit draft codes of conduct and amendments or extensions to existing codes of conduct to the Commission.

Justification

Article 38.2 of the draft proposal states that Associations and other bodies in one Member State represent both controllers and processors while submitting draft codes of conduct, whereas art 38.3 states that Associations and other bodies in several Member States represent only controllers. We believe that both controller and processor should be included.

Amendment 52

Article 39 (Certification)	
Commission proposal	Proposed DIGITALEUROPE amendment
1. The Member States and the Commission shall encourage, in particular at European level, the establishment of data protection certification mechanisms and of data protection seals and marks, allowing data subjects to quickly assess the level of data protection provided by controllers and processors. The data protection certifications mechanisms shall contribute to the proper application of this Regulation, taking account of the specific features of the various sectors and different processing	1. The Member States and the Commission shall encourage, in particular at European level, the <i>voluntary</i> establishment of data protection certification mechanisms and of data protection seals and marks, <i>which shall be capable of global application and affordable. These mechanisms shall also be technology neutral and will be</i> allowing data subjects to quickly assess the level of data protection provided by controllers and processors. <i>Such mechanisms shall: The data</i>



operations.

~~protection certifications mechanisms shall contribute to the proper application of this Regulation, taking account of the specific features of the various sectors and different processing operations.~~

- a) *contribute, amongst other means, to the proper application of this Regulation, taking account of the specific features of the various sectors and different processing operations*
- b) *take due account of the nature and sensitivity of the personal data being processed*
- c) *take due account of existing security measures and regulations in the area of public safety and security*
- d) *follow the principles of technology, service and business model neutrality*
- e) *be elaborated in consultation with the supervisory authorities*
- f) *be based on industry-led efforts*
- g) *take due account of international developments*
- h) *In implementing the provisions of this Regulation, it shall be ensured that no mandatory requirements for specific technical features are imposed on products and services, including terminal or other electronic communications equipment, which could impede the placing of equipment on the market and the free circulation of such equipment in and between Member States.*
- i) *Where required, measures may be adopted to ensure that terminal equipment is constructed in a way that is*



<p>2. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the data protection certification mechanisms referred to in paragraph 1, including conditions for granting and withdrawal, and requirements for recognition within the Union and in third countries.</p> <p>3. The Commission may lay down technical standards for certification mechanisms and data protection seals and marks and mechanisms to promote and recognize certification mechanisms and data protection seals and marks. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).</p>	<p><i>compatible with the right of users to protect and control the use of their personal data, in accordance with Directive 1999/5/EC and Council Decision 87/95/EEC of 22 December 1986 on standardisation in the field of information technology and communications and consistent with international industry-led standardisation efforts.</i></p> <p><i>Independent third parties or industry self regulatory bodies shall be the facilitators of such voluntary data protection certification mechanisms and data protection seals and marks, with easy access for citizens being a top priority. The European Data Protection Board shall serve as an enforcement agent.</i></p> <p>2. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the data protection certification mechanisms referred to in paragraph 1, including conditions for granting and withdrawal, and requirements for recognition within the Union and in third countries, <i>provided such measures are technology neutral.</i></p> <p>3. The Commission may lay down technical standards for certification mechanisms and data protection seals and marks and mechanisms to promote and recognize certification mechanisms and data protection seals and marks. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).</p>
---	--

Justification

Certification mechanisms and data protection seals and marks developed and managed by industry should be favoured, provided they remain voluntary and affordable, particularly for SMEs. Such certification mechanisms should be open to companies both inside and outside the EEA, in order to facilitate international data flows, and be elaborated in consultation with the relevant stakeholders. They should enable competition, be industry-driven and favour innovative solutions for consumers. Indeed, industry is able to adapt to new market realities at a faster pace than government, and government does not have the same competitive incentive to enforce proper use of certifications (e.g., icons or seals on web pages) as industry does. In the long term, a certification mechanism developed and managed by industry, with regulators having backstop regulatory authority, would help to reduce compliance burdens on operators and foster competitiveness.

Amendment 53

Article 42 (Transfers by way of appropriate safeguards)	
Commission proposal	Proposed DIGITALEUROPE amendment
<p>1. Where the Commission has taken no decision pursuant to Article 41, a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has adduced appropriate safeguards with respect to the protection of personal data in a legally binding instrument.</p> <p>2. The appropriate safeguards referred to in paragraph 1 shall be provided for, in particular, by:</p> <p>(a) binding corporate rules in accordance with Article 43; or</p> <p>(b) standard data protection clauses adopted by the Commission. Those implementing</p>	<p>1. Where the Commission has taken no decision pursuant to Article 41, <i>or decides that a third country, or a territory or a processing sector within that third country, or an international organisation does not ensure an adequate level of protection in accordance with Article 41(5)</i>, a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has adduced appropriate safeguards with respect to the protection of personal data in a legally binding instrument.</p> <p>2. The appropriate safeguards referred to in paragraph 1 shall be provided for, in particular, by:</p> <p>(a) binding corporate rules in accordance with Article 43; or</p> <p>(b) standard data protection clauses adopted by the Commission. Those</p>



<p>acts shall be adopted in accordance with the examination procedure referred to in Article 87(2); or</p> <p>(c) standard data protection clauses adopted by a supervisory authority in accordance with the consistency mechanism referred to in Article 57 when declared generally valid by the Commission pursuant to point (b) of Article 62(1); or</p> <p>(d) contractual clauses between the controller or processor and the recipient of the data authorised by a supervisory authority in accordance with paragraph 4.</p> <p>3. A transfer based on standard data protection clauses or binding corporate rules as referred to in points (a), (b) or (c) of paragraph 2 shall not require any further authorisation.</p> <p>4. Where a transfer is based on contractual clauses as referred to in point (d) of paragraph 2 of this Article the controller or processor shall obtain prior authorisation of the contractual clauses according to point (a) of Article 34(1) from the supervisory authority. If the transfer is related to processing activities which concern data subjects in another Member State or other Member States, or substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57.</p>	<p>implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2); or</p> <p>(c) standard data protection clauses adopted by a supervisory authority in accordance with the consistency mechanism referred to in Article 57 when declared generally valid by the Commission pursuant to point (b) of Article 62(1); or</p> <p>(d) contractual clauses between the controller or processor and the recipient of the data authorised by a supervisory authority in accordance with paragraph 4.</p> <p>3. A transfer based on standard data protection clauses or binding corporate rules as referred to in points (a), (b) or (c) of paragraph 2 shall not require any further authorisation.</p> <p>4. Where a transfer is based on contractual clauses as referred to in point (d) of paragraph 2 of this Article the controller or processor shall obtain prior authorisation of the contractual clauses according to point (a) of Article 34(1) from the supervisory authority. If the transfer is related to processing activities which concern data subjects in another Member State or other Member States, or substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57.</p> <p><i>(a) A controller or processor may choose to base transfers on standard data protection clauses as referred to in points (b) and (c) of paragraph 2 of this Article, and to offer in addition to these standard clauses supplemental, legally binding commitments that apply to transferred data. In such cases, these additional commitments shall be subject to prior consultation with the competent</i></p>
---	--

<p>5. Where the appropriate safeguards with respect to the protection of personal data are not provided for in a legally binding instrument, the controller or processor shall obtain prior authorisation for the transfer, or a set of transfers, or for provisions to be inserted into administrative arrangements providing the basis for such transfer. Such authorisation by the supervisory authority shall be in accordance with point (a) of Article 34(1). If the transfer is related to processing activities which concern data subjects in another Member State or other Member States, or substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57. Authorisations by a supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid, until amended, replaced or repealed by that supervisory authority.</p>	<p><i>supervisory authority and shall supplement and not contradict, directly or indirectly, the standard clauses. Member States, supervisory authorities and the Commission shall encourage the use of supplemental and legally binding commitments by offering a data protection seal, mark or mechanism, adopted pursuant to Article 39, to controllers and processors who adopt these heightened safeguards.</i></p> <p>5. Where the appropriate safeguards with respect to the protection of personal data are not provided for in a legally binding instrument, the controller or processor shall obtain prior authorisation for the transfer, or a set of transfers, or for provisions to be inserted into administrative arrangements providing the basis for such transfer. Such authorisation by the supervisory authority shall be in accordance with point (a) of Article 34(1). If the transfer is related to processing activities which concern data subjects in another Member State or other Member States, or substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57. Authorisations by a supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid, until amended, replaced or repealed by that supervisory authority.</p>
--	---

Justification

The wording of the draft proposal could rule out all forms of data transfers to the country, territory, sector or international organization considered as not offering an adequate level of protection regardless of whether other appropriate safeguards are put in place. Article 41(6) of the draft proposal indeed provides that the prohibition to transfer personal data in case of

inadequacy decided by the Commission is “without prejudice to Articles 42 to 44,” while Articles 42(1) and 44(1) mention that they apply only if the Commission has not taken any decision on adequacy.

With the increasing globalisation of business and the evolution of computing models like the cloud, cross-border flows of personal data have become routine. In this environment, it is critical that controllers and processors apply strong safeguards to personal data regardless of where that data is located. Users will only have confidence in cloud computing if they know that their data is safe in the cloud. Helpfully, the Regulation already requires that transfers of personal data to third countries may only be carried out in full compliance with the Regulation. This is an important principle. But controllers and processors should be incentivised to go beyond the Regulation in some cases. Indeed, controllers and processors will often have direct and practical experience that demonstrates that additional safeguards -- i.e., safeguards that supplement those in the Regulation -- may be appropriate in relation to the personal data they are transferring. The Regulation should encourage these controllers and processors to offer supplemental safeguards where these are appropriate. The amendment proposed above would help to achieve this by allowing controllers and processors that base data transfers on standard data protection clauses under Articles 42(2)(b) and 42(2)(c) of the Regulation to also offer additional protections to customers in the form of legally binding contractual commitments (e.g., data processing agreements) that expand on the standard clauses. In this way, controllers and processors can offer additional protections that reflect the ways in which they will be processing data and particular safeguards appropriate to that processing. Of course, these supplemental commitments should not contradict the standard clauses.

Amendment 54

Article 43 (Transfers by way of binding corporate rules)	
Commission proposal	<i>Proposed DIGITALEUROPE amendment</i>



<p>1. A supervisory authority shall in accordance with the consistency mechanism set out in Article 58 approve binding corporate rules, provided that they:</p> <p>(a) are legally binding and apply to and are enforced by every member within the controller's or processor's group of undertakings, and include their employees;</p> <p>(b) expressly confer enforceable rights on data subjects;</p> <p>(c) fulfil the requirements laid down in paragraph 2.</p> <p>2. The binding corporate rules shall at least specify:</p> <p>(a) the structure and contact details of the group of undertakings and its members;</p> <p>(b) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;</p> <p>(c) their legally binding nature, both internally and externally;</p> <p>(d) the general data protection principles, in particular purpose limitation, data quality, legal basis for the processing, processing of sensitive personal data; measures to ensure data security; and the requirements for onward transfers to organisations which are not bound by the policies;</p> <p>(e) the rights of data subjects and the means to exercise these rights, including the right</p>	<p>1. A supervisory authority shall in accordance with the consistency mechanism set out in Article 58 approve binding corporate rules, provided that they:</p> <p>(a) are legally binding and apply to and are enforced by every member within the controller's or processor's group of undertakings and their external subcontractors, and include their employees;</p> <p>(b) expressly confer enforceable rights on data subjects;</p> <p>(c) fulfil the requirements laid down in paragraph 2.</p> <p>2. The binding corporate rules shall at least specify:</p> <p>(a) the structure and contact details of the group of undertakings and its members, and their external subcontractors;</p> <p>(b) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;</p> <p>(c) their legally binding nature, both internally and externally;</p> <p>(d) the general data protection principles, in particular purpose limitation, data quality, legal basis for the processing, processing of sensitive personal data; measures to ensure data security; and the requirements for onward transfers to organisations which are not bound by the policies;</p> <p>(e) the rights of data subjects and the means to exercise these rights, including the right</p>
--	---

<p>not to be subject to a measure based on profiling in accordance with Article 20, the right to lodge a complaint before the competent supervisory authority and before the competent courts of the Member States in accordance with Article 75, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;</p> <p>(f) the acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member of the group of undertakings not established in the Union; the controller or the processor may only be exempted from this liability, in whole or in part, if he proves that that member is not responsible for the event giving rise to the damage;</p> <p>(g) how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this paragraph is provided to the data subjects in accordance with Article 11;</p> <p>(h) the tasks of the data protection officer designated in accordance with Article</p> <p>35, including monitoring within the group of undertakings the compliance with the binding corporate rules, as well as monitoring the training and complaint handling;</p> <p>(i) the mechanisms within the group of undertakings aiming at ensuring the verification of compliance with the binding corporate rules;</p> <p>(j) the mechanisms for reporting and recording changes to the policies and reporting these changes to the supervisory authority;</p> <p>(k) the co-operation mechanism with the supervisory authority to ensure compliance by any member of the group</p>	<p>not to be subject to a measure based on profiling in accordance with Article 20, the right to lodge a complaint before the competent supervisory authority and before the competent courts of the Member States in accordance with Article 75, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;</p> <p>(f) the acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member of the group of undertakings not established in the Union; the controller or the processor may only be exempted from this liability, in whole or in part, if he proves that that member is not responsible for the event giving rise to the damage;</p> <p>(g) how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this paragraph is provided to the data subjects in accordance with Article 11;</p> <p>(h) the tasks of the data protection officer designated in accordance with Article</p> <p>35, including monitoring within the group of undertakings the compliance with the binding corporate rules, as well as monitoring the training and complaint handling;</p> <p>(i) the mechanisms within the group of undertakings aiming at ensuring the verification of compliance with the binding corporate rules;</p> <p>(j) the mechanisms for reporting and recording changes to the policies and reporting these changes to the supervisory authority;</p> <p>(k) the co-operation mechanism with the supervisory authority to ensure compliance by any member of the group</p>
---	---

<p>of undertakings, in particular by making available to the supervisory authority the results of the verifications of the measures referred to in point (i) of this paragraph.</p> <p>3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for binding corporate rules within the meaning of this Article, in particular as regards the criteria for their approval, the application of points (b), (d), (e) and (f) of paragraph 2 to binding corporate rules adhered to by processors and on further necessary requirements to ensure the protection of personal data of the data subjects concerned.</p> <p>4. The Commission may specify the format and procedures for the exchange of information by electronic means between controllers, processors and supervisory authorities for binding corporate rules within the meaning of this Article. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).</p>	<p>of undertakings, in particular by making available to the supervisory authority the results of the verifications of the measures referred to in point (i) of this paragraph.</p> <p>3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for binding corporate rules within the meaning of this Article, in particular as regards the criteria for their approval, the application of points (b), (d), (e) and (f) of paragraph 2 to binding corporate rules adhered to by processors and on further necessary requirements to ensure the protection of personal data of the data subjects concerned.</p> <p>4. The Commission may specify the format and procedures for the exchange of information by electronic means between controllers, processors and supervisory authorities for binding corporate rules within the meaning of this Article. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).</p>
---	---

Justification

In the Cloud Computing services, cloud providers often use the external subcontractors to perform a specific task to deliver 24/7 service and maintenance. Therefore, this should be recognised in the Binding Corporate Rules by the supervising authority.

Amendment 55

Article 44 (Derogations)	
Commission proposal	Proposed DIGITALEUROPE amendment



<p>1. In the absence of an adequacy decision pursuant to Article 41 or of appropriate safeguards pursuant to Article 42, a transfer or a set of transfers of personal data to a third country or an international organisation may take place only on condition that:</p> <ul style="list-style-type: none"> (a) the data subject has consented to the proposed transfer, after having been informed of the risks of such transfers due to the absence of an adequacy decision and appropriate safeguards; or (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; or (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person; or (d) the transfer is necessary for important grounds of public interest; or (e) the transfer is necessary for the establishment, exercise or defence of legal claims; or (f) the transfer is necessary in order to protect the vital interests of the data subject or of another person, where the data subject is physically or legally incapable of giving consent; or (g) the transfer is made from a register which according to Union or Member State law is intended to provide 	<p>1. In the absence of an adequacy decision pursuant to Article 41; <i>or where the Commission decides that a third country, or a territory or a processing sector within that third country, or an international organisation does not ensure an adequate level of protection in accordance with Article 41(5);</i> or <i>in the absence</i> of appropriate safeguards pursuant to Article 42, a transfer or a set of transfers of personal data to a third country or an international organisation may take place only on condition that:</p> <ul style="list-style-type: none"> (a) the data subject has consented to the proposed transfer, after having been informed of the risks of such transfers due to the absence of an adequacy decision and appropriate safeguards; or (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; or (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person; or (d) the transfer is necessary for important grounds of public interest; or (e) the transfer is necessary for the establishment, exercise or defence of legal claims; or (f) the transfer is necessary in order to protect the vital interests of the data subject or of another person, where the data subject is physically or legally incapable of giving consent; or (g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any
--	--

<p>information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in Union or Member State law for consultation are fulfilled in the particular case; or</p> <p>(h) the transfer is necessary for the purposes of the legitimate interests pursued by the controller or the processor, which cannot be qualified as frequent or massive, and where the controller or processor has assessed all the circumstances surrounding the data transfer operation or the set of data transfer operations and based on this assessment adduced appropriate safeguards with respect to the protection of personal data, where necessary.</p> <p>2. A transfer pursuant to point (g) of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. When the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.</p> <p>3. Where the processing is based on point (h) of paragraph 1, the controller or processor shall give particular consideration to the nature of the data, the purpose and duration of the proposed processing operation or operations, as well as the situation in the country of origin, the third country and the country of final destination, and adduced appropriate safeguards with respect to the protection of personal data, where necessary.</p>	<p>person who can demonstrate legitimate interest, to the extent that the conditions laid down in Union or Member State law for consultation are fulfilled in the particular case; or</p> <p>(h) the transfer is necessary for the purposes of the legitimate interests pursued by the controller or the processor, which cannot be qualified as frequent or massive, and where the controller or processor has assessed all the circumstances surrounding the data transfer operation or the set of data transfer operations and based on this assessment adduced appropriate safeguards with respect to the protection of personal data, where necessary.</p> <p>2. A transfer pursuant to point (g) of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. When the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.</p> <p>3. Where the processing is based on point (h) of paragraph 1, the controller or processor shall give particular consideration to the nature of the data, the purpose and duration of the proposed processing operation or operations, as well as the situation in the country of origin, the third country and the country of final destination, and adduced appropriate safeguards with respect to the protection of personal data, where necessary.</p> <p>4. Points (b), (c) and (h) of paragraph 1 shall</p>
--	---

<p>4. Points (b), (c) and (h) of paragraph 1 shall not apply to activities carried out by public authorities in the exercise of their public powers.</p>	<p>not apply to activities carried out by public authorities in the exercise of their public powers.</p>
<p>5. The public interest referred to in point (d) of paragraph 1 must be recognised in Union law or in the law of the Member State to which the controller is subject.</p>	<p>5. The public interest referred to in point (d) of paragraph 1 must be recognised in Union law or in the law of the Member State to which the controller is subject.</p>
<p>6. The controller or processor shall document the assessment as well as the appropriate safeguards adduced referred to in point (h) of paragraph 1 of this Article in the documentation referred to in Article 28 and shall inform the supervisory authority of the transfer.</p>	<p>6. The controller or processor shall document the assessment as well as the appropriate safeguards adduced referred to in point (h) of paragraph 1 of this Article in the documentation referred to in Article 28 and shall inform the supervisory authority of the transfer.</p>
<p>7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying 'important grounds of public interest' within the meaning of point (d) of paragraph 1 as well as the criteria and requirements for appropriate safeguards referred to in point (h) of paragraph 1.</p>	<p>7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying 'important grounds of public interest' within the meaning of point (d) of paragraph 1 as well as the criteria and requirements for appropriate safeguards referred to in point (h) of paragraph 1.</p>

Justification

See justification for proposed amendment to Article 42.

(The wording of the draft proposal could rule out all forms of data transfers to the country, territory, sector or international organization considered as not offering an adequate level of protection regardless of whether other appropriate safeguards are put in place. Article 41(6) of the draft proposal indeed provides that the prohibition to transfer personal data in case of inadequacy decided by the Commission is “without prejudice to Articles 42 to 44,” while Articles 42(1) and 44(1) mention that they apply only if the Commission has not taken any decision on adequacy.

With the increasing globalisation of business and the evolution of computing models like the cloud, cross-border flows of personal data have become routine. In this environment, it is critical that controllers and processors apply strong safeguards to personal data regardless of where that data is located. Users will only have confidence in cloud computing if they know that their data is safe in the cloud. Helpfully, the Regulation already requires that transfers of personal data to third countries may only be carried out in full compliance with the Regulation. This is an important principle. But controllers and processors should be

incentivised to go beyond the Regulation in some cases. Indeed, controllers and processors will often have direct and practical experience that demonstrates that additional safeguards -- i.e., safeguards that supplement those in the Regulation -- may be appropriate in relation to the personal data they are transferring. The Regulation should encourage these controllers and processors to offer supplemental safeguards where these are appropriate. The amendment proposed above would help to achieve this by allowing controllers and processors that base data transfers on standard data protection clauses under Articles 42(2)(b) and 42(2)(c) of the Regulation to also offer additional protections to customers in the form of legally binding contractual commitments (e.g., data processing agreements) that expand on the standard clauses. In this way, controllers and processors can offer additional protections that reflect the ways in which they will be processing data and particular safeguards appropriate to that processing. Of course, these supplemental commitments should not contradict the standard clauses.)

Amendment 56

Article 51 (Competence)	
Commission proposal	Proposed DIGITALEUROPE amendment
<ol style="list-style-type: none"> 1. Each supervisory authority shall exercise, on the territory of its own Member State, the powers conferred on it in accordance with this Regulation. 2. Where the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union, and the controller or processor is established in more than one Member State, the supervisory authority of the main establishment of the controller or processor shall be competent for the supervision of the processing activities of the controller or the processor in all Member States, without prejudice to the provisions of Chapter VII of this Regulation. 	<ol style="list-style-type: none"> 1. Each supervisory authority shall exercise, on the territory of its own Member State, the powers conferred on it in accordance with this Regulation. 2. Where the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union, and the controller or processor is established in more than one Member State, the supervisory authority of the main establishment of the controller or processor shall be competent for the supervision of the processing activities of the controller or the processor in all Member States <i>and any disputes should be decided upon in accordance with the consistency mechanism set out in article 58, and this</i> without prejudice to the <i>other</i> provisions of Chapter VII of this Regulation. <i>Where a group of undertakings has nominated a single main establishment the</i>

<p>3. The supervisory authority shall not be competent to supervise processing operations of courts acting in their judicial capacity.</p>	<p style="text-align: center;"><i>supervisory authority of that establishment shall be competent.</i></p> <p>3. The supervisory authority shall not be competent to supervise processing operations of courts acting in their judicial capacity.</p>
--	--

Justification

See justification under recital 27

(The determination of the main establishment should be done on the basis of various criteria to ensure organisations have enough guidance to determine their main establishment and provide objective measures by which to judge their decision in the event of a dispute. Already there are such criteria to determine the lead DPA in the context of Binding Corporate Rules (BCRs) which have a proven track record. We think inserting the same criteria as outlined in Art 29 WP opinion 108 would provide more clarity and options that would not be covered under the current proposal. Moreover, as many entities are both controllers and processors, we believe that they should be subject to the same set of criteria in determining their main establishment to avoid potentially conflicting results.)

Amendment 57

Article 53 (Powers)	
Commission proposal	Proposed DIGITALEUROPE amendment
<p>1. Each supervisory authority shall have the power:</p> <p>(a) to notify the controller or the processor of an alleged breach of the provisions governing the processing of personal data, and, where appropriate, order the controller or the processor to remedy that breach, in a specific manner, in order to improve the protection of the data subject;</p> <p>(b) to order the controller or the processor to comply with the data subject's requests to exercise the rights provided by this</p>	<p>1. Each The competent supervisory authority pursuant to Article 51(1) or 51(2) shall have the power:</p> <p>(a) to notify the controller or the processor of an alleged breach of the provisions governing the processing of personal data, and, where appropriate, order the controller or the processor to remedy that breach, in a specific manner, in order to improve the protection of the data subject;</p> <p>(b) to order the controller or the processor to comply with the data subject's requests to exercise the rights provided</p>

<p>Regulation;</p> <p>(c) to order the controller and the processor, and, where applicable, the representative to provide any information relevant for the performance of its duties;</p> <p>(d) to ensure the compliance with prior authorisations and prior consultations referred to in Article 34;</p> <p>(e) to warn or admonish the controller or the processor;</p> <p>(f) to order the rectification, erasure or destruction of all data when they have been processed in breach of the provisions of this Regulation and the notification of such actions to third parties to whom the data have been disclosed;</p> <p>(g) to impose a temporary or definitive ban on processing;</p> <p>(h) to suspend data flows to a recipient in a third country or to an international organisation;</p> <p>(i) to issue opinions on any issue related to the protection of personal data;</p> <p>(j) to inform the national parliament, the government or other political institutions as well as the public on any issue related to the protection of personal data.</p> <p>2. Each supervisory authority shall have the investigative power to obtain from the controller or the processor:</p> <p>(a) access to all personal data and to all information necessary for the performance of its duties;</p> <p>(b) access to any of its premises, including to any data processing equipment and means, where there are reasonable grounds for presuming that an activity in violation of this Regulation is being carried out there.</p> <p>The powers referred to in point (b) shall</p>	<p>by this Regulation;</p> <p>(c) to order the controller and the processor, and, where applicable, the representative to provide any information relevant for the performance of its duties;</p> <p>(d) to ensure the compliance with prior authorisations and prior consultations referred to in Article 34;</p> <p>(e) to warn or admonish the controller or the processor;</p> <p>(f) to order the rectification, erasure or destruction of all data when they have been processed in breach of the provisions of this Regulation and the notification of such actions to third parties to whom the data have been disclosed;</p> <p>(g) to impose a temporary or definitive ban on processing;</p> <p>(h) to suspend data flows to a recipient in a third country or to an international organisation;</p> <p>(i) to issue opinions on any issue related to the protection of personal data;</p> <p>(j) to inform the national parliament, the government or other political institutions as well as the public on any issue related to the protection of personal data.</p> <p>2. Each The competent supervisory authority shall have the investigative power to obtain from the controller or the processor:</p> <p>(a) access to all personal data and to all information necessary for the performance of its duties;</p> <p>(b) access to any of its premises, including to any data processing equipment and means, where there are reasonable grounds for presuming that an activity in violation of this Regulation is being carried out there.</p>
---	--

<p>be exercised in conformity with Union law and Member State law.</p> <p>3. Each supervisory authority shall have the power to bring violations of this Regulation to the attention of the judicial authorities and to engage in legal proceedings, in particular pursuant to Article 74(4) and Article 75(2).</p> <p>4. Each supervisory authority shall have the power to sanction administrative offences, in particular those referred to in Article 79(4), (5) and (6).</p>	<p>The powers referred to in point (b) shall be exercised in conformity with Union law and Member State law.</p> <p>3. Each The competent supervisory authority shall have the power to bring violations of this Regulation to the attention of the judicial authorities and to engage in legal proceedings, in particular pursuant to Article 74(4) and Article 75(2).</p> <p>4. Each The competent supervisory authority shall have the power to sanction administrative offences, in particular those referred to in Article 79(4), (5) and (6).</p>
---	---

Justification

This change reinforces the notion of the lead supervisory authority and avoids a situation where there is confusion on the behalf of data controllers, data processors and the data protection authorities as to which body retains competence or where the competencies of the data protection authorities are overlapping in any particular situation.

Amendment 58

Article 58(4) (Opinion of the European Data Protection Board)	
Commission proposal	Proposed DIGITALEUROPE amendment
<p>1. Before a supervisory authority adopts a measure referred to in paragraph 2, this supervisory authority shall communicate the draft measure to the European Data Protection Board and the Commission.</p> <p>2. The obligation set out in paragraph 1 shall apply to a measure intended to produce legal effects and which:</p> <p>(a) relates to processing activities which are related to the offering of goods or services to data subjects in several Member States, or to the monitoring of their behaviour; or</p>	<p>1. Before a supervisory authority adopts a measure referred to in paragraph 2, this supervisory authority shall communicate the draft measure to the European Data Protection Board and the Commission.</p> <p>2. The obligation set out in paragraph 1 shall apply to a measure intended to produce legal effects and which:</p> <p>(a) relates to processing activities which are related to the offering of goods or services to data subjects in several Member States, or to the monitoring of their behaviour; or</p>



<p>(b) may substantially affect the free movement of personal data within the Union; or</p> <p>(c) aims at adopting a list of the processing operations subject to prior consultation pursuant to Article 34(5); or</p> <p>(d) aims to determine standard data protection clauses referred to in point (c) of Article 42(2); or</p> <p>(e) aims to authorise contractual clauses referred to in point (d) of Article 42(2); or</p> <p>(f) aims to approve binding corporate rules within the meaning of Article 43.</p> <p>3. Any supervisory authority or the European Data Protection Board may request that any matter shall be dealt with in the consistency mechanism, in particular where a supervisory authority does not submit a draft measure referred to in paragraph 2 or does not comply with the obligations for mutual assistance in accordance with Article 55 or for joint operations in accordance with Article 56.</p> <p>4. In order to ensure correct and consistent application of this Regulation, the Commission may request that any matter shall be dealt with in the consistency mechanism.</p> <p>5. Supervisory authorities and the Commission shall electronically communicate any relevant information, including as the case may be a summary of the facts, the draft measure, and the grounds which make the enactment of such measure necessary, using a standardised format.</p>	<p>(b) may substantially affect the free movement of personal data within the Union; or</p> <p>(c) aims at adopting a list of the processing operations subject to prior consultation pursuant to Article 34(5); or</p> <p>(d) aims to determine standard data protection clauses referred to in point (c) of Article 42(2); or</p> <p>(e) aims to authorise contractual clauses referred to in point (d) of Article 42(2); or</p> <p>(f) aims to approve binding corporate rules within the meaning of Article 43.</p> <p>3. Any supervisory authority or the European Data Protection Board may request that any matter shall be dealt with in the consistency mechanism, in particular where a supervisory authority does not submit a draft measure referred to in paragraph 2 or does not comply with the obligations for mutual assistance in accordance with Article 55 or for joint operations in accordance with Article 56.</p> <p>4. In order to ensure correct and consistent application of this Regulation, the Commission may, <i>acting on its own behalf, and shall at the request of a stakeholder</i>, request that any matter shall be dealt with in the consistency mechanism. <i>The Commission shall, on an annual basis, provide an overview of the requests made by third parties.</i></p> <p>5. Supervisory authorities and the Commission shall electronically communicate any relevant information, including as the case may be a summary of the facts, the draft measure, and the grounds which make the enactment of such measure necessary, using a standardised format.</p>
---	--



6. The chair of the European Data Protection Board shall immediately electronically inform the members of the European Data Protection Board and the Commission of any relevant information which has been communicated to it, using a standardised format. The chair of the European Data Protection Board shall provide translations of relevant information, where necessary.
7. The European Data Protection Board shall issue an opinion on the matter, if the European Data Protection Board so decides by simple majority of its members or any supervisory authority or the Commission so requests within one week after the relevant information has been provided according to paragraph 5. The opinion shall be adopted within one month by simple majority of the members of the European Data Protection Board. The chair of the European Data Protection Board shall inform, without undue delay, the supervisory authority referred to, as the case may be, in paragraphs 1 and 3, the Commission and the supervisory authority competent under Article 51 of the opinion and make it public.
8. The supervisory authority referred to in paragraph 1 and the supervisory authority competent under Article 51 shall take account of the opinion of the European Data Protection Board and shall within two weeks after the information on the opinion by the chair of the European Data Protection Board, electronically communicate to the chair of the European Data Protection Board and to the Commission whether it maintains or amends its draft measure and, if any, the amended draft measure, using a standardised format.

6. The chair of the European Data Protection Board shall immediately electronically inform the members of the European Data Protection Board and the Commission of any relevant information which has been communicated to it, using a standardised format. The chair of the European Data Protection Board shall provide translations of relevant information, where necessary.
7. The European Data Protection Board shall issue an opinion on the matter, if the European Data Protection Board so decides by simple majority of its members or any supervisory authority or the Commission so requests within one week after the relevant information has been provided according to paragraph 5. The opinion shall be adopted within one month by simple majority of the members of the European Data Protection Board. The chair of the European Data Protection Board shall inform, without undue delay, the supervisory authority referred to, as the case may be, in paragraphs 1 and 3, the Commission and the supervisory authority competent under Article 51 of the opinion and make it public.
8. The supervisory authority referred to in paragraph 1 and the supervisory authority competent under Article 51 shall take account of the opinion of the European Data Protection Board and shall within two weeks after the information on the opinion by the chair of the European Data Protection Board, electronically communicate to the chair of the European Data Protection Board and to the Commission whether it maintains or amends its draft measure and, if any, the amended draft measure, using a standardised format.

Justification

When there are inconsistencies with regards to the application of the Regulation which threaten the harmonized implementation and affect specific stakeholders, the affected stakeholders should be given the right to bring their concerns into the consistency mechanism. We think the European Commission could play a central role in coordinating such requests.

Amendment 59

Article 66 (1) (Tasks of the European Data Protection Board)	
Commission proposal	Proposed DIGITALEUROPE amendment
<p>1. The European Data Protection Board shall ensure the consistent application of this Regulation. To this effect, the European Data Protection Board shall, on its own initiative or at the request of the Commission, in particular:</p> <p>(a) advise the Commission on any issue related to the protection of personal data in the Union, including on any proposed amendment of this Regulation;</p> <p>(b) examine, on its own initiative or on request of one of its members or on request of the Commission, any question covering the application of this Regulation and issue guidelines, recommendations and best practices addressed to the supervisory authorities in order to encourage consistent application of this Regulation;</p> <p>(c) review the practical application of the guidelines, recommendations and best practices referred to in point (b) and report regularly to the Commission on these;</p> <p>(d) issue opinions on draft decisions of supervisory authorities pursuant to the consistency mechanism referred to in Article 57;</p>	<p>1. The European Data Protection Board shall ensure the consistent application of this Regulation. To this effect, the European Data Protection Board shall, on its own initiative—or at the request of the Commission <i>or other stakeholders</i>, in particular:</p> <p>(a) advise the Commission on any issue related to the protection of personal data in the Union, including on any proposed amendment of this Regulation;</p> <p>(b) examine, on its own initiative or on request of one of its members or on request of the Commission, <i>or on request of stakeholders</i> any question covering the application of this Regulation and issue guidelines, recommendations and best practices addressed to the supervisory authorities in order to encourage consistent application of this Regulation;</p> <p>(c) review the practical application of the guidelines, recommendations and best practices referred to in point (b) and report regularly to the Commission on these;</p> <p>(d) issue opinions on draft decisions of supervisory authorities pursuant to the consistency mechanism referred to in Article 57;</p>



<p>(e) promote the co-operation and the effective bilateral and multilateral exchange of information and practices between the supervisory authorities;</p> <p>(f) promote common training programmes and facilitate personnel exchanges between the supervisory authorities, as well as, where appropriate, with the supervisory authorities of third countries or of international organisations;</p> <p>(g) promote the exchange of knowledge and documentation on data protection legislation and practice with data protection supervisory authorities worldwide.</p> <p>2. Where the Commission requests advice from the European Data Protection Board, it may lay out a time limit within which the European Data Protection Board shall provide such advice, taking into account the urgency of the matter.</p> <p>3. The European Data Protection Board shall forward its opinions, guidelines, recommendations, and best practices to the Commission and to the committee referred to in Article 87 and make them public.</p> <p>4. The Commission shall inform the European Data Protection Board of the action it has taken following the opinions, guidelines, recommendations and best practices issued by the European Data Protection Board.</p>	<p>(e) promote the co-operation and the effective bilateral and multilateral exchange of information and practices between the supervisory authorities;</p> <p>(f) promote common training programmes and facilitate personnel exchanges between the supervisory authorities, as well as, where appropriate, with the supervisory authorities of third countries or of international organisations;</p> <p>(g) promote the exchange of knowledge and documentation on data protection legislation and practice with data protection supervisory authorities worldwide.</p> <p>2. Where the Commission requests advice from the European Data Protection Board, it may lay out a time limit within which the European Data Protection Board shall provide such advice, taking into account the urgency of the matter.</p> <p>3. The European Data Protection Board shall forward its opinions, guidelines, recommendations, and best practices to the Commission and to the committee referred to in Article 87 and make them public.</p> <p>4. The Commission shall inform the European Data Protection Board of the action it has taken following the opinions, guidelines, recommendations and best practices issued by the European Data Protection Board.</p>
---	---

Justification

We would encourage the European Parliament to introduce mechanisms to make the Board more accessible and responsive to requests from other stakeholders including the European Parliament for topics that should be addressed by the Board as this is now only a prerogative

of the DPAs or the Commission. Therefore we are proposing language to give stakeholders such opportunities.

Amendment 60

Art 66 (5) NEW (Consultation of European Data Protection Board)	
Commission proposal	Proposed DIGITALEUROPE amendment
	<p><i>5. Where appropriate, the European Data Protection Board shall, in its execution of the tasks as outlined in article 66, consult interested parties and give them the opportunity to comment within a reasonable period. The European Data Protection Board shall, without prejudice to Article 72, make the results of the consultation procedure publicly available.</i></p>

Justification

Before the Board adopts opinions or reports, they should consult interested parties and give them the opportunity to comment within a reasonable period as possible for other regulatory domains (see BEREC example⁴).

Amendment 61

Article 77 (Right to compensation and liability)	
Commission proposal	Proposed DIGITALEUROPE amendment
<p>1. Any person who has suffered damage as a result of an unlawful processing operation or of an action incompatible with this Regulation shall have the right to receive compensation from the controller or the</p>	<p>1. Any person who has suffered damage as a result of an unlawful processing operation or of an action incompatible with this Regulation shall have the right to receive compensation from the</p>

⁴ Regulation on establishment of BEREC (1211/2009); articles 17 (Consultation) and 18 (Transparency) define how BEREC is interacting with public and interested parties.



<p>processor for the damage suffered.</p> <p>2. Where more than one controller or processor is involved in the processing, each controller or processor shall be jointly and severally liable for the entire amount of the damage.</p> <p>3. The controller or the processor may be exempted from this liability, in whole or in part, if the controller or the processor proves that they are not responsible for the event giving rise to the damage.</p>	<p>controller or the processor for the damage suffered.</p> <p>2. Where more than one controller or processor is involved in the processing, each controller or processor shall be jointly and severally liable for the entire amount of the damage, <i>to the extent that liability has not already been established in the determination of responsibilities envisaged in Article 24.</i></p> <p>3. The controller or the processor may be exempted from this the liability <i>under paragraph 2</i>, in whole or in part, if the <i>respective</i> controller or the processor proves that they are not to be responsible for the event giving rise to the damage.</p> <p>4. <i>If a processor processes personal data other than as instructed by the controller, they may be held liable should any person suffer damage as a result of such processing.</i></p>
---	--

Justification

Under the current Directive, liability is correctly attributed to the data controller. Essentially, they direct the data processor and if the processor does not act on those orders then contractual arrangements apply to address the circumstances. Introducing a vague liability clause does not clarify the current situation but creates confusion for controllers, processors and data subjects alike.

Amendment 62

Article 79 (Administrative sanctions)	
Commission proposal	Proposed DIGITALEUROPE amendment
<p>1. Each supervisory authority shall be empowered to impose administrative sanctions in accordance with this Article.</p>	<p>1. Each <i>The competent</i> supervisory authority shall be empowered to impose administrative sanctions in accordance with this Article.</p>



2. The administrative sanction shall be in each individual case effective, proportionate and dissuasive. The amount of the administrative fine shall be fixed with due regard to the nature, gravity and duration of the breach, the intentional or negligent character of the infringement, the degree of responsibility of the natural or legal person and of previous breaches by this person, the technical and organisational measures and procedures implemented pursuant to Article 23 and the degree of co-operation with the supervisory authority in order to remedy the breach.

2. The administrative sanction shall be in each individual case effective, proportionate and dissuasive. The amount of the administrative fine shall be fixed with due regard to the nature, gravity and duration of the breach, ***the sensitivity of the personal data at issue***, the intentional or negligent character of the infringement, ***the degree of harm or risk of significant harm created by the violation***, the degree of responsibility of the natural or legal person and of previous breaches by this person, the technical and organisational measures and procedures implemented pursuant to Article 23 and the degree of co-operation with the supervisory authority in order to remedy the breach. ***While some discretion is granted in the imposition of such sanctions to take into account the circumstances outlined above and other facts specific to the situation, divergences in the application of administrative sanctions may be subject to review pursuant to the consistency mechanism.***

In setting an administrative fine, supervisory authorities shall also take into account fines, damages or other penalties previously imposed by a court or other body on the natural or legal person in respect of the violation in issue.

(a) Aggravating factors that support administrative fines at the upper limits established in paragraphs 4 to 6 shall include in particular:

(i) repeated violations committed in reckless disregard of applicable law;

(ii) refusal to co-operate with or obstruction of an enforcement process; and

(iii) violations that are deliberate, serious



<p>3. In case of a first and non-intentional non-compliance with this Regulation, a warning in writing may be given and no sanction imposed, where:</p> <ul style="list-style-type: none"> (a) a natural person is processing personal data without a commercial interest; or (b) an enterprise or an organisation employing fewer than 250 persons is processing personal data only as an activity ancillary to its main activities. <p>4. The supervisory authority shall impose a fine up to 250 000 EUR, or in case of an enterprise up to 0,5 % of its annual worldwide turnover, to anyone who, intentionally or negligently:</p> <ul style="list-style-type: none"> (c) does not provide the mechanisms for requests by data subjects or does not respond promptly or not in the required format to data subjects pursuant to Articles 12(1) and (2); (d) charges a fee for the information or for responses to the requests of data subjects in violation of Article 12(4). <p>5. The supervisory authority shall impose a</p>	<p><i>and likely to cause substantial damage.</i></p> <p><i>2b. Mitigating factors which support administrative fines at the lower limits shall include:</i></p> <ul style="list-style-type: none"> <i>(i) measures having been taken by the natural or legal person to ensure compliance with relevant obligations;</i> <i>(ii) genuine uncertainty as to whether the activity constituted a violation of the relevant obligations;</i> <i>(iii) immediate termination of the violation upon knowledge; and</i> <i>(iv) co-operation with any enforcement processes.</i> <p>3. In case of a first and non-intentional non-compliance with this Regulation, a warning in writing may be given and no sanction imposed. where:</p> <ul style="list-style-type: none"> (a) a natural person is processing personal data without a commercial interest; or (b) an enterprise or an organisation employing fewer than 250 persons is processing personal data only as an activity ancillary to its main activities. <p>4. The supervisory authority shall <i>may</i> impose a fine up to 250 000 EUR, or in case of an enterprise up to 0,5 % of its annual worldwide turnover, to anyone who, intentionally or negligently.</p> <ul style="list-style-type: none"> (a) does not provide the mechanisms for requests by data subjects or does not respond promptly or not in the required format to data subjects pursuant to Articles 12(1) and (2); (b) charges a fee for the information or for responses to the requests of data subjects in violation of Article 12(4).
--	--



<p>fine up to 500 000 EUR, or in case of an enterprise up to 1 % of its annual worldwide turnover, to anyone who, intentionally or negligently:</p> <ul style="list-style-type: none"> (a) does not provide the information, or does provide incomplete information, or does not provide the information in a sufficiently transparent manner, to the data subject pursuant to Article 11, Article 12(3) and Article 14; (b) does not provide access for the data subject or does not rectify personal data pursuant to Articles 15 and 16 or does not communicate the relevant information to a recipient pursuant to Article 13; (c) does not comply with the right to be forgotten or to erasure, or fails to put mechanisms in place to ensure that the time limits are observed or does not take all necessary steps to inform third parties that a data subjects requests to erase any links to, or copy or replication of the personal data pursuant Article 17; (d) does not provide a copy of the personal data in electronic format or hinders the data subject to transmit the personal data to another application in violation of Article 18; (e) does not or not sufficiently determine the respective responsibilities with co-controllers pursuant to Article 24; (f) does not or not sufficiently maintain the documentation pursuant to Article 28, Article 31(4), and Article 44(3); (g) does not comply, in cases where special categories of data are not involved, pursuant to Articles 80, 82 	<p>5. The supervisory authority <i>shall may</i> impose a fine up to 500 000 EUR, or in case of an enterprise up to 1 % of its annual worldwide turnover, to anyone who, intentionally or negligently:</p> <ul style="list-style-type: none"> (a) does not provide the information, or does provide incomplete information, or does not provide the information in a sufficiently transparent manner, to the data subject pursuant to Article 11, Article 12(3) and Article 14; (b) does not provide access for the data subject or does not rectify personal data pursuant to Articles 15 and 16 or does not communicate the relevant information to a recipient pursuant to Article 13; (c) does not comply with the right to be forgotten or to erasure <i>on websites or data within their control</i>, or fails to put mechanisms in place to ensure that the time limits are observed or does not take all necessary steps to inform third parties that a data subjects requests to erase any links to, or copy or replication of the personal data pursuant Article 17; (d) does not provide a copy of the personal data in electronic format or hinders the data subject to transmit the personal data to another application in violation of Article 18; (e) does not or not sufficiently determine define the respective responsibilities with co-controllers pursuant to Article 24; (f) does not or not sufficiently take reasonable steps to maintain the documentation pursuant to Article 28, Article 31(4), and Article 44(3); (g) does not comply, in cases where special
---	---



<p>and 83 with rules in relation to freedom of expression or with rules on the processing in the employment context or with the conditions for processing for historical, statistical and scientific research purposes.</p> <p>6. The supervisory authority shall impose a fine up to 1 000 000 EUR or, in case of an enterprise up to 2 % of its annual worldwide turnover, to anyone who, intentionally or negligently:</p> <ul style="list-style-type: none"> (a) processes personal data without any or sufficient legal basis for the processing or does not comply with the conditions for consent pursuant to Articles 6, 7 and 8; (b) processes special categories of data in violation of Articles 9 and 81; (c) does not comply with an objection or the requirement pursuant to Article 19; (d) does not comply with the conditions in relation to measures based on profiling pursuant to Article 20; (e) does not adopt internal policies or does not implement appropriate measures for ensuring and demonstrating compliance pursuant to Articles 22, 23 and 30; (f) does not designate a representative pursuant to Article 25; (g) processes or instructs the processing of personal data in violation of the obligations in relation to processing on behalf of a controller pursuant to Articles 26 and 27; (h) does not alert on or notify a personal data breach or does not timely or completely notify the data breach to the supervisory authority or to the 	<p>categories of data are not involved, pursuant to Articles 80, 82 and 83 with rules in relation to freedom of expression or with rules on the processing in the employment context or with the conditions for processing for historical, statistical and scientific research purposes.</p> <p>6. The supervisory authority shall<i>may</i> impose a fine up to 1 000 000 EUR or, in case of an enterprise up to 2 % of its annual worldwide turnover, to anyone who, intentionally or negligently:</p> <ul style="list-style-type: none"> (a) processes personal data without any or sufficient legal basis for the processing or does not comply with the conditions for consent pursuant to Articles 6, 7 and 8; (b) processes special categories of data in violation of Articles 9 and 81; (c) does not comply with an objection or the requirement pursuant to Article 19; (d) does not comply with the conditions in relation to measures based on profiling pursuant to Article 20; (e) does not adopt internal policies or does not implement appropriate measures for ensuring and demonstrating compliance pursuant to Articles 22, 23 and 30; (f) does not designate a representative pursuant to Article 25; (g) processes or instructs the processing of personal data in violation of the obligations in relation to processing on behalf of a controller pursuant to Articles 26 and 27; (h) does not <i>timely or completely</i> alert on or notify a personal data breach or does
--	--



<p>data subject pursuant to Articles 31 and 32;</p> <p>(i) does not carry out a data protection impact assessment pursuant or processes personal data without prior authorisation or prior consultation of the supervisory authority pursuant to Articles 33 and 34;</p> <p>(j) does not designate a data protection officer or does not ensure the conditions for fulfilling the tasks pursuant to Articles 35, 36 and 37;</p> <p>(k) misuses a data protection seal or mark in the meaning of Article 39;</p> <p>(l) carries out or instructs a data transfer to a third country or an international organisation that is not allowed by an adequacy decision or by appropriate safeguards or by a derogation pursuant to Articles 40 to 44;</p> <p>(m) does not comply with an order or a temporary or definite ban on processing or the suspension of data flows by the supervisory authority pursuant to Article 53(1);</p> <p>(n) does not comply with the obligations to assist or respond or provide relevant information to, or access to premises by, the supervisory authority pursuant to Article 28(3), Article 29, Article 34(6) and Article 53(2);</p> <p>(o) does not comply with the rules for safeguarding professional secrecy pursuant to Article 84.</p>	<p><i>not timely or completely notify the data breach</i> to the supervisory authority or <i>where required does not timely and appropriately notify the to the</i> data subject pursuant to Articles 31 and 32;</p> <p>(i) <i>does not carry out a data protection impact assessment where required pursuant or processes personal data without prior authorisation or prior consultation of the supervisory authority pursuant to Articles 33 and 34;</i></p> <p>(j) <i>does not designate a data protection officer or does not ensure the conditions for fulfilling the tasks pursuant to Articles 35, 36 and 37;</i></p> <p>(k) misuses a data protection seal or mark in the meaning of Article 39;</p> <p>(l) carries out or instructs a data transfer <i>or transfers</i> to a third country or an international organisation that is not allowed by an adequacy decision or by appropriate safeguards or by a derogation pursuant to Articles 40 to 44;</p> <p>(m) does not comply with an order or a temporary or definite ban on processing or the suspension of data flows by the supervisory authority pursuant to Article 53(1);</p> <p>(n) does not comply with the obligations to assist or respond or provide relevant information to, or access to premises by, the supervisory authority pursuant to Article 28(3), Article 29, Article 34(6) and Article 53(2);</p> <p>(o) does not comply with the rules for safeguarding professional secrecy pursuant to Article 84.</p>
<p>7. The Commission shall be empowered to</p>	

<p>adopt delegated acts in accordance with Article 86 for the purpose of updating the amounts of the administrative fines referred to in paragraphs 4, 5 and 6, taking into account the criteria referred to in paragraph 2.</p>	<p>7. <i>Where convincing evidence exists of continued negligence or gross negligence by organisations in the execution of their responsibilities under this Regulation or the failure of these sanctions to deter serious abuses that cannot be addressed under the current framework</i> the Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of updating the amounts <i>or conditions</i> of the administrative fines referred to in paragraphs 4, 5 and 6, taking into account the criteria referred to in paragraph 2.</p>
--	---

Justification

DIGITALEUROPE believes that the excessively broad scope and scale of the fines are not commensurate with the associated offences, especially if they are not demonstrated to be intentional.

One of our main concerns is that according to the Regulation both negligent and intentional breaches give rise to fines. Much of the Regulation is new, with limited guidance as to how it should be implemented in practice. As such, in the first few years after the Regulation comes into force questions of interpretation will arise as to its meaning, intent and nuances. Therefore, we would recommend that article 79 is amended to limit fines to intentional non-compliance.

The amendments specify the mitigating and aggravating factors that supervisory authorities should consider when imposing fines. In doing so, the amendments ensure that higher fines are imposed on more serious misconduct, and also encourage compliance and co-operation once a violation is discovered. Specifying these factors will also promote greater consistency across the Member States in terms of the fines imposed.

Even if fines do become limited to intentional acts, we find the range of acts does not commensurate with the scale of fines. Open-ended fines such as 2% of world-wide turn over create open-ended risk that engenders uncertainty. It would be better if each category of fines were to be capped at a particular amount. We would also suggest that the percentage of turnover be retained within the capped amount in order to be fairer to SMEs. Thus a fine

structure may read fines up to 2% of worldwide turnover, but not exceeding, for example €500,000.

We would suggest guidance related to fines and their imposition. Furthermore, we disagree with the fact that the word 'shall' is used for every single fine envisaged in article 79, thus forbidding DPAs from exercising any discretion as to whether a fine should be imposed. We also believe that a coordinating mechanism would be appropriate to assure a reasonable level of correlation between violations and corresponding penalties across Member States.

Amendment 63

Article 86.6 (new) (Exercise of the Delegation)	
Commission proposal	Proposed DIGITALEUROPE amendment
<p>1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.</p> <p>2. The delegation of power referred to in Article 6(5), Article 8(3), Article 9(3), Article 12(5), Article 14(7), Article 15(3), Article 17(9), Article 20(6), Article 22(4), Article 23(3), Article 26(5), Article 28(5), Article 30(3), Article 31(5), Article 32(5), Article 33(6), Article 34(8), Article 35(11), Article 37(2), Article 39(2), Article 43(3), Article 44(7), Article 79(6), Article 81(3), Article 82(3) and Article 83(3) shall be conferred on the Commission for an indeterminate period of time from the date of entry into force of this Regulation.</p> <p>3. The delegation of power referred to in Article 6(5), Article 8(3), Article 9(3), Article 12(5), Article 14(7), Article 15(3), Article 17(9), Article 20(6), Article 22(4), Article 23(3), Article 26(5), Article 28(5), Article 30(3), Article 31(5), Article 32(5), Article 33(6), Article 34(8), Article 35(11), Article 37(2), Article 39(2), Article 43(3), Article 44(7), Article 79(6), Article 81(3), Article 82(3) and Article 83(3) may be revoked at any time by the</p>	<p>1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.</p> <p>2. The delegation of power referred to in Article 6(5), Article 8(3), Article 9(3), Article 12(5), Article 14(7), Article 15(3), Article 17(9), Article 20(6), Article 22(4), Article 23(3), Article 26(5), Article 28(5), Article 30(3), Article 31(5), Article 32(5), Article 33(6), Article 34(8), Article 35(11), Article 37(2), Article 39(2), Article 43(3), Article 44(7), Article 79(6), Article 81(3), Article 82(3) and Article 83(3) shall be conferred on the Commission for an indeterminate period of time from the date of entry into force of this Regulation.</p> <p>3. The delegation of power referred to in Article 6(5), Article 8(3), Article 9(3), Article 12(5), Article 14(7), Article 15(3), Article 17(9), Article 20(6), Article 22(4), Article 23(3), Article 26(5), Article 28(5), Article 30(3), Article 31(5), Article 32(5), Article 33(6), Article 34(8), Article 35(11), Article 37(2), Article 39(2), Article 43(3), Article 44(7), Article 79(6), Article 81(3), Article 82(3) and Article 83(3) may be revoked at any time by the</p>

<p>European Parliament or by the Council. A decision of revocation shall put an end to the delegation of power specified in that decision. It shall take effect the day following the publication of the decision in the <i>Official Journal of the European Union</i> or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.</p> <p>4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.</p> <p>5. A delegated act adopted pursuant to Article 6(5), Article 8(3), Article 9(3), Article 12(5), Article 14(7), Article 15(3), Article 17(9), Article 20(6), Article 22(4), Article 23(3), Article 26(5), Article 28(5), Article 30(3), Article 31(5), Article 32(5), Article 33(6), Article 34(8), Article 35(11), Article 37(2), Article 39(2), Article 43(3), Article 44(7), Article 79(6), Article 81(3), Article 82(3) and Article 83(3) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or the Council.</p>	<p>European Parliament or by the Council. A decision of revocation shall put an end to the delegation of power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.</p> <p>4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.</p> <p>5. A delegated act adopted pursuant to Article 6(5), Article 8(3), Article 9(3), Article 12(5), Article 14(7), Article 15(3), Article 17(9), Article 20(6), Article 22(4), Article 23(3), Article 26(5), Article 28(5), Article 30(3), Article 31(5), Article 32(5), Article 33(6), Article 34(8), Article 35(11), Article 37(2), Article 39(2), Article 43(3), Article 44(7), Article 79(6), Article 81(3), Article 82(3) and Article 83(3) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or the Council.</p> <p><i>6(new). Acts adopted in accordance with this Article shall be technology neutral and non-discriminatory irrespective of the means used for the lawful processing of personal data.</i></p>
--	--

Justification

The present Data Protection Reform package aims at building a strong, consistent and modern data protection framework at EU level that can withstand the test of time and new technological developments. To achieve this goal, the language of the Regulation should remain technology neutral, and future proof for the decades to come.

Amendment 64

Article 87.4 (new) (Exercise of the Delegation)	
Commission proposal	Proposed DIGITALEUROPE amendment
<ol style="list-style-type: none"> 1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011. 2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply. 3. Where reference is made to this paragraph, Article 8 of Regulation (EU) No 182/2011, in conjunction with Article 5 thereof, shall apply. 	<ol style="list-style-type: none"> 1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011. 2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply. 3. Where reference is made to this paragraph, Article 8 of Regulation (EU) No 182/2011, in conjunction with Article 5 thereof, shall apply. <p><i>4(new). Acts adopted in accordance with this Article shall be technology neutral and non-discriminatory irrespective of the means used for the lawful processing of personal data.</i></p>

Justification

The present Data Protection Reform package aims at building a strong, consistent and modern data protection framework at EU level that can withstand the test of time and new technological developments. To achieve this goal, the language of the Regulation should remain technology neutral, and future proof for the decades to come.

ABOUT DIGITALEUROPE

DIGITALEUROPE is the voice of the European digital economy including information and communication technologies and consumer electronics. DIGITALEUROPE is dedicated to improving the business environment for the European digital technology industry and to promoting our sector's contribution to economic growth and social progress in the European Union.

DIGITALEUROPE ensures industry participation in the development and implementation of EU policies. DIGITALEUROPE's members include 60 global corporations and 37 national trade associations from across Europe. In total, 10,000 companies employing two million citizens and generating €1 trillion in revenues. Our website provides further information on our recent news and activities: <http://www.digitaleurope.org>

THE MEMBERSHIP OF DIGITALEUROPE

COMPANY MEMBERS:

Acer, Alcatel-Lucent, AMD, APC by Schneider Electric, Apple, Bang & Olufsen, BenQ Europa BV, Bose, Brother, Canon, Cassidian, Cisco, Dell, Epson, Ericsson, Fujitsu, Hitachi, HP, Huawei, IBM, Ingram Micro, Intel, JVC Kenwood Group, Kodak, Konica Minolta, Kyocera Mita, Lexmark, LG, Loewe, Microsoft, Mitsubishi Electric, Motorola Mobility, Motorola Solutions, NEC, Nokia, Nokia Siemens Networks, Océ, Oki, Optoma, Oracle, Panasonic, Philips, Pioneer, Qualcomm, Research In Motion, Ricoh International, Samsung, SAP, Sharp, Siemens, Smart Technologies, Sony, Sony Ericsson, Swatch Group, Technicolor, Texas Instruments, Toshiba, Xerox, ZTE Corporation.

NATIONAL TRADE ASSOCIATIONS:

Belgium: AGORIA; **Bulgaria:** BAIT; **Cyprus:** CITEA; **Denmark:** DI ITEK, IT-BRANCHEN; **Estonia:** ITL; **Finland:** FFTI; **France:** SIMAVELEC; **Germany:** BITKOM, ZVEI; **Greece:** SEPE; **Hungary:** IVSZ; **Ireland:** ICT IRELAND; **Italy:** ANITEC, **Lithuania:** INFOBALT; **Netherlands:** ICT OFFICE, FIAR; **Poland:** KIGEIT, PIIT; **Portugal:** AGEFE, APDC; **Romania:** APDETIC; **Slovakia:** ITAS; **Slovenia:** GZS; **Spain:** AMETIC; **Sweden:** IT&TELEKOMFÖRETAGEN; **United Kingdom:** INTELLECT; **Belarus:** INFOPARK; **Norway:** IKT NORGE; **Switzerland:** SWICO; **Turkey:** ECID, TESID, TÜBISAD; **Ukraine:** IT UKRAINE

12 March 2012

DIGITALEUROPE

COMMENTS ON

PROPOSED EUROPEAN COMMISSION'S REGULATION ON DATA PROTECTION

Welcome improvements

DIGITALEUROPE welcomes the European Commission's proposed Regulation on Data Protection. This is an important step towards building a future proof legislative framework which should enable a strong protection of privacy while at the same time recognizing the importance of data flows for the internal market.

The proposed legislation contains welcome improvements which are crucial to making this Regulation effective and efficient. First of all, we support the European Commission's goal of enhancing the single market by increasing harmonisation on data protection rules across the 27 Member States. The introduction of the concept of a one stop shop for data protection issues will not only increase legal certainty, but also reduce administrative burdens and create an incentive for DPAs to move to a mutual recognition model. We also welcome the goal of making the framework more efficient by reducing the unnecessary administrative burdens such as the elimination of notification obligations. These developments would allow for DIGITALEUROPE's members, especially SMEs, to focus their efforts on what is important; ensuring strong data protection instead of producing paperwork with no added benefits.

Significant challenges remain: 7 key issues threatening the EU's digital technology industry

There are still some aspects of the Regulation that create significant challenges to the goals of the Regulation but also to continued economic growth. We would like to encourage the European Parliament and the Council to look at the following **7 key issues** as having a crucial impact on the development of the EU's digital technology industry.

The proposed provisions on the relationship between **data processor and controller** risk creating legal uncertainty with regards to responsibility and liability, especially given the complexities of cloud computing. A clear distinction of the obligations of data controller and processor should be maintained.

New administrative burdens are created, thus undermining the Commission's overall objective of creating a more efficient system. The provisions on prior notification/consultation, Privacy Impact Assessments (PIA), Privacy by Design/Default and on an extensive documentation obligation risk creating useless paper trails and impose unnecessary costs instead of focusing on the actual outcomes.

DIGITALEUROPE

Rue de la Science, 14 >> B-1040 Brussels [Belgium]

T. +32 2 609 53 10 >> F. +32 2 609 53 39

www.digitaleurope.org

Transparency register member for the Commission: 64270747023-20

To ensure the goal of **more harmonisation** is achieved, the concept of “main establishment” should be clarified, the new European Data Protection Board (EDPB) should be made more transparent and accessible (following the BEREC example) and the consistency mechanism should be opened to other stakeholder input.

Some of the definitions need to be clarified. **The definition on personal data** risks encompassing almost all data and hence, we would like to see more of a contextual approach being recognized in the framework. Individuals should have the right to make an informed choice about how their data will be processed. Therefore, it is important to recognize this in **the definition of consent**. However, no modalities on the provision of ‘consent’ should be defined and the requirements should not be set artificially high, such as requiring an explicit consent in all cases. The exceptional circumstances under which even ‘consent’ cannot serve as a legal basis for data processing need to be better defined and justified, and consent in employment contexts needs to be still possible in specific cases.

With regards to increasing security measures within organisations, we welcome the introduction of the **data breach notification obligation**. To make it workable and avoid wrong notifications, the 24 hour rule should be removed, an appropriate standard of harm should be introduced as trigger of notifications and technical protection measures should be further incentivised.

Any legislative framework should be backed up by harmonised and predictable enforcement. The provisions on **administrative sanctions** however introduce considerable uncertainty, risk creating fragmentation and lack proportionality. In addition, a DPA should have the discretionary power to look at the overall internal processes when deciding on sanctions.

Finally, many of the changes foreseen in the Regulation will depend on the effectiveness of the DPAs and ability of the Commission to issue **delegated and implementing acts** in efficient, timely and transparent manner, considering stakeholders input. However, we would like to stress that to ensure legal certainty, the Commission does not need to give itself powers to adopt the delegated and implementing acts in all the proposed areas, since in many of the relevant Articles, the requirements and criteria are already enumerated in a detailed manner.

ABOUT DIGITALEUROPE

DIGITALEUROPE is the voice of the European digital economy including information and communication technologies and consumer electronics. DIGITALEUROPE is dedicated to improving the business environment for the European digital technology industry and to promoting our sector's contribution to economic growth and social progress in the European Union.

DIGITALEUROPE ensures industry participation in the development and implementation of EU policies. DIGITALEUROPE's members include 60 global corporations and 37 national trade associations from across Europe. In total, 10,000 companies employing two million citizens and generating €1 trillion in revenues. Our website provides further information on our recent news and activities: <http://www.digitaleurope.org>

THE MEMBERSHIP OF DIGITALEUROPE

COMPANY MEMBERS:

Acer, Alcatel-Lucent, AMD, APC by Schneider Electric, Apple, Bang & Olufsen, BenQ Europa BV, Bose, Brother, Canon, Cassidian, Cisco, Dell, Epson, Ericsson, Fujitsu, Hitachi, HP, Huawei, IBM, Ingram Micro, Intel, JVC Kenwood Group, Kodak, Konica Minolta, Kyocera Mita, Lexmark, LG, Loewe, Microsoft, Mitsubishi Electric, Motorola Mobility, Motorola Solutions, NEC, Nokia, Nokia Siemens Networks, Océ, Oki, Optoma, Oracle, Panasonic, Philips, Pioneer, Qualcomm, Research In Motion, Ricoh International, Samsung, SAP, Sharp, Siemens, Smart Technologies, Sony, Sony Ericsson, Swatch Group, Technicolor, Texas Instruments, Toshiba, Xerox, ZTE Corporation.

NATIONAL TRADE ASSOCIATIONS:

Belgium: AGORIA; **Bulgaria:** BAIT; **Cyprus:** CITEA; **Denmark:** DI ITEK, IT-BRANCHEN; **Estonia:** ITL; **Finland:** FFTI; **France:** SIMAVELEC; **Germany:** BITKOM, ZVEI; **Greece:** SEPE; **Hungary:** IVSZ; **Ireland:** ICT IRELAND; **Italy:** ANITEC, **Lithuania:** INFOBALT; **Netherlands:** ICT OFFICE, FIAR; **Poland:** KIGEIT, PIIT; **Portugal:** AGEFE, APDC; **Romania:** APDETIC; **Slovakia:** ITAS; **Slovenia:** GZS; **Spain:** AMETIC; **Sweden:** IT&TELEKOMFÖRETAGEN; **United Kingdom:** INTELLECT; **Belarus:** INFOPARK; **Norway:** IKT NORGE; **Switzerland:** SWICO; **Turkey:** ECID, TESID, TÜBISAD; **Ukraine:** IT UKRAINE

eBay comments ahead of IMCO vote on the Comi opinion on the General Data Protection Regulation proposal

eBay thanks IMCO MEPs for their work on the General Data Protection Regulation proposal which reflects the objectives of the regulatory review to both increase consumers data protection and facilitate the legitimate use of personal data by businesses established in the Internal Market.

While we very much welcome the intentions of the Internal Market and Consumer Protection Committee draft opinion and amendments tabled by other MEPs, we would like to draw your attention to several issues ahead of tomorrow's vote.

Main establishment and one-stop-shop (Article 4 – paragraph 1 – point 13).

This sensitive to our business issue was not covered by the compromises amendment and will be voted separately.

In order to reinforce legal certainty and avoid disputes over Data Protection authorities (DPAs) competences, we believe it should be the controller's responsibility to designate its main establishment, and **amendment 179** (Andreas Schwab/Marielle Gallo) as well as **180** (Malcolm Harbour/Adam Bielan) suggesting further clarification of the criteria for that designation clarify this.

Such criteria should be similar to the checklist used by the Article 29 Working Party in determining the lead data protection authority for the approval of Binding Corporate Rules¹.

Furthermore, both amendment 179 and 180 strongly support the introduction of a 'one-stop-shop' approach with respect to the competence of the lead data protection authority in the Member States where the company has its main establishment, as it allows companies to operate in multiple Member States, while streamlining companies' relationship with enforcement authorities.

Therefore, eBay would strongly recommend **voting in favour of both amendmet 179 and 180.**

Amendment 179

Andreas Schwab, Marielle Gallo

Proposal for a regulation

Article 4 – paragraph 1 – point 13

Text proposed by the Commission

(13) 'main establishment' means ***as regards the controller, the place of its establishment in the Union where the main decisions as to the purposes, conditions and means of the processing of personal data are taken; if no decisions as to the purposes, conditions and means of the processing of personal data are taken in the Union, the main establishment is the place where the main processing activities in the context of the activities of an establishment of a controller in the Union take place. As regards the processor, 'main establishment' means the place of its central administration in the Union;***

Amendment

(13) 'main establishment' means ***the location as designated by the undertaking or group of undertakings, whether controller or processor, on the basis of, but not limited to, the following optional objective criteria:***

(1) the location of the European headquarters of a group of undertakings;

(2) the location of the entity within a group of undertakings with delegated data protection responsibilities;

¹

(3) the location of the entity within the group which is best placed in terms of management functions and administrative responsibilities to deal with and enforce the rules as set out in this Regulation; or

(4) the location where effective and real management activities are exercised determining the data processing through stable arrangements.

The competent authority shall be informed by the undertaking or group of undertakings of the designation of the main establishment;

Amendment 180

Malcolm Harbour, Adam Bielan

Proposal for a regulation

Article 4 – paragraph 1 – point 13

Text proposed by the Commission

(13) 'main establishment' means **as regards the controller, the place of its establishment in the Union where the main decisions as to the purposes, conditions and means of the processing of personal data are taken; if no decisions as to the purposes, conditions and means of the processing of personal data are taken in the Union, the main establishment is the place where the main processing activities in the context of the activities of an establishment of a controller in the Union take place. As regards the processor, 'main establishment' means the place of its central administration in the Union;**

Amendment

(13) 'main establishment' means **the location as designated by the undertaking or group of undertakings, whether controller or processor, subject to the consistency mechanism set out in Article 57, on the basis of, but not limited to, the following optional objective criteria:**

(1) the location of the European headquarters of a group of undertakings;

(2) the location of the entity within a group of undertakings with delegated data protection responsibilities;

(3) the location of the entity within the group which is best placed in terms of management functions and administrative responsibilities to deal with and enforce the rules as set out in this Regulation; or

(4) the location where effective and real management activities are exercised determining the data processing through stable arrangements.

The competent authority shall be informed by the undertaking or group of undertakings of the designation of the main establishment.

Data portability

eBay welcomes the amendments **128 and 280** (Andreas Schwab, Rafał Trzaskowski, Marielle Gallo) on Recital 55 and Article 18 respectively, on data portability. These again are not covered by the compromises.

We would highly recommend EU decision makers **voting in favour of both amendments 128 and 280**, deleting the provision suggested by the Commission that may have a detrimental effect on both data subjects and data controllers mainly regarding interoperability and transferability.

Amendment 128

Andreas Schwab, Rafał Trzaskowski, Marielle Gallo

Proposal for a regulation

Recital 55

Text proposed by the Commission

(55) To further strengthen the control over their own data and their right of access, data subjects should have the right, where personal data are processed by electronic means and in a structured and commonly used format, to obtain a copy of the data concerning them also in commonly used electronic format. The data subject should also be allowed to transmit those data, which they have provided, from one automated application, such as a social network, into another one. This should apply where the data subject provided the data to the automated processing system, based on their consent or in the performance of a contract.

Amendment

Deleted

Amendment 280

Andreas Schwab, Rafał Trzaskowski, Marielle Gallo

Proposal for a regulation

Article 18

Text proposed by the Commission

Article 18

Right to data portability

1. The data subject shall have the right, where personal data are processed by electronic means and in a structured and commonly used format, to obtain from the controller a copy of data undergoing processing in an electronic and structured format which is commonly used and allows for further use by the data subject.

2. Where the data subject has provided the personal data and the processing is based on

Amendment

Deleted

consent or on a contract, the data subject shall have the right to transmit those personal data and any other information provided by the data subject and retained by an automated processing system, into another one, in an electronic format which is commonly used, without hindrance from the controller from whom the personal data are withdrawn.

3. The Commission may specify the electronic format referred to in paragraph 1 and the technical standards, modalities and procedures for the transmission of personal data pursuant to paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).

Extraterritorial scope of the Regulation

According to Article 3 the scope of the Regulation extends to controllers established outside of the EU where the processing activities relate to goods/services offered to EU citizens or where their behaviour is monitored. We acknowledge that it is desirable to have companies based outside of the EU respect EU data protection standards when processing personal data of EU citizens. However, in a cross-border context, we believe that covering all online services throughout the world is too ambitious. The extension shall be rather limited to the cases where a service intentionally addresses EU consumers. Therefore, we would recommend **voting against of the amendment 155** (Catherine Stihler), **156** (Christel Schaldemose, Anna Hedh, Catherine Stihler), **and in favour of amendments 157** (Rafal Trzaskowski) **and 158**.

Amendment 155
Catherine Stihler

Proposal for a regulation
Article 3 a (new)

Text proposed by the Commission

Amendment

Article 3 a

This regulation applies to the processing of personal data of data subjects not residing in the Union by a controller or processor established in the Union, through their economic activities in a third country(ies)

Amendment 156

Christel Schaldemose, Anna Hedh, Catherine Stihler

Proposal for a regulation

Article 3 – paragraph 1

Text proposed by the Commission

Amendment

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union.

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, *whether the processing takes place in the Union or not.*

Amendment 157

Rafał Trzaskowski

Proposal for a regulation

Article 3 – paragraph 2 – point a

Text proposed by the Commission

(a) the *offering* of goods or services to such data subjects in the Union; or

Amendment

(a) the *directing* of goods or services to such data subjects in the Union, *irrespective of whether these are provided free of charge in relation to the data subject or not*; or

Amendment 158

Morten Løkkegaard

Proposal for a regulation

Article 3 – paragraph 2 – point b

Text proposed by the Commission

Amendment

(b) the monitoring of their behaviour.

(b) monitoring the behaviour of such data subjects with a view to offering goods or services to them.

Anonymous data

CA5

eBay welcomes **CA 5 (Art. 4.2a)** on anonymous data that clarifies that this sort of data should not be considered personal data.

Right to be forgotten

eBay welcomes improvements that **CA 2 (Recital 53)** on the “Right to be forgotten” that was renamed to the “Right to erasure” in particular in recital 53. We welcome similar wording in **CA 8 (Art. 17)**. Nevertheless, the current wording could impose some additional burdens on businesses, in particular with the responsibility for the controllers for providing feedback to the data subject on the actions taken by third parties to delete data. More generally, once information is publicly available, we do not have any control over the way in which these data are treated by third parties – e.g. they may be transferred, duplicated, etc.

Data breach notification

eBay welcomes **CA 3** (Recital 67), and **CA 11** (Art.32.1) and in particular removal of 24 hours deadline mentioned in **CA 10 (Art. 31.1)** with regards to data breach notifications. However, data controllers should only notify data breaches that really matter, i.e. those breaches ‘which are likely to adversely affect the privacy of the data subject’ for notifications to DPAs. We would like to highlight that it will be difficult for the data controller to define “significantly” adverse impact.



Comments on IMCO draft opinion on the General Data Protection Regulation

EDRi welcomes the draft report, but would like to make some comments on selected proposed amendments below.

The left column repeats the Commission proposal; the right column contains the amendments proposed by the rapporteur. EDRi's comments can be found below. For ease of reading, the headings are highlighted:

- **green** for amendments which we welcome;
- **yellow** for amendments which pursue good aims, but could benefit from further suggested improvements;
- **red** for amendments which in our view should be reconsidered.

In each case, a short justification is given. We also provide short comments on some other amendments on which we do not have a strong position.

Amendment 1 Recital 13	
(13) The protection of individuals should be technologically neutral and not depend on the techniques used; otherwise this would create a serious risk of circumvention. The protection of individuals should apply to processing of personal data by automated means as well as to manual processing, if the data are contained or	(13) The protection of individuals should be technologically neutral and not depend on the techniques used; otherwise this would create a serious risk of circumvention. The protection of individuals should apply to processing of personal data by automated means as well as to manual processing, if the data are contained or

are intended to be contained in a filing system. <i>Files or sets of files as well as their cover pages, which are not structured according to specific criteria, should not fall within the scope of this Regulation.</i>	are intended to be contained in a filing system.
Comment: The Commission proposal echoes recital 27 of Directive 95/46/EC, while this amendment would put unsorted heaps of personal data into the scope, enlarging it significantly. If this is the desired change, then the material scope would need to be changed in Article 2(1) (in connection with Article 4(4)) as well.	

Amendment 2 Recital 13 a (new)	
	<i>(13 a) Technological neutrality should also mean that similar acts, in similar conditions and with similar consequences should be legally equivalent, with no regard of their happening online or offline, unless the diverse dynamics of data processing in such environments does not make a substantial difference</i>
Comment: It seems already clear that both on- and offline activities are covered by the regulation (see the short title of the proposal, as well as recital 13 and Article 2). If such clarification is needed, the word “not” in the last sentence, which seems to be typing mistake, should be removed, as it would actually weaken technological neutrality.	

Amendment 3 Proposal for a regulation Recital 23	
(23) The principles of protection should apply to any information concerning an identified or identifiable person. To determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the individual. The principles of data protection should not apply to data rendered anonymous in such a way that the	(23) The principles of protection should apply to any information concerning an identified or identifiable person. To determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the individual. The principles of data protection should not apply to data rendered anonymous in such a way that the

data subject is no longer identifiable.	data subject is no longer <i>directly</i> identifiable, <i>including, where possible, a separation of processed data from identity-revealing data. In the latter case, also pseudonymized data are useful if the key to link the pseudonymous with the identity is safe according to the state of the art.</i>
<p>Comment: This drastically restricts the scope and is a departure from the approach of Directive 95/46/EC. It should be noted that as long as pseudonymous data are in principle identifiable, they should be in the scope of the Regulation. This does of course not prejudice the use of pseudonymisation to increase the protection of individuals. Additionally, removing pseudonymous data from the scope would raise questions of consistency with Council of Europe Convention 108.</p>	

<p>Amendment 4 Proposal for a regulation Recital 23 a (new)</p>	
	<p><i>(23 a) A large amount of personal data might be processed for purposes of fraud detection and prevention. The pursuit of such claims, regulated by Member States' or Union law, should be taken into account when the data minimization principle and the lawfulness of processing are assessed.</i></p>
<p>Comment: It is not clear whether such a recital on anti-fraud measures is needed. If anti-fraud measures are legally mandated (e.g. anti-money-laundering), processing is already lawful under Art. 6(1)(c) (legal obligation on controller). If they are intended for the controller's own aims, 6(1)(f) on legitimate interests (providing barriers to excessive use), or consent under 6(1)(a) could apply. It should also be noted that the current data protection directive does not contain such a recital, which did not seem to hamper fraud detection and prevention. In our opinion this additional recital would bring more confusion than benefit.</p>	

Amendment 5
Proposal for a regulation

Recital 25

(25) Consent should be given explicitly by any appropriate method enabling a freely given specific and informed indication of the data subject's wishes, either by a statement or by a clear affirmative action by the data subject, ensuring that individuals are aware that they give their consent to the processing of personal data, including by ticking a box when visiting an Internet website or by any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data. Silence or inactivity should therefore not constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. If the data subject's consent is to be given following an electronic request, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.

(25) Consent should be given explicitly by any appropriate method enabling a freely given specific and informed indication of the data subject's wishes, either by a statement or by a clear affirmative action by the data subject, ensuring that individuals are aware that they give their consent to the processing of personal data, including by ticking a box when visiting an Internet website or by any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data. ***The consent can be implicit only when the data subject acts in such a way that a certain amount of personal data must necessarily be processed, for instance by asking for particular goods or services, and in such case the consent is referred only to the minimum necessary.*** Silence or inactivity should therefore not constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. If the data subject's consent is to be given following an electronic request, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.

Comment: This amendment seriously dilutes the concept of consent. It also confuses two different grounds for processing personal data: consent and existing contractual relationship. It is worth pointing out that consent is only one ground for lawfulness of data processing among several others. In fact, the situation described in the justification (life insurance) is already covered under Art.6(1)(b) (processing necessary for performance of contract), so there is no need for an exception here. Moreover, it should be noted that according to the principle of data minimisation, data processing (regardless of its legal grounds) should always be limited to the minimum necessary. Finally, the amount of data which is deemed necessary to the performance of a contract does not depend on the actions taken by the data subject (which is suggested in the amended recital) but on the essence and nature of the contract in question. See also the Article 29 Working Part opinion on consent, p. 7: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf and the comments on amendment 33 below.

Amendment 6
Proposal for a regulation
Recital 27

(27) The main establishment of a controller in the Union should be determined according to objective criteria and should imply the effective and real exercise of management activities determining the main decisions as to the purposes, conditions and means of processing through stable arrangements. This criterion should not depend whether the processing of personal data is actually carried out at that location; the presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute such main establishment and are therefore no determining criteria for a main establishment.
The main establishment of the processor should be the place of its central administration in the Union.

(27) The main establishment of a controller ***or a processor*** in the Union should be determined according to objective criteria and should imply the effective and real exercise of management activities determining the main decisions as to the purposes, conditions and means of processing through stable arrangements. This criterion should not depend whether the processing of personal data is actually carried out at that location; the presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute such main establishment and are therefore no determining criteria for a main establishment.

Comment: While consistency is indeed very important, there is a legal reason why the Commission drafted the recital this way: the ability to exercise “management activities determining the main decisions as to the purposes, conditions and means of processing through stable arrangements” is precisely what defines a controller (see Article 4(5) of the Proposal) as opposed to a processor. Processors do per definition not exercise such activities, so using the place where they take place for determining the main establishment does not work. The Commission proposal of using the central administration (and not the place where the processing actually takes place) for determining the main establishment of a processor yields results consistent with those of the procedure for controllers. See amendment 34 below for comments on the active text.

Amendment 7
Proposal for a regulation
Recital 27 a (new)

	<i>(27 a) The representative is liable, together with the controller, for any behaviour that is contrary to the present Regulation.</i>
Comment: This recital further stresses the representative's responsibility, consistent with Article 78(2).	

Amendment 8 Proposal for a regulation Recital 29	
(29) Children deserve specific protection of their personal data, as they may be less aware of risks, consequences, safeguards and their rights in relation to the processing of personal data. <i>To determine when an individual is a child, this Regulation should take over</i> the definition laid down by the UN Convention on the Rights of the Child.	(29) Children deserve specific protection of their personal data, as they may be less aware of risks, consequences, safeguards and their rights in relation to the processing of personal data. <i>At the same time, given the higher average technology-dependence of younger generations, a distinction shall be made between</i> the definition laid down by the UN Convention on the Rights of the Child <i>and the "minor age" criterion.</i>
Comment: This change is not absolutely necessary to create three groups of data subjects by age (children strictly speaking, other minors, adults), see below the comment on amendment 35.	

Amendment 9 Proposal for a regulation Recital 34	
(34) Consent should not provide a valid legal ground for the processing of personal data, where there is a clear imbalance between the data subject and the controller. This is especially the case where the data subject is in a situation of dependence from the controller, among others, where personal data are processed by the employer of employees' personal data in the employment context.	(34) Consent should not provide a valid legal ground for the processing of personal data, where there is a clear imbalance between the data subject and the controller. This is especially the case where the data subject is in a situation of dependence from the controller, among others, where personal data are processed by the employer of employees' personal data in the employment context.

<p>Where the controller is a public authority, there would be an imbalance only in the specific data processing operations where the public authority can impose <i>an</i> obligation by virtue of its relevant public powers and the consent cannot be deemed as freely given, taking into account the interest of the data subject.</p>	<p>Where the controller is a public authority, there would be an imbalance only in the specific data processing operations where the public authority can impose <i>a new and unjustified</i> obligation by virtue of its relevant public powers and the consent cannot be deemed as freely given, taking into account the interest of the data subject.</p>
---	--

Comment: Restricting the application to newly established obligations would create two different levels of protection: a lower one for processing operations related to existing obligations and a higher one for newly established ones. Such a grandfathering clause would impede consistent protection of personal data. Moreover, adding an additional and quite judgemental criterion, i.e. that such new obligation be “unjustified”, will lead to interpretative doubts and limit the application of this principle. Similar to the comment on amendment 5, it should be noted that consent is only of several grounds for lawfulness. For instance, the example given in the justification would be covered under Article 6(1)(e) in any case. For processing by public authorities, this provision, as well as Article 6(1)(c) are often more pertinent than consent.

Amendment 10
Proposal for a regulation
Recital 49

<p>(49) The information in relation to the processing of personal data relating to the data subject should be given to them at the time of collection, or, where the data are not collected from the data subject, within a reasonable period, depending on the circumstances of the case. Where data can be legitimately disclosed to another recipient, the data subject should be informed when the data are first disclosed to the recipient.</p>	<p>(49) The information in relation to the processing of personal data relating to the data subject should be given to them at the time of collection, or, where the data are not collected from the data subject, within a reasonable period, depending on the circumstances of the case. Where data can be legitimately disclosed to another recipient, the data subject should be informed when the data are first disclosed to the recipient. <i>At the same time, no processing other than storing should be allowed before the data subject is fully aware of the information referred to here.</i></p>
---	---

Comment: This amendment helps to protect data subject rights for data collected from third sources. See also below comment on amendment 39.

Amendment 11
Proposal for a regulation
Recital 53

(53) Any person should have the right to have personal data concerning them rectified and *a* ‘right to *be forgotten*’ where the retention of such data is not in compliance with this Regulation. In particular, data subjects should have the right that their personal data are erased and no longer processed, where the data are no longer necessary in relation to the purposes for which the data are collected or otherwise processed, where data subjects have withdrawn their consent for processing or where they object to the processing of personal data concerning them or where the processing of their personal data otherwise does not comply with this Regulation. This right is particularly relevant, when the data subject has given their consent as a child, when not being fully aware of the risks involved by the processing, and later wants to remove such personal data especially on the Internet. However, the further retention of the data should be allowed where it is necessary for historical, statistical and scientific research purposes, for reasons of public interest in the area of public health, for exercising the right of freedom of expression, when required by law or where there is a reason to restrict the processing of the data instead of erasing them.

(53) Any person should have the right to have personal data concerning them rectified and *the* right to *have such personal data erased* where the retention of such data is not in compliance with this Regulation. In particular, data subjects should have the right that their personal data are erased and no longer processed, where the data are no longer necessary in relation to the purposes for which the data are collected or otherwise processed, where data subjects have withdrawn their consent for processing or where they object to the processing of personal data concerning them or where the processing of their personal data otherwise does not comply with this Regulation. This right is particularly relevant, when the data subject has given their consent as a child, when not being fully aware of the risks involved by the processing, and later wants to remove such personal data especially on the Internet. However, the further retention of the data should be allowed where it is necessary for historical, statistical and scientific research purposes, for reasons of public interest in the area of public health, for exercising the right of freedom of expression, when required by law or where there is a reason to restrict the processing of the data instead of erasing them.

Comment:

Amendment 12

Proposal for a regulation

Recital 54

(54) To strengthen the ‘right to *be forgotten*’ in the online environment, *the right to erasure* should also be extended in such a way that a controller who has *made* the personal data public should be obliged to inform third parties which are processing such data that a data subject requests them to erase any links to, or copies or replications of that personal data. To ensure this information, the controller should take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible. In relation to a third party publication of personal data, the controller should be considered responsible for the publication, where the controller has authorised the publication by the third party.

(54) To strengthen the right to *erasure* in the online environment, *such* right should also be extended in such a way that a controller who has *transferred* the personal data *or made them* public *without being instructed to do so by the data subject* should be obliged to inform third parties which are processing such data that a data subject requests them to erase any links to, or copies or replications of that personal data. To ensure this information, the controller should take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible. In relation to a third party publication of personal data, the controller should be considered responsible for the publication, where the controller has authorised the publication by the third party.

Comment: See below comment on amendment 46.

Amendment 13

Proposal for a regulation

Recital 55 a (new)

(55 a) In partial derogation to the principle set out in the previous recital, account must be taken of the cases where the personal data collected represent, for the relevance of such personal data that might be only internal to the controller, property of the data controller. In such cases, if the processed data are meaningless for the data subject, the data controller should have no obligation of portability.

Comment: Article 18, which this recital relates to, serves two related purposes:

- (1) Strengthening the right of access by mandating that data be provided in a commonly used electronic format if they have been processed using such a format.
- (2) Strengthening control over data by mandating that data provided by the DS and processed in an automated system on the basis of contract or consent can be transferred to another automated system.

This recital does not differentiate between these two aspects and could therefore be abused to frustrate the right of access (see also below comments on amendment 49). Moreover, this recital attempts at creating a dangerous limitation on the right to data portability, namely introduces the criterion of “ownership” and “meaningfulness” from the data subject's perspective. Neither of this criteria should be relied on in order to limit data portability if data subject wishes to have his/her data transferred to another automated system.

Amendment 14
Proposal for a regulation
Recital 55 b (new)

(55 b) Some personal data, once processed by the data controller or processor, produce outcomes that are used only internally by the data controller and whose format is meaningless even for the data subject. In this case, the right to data portability should not apply, while the other rights, in particular the right to object and the right of access and the right to rectification, are still valid.

Comment: Recital 55 and Article 18 only mandate using a “commonly used format” for access if such a format is already used by the controller for its own processing. Providing the data in the format used by the controller itself does not create an additional administrative burden, but helps to curtail situations in which controllers provide information in a format which is less useful to the data subject than the format the controller itself uses. Again, this amendment does not clearly distinguish between the right of access and the right to data portability; see also the comments on amendments 13 and 49.

Amendment 15

Proposal for a regulation

Recital 58

(58) Every natural person should have the right not to be subject to a measure which is based on profiling by means of automated processing. However, such measure should be **allowed** when expressly **authorised** by law, carried out in the course of entering or performance of a contract, or when the data subject has **given** his consent. In any case, such processing should be subject to suitable safeguards, including specific information of the data subject and the right to obtain human intervention and that such measure should not concern a child.

(58) Every natural person should have the right not to be subject to a measure which is based on profiling by means of automated processing. However, such measure should be **forbidden only** when expressly **stated** by law, **not** carried out in the course of entering or performance of a contract, or when the data subject has **withdrawn** his consent. In any case, such processing should be subject to suitable safeguards, including specific information of the data subject and the right to obtain human intervention and that such measure should not concern a child. ***The data subject, when this profiling is not necessary for entering or performing a contract, should always have the possibility to opt-out.***

Comment: This amendment further dilutes an already weak and imperfect provision on profiling. It goes exactly to the contrary of what EDRI perceived as consumer (citizen) needs in information society. Profiling has already become one of the main challenges for data and privacy protection and this trend will not be reversed. While the Commission at least noted this problem and suggested a way to limit the risks related to widespread use of profiling, the proposed amendment renders this attempt meaningless. Reversing the approach to profiling is also a departure from the approach of Article 19 of the current Directive 95/46/EC. The wording proposed by the Commission already leaves ample room for exceptions; further extending these, especially by changing to an opt-out approach would hamper DS rights, especially since they might not be aware of the profiling taking place in the first place. It should also be noted that the notions of “withdrawn” consent and opt-out seem to imply implicit consent in the first place, a notion that is not fully consistent with the existing and the proposed legal framework. Additionally, it should be noted that under the amended ePrivacy Directive (2002/58/EC as amended by 2009/136/EC), opt-in is already required for cookies, which are the most common means used for online profiling. See also below comments on amendments 51 and 53.

Amendment 16

Proposal for a regulation

Recital 61 a (new)

	<p><i>(61 a) Data protection by design is a very useful tool as it allows the data subject to be fully in control of his own data protection, of the information he shares and with the subject with whom he shares. When considering this principle as well as data protection by default, the context should heavily influence the assessment of lawfulness of processing.</i></p>
<p>Comment: See comments on amendment 55 below.</p>	

<p>Amendment 17 Proposal for a regulation Recital 63</p>	
<p>(63) Where a controller not established in the Union is processing personal data of data subjects residing in the Union whose processing activities are related to the offering of goods or services to such data subjects, or to the monitoring their behaviour, the controller should designate a representative, unless the controller is established in a third country ensuring an adequate level of protection, or the controller is a <i>small or medium sized enterprise or a</i> public authority or body or where the controller is only occasionally offering goods or services to such data subjects. The representative should act on behalf of the controller and may be addressed by any supervisory authority.</p>	<p>(63) Where a controller not established in the Union is processing personal data of data subjects residing in the Union whose processing activities are related to the offering of goods or services to such data subjects, or to the monitoring their behaviour, the controller should designate a representative, unless the controller is established in a third country ensuring an adequate level of protection, or the controller is a public authority or body or where the controller is only occasionally offering goods or services to such data subjects. The representative should act on behalf of the controller and may be addressed by any supervisory authority.</p>
<p>Comment: This amendment would increase the accountability of controllers based in 3rd countries; see also below comment on amendment 57.</p>	

Amendment 18
Proposal for a regulation

Recital 67

(67) A personal data breach may, if not addressed in an adequate and timely manner, result in substantial economic loss and social harm, including identity fraud, to the individual concerned. Therefore, ***as soon as the controller becomes aware that such a breach has occurred***, the controller should notify the breach to the supervisory authority without undue delay ***and, where feasible, within 24 hours. Where this cannot be achieved within 24 hours, an explanation of the reasons for the delay should accompany the notification***. The individuals whose personal data could be adversely affected by the breach should be notified without undue delay in order to allow them to take the necessary precautions. A breach should be considered as adversely affecting the personal data or privacy of a data subject where it could result in, for example, identity theft or fraud, physical harm, significant humiliation ***or*** damage to reputation. The notification should describe the nature of the personal data breach as well as recommendations as well as recommendations for the individual concerned to mitigate potential adverse effects. Notifications to data subjects should be made as soon as reasonably feasible, and in close cooperation with the supervisory authority and respecting guidance provided by it or other relevant authorities (e.g. law enforcement authorities). For example, the chance for data subjects to mitigate an immediate risk of harm would call for a prompt notification of data subjects whereas the need to implement appropriate measures against continuing or similar data breaches may justify a longer delay.

(67) A personal data breach may, if not addressed in an adequate and timely manner, result in substantial economic loss and social harm, including identity fraud, to the individual concerned. Therefore, ***addressing such economic loss and social harm should be the first and utmost priority. After that***, the controller should notify the breach to the supervisory authority without undue delay. The individuals whose personal data could be adversely affected by the breach should be notified without undue delay in order to allow them to take the necessary precautions. A breach should be considered as adversely affecting the personal data or privacy of a data subject where it could result in, for example, identity theft or fraud, physical harm, significant humiliation, damage to reputation ***or money loss***. The notification ***to the supervisory authority*** should describe the nature of the personal data breach as well as recommendations as well as recommendations for the individual concerned to mitigate potential adverse effects. Notifications to data subjects should be made as soon as reasonably feasible, and in close cooperation with the supervisory authority and respecting guidance provided by it or other relevant authorities (e.g. law enforcement authorities). For example, the chance for data subjects to mitigate an immediate risk of harm would call for a prompt notification of data subjects whereas the need to implement appropriate measures against continuing or similar data breaches may justify a longer delay.

Comment: The intention of the amendment is laudable, but it opens a door for controllers to delay notification by claiming to focus on fixing the breach first. However, taking measures to contain and mitigate the breach and the requirements for notifying the DPA within a set amount

of time go hand in hand: once a breach has been notified to the DPA, its follow-up actions will in turn increase pressure on the controller to fix the breach. Removing the clear time limit (and the need for a justification if it is exceeded) would reduce the perceived urgency of fixing breaches from the controllers' point of view. Additionally, it should be noted that a lot of the information required in the notification is in fact related to measures taken to contain or mitigate the breach, so that "fixing vs. notifying" becomes a false dichotomy, because the strict deadline for controllers to notify the breach in fact forces them to address the breach and notify quickly.

See also the comment on amendments 62 and 63 below

Amendment 19
Proposal for a regulation

Recital 69

(69) In *setting detailed rules concerning the format and procedures applicable to* the notification of personal data breaches, due consideration should be given to the circumstances of the breach, including whether or not personal data had been protected by appropriate technical protection measures, effectively limiting the likelihood of identity fraud or other forms of misuse. Moreover, such rules and procedures should take into account the legitimate interests of law enforcement authorities in cases where early disclosure could unnecessarily hamper the investigation of the circumstances of a breach.

(69) In *assessing the level of detail of* the notification of personal data breaches, due consideration should be given to the circumstances of the breach, including whether or not personal data had been protected by appropriate technical protection measures, effectively limiting the likelihood of identity fraud or other forms of misuse. Moreover, such rules and procedures should take into account the legitimate interests of law enforcement authorities in cases where early disclosure could unnecessarily hamper the investigation of the circumstances of a breach.

Comment: Empowering the Commission to set detailed rules on breach notifications could contribute to a consistent application of the regulation.

Amendment 20
Proposal for a regulation

Recital 75

(75) Where the processing is carried out in the public sector or where, in the private sector,

(75) Where the processing is carried out in the public sector or where, in the private sector,

<p>processing is carried out by a large enterprise, or where its core activities, regardless of the size of the enterprise, involve processing operations which require regular and systematic monitoring, a person should assist the controller or processor to monitor internal compliance with this Regulation. Such data protection officers, whether or not an employee of the controller, should be in a position to perform their duties and tasks independently.</p>	<p>processing is carried out by an enterprise whose core activities, regardless of the size of the enterprise, involve processing operations which require regular and systematic monitoring, a person should assist the controller or processor to monitor internal compliance with this Regulation. Such data protection officers, whether or not an employee of the controller, should be in a position to perform their duties and tasks independently.</p>
<p>Comment: Also when regular and systematic monitoring is not a controller's core business, compliance with data protection requirements is important. Data Protection Officers (DPOs) are a proven organisational measure to increase this compliance. While appointing a DPO entails a certain amount of administrative burden, the higher number of data subjects (employees, customers, etc.) who would be affected by non-compliance by a large controller justifies this. Already now, some Member States demand the appointment of a DPO for significantly smaller enterprises. See also below the comments on amendments to 67 to 69.</p>	

<p>Amendment 21 Proposal for a regulation Recital 97</p>	
<p>(97) Where the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union takes place in more than one Member State, one single supervisory authority should be competent for monitoring the activities of the controller or processor throughout the Union and taking the related decisions, in order to increase the consistent application, provide legal certainty and reduce administrative burden for such controllers and processors.</p>	<p>(97) Where the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union takes place in more than one Member State, one single supervisory authority should be competent for monitoring the activities of the controller or processor throughout the Union and taking the related decisions, in order to provide legal certainty and reduce administrative burden for such controllers and processors.</p>
<p>Comment: While it is true that the one-stop-shop does not necessarily improve consistency between DPAs, it increases consistency seen from the controller's point of view, as its subsidiaries in different MS are all supervised by the same DPA.</p>	

Amendment 22
Proposal for a regulation
 Recital 105

(105) In order to ensure the consistent application of this Regulation throughout the Union, a consistency mechanism for co-operation between the supervisory authorities themselves and the Commission should be established. This mechanism should in particular apply where a supervisory authority intends to take a measure as regards processing operations that are related to the offering of goods or services to data subjects in several Member States, , or to the monitoring such data subjects, or that might substantially affect the free flow of personal data. It should also apply where any supervisory authority or the Commission requests that the matter should be dealt with in the consistency mechanism. This mechanism should be without prejudice to any measures that the Commission may take in the exercise of its powers under the Treaties.

(105) In order to ensure the consistent application of this Regulation throughout the Union, a consistency mechanism for co-operation between the supervisory authorities themselves and the Commission should be established. This mechanism should in particular apply where a supervisory authority intends to take a measure as regards processing operations that are related to the offering of goods or services to data subjects in several Member States, or to the monitoring *of* such data subjects, or that might substantially affect the free flow of personal data. It should also apply where any supervisory authority or the Commission requests that the matter should be dealt with in the consistency mechanism. ***Furthermore, the data subjects should have the right to obtain consistency, if they deem a measure by a Data Protection Authority of a Member State has not fulfilled this criterion.*** This mechanism should be without prejudice to any measures that the Commission may take in the exercise of its powers under the Treaties.

Comment: See comments on amendment 74 below.

Amendment 23
Proposal for a regulation
 Recital 111

(111) Every data subject should have the right to lodge a complaint with a supervisory authority in any Member State and have the right to a judicial remedy if they consider that their rights under this Regulation are infringed

(111) Every data subject should have the right to lodge a complaint with a supervisory authority in any Member State and have the right to a judicial remedy if they consider that their rights under this Regulation are infringed

or where the supervisory authority does not react on a complaint or does not act where such action is necessary to protect the rights of the data subject.	or where the supervisory authority does not react on a complaint or does not act where such action is necessary to protect the rights of the data subject. <i>If the data subject deems consistency is not fulfilled, a complaint to the European Data Protection Board can be filed.</i>
Comment: see comments on amendments 74, 78, and 79 below.	

Amendment 24 Proposal for a regulation Recital 112	
(112) Any body, organisation or association which aims to protect the rights and interests of <i>data subjects in relation to the protection of their data and is constituted according to the law of a Member State</i> should have the right to lodge a complaint with a supervisory authority or exercise the right to a judicial remedy on behalf of data subjects, or to lodge, independently of a data subject's complaint, an own complaint where it considers that a personal data breach has occurred.	(112) Any body, organisation or association which aims to protect the rights and interests of <i>citizens</i> should have the right to lodge a complaint with a supervisory authority or exercise the right to a judicial remedy on behalf of data subjects, or to lodge, independently of a data subject's complaint, an own complaint where it considers that a personal data breach has occurred.
Comment: Enlarging the range of those bodies, organisations and associations entitled to lodge complaints with DPAs can contribute to wider use of collective redress mechanisms. Relaxing the criterion of being “established according to the law of a Member State” would increase the range of bodies, organizations and associations entitled to bring complaints to informal associations and entities constituted in third states. See also amendment 76 below.	

Amendment 25 Proposal for a regulation Recital 113	
(113) Each natural or legal person should have the right to a judicial remedy against decisions	(113) Each natural or legal person should have the right to a judicial remedy against decisions

<p>of a supervisory authority concerning them. Proceedings against a supervisory authority should be brought before the courts of the Member State, where the supervisory authority is established.</p>	<p>of a supervisory authority concerning them. Proceedings against a supervisory authority should be brought before the courts of the Member State, where the supervisory authority is established, <i>or before the European Data Protection Board on grounds of inconsistency with the application of the present Regulation in other Member States</i></p>
<p>Comment: See comments on amendments 74 below.</p>	

<p>Amendment 26 Proposal for a regulation Recital 114</p>	
<p>(114) In order to strengthen the judicial protection of the data subject in situations where the competent supervisory authority is established in another Member State than the one where the data subject is residing, the data subject may request any body, organisation or association aiming to protect the rights and interests of <i>data subjects in relation to the protection of their data</i> to bring on the data subject's behalf proceedings against that supervisory authority to the competent court in the other Member State.</p>	<p>(114) In order to strengthen the judicial protection of the data subject in situations where the competent supervisory authority is established in another Member State than the one where the data subject is residing, the data subject may request any body, organisation or association aiming to protect the rights and interests of <i>citizens</i> to bring on the data subject's behalf proceedings against that supervisory authority to the competent court in the other Member State.</p>
<p>Comment: See comments on amendment 24 above and 76 below.</p>	

<p>Amendment 27 Proposal for a regulation Recital 120</p>	
---	--

<p>(120) In order to strengthen and harmonise administrative sanctions against infringements of this Regulation, each supervisory authority should have the power to sanction administrative offences. This Regulation should indicate these offences and the upper limit for the related administrative fines, which should be fixed in each individual case proportionate to the specific situation, with due regard in particular to the nature, gravity and duration of the breach. The consistency mechanism may also be used to cover divergences in the application of administrative sanctions.</p>	<p>(120) In order to strengthen and harmonise administrative sanctions against infringements of this Regulation, each supervisory authority should have the power to sanction administrative offences. This Regulation should indicate these offences and the upper limit for the related administrative fines, which should be fixed in each individual case proportionate to the specific situation, with due regard in particular to the nature, gravity and duration of the breach. <i>In order to strengthen the internal market, the administrative sanctions should be consistent across Member States.</i> The consistency mechanism may also be used to cover divergences in the application of administrative sanctions.</p>
<p>Comment: While a level playing field in the internal market is desirable, such a provision would raise several problems: (1) it is not clear how this could be reconciled with the independence of DPAs; (2) there may very well be differences between the amounts needed to be effective and dissuasive.</p> <p>See also below comments on amendment 79.</p>	

<p>Amendment 28 Proposal for a regulation Recital 122</p>	
<p>(122) The processing of personal data concerning health, as a special category of data which deserves higher protection, may often be justified by a number of legitimate reasons for the benefit of individuals and society as a whole, in particular in the context of ensuring continuity of cross-border healthcare. Therefore this Regulation should provide for harmonised conditions for the processing of personal data concerning health, subject to specific and suitable safeguards so as to protect the fundamental rights and the personal data of</p>	<p>(122) The processing of personal data concerning health, as a special category of data which deserves higher protection, may often be justified by a number of legitimate reasons for the benefit of individuals and society as a whole, in particular in the context of ensuring continuity of cross-border healthcare. Therefore this Regulation should provide for harmonised conditions for the processing of personal data concerning health, subject to specific and suitable safeguards so as to protect the fundamental rights and the personal data of</p>

individuals. This includes the right for individuals to have access to their personal data concerning their health, for example the data in their medical records containing such information as diagnosis, examination results, assessments by treating physicians and any treatment or interventions provided.	individuals. This includes the right for individuals to have access, <i>directly or through previously delegated persons</i> , to their personal data concerning their health, for example the data in their medical records containing such information as diagnosis, examination results, assessments by treating physicians and any treatment or interventions provided.
Comment: Following the justification for this amendment, the possibility of delegation could be narrowed to cases in which this has been (1) previously delegated and (2) the DS is currently unable to exercise those rights herself.	

Amendment 29 Proposal for a regulation Recital 122 a (new)	
	<i>(122 a) A professional who process personal data concerning health should receive, if possible, anonymized or pseudonymized data, leaving the knowledge of the identity only to the General Practitioner or to the Specialist who has requested such data processing.</i>
Comment: This amendment further stresses the general requirement of data minimization.	

Amendment 30 Proposal for a regulation Article 3 – paragraph 2 – point a	
(a) the offering of goods <i>or</i> services to such data subjects in the Union; <i>or</i>	(a) the offering of goods <i>and</i> services to such data subjects in the Union, <i>including services provided without financial costs to the individual, or;</i>
Comment: While such services would also be covered under the Commission proposal, this amendment would further clarify this. However, it would technically exclude goods offered for free (which would be covered under Commission’s proposed wording).	

Amendment 31
Proposal for a regulation
Article 4 – paragraph 1 – point 1

(1) ‘data subject’ means an identified natural person or a natural person who can be identified, directly or indirectly, by ***means reasonably likely to be used by*** the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;

(1) ‘data subject’ means an identified natural person or a natural person who can be identified, directly or indirectly, by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. ***In order to determine whether a person can be identified, account should be taken of:***

a) the means likely reasonably to be used by the controller or any other natural or legal person who accesses the data to identify such a person and

b) the measures that the controller or the processor has put in place in order to prevent the information from fully identifying a natural person

A natural person is "indirectly identifiable" when the data processed allows the controller to solely individualise one person from another and the controller cannot verify its identity.

Comment: As mentioned above in the comments on amendment 3, this would be a departure from the proven concept of data subject. Introducing the additional category of “indirectly identifiable” data subject is not helpful, since for many applications (e.g. targeted advertising), “direct identification” is not needed; in these cases, the amendment would reduce the protection afforded to individuals.

Amendment 32
Proposal for a regulation
Article 4 – paragraph 1 – point 2

(2) ‘personal data’ means *any* information relating to *a* data subject;

(2) ‘personal data’ means information relating to *an identifiable* data subject;

Comment: this follows from amendment 31 (as with the wording proposed by the Commission, data subjects are by definition identifiable) and would exclude data on “indirectly identifiable” persons from the scope. This would unduly restrict the protection offered by the Regulation.

Amendment 33
Proposal for a regulation
Article 4 – paragraph 1 – point 8

(8) ‘the data subject’s consent’ means any freely given specific, informed and explicit indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed;

(8) ‘the data subject’s consent’ means any freely given specific, informed and explicit indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed; *by 'clear affirmative action' is meant any unequivocal action that is the result of a choice and that implies, for its complete execution, a necessary data processing;*

Comment: This amendment would create a category of situations in which consent is assumed and inferred from the action taken by the data subject, thus diluting the concept. In our opinion the protection of consumer (citizen) interests would require quite the opposite amendment, i.e. stressing the fact that informed consent can never be interpreted from behaviour that is not an explicit indication of wishes. It should also be kept in mind that consent is only one of several possible reasons for lawful processing. The situation envisaged in the justification (if processing personal data is strictly necessary for the provision of a good or a service, requiring such good or service can be considered as an explicit indication of wishes) is essentially equivalent to “processing that is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering a contract”, which is already a reason for lawfulness under Article 6(1)(b). Consequently, there is no need to change the definition of “consent”. See also the Article 29 Working Part opinion on consent, p. 7: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion->

[recommendation/files/2011/wp187_en.pdf](https://ec.europa.eu/digital-single-market/en/recommendation/files/2011/wp187_en.pdf), as well as the comments on amendment 5 above.

Amendment 34
Proposal for a regulation
Article 4 – paragraph 1 – point 13

(13) ‘main establishment’ means *as regards* the controller, *the place of* its establishment in the Union where the main decisions as to the purposes, conditions and means of the processing of personal data are taken; if no decisions as to the purposes, conditions and means of the processing of personal data are taken in the Union, the main establishment is the place where the main processing activities in the context of the activities of an establishment of a controller in the Union take place. *As regards the processor, ‘main establishment’ means the place of its central administration in the Union;*

(13) ‘main establishment’ means *the place where* the controller *or the processor has* its establishment in the Union where the main decisions as to the purposes, conditions and means of the processing of personal data are taken; if no decisions as to the purposes, conditions and means of the processing of personal data are taken in the Union, the main establishment is the place where the main processing activities in the context of the activities of an establishment of a controller *or a processor* in the Union take place.

Comment: As mentioned in the comments on amendment 6 above, there is a legal reason for the Commission to draft this provision in this way: as a processor is per definition not able to take “main decisions as to the purposes, conditions and means of the processing of personal data”, the place where such decisions take place cannot be used as a criterion to determine the main establishment. Following the logic that the place where decisions are made and not the physical site of the processing matters, using the central administration as the main establishment is an appropriate solution.

Amendment 35
Proposal for a regulation
Article 4 – paragraph 1 – point 18

(18) ‘child’ means any person below the age of **18** years;

(18) ‘child’ means any person below the age of **14** years;

Comment: While it is true that further differentiation between minors of different ages could be

helpful to address the different issues faced by them, this amendment would simply remove all additional protections from minors aged 14 to 17 and treat them as adults, unless a separate category of “minor persons” would be introduced.

In fact, the COM proposal already contains a distinction between two categories of minors:

- (1) Processing personal data of children below the age of 13 is prohibited under Article 8(1) unless the parents/custodians give or authorise consent (this provision is partly meant to provide consistency with US law);
- (2) For all minors, recitals 38, 46, 53 and 58 as well as Articles 6(1)(f), 11(2), 17(1), 33(2)(d) and 38(1)(e) need to be taken into account when offering services to them; these do not prohibit the offering of online services to such minors, but provide for some additional safeguards.

This approach allows offering information society services to minors, while also providing for appropriate safeguards, taking into their age into account.

Amendment 36
Proposal for a regulation
Article 6 – paragraph 5

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the conditions referred to in point (f) of paragraph 1 for various sectors and data processing situations, including as regards the processing of personal data related to a child.

deleted

Comment: Given that the point referred to contains two assessments to be made (on the balance between (a) controllers’ interests and (b) data subjects’ interests and fundamental rights and freedoms for adults and minors separately), it could be helpful to delegate to the Commission the power to further specify these conditions, as else there could be a risk of incoherent application of the regulation in different MS, which could impede on the functioning of the internal market.

Amendment 37

**Proposal for a regulation
Article 7 – paragraph 3**

3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. ***If the consent is still necessary for the execution of a contract, its withdrawal implies the willingness to terminate the contract.***

Comment: It should be noted that consent is not the only reason for lawfulness of processing. Necessity of processing for the performance of a contract is an independent reason for lawfulness (see Article 6(1)(b)), so no consent would be necessary in the example given in the justification. In the light of this, it would not be advisable to dilute the concept of consent; please see also the comments on amendments 5 and 33 for similar issues. The proposed amendment is not only unnecessary, as explained above, but dangerous as it may be interpreted as a justification for making the conclusion of the contract conditional upon obtaining consent for data processing (“forced consent”), while this tendency should be perceived as harmful and infringing data protection standards. As long as data is necessary for the conclusion or execution of the contract, such data can be processed without consent. At the same time data subject's consent for the processing of additional data cannot be treated as condition of obtaining a given good or a service.

**Amendment 38
Proposal for a regulation
Article 13 – paragraph 1**

The controller shall communicate any rectification or erasure carried out in accordance with Articles 16 and 17 to each recipient to whom the data have been disclosed, ***unless this proves impossible or involves a disproportionate effort.***

Any rectification or erasure carried out in accordance with Articles 16 and 17 ***is extended*** to each recipient to whom the data have been disclosed ***without the control of the data subject.***

Comment: This amendment would reduce the enforcement of data subject rights in situations where data have been transferred to third parties. It would for example exclude data shared with third parties for direct marketing purposes if the data subject (possibly unwittingly) consented.

Also, data subjects may forget that they authorised such a transfer, while on the other hand the controller would need to store proof of the authorisation to prove the lawfulness of the transfer. In the light of this, the Commission proposal provides a way to safeguard data subject rights while at the same time providing a hedge against disproportionate efforts.

Amendment 39
Proposal for a regulation
Article 14 – paragraph 4 – point b

(b) where the personal data are not collected from the data subject, at the time of the recording or within a reasonable period after the collection, having regard to the specific circumstances in which the data are collected or otherwise processed, or, if a disclosure to another recipient is envisaged, **and** at the latest when the data are first disclosed.

(b) where the personal data are not collected from the data subject, at the time of the recording or within a reasonable period after the collection, having regard to the specific circumstances in which the data are collected or otherwise processed, or, if a disclosure to another recipient is envisaged; at the latest, **either** when the data are first disclosed **or when they are first processed, according to which occurs first.**

Comment: “processing” as defined in Article 4(3) includes collecting and storing, so this amendment would require information at the moment of collection. This would impose a stricter standard in case disclosure is envisaged.

Amendment 40
Proposal for a regulation
Article 14 – paragraph 5 – point b

(b) the data are not collected from the data subject and the provision of such information proves impossible or would involve a disproportionate effort; or

(b) the data are **meant to serve solely the purposes of art. 83, are** not collected from the data subject and the provision of such information proves impossible or would involve a disproportionate effort; or

Comment: This amendment limits the use of exceptions to data subject rights.

Amendment 41
Proposal for a regulation
Article 14 – paragraph 7

7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria for categories of recipients referred to in point (f) of paragraph 1, the requirements for the notice of potential access referred to in point (g) of paragraph 1, the criteria for the further information necessary referred to in point (h) of paragraph 1 for specific sectors and situations, and the conditions and appropriate safeguards for the exceptions laid down in point (b) of paragraph 5. In doing so, the Commission shall take the appropriate measures for micro, small and medium-sized-enterprises.

deleted

Comment: Point (h) of Article 14(1) could indeed benefit from further guidance.

Amendment 42
Proposal for a regulation
Article 15 – paragraph 1 – point d

(d) the period for which the personal data will be stored;

(d) the period for which the personal data will be stored ***and the time of collection;***

Comment: In principle this could be a good addition, but it could rather go under point (g) of the same Article, as the date of collection would well complement information on the source of the data.

Additionally, the justification for the amendment links providing the date of collection to proving consent, which according to recital 32 is in any case incumbent on the controller. Here, it should be noted that the obligation to prove consent if it is used as the reason for lawfulness is independent from access rights.

Amendment 43
Proposal for a regulation
Article 15 – paragraph 1 – subparagraph 1 (new)

(i) on request, and free of charge, the data controller shall also provide a proof of the lawfulness of processing in a reasonable time;

Comment: While the idea is good (and seems to be inspired by Article 11(1)(i) of Regulation 45/2001: “(i) the legal basis of the processing operation for which the data are intended,”), the wording could be improved. Replacing “proof of” by “reasons for” would reflect the fact that in the end, determination of lawfulness is left to the Courts.

Amendment 44
Proposal for a regulation
Article 15 – paragraph 3

3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the communication to the data subject of the content of the personal data referred to in point (g) of paragraph 1.

deleted

Comment:

Amendment 45
Proposal for a regulation
Article 17 – title

Right to *be forgotten and to* erasure

Right to erasure

Amendment 46
Proposal for a regulation
Article 17 – paragraph 2

2. Where the controller referred to in paragraph 1 has *made* the personal data public, it shall take all reasonable steps, *including technical measures*, in relation to data for the publication of which the controller is responsible, to inform third parties which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data. Where the controller has authorised a third party publication of personal data, the controller shall be considered responsible for that publication.

2. Where the controller referred to in paragraph 1 has *transferred* the personal data, *or has made such data* public *without being clearly instructed by the data subject to do so*, it shall take all reasonable steps in relation to data for the publication of which the controller is responsible, to inform third parties which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data. Where the controller has authorised a third party publication of personal data, the controller shall be considered responsible for that publication.

Comment: The inclusion of transfers here mostly duplicates existing obligations under Article 13, while adding “without being clearly instructed to do so” reduces the scope of the obligations under this Article. In any case, extreme care should be taken to reconcile the requirements under Article 17 with the freedom of expression. See on this also the opinion of the Fundamental Rights Agency (<http://fra.europa.eu/sites/default/files/fra-opinion-data-protection-oct-2012.pdf>)

Amendment 47
Proposal for a regulation
Article 17 – paragraph 9

9. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying:

(a) the criteria and requirements for the application of paragraph 1 for

deleted

<p><i>specific sectors and in specific data processing situations;</i></p> <p><i>(b) the conditions for deleting links, copies or replications of personal data from publicly available communication services as referred to in paragraph 2;</i></p> <p><i>(c) the criteria and conditions for restricting the processing of personal data referred to in paragraph 4.</i></p>	
<p>Comment:</p>	

<p>Amendment 48 Proposal for a regulation Article 18 – paragraph 3</p>	
<p><i>3. The Commission may specify the electronic format referred to in paragraph 1 and the technical standards, modalities and procedures for the transmission of personal data pursuant to paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</i></p>	<p><i>deleted</i></p>
<p>Comment:</p>	

<p>Amendment 49 Proposal for a regulation Article 18 – paragraph 3 a (new)</p>	
	<p><i>3 a. Where the processed data are, at least partially, meaningless for the data subject,</i></p>

	<i>the obligations following from the present article do not apply,</i>
<p>Comment: As mentioned above in the comments on amendments 13 and 14, this amendment conflates two different aspects of this Article. The obligation under Article 18(1) to provide data in a commonly readable format further safeguards the right to access (by adding this requirement, which is absent from Article 15(2)). Article 18(2) in turn only applies to data provided by the DS. It is not clear how this data might be “meaningless” to the data subject. In any case, the term “meaningless” is unclear and would only cause confusion.</p>	

<p>Amendment 50 Proposal for a regulation Article 19 – paragraph 3</p>	
<p>3. Where an objection is upheld pursuant to paragraphs 1 and 2, the controller shall no longer use or otherwise process the personal data concerned.</p>	<p>3. Where an objection is upheld pursuant to paragraphs 1 and 2, the controller shall no longer use, <i>store</i> or otherwise process the personal data concerned.</p>
<p>Comment: As the justification states, this is for clarification, since strictly speaking “storing” is processing.</p>	

<p>Amendment 51 Proposal for a regulation Article 20 – paragraph 1</p>	
<p><i>1. Every natural person shall have the right not to be subject to a measure which produces legal effects concerning this natural person or significantly affects this natural person, and which is based solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour.</i></p>	<p><i>Deleted</i></p>

Comment: Given the adverse effects profiling can have on data subjects and the risks for discrimination inherent in such measures, upholding a general prohibition with some exception would be strongly advisable.

However, it also has to be noted that the approach put forward in the amendment would result in fewer changes as it might seem at first. The Commission proposal set out a general prohibition with some exceptions. The amendment removes the general prohibition, but still maintains that profiling may only be used in a limited list of cases that are substantially identical to those given as exceptions from the general prohibition in the original proposal.

Nevertheless, given the risks involved, having a general prohibition as the baseline is preferable because it sends a clear message to controllers against the use of profiling unless such use falls within one of the exceptions. In those cases where profiling is used, there should be strong safeguards to ensure that data subject know the logic involved in the profiling mechanism. In our opinion this is necessary in order to revert, or at least constrain, an existing trend to rely on profiling in all types of marketing and economic activity. For the same reason our advise would be to strengthen Article 20 by broadening the definition of “measures based on profiling”.

Amendment 52
Proposal for a regulation
Article 20 – paragraph 2 – introductory part

2. Subject to the other provisions of this Regulation, a person *may be subjected to a measure of the kind referred to in paragraph 1* only if the processing:

2. Subject to the other provisions of this Regulation, a *measure which produces legal effects on a person or significantly affects this person, based solely on automated processing intended to evaluate certain personal aspects relating to this person or to analyse or predict in particular the person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour, is lawful* only if the processing:

Comment: See comment on amendment 51 above. In addition, our advice would be to strengthen article 20 par. 2 by extending the application of the principles contained in this article to profiling itself, as a specific type of data processing.

Amendment 53
Proposal for a regulation
Article 20 – paragraph 2 – point c

(c) is based on the data subject's consent, subject to the conditions laid down in Article 7 *and to suitable safeguards*.

(c) is based on the data subject's consent, subject to the conditions laid down in Article 7, *in Article 15 and Article 16*.

Comment: The proposed wording would further weaken the protection of data subjects, as the wording “suitable safeguards” is wider and can contain conditions going beyond those stipulated in the amendment.

Amendment 54
Proposal for a regulation
Article 22 – paragraph 4

4. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures referred to in paragraph 1 other than those already referred to in paragraph 2, the conditions for the verification and auditing mechanisms referred to in paragraph 3 and as regards the criteria for proportionality under paragraph 3, and considering specific measures for micro, small and medium-sized-enterprises.

deleted

Comment:

Amendment 55
Proposal for a regulation
Article 23 – paragraph 2

2. The controller shall implement mechanisms

2. The controller shall implement mechanisms

<p>for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. <i>In particular</i>, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals.</p>	<p>for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. <i>Also</i>, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals, <i>unless justified pursuant to Article 6.</i></p>
<p>Comment: The principle of data protection by default, to which the amendment proposes changes, states that controllers shall provide data protection-friendly standard settings. The amendment would open a wide door for ignoring this principle, going far beyond the cases mentioned in the justification, as for example “legitimate interests of the controller” would be included as well. The principle simply states that within the range of possible and lawful settings, the most privacy-friendly ones shall be chosen by default. The example of election law mandating the publication of birth dates of candidates given in the justification would not be affected by this, as it creates a clear legal obligation on the controller to publish (<i>lex specialis</i>). In the context of a social network, the principle would for example require that profiles shall not be publicly visible by default.</p>	

<p>Amendment 56 Proposal for a regulation Article 24 – paragraph 1</p>	
<p>Where a controller determines the purposes, conditions and means of the processing of personal data jointly with others, the joint controllers shall determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the procedures and mechanisms for exercising the rights of the data subject, by means of an arrangement between them.</p>	<p>Where a controller determines the purposes, conditions and means of the processing of personal data jointly with others, the joint controllers shall determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the procedures and mechanisms for exercising the rights of the data subject, by means of an arrangement between them. <i>Where such determination is lacking or is not sufficiently clear, the data subject can exercise his rights with any of the controllers</i></p>

	<i>and they shall be equally liable.</i>
Comment: This amendment creates an incentive for controllers to clearly delineate their respective responsibilities.	

Amendment 57 Proposal for a regulation Article 25 – paragraph 2 – point b	
<i>(b) an enterprise employing fewer than 250 persons; or</i>	<i>deleted</i>
Comment: The size of a controller should not affect its accountability.	

Amendment 58 Proposal for a regulation Article 26 – paragraph 5	
<i>5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the responsibilities, duties and tasks in relation to a processor in line with paragraph 1, and conditions which allow facilitating the processing of personal data within a group of undertakings, in particular for the purposes of control and reporting.</i>	<i>deleted</i>
Comment:	

Amendment 59 Proposal for a regulation Article 28 – paragraph 3
--

3. The controller and the processor and, if any, the controller's representative, shall make the documentation available, on request, to the supervisory authority.	3. The controller and the processor and, if any, the controller's representative, shall make the documentation available, on request, to the supervisory authority and, in an electronic format, to the data subject.
Comment: The justification seems to confuse this documentation and the information to be given to DS (which does not need to include point (h) of art 28(2)). These two serve different purposes and audiences – the documentation to be provided to the DPA will be far more technical and legal in style and possibly less understandable for a lay public.	

Amendment 60 Proposal for a regulation Article 28 – paragraph 4 – point b	
(b) an enterprise or an organisation employing fewer than 250 persons that is processing personal data only as an activity ancillary to its main activities.	(b) an enterprise or an organisation that is processing personal data only as an activity ancillary to its main activities.
<p>Comment: This amendment would exclude all enterprises that only process personal data as an ancillary activity from having to keep proper documentation, so for example a large industrial enterprise would not need to document its processing of staff data. In addition, the very concept of “ancillary activity” when it comes to data processing will pose serious interpretative doubts, taking into account the fact that economic activity in general is increasingly based on processing personal data even if this is not the core business of the company (e.g. building profiles, targeted advertising etc.).</p> <p>The intention of the threshold was to create an exception to lower the administrative burden on MSMEs. For larger enterprises, the higher number of data subjects who could be harmed by noncompliance justifies having to keep this documentation. Instead of creating an exception to lower administrative burden on MSMEs, the amendments harmonises the requirements on a lower level. While we agree that the threshold of 250 employees may not be tailored to serve the purpose behind this legal provision, we would rather advise replacing it with a threshold of a given number of customers (i.e. persons possibly affected by noncompliance).</p> <p>See also comments on amendment 67 (obligation to appoint DPOs) for similar reasoning.</p>	

Amendment 61

Proposal for a regulation Article 28 – paragraph 5	
<i>5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the documentation referred to in paragraph 1, to take account of in particular the responsibilities of the controller and the processor and, if any, the controller's representative.</i>	<i>deleted</i>
Comment: While the main contents of the documentation are set out in Article 28(2), the Commission proposal would allow complementing these with additional information, providing a level playing field in the internal market.	

Amendment 62 Proposal for a regulation Article 31 – paragraph 1	
1. In the case of a personal data breach, the controller shall without undue delay <i>and, where feasible, not later than 24 hours after having become aware of it,</i> notify the personal data breach to the supervisory authority. <i>The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within 24 hours.</i>	1. In the case of a personal data breach, the controller shall without undue delay notify the personal data breach to the supervisory authority.
Comment: In the absence of a fixed period for notification, there would be significantly less pressure on controllers to promptly notify breaches. Of course, measures to contain and mitigate breaches are very important immediately following a breach, but this does not make notification less of a priority. In fact, by demanding that the notification shall include recommendations on how to mitigate possible adverse effect and a description of the measures taken to address the breach (Article 31(3) (c) and (e)), the Commission proposal further pushes controllers to quick reactions. Having notified in turn creates further pressure to fix the breach, as the DPA will be aware of the breach. Additionally, having a fixed period in which to notify creates a level playing field for controllers in different Member States, as otherwise interpretations might differ.	

In short: the message of the amendment to controllers is “fix it first, and then tell the DPA without waiting too long”, while the Commission proposal’s message is “fix it and tell the DPA how you did it/what you plan to do and do so within 24 hours”. The latter sends a stronger signal that breaches must be addressed as a matter of urgency.

See also comment on amendment 18 above.

Amendment 63
Proposal for a regulation
Article 31 – paragraph 4

4. The controller shall document any personal data breaches, comprising the facts surrounding the breach, its effects and the remedial action taken. This documentation must enable the supervisory authority to verify compliance with this Article. The documentation shall only include the information necessary for that purpose.

4. The controller shall document any personal data breaches, comprising the facts surrounding the breach, its effects and the remedial action taken. This documentation must enable the supervisory authority to verify compliance with this Article *and with Article 30*. The documentation shall only include the information necessary for that purpose.

Comment: This amendment only further reiterates existing obligations, as controllers have to be able to prove compliance with Article 30 in any case (see Articles 22(1) in connection with 22(2)(b)).

Amendment 64
Proposal for a regulation
Article 31 – paragraph 5

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for establishing the data breach referred to in paragraphs 1 and 2 and for the particular circumstances in which a controller and a processor is required to notify the personal

deleted

<i>data breach.</i>	
Comment:	

Amendment 65 Proposal for a regulation Article 32 – paragraph 1	
<p>1. When the personal data breach is likely to adversely affect the protection of the personal data or privacy of the data subject, the controller shall, <i>after</i> the notification referred to in Article 31, communicate the personal data breach to the data subject without undue delay.</p>	<p>1. When the personal data breach is likely to adversely affect the protection of the personal data or privacy of the data subject, <i>or when the intervention of the data subject can decisively mitigate the possible adverse effects of the personal data breach</i>, the controller shall, <i>together with the other urgent measures and before</i> the notification referred to in Article 31, communicate the personal data breach to the data subject without undue delay.</p>
<p>Comment: Removing the obligation to wait until after the notification to the DPA can indeed be helpful for quick information of DS in situations like the one mentioned in the justification. On the other hand, mandating that this information be sent before the notification to the DPA could result in premature information based on an insufficient understanding of the breach, especially if the controller wants to quickly notify the breach to the DPA. The best way might be to remove the coupling with the notification and simply state that the controller shall inform the DS without undue delay.</p>	

Amendment 66 Proposal for a regulation Article 32 – paragraph 5	
<p><i>5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements as to the circumstances in which a personal data breach is likely to adversely affect the personal data referred to in paragraph 1.</i></p>	<p><i>deleted</i></p>

Comment: The justification links the criteria for notifying data subjects of a breach to the data protection impact assessment (DPIA). However, not every processing operation that could have such consequences if a breach occurs would necessitate a DPIA (e.g. credit card information in payment systems). For this reason, it would make sense to allow the Commission to establish clear rules on when notification of data subjects is necessary (e.g. making it mandatory for credit card breaches).

Amendment 67
Proposal for a regulation
Article 35 – paragraph 1 – point b

<i>(b) the processing is carried out by an enterprise employing 250 persons or more; or</i>	<i>deleted</i>
---	----------------

Comment: While, as the justification for the proposed deletion correctly states, the controller’s size on its own should not affect the level of data protection, the threshold of 250 employees should not be seen as an additional burden on large controllers, but as an exception for small controllers: appointing a DPO is a proven way of enhancing controllers’ accountability and compliance; however, the additional administrative burden created by this might outweigh the benefits (since the number of concerned DS tends to be lower) in the case of small controllers, which is the reason for this exception. It should also be noted that currently some MS already require the appointment of DPOs for smaller controllers. While we agree that the threshold of 250 employees may not be tailored to serve the purpose behind this legal provision, we would rather advise replacing it with a different criterion, such as the number of persons possibly affected by noncompliance.

Amendment 68
Proposal for a regulation
Article 35 – paragraph 2

<i>2. In the case referred to in point (b) of paragraph 1, a group of undertakings may appoint a single data protection officer.</i>	<i>deleted</i>
--	----------------

Comment: see above comment on amendment 67.

Amendment 69
Proposal for a regulation
Article 35 – paragraph 11

11. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the core activities of the controller or the processor referred to in point (c) of paragraph 1 and the criteria for the professional qualities of the data protection officer referred to in paragraph 5.

deleted

Comment: Having clear and uniform rules on what such “core activities” are would contribute to a consistent application of the Regulation and a level playing field in the internal market. The same applies to having consistent rules on the professional qualities of DPOs. In case the delegation is removed, substantive rules should be included in the Regulation itself.

Amendment 70
Proposal for a regulation
Article 37 – paragraph 2

2. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for tasks, certification, status, powers and resources of the data protection officer referred to in paragraph 1.

deleted

Comment: The text in Art. 37(1), as it currently stands, only refers to the tasks and powers of DPOs; it does not lay out the required status (for example a certain amount of organizational independence, or protection against disciplinary measures for actions carried out in their role of DPO). Such further clarification via delegated acts might therefore be useful.

Amendment 71
Proposal for a regulation
Article 41 – paragraph 2 – point a

(a) the rule of law, relevant legislation in force, both general and sectoral, including concerning public security, defence, national security and criminal law, the professional rules and security measures which are complied with in that country or by that international organisation, as well as effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects residing in the Union whose personal data are being transferred;

(a) the rule of law, relevant legislation in force, both general and sectoral, including concerning public security, defence, national security and criminal law, the professional rules and security measures which are complied with in that country or by that international organisation, *jurisprudential precedents* as well as effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects residing in the Union whose personal data are being transferred;

Comment: Precedents are indeed worth considering for assessing the adequacy of the level of data protection in common law countries.

Amendment 72
Proposal for a regulation
Article 41 – paragraph 7

7. The Commission shall publish in the Official Journal of the European Union a list of those third countries, territories and processing sectors within a third country and international organisations where it has decided that an adequate level of protection is or is not ensured.

7. The Commission shall publish in the Official Journal of the European Union *and on its website* a list of those third countries, territories and processing sectors within a third country and international organisations where it has decided that an adequate level of protection is or is not ensured.

Comment: This would help to ensure transparency regarding adequacy decisions and would also codify current practices, since these decisions are already published on the Commission website, although so far there is no requirement to do so.

Amendment 73
Proposal for a regulation
Article 62

[...]

deleted

Comment: In addition to the reasons given in the justification for deleting this article, it should also be noted that paragraph 1 point (a) of the Commission proposal would likely have infringed on the DPAs independence. Points (c) and (d) of the same paragraph can indeed better be done by the EDPB itself. However, declaring standard data protection clauses generally valid would not be covered by the EDPB's proposed mandate in Article 66 and would require further amendments.

Amendment 74
Proposal for a regulation
Article 63 a (new)

Article 63 a

Appealing procedures

Without prejudice to the competences of the judiciary system of the Member States and of the Union, the European Data Protection Board can issue binding opinions if:

- (a) a data subject or data controller appeals on ground of inconsistent application of the present Regulation across the Member States and*
- (b) the Consistency Mechanism described in Article 58 to 63 has failed to ensure that a simple majority of the members of the European Data Protection Board agrees on a measure.*

Before issuing such opinion, the European Data Protection Board shall

	<i>take into consideration every information the competent Data Protection Authority knows, including the point of view of the interested parties.</i>
--	--

Comment:
 Point (a) would task the EDPB with dealing with complaints against “inconsistent application” of the Regulation; the question remains whether such a procedure is really necessary, given that incorrect application of the Regulation by DPAs can already be appealed against in Court.
 Point (b) of this amendment replaces the Commission’s power under Article 62(1)(a). Removing the replace the Commission’s final power of deciding disputes between the DPAs in the EDPB is a good thing, as having this power would constitute an interference with the independence of the DPAs (see on this points also the EDPS Opinion on the Data Protection Reform Package, especially pts. 248-255, as well as the Opinion of the Article 29 Working Party, p. 20).
 Removing the Commission from such decisions would additionally require amendments to Article 60.

Amendment 75
Proposal for a regulation
Article 66 – paragraph 1 – point d

(d) issue opinions on draft decisions of supervisory authorities pursuant to the consistency mechanism referred to in Article 57;	(d) issue opinions on draft decisions of supervisory authorities pursuant to the consistency mechanism referred to in Article 57 <i>and in Article 63a</i> ;
---	--

Comment:

Amendment 76
Proposal for a regulation
Article 73 – paragraph 2

2. Any body, organisation or association which aims to protect <i>data subjects</i> ’ rights and	2. Any body, organisation or association which aims to protect <i>citizens</i> ’ rights and interests
--	---

<p>interests <i>concerning the protection of their personal data and has been properly constituted according to the law of a Member State</i> shall have the right to lodge a complaint with a supervisory authority in any Member State on behalf of one or more data subjects if it considers that a data subject's rights under this Regulation have been infringed as a result of the processing of personal data.</p>	<p>shall have the right to lodge a complaint with a supervisory authority in any Member State on behalf of one or more data subjects if it considers that a data subject's rights under this Regulation have been infringed as a result of the processing of personal data.</p>
<p>Comment: This provision could contribute to wider use of collective redress mechanisms. Keeping “data subjects' rights” instead of “citizens” could cause uncertainty as regards complaints by third-country nationals and stateless persons. Therefore we would advocate for changing the wording of this article as proposed in the amendment. See also amendment 24 above.</p>	

<p>Amendment 77 Proposal for a regulation Article 74 – paragraph 1</p>	
<p>1. Each natural or legal person shall have the right to a judicial remedy against decisions of a supervisory authority concerning them.</p>	<p>1. <i>Without prejudice to the procedure described in Article 63a</i>, each natural or legal person shall have the right to a judicial remedy against decisions of a supervisory authority concerning them.</p>
<p>Comment:</p>	

<p>Amendment 78 Proposal for a regulation Article 78 – paragraph 1</p>	
<p>1. Member States shall lay down the rules on penalties, applicable to infringements of the provisions of this Regulation and shall take all measures necessary to ensure that they are implemented, including where the controller</p>	<p>1. Member States shall lay down the rules on penalties, applicable to infringements of the provisions of this Regulation and shall take all measures necessary to ensure that they are implemented, including where the controller</p>

did not comply with the obligation to designate a representative. The penalties provided for must be effective, proportionate and dissuasive.	did not comply with the obligation to designate a representative. The penalties provided for must be effective, <i>consistent</i> proportionate and dissuasive.
Comment: It is not clear how this provision could be interpreted and enforced in practice, neither is it clear whether this refers to consistency regarding different kinds of breaches or between Member States or the “jurisprudence” of a given Data Protection Authority or else. In any case, there might very well be different perceptions based on historical and cultural factors.	

<p>Amendment 79 Proposal for a regulation Article 79 – paragraph 2</p>	
2. The administrative sanction shall be in each individual case effective, proportionate and dissuasive. The amount of the administrative fine shall be fixed with due regard to the nature, gravity and duration of the breach, the intentional or negligent character of the infringement, the degree of responsibility of the natural or legal person and of previous breaches by this person, the technical and organisational measures and procedures implemented pursuant to Article 23 and the degree of co-operation with the supervisory authority in order to remedy the breach.	2. The administrative sanction shall be in each individual case effective, <i>consistent</i> proportionate and dissuasive. The amount of the administrative fine shall be fixed with due regard to the nature, gravity and duration of the breach, the intentional or negligent character of the infringement, the degree of responsibility of the natural or legal person and of previous breaches by this person, the technical and organisational measures and procedures implemented pursuant to Article 23 and the degree of co-operation with the supervisory authority in order to remedy the breach.
Comment: It is not clear how this consistency criterion would be enforced, given that it is wider in scope than the procedure introduced in amendment 74 (which only covers consistency between Member States). Additionally, this would likely infringe on DPA’s independence. Incorrect application of the Regulation by DPAs can always be addressed using judicial procedures.	

<p>Amendment 80 Proposal for a regulation Article 81 – paragraph 1 – introductory part</p>

1. Within the limits of this Regulation and in accordance with point (h) of Article 9(2), processing of personal data concerning health must be on the basis of Union law or Member State law which shall provide for suitable and specific measures to safeguard the data subject's legitimate interests, and be necessary for:	1. Within the limits of this Regulation and in accordance with point (h) of Article 9(2), processing of personal data concerning health must be on the basis of Union law or Member State law which shall provide for suitable, consistent and specific measures to safeguard the data subject's legitimate interests, and be necessary for:
Comment:	

Amendment 81 Proposal for a regulation Article 81 – paragraph 3	
<i>3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying other reasons of public interest in the area of public health as referred to in point (b) of paragraph 1, as well as criteria and requirements for the safeguards for the processing of personal data for the purposes referred to in paragraph 1.</i>	<i>deleted</i>
Comment: These delegated acts would in fact contribute to the consistency of the application of the Regulation, the exact aim of amendment 80.	

Amendment 82 Proposal for a regulation Article 83 – paragraph 3	
<i>3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for</i>	<i>deleted</i>

<p><i>the processing of personal data for the purposes referred to in paragraph 1 and 2 as well as any necessary limitations on the rights of information to and access by the data subject and detailing the conditions and safeguards for the rights of the data subject under these circumstances.</i></p>	
<p>Comment: These delegated acts could in fact contribute to the consistency of the application of the Regulation.</p>	

<p>Amendment 83 Proposal for a regulation Article 84 – paragraph 2</p>	
<p>2. Each Member State shall notify to the Commission the rules adopted pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.</p>	<p>2. Each Member State shall notify to the Commission the rules adopted pursuant to paragraph 1, <i>in order for the Commission to verify the consistency with the other Member States rules</i>, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.</p>
<p>Comment: According to paragraph (1) of the same article, these rules have to stay “within the limits of this Regulation”, already ensuring a certain degree of consistency. Additionally, the perceptions on the best way to reconcile these two might differ between MS.</p>	

<p>Amendment 84 Proposal for a regulation Article 86 – paragraph 2</p>	
<p>2. The delegation of power referred to in Article 6(5), Article 8(3), Article 9(3), Article 12(5), Article 14(7), Article 15(3), Article 17(9), Article 20(6), Article 22(4), Article 23(3), Article 26(5), Article 28(5), Article 30(3), Article 31(5), Article 32(5), Article</p>	<p>2. The delegation of power referred to in Article 8(3), Article 9(3), Article 12(5), Article 20(5), Article 23(3), Article 30(3), Article 33(6), Article 34(8), Article 39(2), Article 43(3), Article 44(7), Article 79(7) and Article 82(3) shall be conferred on the Commission for</p>

<p>336), Article 34(8), Article 35(11), Article 37(2), Article 39(2), Article 43(3), Article 44(7), Article 79(6), Article 81(3), Article 82(3) and Article 83(3) shall be conferred on the Commission for an indeterminate period of time from the date of entry into force of this Regulation.</p>	<p>an indeterminate period of time from the date of entry into force of this Regulation.</p>
<p>Comment: see comments made on the respective Articles.</p>	

<p>Amendment 85 Proposal for a regulation Article 86 – paragraph 3</p>	
<p>3. The delegation of power referred to in Article 6(5), Article 8(3), Article 9(3), Article 12(5), Article 14(7), Article 15(3), Article 17(9), Article 20(6), Article 22(4), Article 23(3), Article 26(5), Article 28(5), Article 30(3), Article 31(5), Article 32(5), Article 33(6), Article 34(8), Article 35(11), Article 37(2), Article 39(2), Article 43(3), Article 44(7), Article 79(6), Article 81(3), Article 82(3) and Article 83(3) may be revoked at any time by the European Parliament or by the Council. A decision of revocation shall put an end to the delegation of power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.</p>	<p>3. The delegation of power referred to in Article 8(3), Article 9(3), Article 12(5), Article 20(5), Article 23(3), Article 30(3), Article 33(6), Article 34(8), Article 39(2), Article 43(3), Article 44(7), Article 79(7), and Article 82(3) may be revoked at any time by the European Parliament or by the Council. A decision of revocation shall put an end to the delegation of power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.</p>
<p>Comment: see comments made on the respective Articles.</p>	

<p>Amendment 86 Proposal for a regulation</p>
--

Article 86 – paragraph 5

5. A delegated act adopted pursuant to Article **6(5)**, **Article 8(3)**, Article 9(3), Article 12(5), Article **14(7)**, **Article 15(3)**, **Article 17(9)**, **Article 20(6)**, **Article 22(4)**, Article 23(3), Article **26(5)**, **Article 28(5)**, **Article 30(3)**, Article **31(5)**, **Article 32(5)**, **Article 33(6)**, Article 34(8), Article **35(11)**, **Article 37(2)**, **Article 39(2)**, Article 43(3), Article 44(7), Article **79(6)**, **Article 81(3)**, Article 82(3) **and Article 83(3)** shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or the Council.

5. A delegated act adopted pursuant to Article 8(3), Article 9(3), Article 12(5), Article **20(5)**, Article 23(3), Article 30(3), Article 33(6), Article 34(8), Article 39(2), Article 43(3), Article 44(7), Article 79(7), **and** Article 82(3) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or the Council.

Comment: see comments made on the respective Articles.



Comments on the draft JURI opinion on the General Data Protection Regulation

EDRi welcomes the draft opinion, but would like to provide some comments on the Rapporteur's proposed amendments. For ease of reading, the amendments on which EDRi has comments are highlighted as follows:

- **Green** for amendments EDRi supports;
- **Yellow** for amendments that could benefit from certain improvements, but which go in the right direction;
- **Red** for amendments which should be reconsidered;
- **Grey** for amendments on which EDRi does not have a strong position.

The left column repeats the Commission proposal with the elements the Rapporteur wants to delete highlighted in bold, while the right column repeats the amendments proposed by the Rapporteur, with her additions highlighted in bold. Below, you will find a short justification for EDRi's position. We also provide some comments on some amendments on which we do not have a strong position.

We would also like to draw your attention to our website <http://protectmydata.eu/>, where we provide further analysis of the proposal and propose amendments to many recitals and Articles.

Amendment 1 Proposal for a Regulation Recital 15	
<i>Commission Proposal</i>	<i>Amendment</i>
(15) This Regulation should not apply to processing of personal data by a natural person, which are exclusively personal or domestic, such as correspondence and the holding of addresses, and without any gainful interest and thus without any connection with a professional or commercial activity. The exemption should	(15) This Regulation should not apply to processing of personal data by a person, which are exclusively personal or domestic, such as correspondence and the holding of addresses, and without any gainful interest and thus without any connection with a professional or commercial activity, and which do not involve

also not apply to controllers or processors which provide the means for processing personal data for such personal or domestic activities.	<i>making such data accessible to an indefinite number of people.</i> The exemption should also not apply to controllers or processors which provide the means for processing personal data for such personal or domestic activities.
Comment: EDRi supports this stricter definition of the household exception, which brings greater clarity, especially in the online context.	

Amendment 2 Proposal for a Regulation Recital 24	
<i>Commission Proposal</i>	<i>Amendment</i>
(24) When using online services, individuals may be associated with online identifiers provided by their devices, applications, tools and protocols, such as Internet Protocol addresses or cookie identifiers. This may leave traces which, combined with unique identifiers and other information received by the servers, may be used to create profiles of the individuals and identify them. It follows that identification numbers, location data, online identifiers or other specific factors as such need not necessarily be considered as personal data in all circumstances.	(24) When using online services, individuals may be associated with online identifiers provided by their devices, applications, tools and protocols, such as Internet Protocol addresses or cookie identifiers. This may leave traces which, combined with unique identifiers and other information received by the servers, may be used to create profiles of the individuals and identify them. It follows that <i>a study should be undertaken, on a case-by-case basis and in accordance with technological developments, of whether</i> identification numbers, location data, online identifiers or other specific factors as such need not necessarily be considered as personal data in all circumstances.
Comment: EDRi completely agrees that online identifiers merit protections. For this reason, we support this amendment's intention, but would call for stronger wording. We suggested wording on http://protectmydata.eu/recitals/recitals-21-30/recital-24/ , saying that online identifiers should be considered personal data unless they are demonstrably not linked to natural persons (for example, IP addresses of email servers).	

Amendment 3 Proposal for a Regulation Recital 25	
<i>Commission Proposal</i>	<i>Amendment</i>
(25) Consent should be given explicitly by any <i>appropriate method</i> enabling a freely given	(25) Consent should be given explicitly by any <i>method appropriate to the media used</i> enabling

<p>specific and informed indication of the data subject's wishes, either by a statement or by a clear affirmative action by the data subject, ensuring that individuals are aware that they give their consent to the processing of personal data, including by ticking a box when visiting an Internet website or by any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data. Silence or inactivity should therefore not constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. If the data subject's consent is to be given following an electronic request, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.</p>	<p>a freely given specific and informed indication of the data subject's wishes, either by a statement or by a clear affirmative action by the data subject, ensuring that individuals are aware that they give their consent to the processing of personal data, including by ticking a box when visiting an Internet website or by any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data. Silence or inactivity should therefore not constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. If the data subject's consent is to be given following an electronic request, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.</p>
<p>Comment: It seems appropriate to also specify that consent needs to be given in an active way, that is to say that inactivity (for example, not unchecking pre-ticked boxes) and simple usage of a service on their own do not constitute consent.</p>	

<p>Amendment 4 Proposal for a Regulation Recital 27</p>	
<p><i>Commission Proposal</i></p>	<p><i>Amendment</i></p>
<p>(27) The main establishment of a controller in the Union should be determined according to objective criteria and should imply the effective and real exercise of management activities determining the main decisions as to the purposes, conditions and means of processing through stable arrangements. This criterion should not depend whether the processing of personal data is actually carried out at that location; the presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute such main establishment and are therefore no determining criteria for a main establishment. The main establishment of the processor should be the place of its central administration in the Union.</p>	<p>(27) The main establishment of a controller in the Union should be determined according to objective criteria and should imply the effective and real exercise of management activities determining the main decisions as to the purposes, conditions and means of processing through stable arrangements. This criterion should not depend whether the processing of personal data is actually carried out at that location; the presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute such main establishment and are therefore no determining criteria for a main establishment. <i>‘Main establishment of the controller’ means the place in the EU where personal data protection policy is determined,</i></p>

	<p><i>taking into account the dominant influence of the establishment over others, particularly in the case of a group of companies, the implementation of rules on personal data protection and rules relevant for data protection.</i> The main establishment of the processor should be the place of its central administration in the Union.</p>
<p>Comment: This amendment follows the call for more clarity launched by several organisations, including EDRI. See also amendment 23 below</p>	

<p>Amendment 5 Proposal for a regulation Recital 38</p>	
<p><i>Commission Proposal</i></p>	<p><i>Amendment</i></p>
<p>(38) The legitimate interests of a controller may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding. This would need careful assessment in particular where the data subject is a child, given that children deserve specific protection. The data subject should have the right to object the processing, on grounds relating to their particular situation and free of charge. To ensure transparency, the controller should be obliged to explicitly inform the data subject on the legitimate interests pursued and on the right to object, and also be obliged to document these legitimate interests. Given that it is for the legislator to provide by law the legal basis for public authorities to process data, this legal ground should not apply for the processing by public authorities in the performance of their tasks.</p>	<p>(38) The legitimate interests of a person may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding. This would need careful assessment in particular where the data subject is a child, given that children deserve specific protection. The data subject should have the right to object the processing, on grounds relating to their particular situation and free of charge. To ensure transparency, the controller or the third parties to whom the data are sent should be obliged to explicitly inform the data subject on the legitimate interests pursued and on the right to object, and also be obliged to document these legitimate interests. Given that it is for the legislator to provide by law the legal basis for public authorities to process data, this legal ground should not apply for the processing by public authorities in the performance of their tasks.</p>
<p>Comment: See comment on amendment 24 below.</p>	

Amendment 6
Proposal for a Regulation
Recital 48

<i>Commission Proposal</i>	<i>Amendment</i>
<p>(48) The principles of fair and transparent processing require that the data subject should be informed in particular of the existence of the processing operation and its purposes, how long the data will be stored, on the existence of the right of access, rectification or erasure and on the right to lodge a complaint. Where the data are collected from the data subject, the data subject should also be informed whether they are obliged to provide the data and of the consequences, in cases they do not provide such data.</p>	<p>(48) The principles of fair and transparent processing require that the data subject should be informed in particular of the existence of the processing operation and its purposes, <i>the criteria enabling determination of</i> how long the data will be stored <i>for each purpose</i>, on the existence of the right of access, rectification or erasure and on the right to lodge a complaint. Where the data are collected from the data subject, the data subject should also be informed whether they are obliged to provide the data and of the consequences, in cases they do not provide such data.</p>
<p>Comment: This amendment will lead to more clarity in cases where data are conserved for several purposes. We welcome this part of the amendment. Nonetheless, it is important that data subjects are provided with precise periods, in order to avoid a situation in which controllers only provide unclear criteria which do not clarify the situation for the data subject. See also the following amendment 7 and amendment 31 below.</p>	

<p>Amendment 7 Proposal for a Regulation Recital 51</p>	
<i>Commission Proposal</i>	<i>Amendment</i>

<p>(51) Any person should have the right of access to data which has been collected concerning them, and to exercise this right easily, in order to be aware and verify the lawfulness of the processing. Every data subject should therefore have the right to know and obtain communication in particular for what purposes the data are processed, <i>for what period</i>, which recipients receive the data, what is the logic of the data that are undergoing the processing and what might be, at least when based on profiling, the consequences of such processing. This right should not adversely affect the rights and freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of these considerations should not be that all information is refused to the data subject.</p>	<p>(51) Any person should have the right of access to data which has been collected concerning them, and to exercise this right easily, in order to be aware and verify the lawfulness of the processing. Every data subject should therefore have the right to know and obtain communication in particular for what purposes the data are processed, <i>the criteria enabling determination of how long the data will be stored for each purpose</i>, which recipients receive the data, what is the logic of the data that are undergoing the processing and what might be, at least when based on profiling, the consequences of such processing. This right should not adversely affect the rights and freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of these considerations should not be that all information is refused to the data subject.</p>
<p>Comment: See comment on amendment 6 above.</p>	

<p>Amendment 8 Proposal for a Regulation Recital 55</p>	
<p><i>Commission Proposal</i></p>	<p><i>Amendment</i></p>
<p><i>(55) To further strengthen the control over their own data and their right of access, data subjects should have the right, where personal data are processed by electronic means and in a structured and commonly used format, to obtain a copy of the data concerning them also in commonly used electronic format. The data subject should also be allowed to transmit those data, which they have provided, from one automated application, such as a social network, into another one. This should apply where the data subject provided the data to the automated processing system, based on their consent or in the performance of a contract.</i></p>	<p><i>deleted</i></p>
<p>Comment: The right to data portability is a corollary to the right of access. Currently, the problem</p>	

is that when replying to access requests, controllers sometimes provide data in a format that does not lend itself to further use by the data subject. This creates lock-in effects, especially for social networks and other online services. The right to data portability would contribute to a more competitive environment for this kind of services by allowing people to change service providers more easily. If the aim is simply to avoid any possible confusion due to the fact that these two related rights are regulated in two different Articles, it would be possible to include the provisions of Article 18 in Article 15. See also amendment [36](#) below.

Amendment 9 Proposal for a Regulation Recital 60	
<i>Commission Proposal</i>	<i>Amendment</i>
(60) Comprehensive responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should ensure and be obliged to demonstrate the compliance of each processing operation with this Regulation.	(60) Overall responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should ensure and be obliged to demonstrate the compliance of each processing operation with this Regulation.
Comment:	

Amendment 10 Proposal for a Regulation Recital 62	
<i>Commission Proposal</i>	<i>Amendment</i>
(62) The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processor, also in relation to the monitoring by and measures of supervisory authorities, requires a clear attribution of the responsibilities under this Regulation, including where a controller determines the purposes, conditions and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller.	<i>(62) The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processor, also in relation to the monitoring by and measures of supervisory authorities, requires a clear attribution of the responsibilities under this Regulation, including where a controller determines the purposes, conditions and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller. In the event of joint and several liability, a processor which has made amends for damage done to the data subject may appeal against the controller for reimbursement if it has acted in conformity</i>

	<i>with the legal act binding it to the controller.</i>
Comment: This amendment creates a clearer situation for processors.	

Amendment 11 Proposal for a Regulation Recital 65	
<i>Commission Proposal</i>	<i>Amendment</i>
(65) In order to demonstrate compliance with this Regulation, the controller or processor should document each processing operation . Each controller and processor should be obliged to co-operate with the supervisory authority and make this documentation, on request, available to it, so that it might serve for monitoring those processing operations.	(65) In order to demonstrate compliance with this Regulation, the controller or processor should keep a documentary record of all the processing systems and procedures for which they are responsible . Each controller and processor should be obliged to co-operate with the supervisory authority and make this documentation, on request, available to it, so that it might serve for monitoring those processing operations.
Comment:	

Amendment 12 Proposal for a Regulation Recital 67	
<i>Commission Proposal</i>	<i>Amendment</i>
(67) A personal data breach may, if not addressed in an adequate and timely manner, result in substantial economic loss and social harm, including identity fraud, to the individual concerned. Therefore, as soon as the controller becomes aware that such a breach has occurred, the controller should notify the breach to the supervisory authority without undue delay and, where feasible, within 24 hours. Where this cannot be achieved within 24 hours, an explanation of the reasons for the delay should accompany the notification . The individuals whose personal data could be adversely affected by the breach should be notified without undue delay in order to allow them to take the necessary precautions. A breach should be	(67) A personal data breach may, if not addressed in an adequate and timely manner, result in substantial economic loss and social harm, including identity fraud, to the individual concerned. Therefore, as soon as the controller becomes aware that a breach which would have a significant impact on the data subject has occurred, the controller should notify the breach to the supervisory authority without undue delay. The individuals whose personal data could be significantly adversely affected by the breach should be notified without undue delay in order to allow them to take the necessary precautions. A breach should be considered as significantly adversely affecting the personal data or privacy of a data subject where it could

<p>considered as adversely affecting the personal data or privacy of a data subject where it could result in, for example, identity theft or fraud, physical harm, significant humiliation or damage to reputation. The notification should describe the nature of the personal data breach as well as recommendations as well as recommendations for the individual concerned to mitigate potential adverse effects. Notifications to data subjects should be made as soon as reasonably feasible, and in close cooperation with the supervisory authority and respecting guidance provided by it or other relevant authorities (e.g. law enforcement authorities). For example, the chance for data subjects to mitigate an immediate risk of harm would call for a prompt notification of data subjects whereas the need to implement appropriate measures against continuing or similar data breaches may justify a longer delay.</p>	<p>result in, for example, identity theft or fraud, physical harm, significant humiliation or damage to reputation. The notification should describe the nature of the personal data breach as well as recommendations as well as recommendations for the individual concerned to mitigate potential adverse effects. Notifications to data subjects should be made as soon as reasonably feasible, and in close cooperation with the supervisory authority and respecting guidance provided by it or other relevant authorities (e.g. law enforcement authorities). For example, the chance for data subjects to mitigate an immediate risk of harm would call for a prompt notification of data subjects whereas the need to implement appropriate measures against continuing or similar data breaches may justify a longer delay.</p>
---	---

Comment: As the Rapporteur rightly points out, the main aim of a controller who became aware of a breach in the first period of time is to stop the breach. However, it is advisable to have a fixed and short deadline for the notification to the DPA, since such a deadline puts more pressure on the controller to stop the breach. In the absence of such a clear deadline, there is a risk that controllers will justify considerably delaying notifications by saying that fixing the breach a long time. The preferable solution would be to have a fixed, but slightly longer deadline. This could be 72 hours, as already suggested by the EDPS and EDRI. See also amendment 48 below.

<p>Amendment 13 Proposal for a Regulation Recital 82</p>	
<i>Commission Proposal</i>	<i>Amendment</i>
<p>(82) The Commission may equally recognise that a third country, or a territory or a processing sector within a third country, or an international organisation offers no adequate level of data protection. Consequently the transfer of personal data to that third country should be <i>prohibited</i>. <i>In that case, provision should be made for consultations between the Commission and such third countries or international organisations.</i></p>	<p>(82) The Commission may equally recognise that a third country, or a territory or a processing sector within a third country, or an international organisation offers no adequate level of data protection. Consequently the transfer of personal data to that third country should be <i>authorised subject to appropriate guarantees or under the derogations set out in this Regulation.</i></p>

Comment: Although the amendment is an improvement compared to the Commission proposal, it would be preferable to have a ban on transfers as the starting point, if there is a negative adequacy decision. Such wording would underline that transfers to non-adequate recipients would be exceptions.

Amendment 14
Proposal for a Regulation
Recital 85 a (new)

<i>Commission Proposal</i>	<i>Amendment</i>
	<i>(85a) A group of companies planning to submit for approval binding corporate rules may propose a supervisory authority as the lead authority. This should be the supervisory authority of the Member State in which the main establishment of the controller or processor is situated.</i>

Comment: Given that the active text (see amendment 56 below) clearly says that the lead DPA is the DPA competent for the main establishment, the added value of letting the group of undertakings propose a lead DPA is not clear.

Amendment 15
Proposal for a Regulation
Recital 115

<i>Commission Proposal</i>	<i>Amendment</i>
<i>(115) In situations where the competent supervisory authority established in another Member State does not act or has taken insufficient measures in relation to a complaint, the data subject may request the supervisory authority in the Member State of his or her habitual residence to bring proceedings against that supervisory authority to the competent court in the other Member State. The requested supervisory authority may decide, subject to judicial review, whether it is appropriate to follow the request or not.</i>	<i>deleted</i>

Comment:

Amendment 16
 Proposal for a Regulation
Recital 118

<i>Commission Proposal</i>	<i>Amendment</i>
(118) Any damage which a person may suffer as a result of unlawful processing should be compensated by the controller or processor, who may be exempted from liability if they prove that they are not responsible for the damage, in particular where he establishes fault on the part of the data subject or in case of force majeure.	<i>(118) Any damage which a person may suffer as a result of unlawful processing should be compensated by the controller or processor, who may be exempted from liability if they prove that they are not responsible for the damage, in particular where he establishes fault on the part of the data subject or in case of force majeure. In the event of joint and several liability, a processor which has made amends for damage done to the person concerned may appeal against the controller for reimbursement if it has acted in conformity with the legal act binding it to the controller.</i>
<p>Comment: This amendment clarifies that a processor which acted in compliance with its contract with the controller can have recourse against the controller. This reinforces the final responsibility of the controller.</p>	

Amendment 17
 Proposal for a Regulation
Recital 129

<i>Commission Proposal</i>	<i>Amendment</i>
(129) In order to fulfil the objectives of this Regulation, namely to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data and to ensure the free movement of personal data within the Union, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the Commission. In particular, delegated acts should be adopted in respect of lawfulness of processing; specifying the criteria and conditions in relation to the consent of a child; processing of special categories of data; <i>specifying the criteria and conditions for manifestly excessive requests and fees for exercising the rights of the data</i>	(129) In order to fulfil the objectives of this Regulation, namely to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data and to ensure the free movement of personal data within the Union, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the Commission. In particular, delegated acts should be adopted in respect of lawfulness of processing; specifying the criteria and conditions in relation to the consent of a child; processing of special categories of data; criteria and requirements for the information to the data subject and in relation to the right of access; the right to be

<p>subject; criteria and requirements for the information to the data subject and in relation to the right of access; the right to be forgotten and to erasure; measures based on profiling; criteria and requirements in relation to the responsibility of the controller and to data protection by design and by default; a processor; criteria and requirements for the documentation and the security of processing; criteria and requirements for establishing a personal data breach and for its notification to the supervisory authority, and on the circumstances where a personal data breach is likely to adversely affect the data subject; the criteria and conditions for processing operations requiring a data protection impact assessment; the criteria and requirements for determining a high degree of specific risks which require prior consultation; designation and tasks of the data protection officer; codes of conduct; criteria and requirements for certification mechanisms; criteria and requirements for transfers by way of binding corporate rules; transfer derogations; administrative sanctions; processing for health purposes; processing in the employment context and processing for historical, statistical and scientific research purposes. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level. The Commission, when preparing and drawing-up delegated acts, should ensure a simultaneous, timely and appropriate transmission of relevant documents to the European Parliament and Council.</p>	<p>forgotten and to erasure; measures based on profiling; criteria and requirements in relation to the responsibility of the controller; a processor; criteria and requirements for the documentation; criteria and requirements for establishing a personal data breach and for its notification to the supervisory authority, and on the circumstances where a personal data breach is likely to adversely affect the data subject; the criteria and conditions for processing operations requiring a data protection impact assessment; the criteria and requirements for determining a high degree of specific risks which require prior consultation; designation and tasks of the data protection officer; codes of conduct; criteria and requirements for certification mechanisms; transfers by way of binding corporate rules; derogations concerning transfers; processing for health purposes; processing in the employment context and processing for historical, statistical and scientific research purposes. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level. The Commission, when preparing and drawing-up delegated acts, should ensure a simultaneous, timely and appropriate transmission of relevant documents to the European Parliament and Council.</p>
<p>Comment:</p>	

Amendment 18 Proposal for a Regulation Recital 130	
<i>Commission Proposal</i>	<i>Amendment</i>
(130) In order to ensure uniform conditions for the implementation of this Regulation,	(130) In order to ensure uniform conditions for the implementation of this Regulation,

<p>implementing powers should be conferred on the Commission for: specifying standard forms in relation to the processing of personal data of a child; standard procedures and forms for exercising the rights of data subjects; standard forms for the information to the data subject; standard forms and procedures in relation to the right of access; the right to data portability; standard forms in relation to the responsibility of the controller to data protection by design and by default and to the documentation; specific requirements for the security of processing; the standard format and the procedures for the notification of a personal data breach to the supervisory authority and the communication of a personal data breach to the data subject; standards and procedures for a data protection impact assessment; forms and procedures for prior authorisation and prior consultation; technical standards and mechanisms for certification; the adequate level of protection afforded by a third country or a territory or a processing sector within that third country or an international organisation; disclosures not authorized by Union law; mutual assistance; joint operations; decisions under the consistency mechanism. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers. In this context, the Commission should consider specific measures for micro, small and medium-sized enterprises.</p>	<p>implementing powers should be conferred on the Commission for: specifying standard forms in relation to the processing of personal data of a child; standard forms for the information to the data subject; standard forms and procedures in relation to the right of access; standard forms in relation to the responsibility of the controller to the documentation; specific requirements for the security of processing; the standard format and the procedures for the notification of a personal data breach to the supervisory authority and the communication of a personal data breach to the data subject; standards and procedures for a data protection impact assessment; forms and procedures for prior authorisation and prior consultation; technical standards and mechanisms for certification; the adequate level of protection afforded by a third country or a territory or a processing sector within that third country or an international organisation; disclosures not authorized by Union law; mutual assistance; joint operations; decisions under the consistency mechanism. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers. In this context, the Commission should consider specific measures for micro, small and medium-sized enterprises.</p>
<p>Comment:</p>	

Amendment 19 Proposal for a Regulation Recital 131	
<i>Commission Proposal</i>	<i>Amendment</i>
(131) The examination procedure should be used	(131) The examination procedure should be used

<p>for the adoption of specifying standard forms in relation to the consent of a child; standard procedures and forms for exercising the rights of data subjects; standard forms for the information to the data subject; standard forms and procedures in relation to the right of access; the right to data portability; standard forms in relation to the responsibility of the controller to data protection by design and by default and to the documentation; specific requirements for the security of processing; the standard format and the procedures for the notification of a personal data breach to the supervisory authority and the communication of a personal data breach to the data subject; standards and procedures for a data protection impact assessment; forms and procedures for prior authorisation and prior consultation; technical standards and mechanisms for certification; the adequate level of protection afforded by a third country or a territory or a processing sector within that third country or an international organisation; disclosures not authorized by Union law; mutual assistance; joint operations; decisions under the consistency mechanism, given that those acts are of general scope.</p>	<p>for the adoption of specifying standard forms in relation to the consent of a child; standard procedures and forms for exercising the rights of data subjects; standard forms for the information to the data subject; standard forms and procedures in relation to the right of access; standard forms in relation to the responsibility of the controller to the documentation; specific requirements for the security of processing; the standard format and the procedures for the notification of a personal data breach to the supervisory authority and the communication of a personal data breach to the data subject; standards and procedures for a data protection impact assessment; forms and procedures for prior authorisation and prior consultation; technical standards and mechanisms for certification; disclosures not authorized by Union law; mutual assistance; joint operations; decisions under the consistency mechanism, given that those acts are of general scope.</p>
<p>Comment:</p>	

<p>Amendment 20 Proposal for a Regulation Recital 139</p>	
<p><i>Commission Proposal</i></p>	<p><i>Amendment</i></p>
<p>(139) In view of the fact that, as underlined by the Court of Justice of the European Union, the right to the protection of personal data is not an absolute right, but must be considered in relation to its function in society and be balanced with other fundamental rights, in accordance with the principle of proportionality, this Regulation respects all fundamental rights and observes the principles recognised in the Charter of Fundamental Rights of the European Union as enshrined in the Treaties, notably the right to</p>	<p>(139) In view of the fact that, as underlined by the Court of Justice of the European Union, the right to the protection of personal data is not an absolute right, but must be considered in relation to its function in society and be balanced with other rights established by the Charter of Fundamental Rights of the European Union, in accordance with the principle of proportionality, this Regulation respects all fundamental rights and observes the principles recognised in the Charter of Fundamental Rights</p>

respect for private and family life, home and communications, the right to the protection of personal data, the freedom of thought, conscience and religion, the freedom of expression and information, the freedom to conduct a business, the right to an effective remedy and to a fair trial as well as cultural, religious and linguistic diversity.	of the European Union as enshrined in the Treaties, notably the right to respect for private and family life, home and communications, the right to the protection of personal data, the freedom of thought, conscience and religion, the freedom of expression and information, the freedom to conduct a business, the right to an effective remedy and to a fair trial as well as cultural, religious and linguistic diversity.
<p>Comment: This amendment appears, possibly unintentionally, to restrict the right of Member States to take their own national constitutions and priorities into account when assessing the fundamental right to privacy in the context of other rights. On the other hand, as current commercial practice has created an environment whereby personal data are a property right within the context of the Charter, this amendment would most probably result in privacy being given an even higher ranking when courts come to “balance” rights..</p>	

Amendment 21 Proposal for a Regulation Article 2 – paragraph 2 – point d	
<i>Commission Proposal</i>	<i>Amendment</i>
d) by a natural person without any gainful interest in the course of its own exclusively personal or household activity;	d) by a natural person without any gainful interest in the course of its own exclusively personal or household activity <i>and on condition that no personal data are made accessible to an indefinite number of people;</i>
<p>Comment: As already mentioned in our comments on amendment 1, EDRI welcomes this change, which limits the application of this exception.</p>	

Amendment 22 Proposal for a Regulation Article 4 – point 2 bis	
<i>Commission Proposal</i>	<i>Amendment</i>
	<i>(2a) ‘data rendered sufficiently anonymous’ means data, the information on personal or material characteristics contained in which can no longer be associated with an identified or identifiable individual or could only be so associated at a disproportionate cost in terms</i>

	<i>of time and financial and human resources;</i>
<p>Comment: The problem with this formulation is that with technological progress, the means for de-anonymising data advance quickly. In other words: it is likely that measures that are 'disproportionate' today will not be 'disproportionate' in several years, which removes the increased legal certainty that the amendment was intended to create.</p> <p>Furthermore, it should be noted that the French version of recital 23, which is the motivation behind this amendment, is slightly different from other language versions:</p> <p>French: “données qui ont été rendues suffisamment anonymes pour que la personne concernée ne soit plus identifiable”</p> <p>English: “data rendered anonymous in such a way the data subject is no longer identifiable”</p> <p>German: “Daten [...], die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht mehr identifiziert werden kann”</p> <p>Spanish: “datos convertidos en anónimos de forma que el interesado a quien se refieren ya no resulte identificable”</p> <p>In the other language versions, there is no element of 'suffisamment' ('sufficiently'), which suggests the possibility of varying degrees of anonymisation. Instead, they talk about complete anonymisation. For this reason, it seems appropriate to interpret recital 23 in line with other language versions. This is also more prudent, taking technological progress into account.</p>	

Amendment 23 Proposal for a Regulation Article 4 – point 13	
<i>Commission Proposal</i>	<i>Amendment</i>
<p>(13) ‘main establishment’ means as regards the controller, the place of its establishment in the Union where <i>the main decisions as to the purposes, conditions and means of the processing of personal data are taken</i>; if no decisions as to the purposes, conditions and means of the processing of personal data are taken in the Union, the main establishment is the place where the main processing activities in the context of the activities of an establishment of a controller in the Union take place. As regards the processor, ‘main establishment’ means the place of its central administration in the Union;</p>	<p>(13) ‘main establishment’ means as regards the controller, the place of its establishment in the Union where personal data <i>protection policy is determined, taking into account the dominant influence of the establishment over others, particularly in the case of a group of companies, the implementation of rules on personal data protection and rules relevant for data protection</i>; if no decisions as to the purposes, conditions and means of the processing of personal data are taken in the Union, the main establishment is the place where the main processing activities in the context of the activities of an establishment of a controller in the Union take place. As regards the processor, ‘main establishment’ means the</p>

	place of its central administration in the Union;
Comment: As already indicated in our comments on amendment 4 , EDRI supports this definition of the term 'main establishment'.	

Amendment 24 Proposal for a Regulation Article 6 – paragraph 1 – point f	
<i>Commission Proposal</i>	<i>Amendment</i>
f) processing is necessary for the purposes of the legitimate interests pursued by a controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks.	f) processing is necessary for the purposes of the legitimate interests pursued by a controller or by a third party or third parties to whom the data are communicated , except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks.
Comment: This formulation dilutes the concept of purpose limitation, effectively destroying one of the key pillars of data protection. To give an example: when a data consents to a data transfer, this is usually done for a specific purpose. If the legitimate interest of this third party, which can be different from those of the controller, constituted a reason for lawfulness, the principle of purpose limitation would be seriously infringed. This would leave citizens with little or no control over their personal data. See also amendment 5 above.	

Amendment 25 Proposal for a Regulation Article 6 – paragraph 5	
<i>Commission Proposal</i>	<i>Amendment</i>
5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the conditions referred to in point (f) of paragraph 1 for various sectors and data processing situations, including as regards the processing of personal data related to a child.	deleted
Comment:	

Amendment 26
 Proposal for a Regulation
Article 7 – paragraph 4 a (new)

<i>Commission Proposal</i>	<i>Amendment</i>
	4a. The legislation of the Member State in which a person lacking the legal capacity to act resides shall apply when determining the conditions under which consent is given or authorised by that person.

Comment: This amendment increases legal certainty regarding the consent of persons without legal capacity to act.

Amendment 27
 Proposal for a Regulation
Article 8 – paragraph 1

<i>Commission Proposal</i>	<i>Amendment</i>
1. For the purposes of this Regulation, in relation to the offering of information society services directly to a child, the processing of personal data of a child below the age of 13 years shall only be lawful if and to the extent that consent is given or authorised by the child's parent or custodian . The controller shall make reasonable efforts to obtain verifiable consent, taking into consideration available technology.	1. For the purposes of this Regulation, in relation to the offering of goods or services directly to a child, the processing of personal data of a child below the age of 13 years shall only be lawful if and to the extent that consent is given or authorised by the child's parent or legal representative . The controller shall make reasonable efforts to obtain verifiable consent, taking into consideration available technology.

Comment: EDRi welcomes the Rapporteur's proposal to enlarge the scope of this provision to all goods and services offered directly to children below the age of 13. This will ensure better protection for them.

Amendment 28
 Proposal for a Regulation
Article 11 – paragraph 2

<i>Commission Proposal</i>	<i>Amendment</i>
2. The controller shall provide any information and any communication relating to the processing of personal data to the data subject in	2. The controller shall provide any information and any communication relating to the processing of personal data to the data subject in

an intelligible form, using clear and plain language, <i>adapted to the data subject</i> , in particular for any information addressed specifically to a child.	an intelligible form, using clear and plain language, in particular for any information addressed specifically to a child.
Comment: In her justification for this amendment, the rapporteur considers that children are the only group in need of adapted information, but there are also other groups which could benefit from such adapted information, for example people with physical limitations or lack of technical awareness.	

Amendment 29 Proposal for a Regulation Article 12 – paragraph 5	
<i>Commission Proposal</i>	<i>Amendment</i>
5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the manifestly excessive requests and the fees referred to in paragraph 4.	<i>deleted</i>
Comment:	

Amendment 30 Proposal for a Regulation Article 12 – paragraph 6	
<i>Commission Proposal</i>	<i>Amendment</i>
6. The Commission may lay down standard forms and specifying standard procedures for the communication referred to in paragraph 2, including the electronic format. In doing so, the Commission shall take the appropriate measures for micro, small and medium-sized-enterprises. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	<i>deleted</i>
Comment:	

Amendment 31
 Proposal for a Regulation
Article 14 – paragraph 1 – point c

<i>Commission Proposal</i>	<i>Amendment</i>
c) the period for which the personal data will be stored;	c) <i>the criteria for determining</i> the period for which the personal data will be stored <i>for each purpose</i> ;
<p>Comment: This amendment includes two changes: (1) distinguishing between retention for different purposes (if they exist) and (2) to replace the 'period' with the 'criteria allowing' to determine it. EDRi supports the first part, but has some doubts on the wording of the second part. The reason is that this part could open a loophole allowing controllers to provide data subjects only with unclear criteria instead of a fixed period (see also comments on amendment 6).</p>	

Amendment 32
 Proposal for a Regulation
Article 14 – paragraph 1 – point g

<i>Commission Proposal</i>	<i>Amendment</i>
g) where applicable, that the controller intends to transfer to a third country or international organisation and <i>on the level of protection afforded by that third country or international organisation by reference to</i> an adequacy decision by the Commission;	h) any further information <i>which the controller considers</i> necessary to guarantee fair processing in respect of the data subject, having regard to the specific circumstances in which the personal data are collected.
<p>Comment: On the one hand, it seems reasonable that if an adequacy decision exists, the controller should not have to supply additional information. On the other hand, if there is no decision, it seems appropriate to include an obligation for the controller to specify the appropriate safeguards adduced, namely the binding corporate rules or other basis for the transfer.</p>	

Amendment 33
 Proposal for a Regulation
Article 14 – paragraph 1 – point h

<i>Commission Proposal</i>	<i>Amendment</i>
h) any further information necessary to guarantee fair processing in respect of the data subject, having regard to the specific circumstances in which the personal data are collected.	h) any further information <i>which the controller considers</i> necessary to guarantee fair processing in respect of the data subject, having regard to the specific circumstances in which the personal data are collected.

Comment: As the Rapporteur explains, it should be clarified that controllers can provide a higher level of transparency. Nonetheless, the Commission proposal does not stop controllers from providing additional information. On the other hand, by specifying that the decision on which other elements are deemed necessary is to be made by the controller, the risk of less benevolent controllers omitting this information is created. To give an example: for measures based on profiling, additional information on the logic behind the measure should be provided. In this case, it would seem advisable to leave the decision which other information should be provided to the DPA, which could oblige the controller to supply it.

Amendment 34
Proposal for a Regulation
Article 15 – paragraph 2

<i>Commission Proposal</i>	<i>Amendment</i>
2. The data subject shall have the right to obtain from the controller communication of the personal data undergoing processing. Where the data subject makes the request in electronic form, the information shall be provided in electronic form, unless otherwise requested by the data subject.	2. The data subject shall have the right to obtain from the controller communication of the personal data undergoing processing. Where the data subject makes the request in electronic form, the information shall be provided in electronic form, unless otherwise requested by the data subject. <i>The controller shall use all reasonable measures to verify the identity of a data subject requesting access to data.</i>

Comment: It is true, as the Rapporteur says, that the right of access should not be abused. It is also true that controllers may not collect and store data just to be able to respond to access requests (see recital 52). In any case, the controller already has to verify the authenticity of the request. It should be specified that data collected for the purpose of verifying requests must only be used for this purpose.

Amendment 35
Proposal for a Regulation
Article 17 – paragraph 2 a (new)

<i>Commission Proposal</i>	<i>Amendment</i>
	<i>2a. The controller referred to in paragraph 1 shall inform the data subject of the action taken in response to their request by the third parties referred to in paragraph 2.</i>

Comment: A similar provision should also be added to Article 13.

Amendment 36
 Proposal for a Regulation
Article 18

<i>Commission Proposal</i>	<i>Amendment</i>
[...]	<i>deleted</i>
Comment: See comment on amendment 8 above.	

Amendment 37
 Proposal for a Regulation
Article 21 – paragraph 2

<i>Commission Proposal</i>	<i>Amendment</i>
2. In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions at least as to the objectives to be pursued by the processing and the determination of the controller.	2. In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions at least as to <i>the aim of the processing</i> , the objectives to be pursued by the processing and the determination of the controller.
Comment: EDRi advocates phrasing the restrictions in Article 21 more narrowly. The Rapporteur's amendment is a good first step in this direction. However, we would suggest adding further specifications. See http://protectmydata.eu/articles/articles-21-30/article-21/ for suggested wording.	

Amendment 38
 Proposal for a Regulation
Article 22 – titre

<i>Commission Proposal</i>	<i>Amendment</i>
<i>Responsibility</i> of the controller	<i>Overall principle of responsibility</i> of the controller.
Comment: Giving a new and clearer name to this Article helps to reinforce this principle.	

Amendment 39
 Proposal for a Regulation
Article 23 – paragraph 2

<i>Commission Proposal</i>	<i>Amendment</i>
----------------------------	------------------

<p>2. The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals.</p>	<p>2. The controller shall implement mechanisms for ensuring that, by default, only those personal data are collected for purposes which are defined, explicit and legitimate and only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals.</p>
<p>Comment: Limiting data collection is a corollary of the principles of data protection by design and by default. It should also be specified that these measures should be put in place using technical and/or organisational measures and that the aim is to increase data subjects' ability to control their own data. EDRproposes wording to improve this provision on http://protectmydata.eu/articles/articles-21-30/article-23/ .</p>	

Amendment 40 Proposal for a Regulation Article 23 – paragraph 3	
<i>Commission Proposal</i>	<i>Amendment</i>
<p>3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures and mechanisms referred to in paragraph 1 and 2, in particular for data protection by design requirements applicable across sectors, products and services.</p>	<p>deleted</p>
<p>Comment:</p>	

Amendment 41 Proposal for a Regulation Article 23 – paragraph 4	
<i>Commission Proposal</i>	<i>Amendment</i>

4. The Commission may lay down technical standards for the requirements laid down in paragraph 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).	<i>deleted</i>
Comment:	

Amendment 42 Proposal for a Regulation Article 28 – paragraph 1	
<i>Commission Proposal</i>	<i>Amendment</i>
1. Each controller and processor and, if any, the controller's representative, shall maintain documentation of all processing operations under its responsibility.	1. Each controller and processor and, if any, the controller's representative, shall maintain documentation of all processing systems and procedures under its responsibility.
Comment: This amendment and the following ones (until amendment 46) aim at a reorganisation of the documentation obligations. The Rapporteur justifies them by referring to the EDPS opinion. However, these amendments only introduce part of the EDPS' recommendations: documentation obligations are eased, but the balancing measures – that is to say the obligation to provide additional documentation on request of the DPA and removing the exemption for SMEs – are missing (see pt. 190 of the EDPS opinion). For this reason, EDRi suggests to follow the EDPS' recommendation more comprehensively.	

Amendment 43 Proposal for a Regulation Article 28 – paragraph 2 – partie introductive	
<i>Commission Proposal</i>	<i>Amendment</i>
2. The documentation shall contain at least the following information:	2. The documentation shall contain the following information:
Comment: It is obvious that, in order to be in compliance with this Article, it is enough to document the elements listed in it. The Commission proposal also allows controllers who want to be more transparent to add additional elements.	

Amendment 44

Proposal for a Regulation Article 28 – paragraph 2 – point d	
<i>Commission Proposal</i>	<i>Amendment</i>
<i>d) a description of categories of data subjects and of the categories of personal data relating to them;</i>	<i>deleted</i>
Comment: See comments on amendment 42 above.	

Amendment 45	
Proposal for a Regulation Article 28 – paragraph 2 – point e	
<i>Commission Proposal</i>	<i>Amendment</i>
<i>e) the recipients or categories of recipients of the personal data, including the controllers to whom personal data are disclosed for the legitimate interest pursued by them;</i>	<i>deleted</i>
Comment: See comments on amendment 42 above.	

Amendment 46	
Proposal for a Regulation Article 28 – paragraph 2 – point g	
<i>Commission Proposal</i>	<i>Amendment</i>
<i>g) a general indication of the time limits for erasure of the different categories of data;</i>	<i>deleted</i>
Comment: See comments on amendment 42 above.	

Amendment 47	
Proposal for a Regulation Article 30 – paragraph 3	
<i>Commission Proposal</i>	<i>Amendment</i>

<p>3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the technical and organisational measures referred to in paragraphs 1 and 2, including the determinations of what constitutes the state of the art, for specific sectors and in specific data processing situations, in particular taking account of developments in technology and solutions for privacy by design and data protection by default, unless paragraph 4 applies.</p>	<p><i>deleted</i></p>
<p>Comment:</p>	

<p>Amendment 48 Proposal for a Regulation Article 31 – paragraph 1</p>	
<p><i>Commission Proposal</i></p>	<p><i>Amendment</i></p>
<p>1. In the case of a personal data breach, the controller shall, without undue delay and, where feasible, not later than 24 hours after having become aware of it, notify the personal data breach to the supervisory authority. The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within 24 hours.</p>	<p>1. In the case of a personal data breach which has a considerable effect on the data subject, the controller shall, without undue delay after having become aware of it, notify the personal data breach to the supervisory authority.</p>
<p>Comment: EDRi would be in favour of a fixed period for the notification, for the reasons given in our comments to amendment 12.</p>	

<p>Amendment 49 Proposal for a Regulation Article 33 – paragraph 2 – introduction</p>	
<p><i>Commission Proposal</i></p>	<p><i>Amendment</i></p>
<p>2. The following processing operations <i>in particular</i> present specific risks referred to in paragraph 1:</p>	<p>2. The following processing operations present specific risks referred to in paragraph 1:</p>

Comment: In order to ensure that these categories can be interpreted to adapt to new technological developments, it is preferable to have a non-exhaustive list.

Amendment 50
Proposal for a Regulation
Article 33 – paragraph 4

<i>Commission Proposal</i>	<i>Amendment</i>
4. The controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations.	deleted
<p>Comment: Consulting data subjects can help to obtain important information on the impact of planned processing operations. For this reason, the Commission's wording should be upheld.</p>	

Amendment 51
Proposal for a Regulation
Article 34 – titre

<i>Commission Proposal</i>	<i>Amendment</i>
Prior authorisation and prior consultation	Prior consultation
<p>Comment:</p>	

Amendment 52
Proposal for a Regulation
Article 34 – paragraph 1

<i>Commission Proposal</i>	<i>Amendment</i>
1. The controller or the processor as the case may be shall obtain an authorisation from the supervisory authority prior to the processing of personal data, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where a controller or processor adopts contractual clauses as provided for in point (d) of Article 42(2) or does not provide for the appropriate	deleted

<i>safeguards in a legally binding instrument as referred to in Article 42(5) for the transfer of personal data to a third country or an international organisation.</i>	
Comment: This amendment simply moves part of the Article to a different part of the Regulation.	

Amendment 53 Proposal for a Regulation Article 40 a (new)	
<i>Commission Proposal</i>	<i>Amendment</i>
	Article 40 a Prior authorisation <i>The controller or the processor as the case may be shall obtain an authorisation from the supervisory authority prior to the processing of personal data, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where a controller or processor adopts contractual clauses as provided for in point (d) of Article 42(2) or does not provide for the appropriate safeguards in a legally binding instrument as referred to in Article 42(5) for the transfer of personal data to a third country or an international organisation.</i>
Comment: This amendment simply moves part of the Article to a different part of the Regulation.	

Amendment 54 Proposal for a Regulation Article 41 – paragraph 3	
<i>Commission Proposal</i>	<i>Amendment</i>
3. The Commission may decide that a third country, or a territory or a processing sector within that third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure set	3. The Commission may decide that a third country, or a territory or a processing sector within that third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2.

<i>out in Article 87(2).</i>	
Comment: As the Rapporteur explains, the EDPB should be consulted in this context. It seems appropriate to specifically mention this consultation in this Article.	

Amendment 55 Proposal for a Regulation Article 42 – paragraph 1	
<i>Commission Proposal</i>	<i>Amendment</i>
1. Where the Commission has taken no decision pursuant to Article 41, a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has adduced appropriate safeguards with respect to the protection of personal data in a legally binding instrument.	1. Where the Commission has taken no decision pursuant to Article 41, <i>or if it finds that a third country, a region or a data processing sector in a third country, or an international organisation, does not offer a sufficient level of data protection</i> , a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has adduced appropriate safeguards with respect to the protection of personal data in a legally binding instrument.
Comment: This amendment follows the EDPS opinion.	

Amendment 56 Proposal for a Regulation Article 43 – paragraph 2 a (new)	
<i>Commission Proposal</i>	<i>Amendment</i>
	<i>2a. The supervisory authority which approves the binding corporate rules shall be that of the place of the main establishment of the controller or processor.</i>
Comment: EDRi welcomes the clarification on the competent DPA, but has some fears regarding a race to the bottom. It would seem advisable to specifically submit this kind of approval to the consistency mechanism.	

Amendment 57 Proposal for a Regulation Article 51 – paragraph 1 a (new)
--

<i>Commission Proposal</i>	<i>Amendment</i>
	<i>1a. In the event of a complaint by a data subject or a body, organisation or association referred to in Article 73(2), the supervisory authority responsible shall be that of the Member State in which the complaint was made. It shall be competent to take action on the complaint. It shall also be competent to supervise the controller's processing activities or those of a processor, without prejudice to paragraph 2.</i>
Comment:	

Amendment 58 Proposal for a Regulation Article 51 – paragraph 2	
<i>Commission Proposal</i>	<i>Amendment</i>
<i>2. Where the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union, and the controller or processor is established in more than one Member State, the supervisory authority of the main establishment of the controller or processor shall be competent for the supervision of the processing activities of the controller or the processor in all Member States, without prejudice to the provisions of Chapter VII of this Regulation.</i>	<i>2. In the context of the activities of a controller or a processor established in more than one Member State, the supervisory authority of the Member State where the main establishment of the controller or processor is situated shall be competent for the supervision of the processing activities of the controller or the processor in all Member States. This supervisory authority shall be obliged to cooperate with the other supervisory authorities and with the Commission, pursuant to the provisions of Chapter VII of this Regulation.</i>
Comment: Improving cooperation between DPAs also helps to reduce the burden on DPAs competent for supervising big controllers. We welcome this provision, but have to point out that the aim is above all cooperation between the DPAs themselves. As the Rapporteur notes in her justification for amendment 60 , Chapter VII gives too much weight to the Commission.	

Amendment 59 Proposal for a Regulation Article 59 – paragraph 4	
<i>Commission Proposal</i>	<i>Amendment</i>

4. Where the supervisory authority concerned intends not to follow the opinion of the Commission, it shall inform the Commission and the European Data Protection Board thereof within the period referred to in paragraph 1 and provide a justification. <i>In this case the draft measure shall not be adopted for one further month.</i>	4. Where the supervisory authority concerned intends not to follow the opinion of the Commission, it shall inform the Commission and the European Data Protection Board thereof within the period referred to in paragraph 1 and provide a justification.
Comment: It is important to safeguard the independence of DPAs.	

Amendment 60 Proposal for a Regulation Article 62 – paragraph 2	
<i>Commission Proposal</i>	<i>Amendment</i>
<i>2. On duly justified imperative grounds of urgency relating to the interests of data subjects in the cases referred to in point (a) of paragraph 1, the Commission shall adopt immediately applicable implementing acts in accordance with the procedure referred to in Article 87(3). Those acts shall remain in force for a period not exceeding 12 months.</i>	<i>deleted</i>
Comment: As the Rapporteur points out, the Commission proposal infringes on the independence of the EDPB.	

Amendment 61 Proposal for a Regulation Article 74 – paragraph 4	
<i>Commission Proposal</i>	<i>Amendment</i>
<i>4. A data subject which is concerned by a decision of a supervisory authority in another Member State than where the data subject has its habitual residence, may request the supervisory authority of the Member State where it has its habitual residence to bring proceedings on its behalf against the competent supervisory authority in the other Member State.</i>	<i>deleted</i>

Comment: Although the Rapporteur's reservations towards this provision have their reasons, the alternative has to be considered as well: if the data subject would be obliged to go to court against the DPA of another Member State, this would pose problem regarding language and access to justice.

Amendment 62
Proposal for a Regulation
Article 79 – paragraph 2

<i>Commission Proposal</i>	<i>Amendment</i>
2. The administrative sanction shall be in each individual case effective, proportionate and dissuasive. The amount of the administrative fine shall be fixed with due regard to the nature, gravity and duration of the breach, the intentional or negligent character of the infringement, the degree of responsibility of the natural or legal person and of previous breaches by this person, the technical and organisational measures and procedures implemented pursuant to Article 23 and the degree of co-operation with the supervisory authority in order to remedy the breach.	2. The administrative sanction shall be in each individual case effective, proportionate and dissuasive. The amount of the administrative fine shall be fixed with due regard to the nature, gravity and duration of the breach, the intentional or negligent character of the infringement, <i>the particular categories of personal data</i> , the degree of responsibility of the natural or legal person and of previous breaches by this person, the technical and organisational measures and procedures implemented pursuant to Article 23 and the degree of co-operation with the supervisory authority in order to remedy the breach.

Comment: If sensitive data have been involved in a breach of the Regulation, this should lead to higher fines. Additionally, it should be added that repeat offenders could face higher fines.

Amendment 63
Proposal for a Regulation
Article 79 – paragraph 3

<i>Commission Proposal</i>	<i>Amendment</i>
<p><i>3. In case of a first and non-intentional non-compliance with this Regulation, a warning in writing may be given and no sanction imposed, where:</i></p> <p><i>a) a natural person is processing personal data without a commercial interest; or</i></p> <p><i>b) an enterprise or an organisation employing fewer than 250 persons is processing personal data only as an activity ancillary to its main</i></p>	<p><i>3. The supervisory authority may give a written warning without imposing a sanction. The supervisory authority may impose a fine of up to EUR 1 000 000 for repeated, deliberate breaches or, in the case of a company, of up to 2 % of its annual worldwide turnover.</i></p>

<i>activities.</i>	
<p>Comment: this radical reduction of the provisions on administrative sanctions would help to protect the independence of DPAs by giving them a bigger margin of appreciation. On the other hand, EDRi would like to recall the opinion of the EDPS (pts. 275-279), which called for more guidance on the level of fines. It would seem a good idea for the EDPB to take care of this quickly after being constituted by issuing guidelines. See also the following amendments until amendment 66.</p>	

Amendment 64 Proposal for a Regulation Article 79 – paragraph 4	
<i>Commission Proposal</i>	<i>Amendment</i>
[...]	<i>deleted</i>
<p>Comment: see comments on amendment 63 above.</p>	

Amendment 65 Proposal for a Regulation Article 79 – paragraph 5	
<i>Commission Proposal</i>	<i>Amendment</i>
[...]	<i>deleted</i>
<p>Comment: see comments on amendment 63 above.</p>	

Amendment 66 Proposal for a Regulation Article 79 – paragraph 6	
<i>Commission Proposal</i>	<i>Amendment</i>
[...]	<i>deleted</i>
<p>Comment: see comments on amendment 63 above.</p>	

Amendment 67 Proposal for a Regulation Article 79 – paragraph 7	
--	--

<i>Commission Proposal</i>	<i>Amendment</i>
[...]	<i>deleted</i>
Comment:	

Amendment 68	
Proposal for a Regulation Article 86 – paragraph 2	
<i>Commission Proposal</i>	<i>Amendment</i>
2. The <i>delegation of</i> power referred to in Article 6(5) , Article 8(3), Article 9(3), Article 12(5) , Article 14(7), Article 15(3), Article 17(9), Article 20(6), Article 22(4), Article 23(3), Article 26(5), Article 28(5), Article 30(3), Article 31(5), Article 32(5), Article 33(6), Article 34(8), Article 35(11), Article 37(2), Article 39(2), Article 43(3), Article 44(7), Article 79(6) , Article 81(3), Article 82(3) and Article 83(3) shall be conferred on the Commission for an indeterminate period of time from the date of entry into force of this Regulation.	2. The <i>delegation of</i> power referred to in Article 6(5) , Article 8(3), Article 9(3), Article 12(5) , Article 14(7), Article 15(3), Article 17(9), Article 20(6), Article 22(4), Article 23(3), Article 26(5), Article 28(5), Article 30(3), Article 31(5), Article 32(5), Article 33(6), Article 34(8), Article 35(11), Article 37(2), Article 39(2), Article 43(3), Article 44(7), Article 79(6) , Article 81(3), Article 82(3) and Article 83(3) shall be conferred on the Commission for an indeterminate period of time from the date of entry into force of this Regulation.
CommentComment:	

Amendment 69	
Proposal for a Regulation Article 86 – paragraph 3	
<i>Commission Proposal</i>	<i>Amendment</i>
3. The delegation of power referred to in Article 6(5) , Article 8(3), Article 9(3), Article 12(5) , Article 14(7), Article 15(3), Article 17(9), Article 20(6), Article 22(4), Article 23(3), Article 26(5), Article 28(5), Article 30(3) , Article 31(5), Article 32(5), Article 33(6), Article 34(8), Article 35(11), Article 37(2), Article 39(2), Article 43(3), Article 44(7), Article 79(6) , Article 81(3), Article 82(3) and	3. The delegation of power referred to in Article 8(3), Article 9(3), Article 14(7), Article 15(3), Article 17(9), Article 20(6), Article 22(4), Article 23(3), Article 26(5), Article 28(5), Article 31(5), Article 32(5), Article 33(6), Article 34(8), Article 35(11), Article 37(2), Article 39(2), Article 43(3), Article 44(7), Article 81(3), Article 82(3) and Article 83(3) may be revoked at any time by the European

Article 83(3) may be revoked at any time by the European Parliament or by the Council. A decision of revocation shall put an end to the delegation of power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.	Parliament or by the Council. A decision of revocation shall put an end to the delegation of power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.
---	--

Comment:

Amendment 70

Proposal for a Regulation
Article 86 – paragraph 5

<i>Commission Proposal</i>	<i>Amendment</i>
5. A delegated act adopted pursuant to Article 6(5) , Article 8(3), Article 9(3), Article 12(5) , Article 14(7), Article 15(3), Article 17(9), Article 20(6), Article 22(4), Article 23(3), Article 26(5), Article 28(5), Article 30(3) , Article 31(5), Article 32(5), Article 33(6), Article 34(8), Article 35(11), Article 37(2), Article 39(2), Article 43(3), Article 44(7), Article 79(6) , Article 81(3), Article 82(3) and Article 83(3) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or the Council.	5. A delegated act adopted pursuant to Article 8(3), Article 9(3), Article 14(7), Article 15(3), Article 17(9), Article 20(6), Article 22(4), Article 23(3), Article 26(5), Article 28(5), Article 31(5), Article 32(5), Article 33(6), Article 34(8), Article 35(11), Article 37(2), Article 39(2), Article 43(3), Article 44(7), Article 81(3), Article 82(3) and Article 83(3) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or the Council.

Comment:

Amendment 71

Proposal for a Regulation

Article 86 – paragraph 5a (new)

<i>Commission Proposal</i>	<i>Amendment</i>
	<i>5a. The Commission will promote technological neutrality on adoption of the acts referred to in this Article.</i>
Comment: Ensuring technological neutrality is very important in order to make sure that these acts are “future-proof”.	



European-American
Business Council



UNITED STATES COUNCIL FOR
INTERNATIONAL BUSINESS

16 October 2012
Ms Amelia Andersdotter
Member of the European Parliament
Brussels

Re: EU Data Protection Regulation

Dear Ms Andersdotter,

We, the undersigned organizations, provide the following comments as uniform input into the legislative review process currently being undertaken of the draft General Data Protection Regulation formally proposed by the European Commission on 25 January 2012. Business shares with government the desire for data protection regulation that accomplishes the twin goals of providing for effective protection of personal data and privacy while enabling the data flows that are needed by new technologies and business models to foster both economic growth and societal benefit in Europe and globally. We also wish to recognize and applaud the commitment to multi-stakeholder consultation that has been evidenced by the EU, the US and other countries in their consideration of data protection issues and development of policy and regulatory instruments.

The topics outlined in this letter represent a high-level consensus among all the undersigned organizations of important considerations which should be taken into account in the review of this draft Regulation, both to ensure the intended benefits and to ensure that other requirements, as drafted or further elaborated in delegated or implementing acts, do not create undue burdens for business or data protection authorities (DPAs) or unintended consequences. While seeking to enhance the fundamental right of the protection of personal data, an overall objective of the new data protection rules must be to not unduly constrain innovation, hamper economic growth, limit the competitiveness of the EU economy or otherwise diminish the potential for societal benefits of new or established technologies and business models. We believe this balance is not yet achieved and the current text considerably adds additional burden for businesses. The draft regulation lacks a risk-based approach to data protection and does not appropriately recognize the need to more carefully consider the context of application or the varying consequences of failures of protection. All data is not equal and should not be treated as such. For the majority of

the changes being proposed, there is no indication as to why the high level of protection under the existing data protection framework should have to be increased any further. To strike an appropriate balance we suggest the following.

High-level Recommendations for Review of the Draft Regulation:

1. **Reduced administrative burdens:** While the choice of instrument, a Regulation, stands to harmonize applicable law for the protection of personal data across the EU, it is essential that provisions pertaining to jurisdiction, in particular the concept of the lead supervisory authority, are clarified, strengthened and implemented in a practical fashion. Business considers clarity over applicable law and jurisdiction to be key benefits to the revised rules and essential to the endorsement of the Draft Regulation.
2. **Practical operational requirements:** The need to ensure that operational requirements for organizations are practicable, not unduly burdensome, take cost appropriately into account and do not result in unintended consequences that could constrain growth, benefits or innovation. Some of the most important issues include:
 - The range and specificity of detail required of documentation which could create significant and needless burdens. These requirements need to be flexible to address different business models and levels of data risk for different businesses.
 - The number of Data Protection Impact Assessments (DPIAs) required: their content, scope and need for prior notification or approval which could needlessly increase cost and unduly constrain both innovation and the timely provision of services.
 - The scope of the definition of breach and associated notification requirements, especially the concepts of notification within a reasonable timeframe, mitigating effects of safeguards (encryption, etc) and potential for harm or adverse impact which pose issues of practicability and undue burden.
 - The limited practicability of the right to be forgotten beyond the site collecting the information.
3. **Clarity and predictability:** The need for clarity and predictability in the requirements and their implementation. Issues for consideration include:
 - The need to recognize that harmonization and predictability relate to how the Regulation will be applied and do not imply the need for overly detailed and prescriptive requirements.
 - New independent obligations on processors, which would create confusion as to obligations and responsibilities between controllers and processors, should be reconsidered in favor of better applying existing requirements.
 - The need for further guidance on the potential development of certification, Privacy by Design and Privacy by Default concepts, and the appropriateness of their inclusion in a Regulation.

- The overuse of the provision for delegated acts and the failure to scope or limit the nature or potential impact of the delegated acts or provide for stakeholder consultation related to their practicability and impact.
4. Proportionality, cost-effectiveness and competitiveness: The need to increase consideration of proportionality, cost-effectiveness and competitiveness. Issues for consideration include:
- The need to review the alignment between the recitals stating the objectives of the Regulation, broadly supported by Business, with the requirements set out in the articles which are often more problematic. Overly prescriptive requirements inhibit the goal of the Regulation to be technology neutral and to reflect appropriate compliance for different business types i.e. data focused models such as social media companies vs. businesses which process only employee and business contact details.
 - The need to consider the potential negative implications, both for the protection of personal data and for the development, whether by government or the private sector, of new and existing services, of an overbroad definition of personal information, an overly strict and inflexible approach to “consent” or excessively strict limitations on profiling which could affect the legitimate interests of data controllers.
 - While there is a general recognition of the need to enhance credible enforcement mechanisms, specifically sanctions and fines, the current proposal lacks proportionality and may make the EU less competitive in attracting investment in facilities or services without necessarily adding to the protection of personal data and privacy. Furthermore, the mandatory nature of the fine may not allow mitigating factors and the context of the acts to be properly taken into account. Other sanctions, such as specific performance, may be more effective and appropriate than fines, and DPAs need to have discretion to enforce based on the facts of each case.
5. Interoperability of privacy frameworks: The need to consider opportunities for facilitating responsible global information flows by evaluating interoperability of EU frameworks with those outside the EU. European and global companies have a substantial economic need for cross-border data flows between countries and regions with very different privacy regimes. An interoperable international privacy regime that recognizes differing privacy rules (such as the US multi-stakeholder process) to the greatest extent possible, and honors these rules, would greatly accommodate companies operating in multiple jurisdictions and facilitate global economic growth. Topics for consideration could include:
- While specific inclusion of Binding Corporate Rules (BCRs) is welcome, BCRs for processors and the ability to use BCRs across groups of companies would enhance the utility of BCRs in the cloud and other global environments.
 - Guidance of how codes of conduct, sectoral adequacy, appropriate safeguards and legitimate interest may be used as a basis for transfers would ensure that businesses can optimize responsible information transfers in ways that comply with the draft Regulation.
6. Clarification of “Profiling”: The need to ensure that the provisions relating to “profiling” do not prevent businesses from being able to evaluate and analyze data and use such data

predicatively for legitimate business purposes, including identity verification and fraud detection and prevention. Additional issues for consideration include:

- Clarification of the phrase “measures based on profiling” to make it clear that legitimate business uses of data will be permissible.
- Clarification of the terms “legal effects” or “significantly affects” as applicable to “profiling” and how permissible uses of data are otherwise limited.

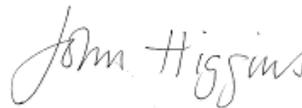
The topics presented above represent a consensus among the undersigned organizations of important issues that need to be addressed in the review of the draft Regulation. The undersigned organizations will, as appropriate to their membership and expertise, provide more detailed comments outlining substantive concerns and suggested resolutions to those concerns as well as more specific topics which may be more directed at specific sectors of types of services.

We look forward to working with the EU Council, Parliament, Member States and the Commission in the further enhancement of the Regulation. We seek to ensure the continued and effective protection of personal data and privacy while also ensuring that Business can remain innovative and flexible in using the new technologies and business models to enhance continued economic growth, societal benefit and EU competitiveness.

Sincerely,



Susan Danger
Managing Director
AmCham EU



John Higgins
Director-General
DIGITALEUROPE



Kristen Verderame
Interim President & CEO
European-American Business Council



Ken Wasch
President
Software & Information Industry Association



Peter Robinson
President & CEO
United States Council for International Business

Eurofinas proposals for amendments on the Commission's Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (COM(2012) 11 final)

October 2012

ABOUT EUROFINAS

Eurofinas, the European Federation of Finance House Associations, is the voice of the specialised consumer credit providers in the EU. As a Federation, Eurofinas brings together associations throughout Europe that represent finance houses, universal banks, specialised banks and captive finance companies of car, equipment, etc. manufacturers. The scope of products covered by Eurofinas members includes all forms of consumer credit products such as personal loans, linked credit, credit cards and store cards. Consumer credit facilitates access to assets and services as diverse as cars, education, furniture, electronic appliances, etc. It is estimated that together Eurofinas members financed over 328 billion Euros worth of new loans during 2011 with outstandings reaching 821 billion Euros at the end of the year.



General Observations

Eurofinas believes that the Commission's Proposal for a General Data Protection Regulation¹ provides a good starting point to further discussions and debate on the EU framework for the protection of personal data.

Although we appreciate that this Proposal is a horizontal instrument applicable across sectors, we feel that a number of aspects are ill-suited for financial services, and in particular consumer credit. We believe it is critical to ensure that the framework would also be workable and efficient for highly regulated sectors such as consumer credit providers, taking into account their operational functioning, key features and the data processing they must carry out in accordance with other legislation.

Against this backdrop, Eurofinas would like to draw your attention to some suggested amendments, which we believe are essential to ensure that lenders can adhere to the aforementioned legislation and carry out sound and responsible lending practices when adopting the new legislative proposal.

The document in hand should be read in conjunction with the March 2012 Eurofinas observations on the Commission's Proposal² as well as the work the Federation has recently conducted together with ACCIS on fraud and consumer lending resulting in the release of a report on fraud prevention and data protection (available [here](#)).

We would be pleased to answer any question you may have on these elements. Feel free to contact Eurofinas legal adviser Anke Delava (a.delava@eurofinas.org, T: +32 2 778 05 73).

¹ European Commission Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (COM(2012) 11 final).

² See <http://www.eurofinas.org/uploads/documents/positions/Eurofinas%20observations%20-%20final.pdf>.



Summary of concerns and suggested amendments

Proposal for a General Data Protection Regulation

Priority concerns:

Data minimisation – Amendment 6, 8 and 49

The obligation to process the minimum data necessary would contradict with legal provisions which require, e.g. lending institutions, to process personal data such as the Consumer Credit Directive and the Capital Requirements Package. Therefore wording of Directive 95/46/EC which permits “not excessive” processing is more appropriate.

Lawfulness of processing – Amendment 10

Article 6(1)(c) should be widened-up to include also the requirements of supervisory authorities.

Fraud prevention and detection – Amendment 11, 14, 15, 38

Experience in practice has shown that these provisions often do not permit the processing of data for fraud prevention and detection purposes. Detecting and preventing fraud is of paramount importance for data controllers. Not only for the controller in question but also to protect data subjects from, for example, falling victim to a loan fraudulently being taken out in their name. Fraud prevention and detection should be explicitly recognised as a legitimate purpose for data processing.

Fraud databases – Amendment 20

In some Member States credit and financial institutions can set up databases which contain data on fraud committed against consumer credit providers. Processing and sharing of this data with other providers is permitted in order to allow credit providers to prevent fraud and minimise risks. To ensure that these databases, whose existence is essential to protect both consumers and businesses, can continue to exist and operate, this provision should reflect the rules currently in place (Article 8(7) of Directive 95/46/EC).

Definition of consent – Amendment 1, 2

The current definition of the data subject’s consent requires more clarification. The word “explicit” should be deleted. Consent given by the data subject in a tacit way should be allowed, and therefore the definition should also cover a tacit consent.

Burden of proof for consent – Amendment 16

There is no justification for a burden of proof for the controller only, especially in cases, where the data subject has the consent in his personal documents.

Withdrawal of consent – Amendment 17

Data controllers will need to process data even after the withdrawal of consent by the data subject, in order to, for example, continue the contractual relationship that may exist between the controller and the subject, as well as allowing for the fulfillment of any obligation on the part of the controller incurred at the request of or under a contract with the data subject. Therefore, where consent has been withdrawn, the continued processing in accordance with another legal basis, as set out in Article 6(1) of the Proposal should be permitted.

Significant imbalance – Amendment 18 and 19

What can be considered as a “significant imbalance” or “free” consent will be subject to differing national interpretations. This provision should not result in the inability for businesses to process data because an



automatic presumption of an imbalance between the positions of the consumer and business within every relationship between the two parties. To avoid legal uncertainty, paragraph 4 should be deleted or at least amended to ensure that where consent cannot provide a legal basis due to an imbalance, the controller should be permitted to process the data in accordance with another legal basis, as set out in Article 6(1) of the Proposal.

Provision free of charge – Amendment 23 and 24

The provision of data held within a database has a cost. Requesting an appropriate (not for profit) contribution from data subjects for data access is critical in deterring fraudsters from obtaining high volumes of consumers' credit data. If data access upon request were to become free of charge then consumers would face an increased risk of frauds (e.g. 'account takeover') with its attendant detrimental consequences.

Publicly available data – Amendment 28

As the data is already publicly available, such a warranty is not necessary to ensure the protection of fundamental rights. The data has already been published and the data subject already knows this and that his or her data may be processed by third parties.

Right to be forgotten and to erasure – Amendment 31 and 32

The article is designed to protect internet social media users. However, it is difficult to execute for example in the financial sector. The data controllers in, for example, the financial sector are obliged to store some data and therefore they are not able to erase all the data processed on the request of the data subject.

Where controllers are subject to a legal obligation to retain and process data, they may also be obliged to transfer this data to relevant supervisory authorities, such as suspicious transaction reports to financial intelligence units in the context of anti-money laundering rules. Therefore further dissemination should be possible. The "without delay" requirement must be qualified to ensure that it is realistic.

Automated decisions – Amendment 39-47

Art. 20 concerns automated processing. The title of this article should therefore be amended to "Measures based on automated processing." Art. 20(1) should retain the reference to "creditworthiness" introduced under Directive 95/46/EC and is preferable to "economic situation."

It cannot be the task of data controllers to check, whether the Member State law "lays down suitable measures to safeguard the data subject's legitimate interests". On the contrary, firms have to be able to rely on the law.

Implementing acts – Amendment 36, 51 and 86

The aim of the Proposal is to introduce a new European framework for data protection that ensures protection of individual's rights and the free movement of data (Article 1), not to standardise processing systems. We strongly oppose any standardisation of IT solutions and technical systems used by controllers to process data, through the adoption of implementing measures.

Delegated acts – Amendment 13, 33, 44, 50, 58, 62, 82-85

Delegated acts would leave the Regulation to be changed substantially over time, likely resulting in business as well as legal uncertainty. In accordance with the provisions of the Treaty delegated acts can only be applied to "non-essential" aspects of the Regulation, rather than, as in the Proposal, on all essential aspects of the Regulation.

The Regulation should therefore not be subject to change in particular on the following issues:

- Lawfulness of processing;
- Right to be forgotten;
- Measures based on profiling;



- Design;
- Communication of personal data breach;
- Data protection impact assessment.

Further key concerns:

Groups of undertakings – Amendment 4

The definition of a ‘group of undertakings’ in Art 4(16) as a controlling undertaking and its controlled undertakings is too narrow and it should be expanded to any group of companies or another comparable economic grouping. A level playing field should be guaranteed to all kind of groups of undertakings.

Principles relating to personal data processing – Amendment 5, 7 and 8

“In a transparent manner” is vague, legally uncertain and redundant, as Article 11 and 14 of the Proposal already require controllers to have transparent and accessible policies and to provide data subjects with substantive information. This should therefore be deleted, reverting back to the wording of Directive 95/46/EC.

The “without delay” requirement must be qualified to ensure that it is realistic.

Further processing – Amendment 5

Article 5(b) and Article 6(4), are contradictory with regard to further processing for purposes incompatible with the purpose for which the data was collected. To clarify the relation between the two Articles and increase legal certainty, Article 5(b) should be rephrased so as to specify that personal data must not be further processed in a way incompatible with the purposes for which it has been collected, unless specific provisions of the regulation provide otherwise.

Specific purposes – Amendment 9

In some Member States, consumers give explicit consent for the processing of their data for general purposes. If explicit consent were to be required for each separate purpose, this would be disproportionately time-consuming, resource-intensive and costly. It is therefore proposed to align the wording with Directive 95/46/EC, currently already in force in the Member States.

Basis provided for in law – Amendment 12 and 32

Whilst it is the responsibility of the Member States to ensure that their national legislation meets the above requirements, data controllers would bear the risks when processing data in accordance with a potentially non-conforming law. This should be avoided to increase legal certainty for controllers and processors.

Providing information electronically – Amendment 21 and 22

The requirement to provide information in electronic form raises concerns about the security of the data. It is not current practice in credit markets. An email request does not enable a lender to validate that the request is from the data subject as there is no guarantee that it will be secure. It would also be a considerable challenge to take appropriate technological measures to ensure security of the data in a way that would work for every customer.

Contract terms and general conditions – Amendment 25

The information to be provided to data subjects shall be an exhaustive list, to ensure that controllers have legal certainty with regard to their information obligations. Data subjects will already have been provided the contract terms and conditions when they signed this contract. The duplication of such a requirement would lead to overloading consumers with information.

Storage period – Amendment 26, 29, 30



Periods for data storage are often not known at the time the data is collected, especially in highly regulated sectors such as financial services where anti-money laundering requires the collection and storage of data throughout the relationship with the client, which may be of an indeterminate period of time.

Information to the data subject – Amendment 27

The term “disproportionate effort” is open to various interpretations and should be clarified.

Right to data portability – Amendment 34 - 37

Article 15 of the Regulation already provides the right of data subjects to access personal data and to obtain communication thereon, i.e. to obtain a copy. Article 18(1) is therefore a repetition and redundant.

Data portability could be open to abuse, as an ill-intended applicant borrower may alter the data in between receiving, for example, his credit history from one processor and presenting it to a lender. The receiving processor would thus not be able to rely on the accuracy of the data. Data may not be stored or processed in the same language, according to the same categories or procedures. This may render data portability of little value. There is also a risk that this provision could require organisations to disclose trade secrets, internal know-how or information on other customers. We are also concerned that data portability may increase the risk of disclosure of personal data to third parties.

In the specific context of credit data, the European Commission’s Expert Group on Credit Histories decided that it should be left to each individual lender to decide which data access model offers the most convenient and cost-effective solution to data portability. The obligation for data portability would not be in line with these findings.

The imposition of technical requirements to enable personal data to become portable, would come at a significant cost for businesses.

Responsibility of the controller – Amendment 48

Introducing an obligation to have the verification carried out by internal/external auditors would introduce an unnecessary duplication of the measures taken by controllers to ensure compliance and an unjustified expense. It should be left to controllers to decide and assess what steps need to be taken to verify adherence to the Regulation.

Processor – Amendment 52-54

The scope of some of the provisions of Article 26 is unclear or repeat obligations already contained in other articles.

Processing under the authority of the controller and processor – Amendment 55

The exemption should not only cover situations where the data processor or the person acting under the authority of the controller or of the processor who has access to personal data is required to process personal data, but also situations where they have the right to process data under the national or EU legislation.

Notification of a personal data breach – Amendment 56, 57, 59

An appropriate time period should be foreseen for notifying the supervisory authority of the substantial amount of information required in Article 31(3) regarding data breaches which are likely to substantially adversely affect data subjects.

In some Member States, credit and financial institutions shall notify the Financial Services Authority where substantial disruptions in services provided to the customers and in payment and IT systems occur. Where such an obligation already exists in national law, this should not be duplicated by an additional obligation to



also notify the data protection supervisor. This sectoral supervisor should instead notify the data protection supervisor.

Data subjects should be informed of a breach where there could be a significant impact on them.

Data Protection Impact Assessment – Amendment 60

Data processors cannot and should not be asked to make the assessment as to whether or not a legal obligation placed upon them poses “a high degree of specific risks”. This is a consideration for the legislator and, at European level, through the opinion of the European Data Protection Supervisor, who advises the Institutions on legislation that affects privacy.

Views of data subjects –Amendment 61

It will be impossible to implement in practice and data subjects’ representatives may not always have the expertise, qualifications or resources to respond to such imposed requests for their views. The supervisory authority will be in better qualified to respond to such requests.

Data Protection Officer – Amendment 63

This provision will prevent someone being replaced in the normal course of the management of a company and its employees. This is particularly pertinent for smaller companies where the data protection officer may well be only part of the individual’s job designation. There has to be flexibility for the firm to be able to reorganise and reshape its employee resources. The officer should be no different position from any other person in a compliance function as far as these issues are concerned.

Transfers by way of appropriate safeguards – Amendment 64--66

The reference to the processor or controller restricts the authorisation to them as the only appropriate parties to provide guarantees for the performance of the international data transfer to a third country, eliminating others such as the importer of the data.

We included as appropriate guarantees the binding declaration of the international organisation or corporate group acting as data importer as an alternative instrument to further facilitate international data flows, thereby avoiding directly subordinating the legality of the transfer to the signing of a contract between the parties, and therefore, the development of multiple contract terms with each of the exporters.

Said declarations could incorporate such elements as the Commission deems necessary in order to safeguard the right to privacy of the citizens of the European Union, in addition to the development of the principle of international cooperation laid down in Article 45(1) of the Regulation.

Derogations to transfer by way of adequacy decision or appropriate safeguards – Amendment 67--69

The reference to the processor or controller restricts the authorisation to them as the only appropriate parties to provide guarantees for the performance of the international data transfer to a third country, eliminating others such as the importer of the data.

Given the new regime for data processors, which includes:

- (i) A written contract between the parties governing the mandated processing of personal data.
 - (ii) The obligation of the controller to select a processor that offers sufficient guarantees that the processing will be tailored to the provisions of these rules,
 - (iii) The documentation of the entire process (art. 28) with details of processing, transfers, documentation, guarantees adopted in the event of transfers, and
 - (iv) The requirement that this documentation is made available to the supervisory authority,
- It should be possible to transfer data in these cases.



Where an activity is conducted subject to specific regulation and supervision, including financial and banking or insurance services, the approval process in these cases should also be exempted given the guarantee that the processing in such activities is subject to regulation and the legitimacy thereof.

Supervisory authorities – Amendment 70--72

The principle of concentration of functions preached by this article should apply in the case of branches and subsidiary companies, affiliates and investees of a parent company, since they share the same foundation.

We understand that it is essential that the supervisory authority support those responsible for compliance with the rules and most especially the Data Protection Officers, in terms of training, information and cooperation to increase the level of compliance with the regulation.

The free services of the supervisory authority must exist regardless of the party requesting it.

Consistency mechanism – Amendment 73

We understand that the consistency mechanism should also be able to be activated by a controller or processor directly or indirectly affected by the measure on which the request applies or any other accredited third party with a legitimate interest in confirming the adequacy of country-level measures applied by a supervisory authority.

Collective redress – Amendment 74, 75

We are opposed to the introduction of class action mechanisms at European level, especially through sector specific legislation. It has not been shown that the absence of such mechanisms has prevented data subjects from exercising their rights.

Sanctions – Amendment 76 - 81

Supervisory authorities should not be obliged to impose sanctions, instead they should only impose sanctions after taking into account all circumstances of each individual case.

The written warning is a persuasive tool which must be used by the supervisory authority the times and where it deems appropriate. In keeping with the spirit and purpose of the Regulation, only intentional non-compliance or impairment of the principles and rights set forth in the Regulation should be subject to financial penalty.



CHAPTER II – Principles

Amendment 1

Article 4(8)

Original wording	Proposed amendment
<p>For the purposes of this Regulation:</p> <p>(8) 'the data subject's consent' means any freely given specific, informed and explicit indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed;</p>	<p>For the purposes of this Regulation:</p> <p>(8) 'the data subject's consent' means any freely given specific, informed, explicit or tacit indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed;</p>

Justification

The current definition of the data subject's consent requires more clarification. The word "explicit" should be deleted. Consent given by the data subject in a tacit way should be allowed, and therefore the definition should also cover a tacit consent.

Amendment 2

Recital 25 – the accompanying recital to Article 4(8)

Original wording	Proposed amendment
<p>Consent should be given explicitly by any appropriate method enabling a freely given specific and informed indication of the data subject's wishes, either by a statement or by a clear affirmative action by the data subject, ensuring that individuals are aware that they give their consent to the processing of personal data, including by ticking a box when visiting an Internet website or by any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data. Silence or inactivity should therefore not constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. If the data subject's consent is to be given following an electronic request, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.</p>	<p>Consent should be given explicitly or tacitly by any appropriate method enabling a freely given specific and informed indication of the data subject's wishes, either by a statement or by a clear affirmative action by the data subject, ensuring that individuals are aware that they give their consent to the processing of personal data, including by ticking a box when visiting an Internet website or by any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data. Silence or inactivity should therefore not constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. If the data subject's consent is to be given following an electronic request, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.</p>



Justification

See justification amendment 1.

Amendment 3

Article 4(16)

Original wording	Proposed amendment
<p>For the purposes of this Regulation:</p> <p>(16) 'group of undertakings' means a controlling undertaking and its controlled undertakings;</p>	<p>For the purposes of this Regulation:</p> <p>(16) 'group of undertakings' means a controlling undertaking and its controlled undertakings; the controlling undertaking should be the undertaking which can exercise a dominant influence over the other undertakings by virtue, for example, of ownership, financial participation or the rules which govern it or the power to have personal data protection rules implemented.;</p>

Justification

The definition of a 'group of undertakings' in Art 4(16) as a controlling undertaking and its controlled undertakings is too narrow and it should be aligned to recital 28. A level playing field should be guaranteed to all kind of groups of undertakings.

Amendment 4

Article 5(a)

Original wording	Proposed amendment
<p>Personal data must be:</p> <p>(a) processed lawfully, fairly and in a transparent manner in relation to the data subject;</p>	<p>Personal data must be:</p> <p>(a) processed lawfully and fairly;</p>

Justification

“In a transparent manner” is vague, legally uncertain and redundant, as Article 11 and 14 of the Proposal already require controllers to have transparent and accessible policies and to provide data subjects with substantive information. This should therefore be deleted, reverting back to the wording of Directive 95/46/EC.



Amendment 5

Article 5(b)

Original wording	Proposed amendment
Personal data must be: (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;	Personal data must be: (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes unless provisions of this Regulation provide otherwise ;

Justification

Article 5(b) and Article 6(4), are contradictory with regard to further processing for purposes incompatible with the purpose for which the data was collected. To clarify the relation between the two Articles and increase legal certainty, Article 5(b) should be rephrased so as to specify that personal data must not be further processed in a way incompatible with the purposes for which it has been collected, unless specific provisions of the regulation provide otherwise.

Amendment 6

Article 5(c)

Original wording	Proposed amendment
Personal data must be: (c) adequate, relevant, and limited to the minimum necessary in relation to the purposes for which they are processed; they shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data;	Personal data must be: (c) adequate, relevant, and not excessive in relation to the purposes for which they are processed; they shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data;

Justification

The obligation to process the minimum data necessary would contradict with legal provisions which require, e.g. lending institutions, to process personal data such as the Consumer Credit Directive and the Capital Requirements Package. Therefore wording of Directive 95/46/EC which permits “not excessive” processing is more appropriate.



Amendment 7

Article 5(d)

Original wording	Proposed amendment
<p>Personal data must be:</p> <p>(d) accurate and kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;</p>	<p>Personal data must be:</p> <p>(d) accurate and kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without unreasonable delay;</p>

Justification

The “without delay” requirement must be qualified to ensure that it is realistic.

Amendment 8

Recital 30 – the accompanying recital to Article 5

Original wording	Proposed amendment
<p>Any processing of personal data should be lawful, fair and transparent in relation to the individuals concerned. In particular, the specific purposes for which the data are processed should be explicit and legitimate and determined at the time of the collection of the data. The data should be adequate, relevant and limited to the minimum necessary for the purposes for which the data are processed; this requires in particular ensuring that the data collected are not excessive and that the period for which the data are stored is limited to a strict minimum. Personal data should only be processed if the purpose of the processing could not be fulfilled by other means. Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted. In order to ensure that the data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review.</p>	<p>Any processing of personal data should be lawful and fair. In particular, the specific purposes for which the data are processed should be explicit and legitimate and determined at the time of the collection of the data. The data should be adequate, relevant and not excessive. Personal data should only be processed if the purpose of the processing could not be fulfilled by other means. Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted. In order to ensure that the data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review.</p>

Justification

See justification amendments 4-7.



Amendment 9

Article 6(1)(a)

Original wording	Proposed amendment
<p>1. Processing of personal data shall be lawful only if and to the extent that at least one of the following applies:</p> <p>(a) the data subject has given consent to the processing of their personal data for one or more specific purposes;</p>	<p>1. Processing of personal data shall be lawful only if and to the extent that at least one of the following applies:</p> <p>(a) the data subject has given consent to the processing of their personal data for one or more purposes;</p>

Justification

In some Member States, consumers give consent for the processing of their data for general purposes. If consent were to be required for each separate purpose, this would be disproportionately time-consuming, resource-intensive and costly. It is therefore proposed to align the wording with Directive 95/46/EC, currently already in force in the Member States.

Amendment 10

Article 6(1)(c)

Original wording	Proposed amendment
<p>1. Processing of personal data shall be lawful only if and to the extent that at least one of the following applies:</p> <p>(c) processing is necessary for compliance with a legal obligation to which the controller is subject;</p>	<p>1. Processing of personal data shall be lawful only if and to the extent that at least one of the following applies:</p> <p>(c) processing is necessary for compliance with a legal obligation, regulatory rule, guidance, industry code of practice, either domestically or internationally to which the controller is subject including the requirements of supervisory authorities;</p>

Justification

Article 6(1)(c) should be widened-up to ensure that domestic financial regulation or codes of conduct are included, in particular the requirements of supervisory authorities.



Amendment 11

Article 6(1)(f)

Original wording	Proposed amendment
<p>1. Processing of personal data shall be lawful only if and to the extent that at least one of the following applies:</p> <p>(f) processing is necessary for the purposes of the legitimate interests pursued by a controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks.</p>	<p>1. Processing of personal data shall be lawful only if and to the extent that at least one of the following applies:</p> <p>(f) processing is necessary for the purposes of the legitimate interests pursued by a controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks. <i>It is within the controller’s legitimate interests to prevent and detect fraud.</i></p> <p>OR</p> <p>(f) processing is necessary for the purposes of the legitimate interests pursued by a controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks.</p> <p><i>It is within the controller’s legitimate interests to prevent and detect fraud, to consult and input into a database for the purpose of the approval, monitoring and recovery of risks, credit transactions and recurring billing services, through the sharing of both positive information and information on defaults. This processing may be managed by service providers with capital and credit solvency subject to compliance with these rules.</i></p>

Justification

The lawfulness of processing based on the legitimate interest must be extended to legitimate interests pursued by third parties to whom the data are disclosed by a controller. To exclude this provision might compromise an essential principle of legitimacy that is very important in the market. It would be contradictory to admit this principle with reference to the controller itself but not with reference to another party (the second controller) receiving data from the former. The result would be



to exclude the possibility for data suppliers to supply on a legitimate basis data to final users of such data even if the legitimate interest is recognised and justified. The limitation is not reasonable and only has the effect to limit the market without providing greater protection for data subjects.

Experience in practice has shown that these provisions often do not permit the processing of data for fraud prevention and detection purposes. Detecting and preventing fraud is of paramount importance for data controllers. Not only for the controller in question but also to protect data subjects from, for example, falling victim to a loan fraudulently being taken out in their name. Fraud prevention and detection should be explicitly recognised as a legitimate purpose for data processing.

Credit reports should also be explicitly recognised as a legitimate purpose for data processing. The Judgement of the Court of Justice of the European Union in joined Cases C 468/10 and C 469/10 established the presumption in favour of the legitimate interest in cases where the data come from public sources when considering the possible violation of fundamental rights. With regard to fraud prevention files and credit reports, the prevention of fraud, defaults, and over-indebtedness of families are legitimate interests of operators, most notably in the cases of compliance with the rules on responsible lending. Each country has regulated these purposes differently. The above points legitimise the need to include these assumptions within the cases of data processing based on legitimate interest.

Amendment 12

Article 6(3)

Original wording	Proposed amendment
<p>3. Processing referred to in points (c) and (e) of paragraph 1 must be provided for in:</p> <p>(a) Union law, or</p> <p>(b) the law of the Member State to which the controller is subject.</p> <p>The law of the Member State must meet an objective of public interest or must be necessary to protect the rights and freedoms of others, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued.</p>	<p>3. Processing referred to in points (c) and (e) of paragraph 1 must be provided for in:</p> <p>(a) Union law, or</p> <p>(b) the law of the Member State to which the controller is subject.</p>

Justification

Whilst it is the responsibility of the Member States to ensure that their national legislation meets the above requirements, data controllers would bear the risks when processing data in accordance with a potentially non-conforming law. This should be avoided to increase legal certainty for controllers and processors.

In any case, as privacy is a fundamental right, national courts do not need this explicit reference in order to assess whether a law allowing for data protection impedes upon a fundamental right.



Amendment 13

Article 6(5)

Original wording	Proposed amendment
<p>5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the conditions referred to in point (f) of paragraph 1 for various sectors and data processing situations, including as regards the processing of personal data related to a child.</p>	<p><i>Deleted</i></p>

Justification

Delegated acts would leave the Regulation to be changed substantially over time, likely resulting in business as well as legal uncertainty. In accordance with the provisions of the Treaty delegated acts can only be applied to “non-essential” aspects of the Regulation. What constitutes a “legitimate interests pursued by controllers” cannot be seen as non-essential.

Amendment 14

Recital 31 – the accompanying recital to Article 6

Original wording	Proposed amendment
<p>In order for processing to be lawful, personal data should be processed on the basis of the consent of the person concerned or some other legitimate basis, laid down by law, either in this Regulation or in other Union or Member State law as referred to in this Regulation.</p>	<p>In order for processing to be lawful, personal data should be processed on the basis of the consent of the person concerned or some other legitimate basis, <i>for example to detect and prevent fraud</i>, laid down by law, either in this Regulation or in other Union or Member State law as referred to in this Regulation.</p>

Justification

Experience in practice has shown that these provisions often do not permit the processing of data for fraud prevention and detection purposes. Detecting and preventing fraud is of paramount importance for data controllers. Not only for the controller in question but also to protect data subjects from, for example, falling victim to a loan fraudulently being taken out in their name. Fraud prevention and detection should be explicitly recognised as a legitimate purpose for data processing.



Amendment 15

Recital 38 – the accompanying recital to Article 6

Original wording	Proposed amendment
<p>The legitimate interests of a controller may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding. This would need careful assessment in particular where the data subject is a child, given that children deserve specific protection. The data subject should have the right to object the processing, on grounds relating to their particular situation and free of charge. To ensure transparency, the controller should be obliged to explicitly inform the data subject on the legitimate interests pursued and on the right to object, and also be obliged to document these legitimate interests. Given that it is for the legislator to provide by law the legal basis for public authorities to process data, this legal ground should not apply for the processing by public authorities in the performance of their tasks.</p>	<p>The legitimate interests of a controller, such as fraud prevention and detection, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding. This would need careful assessment in particular where the data subject is a child, given that children deserve specific protection. The data subject should have the right to object the processing, on grounds relating to their particular situation and free of charge. To ensure transparency, the controller should be obliged to explicitly inform the data subject on the legitimate interests pursued and on the right to object, and also be obliged to document these legitimate interests. Given that it is for the legislator to provide by law the legal basis for public authorities to process data, this legal ground should not apply for the processing by public authorities in the performance of their tasks.</p>

Justification

Experience in practice has shown that these provisions often do not permit the processing of data for fraud prevention and detection purposes. Detecting and preventing fraud is of paramount importance for data controllers. Not only for the controller in question but also to protect data subjects from, for example, falling victim to a loan fraudulently being taken out in their name. Fraud prevention and detection should be explicitly recognised as a legitimate purpose for data processing.

Amendment 16

Article 7(1)

Original wording	Proposed amendment
<p>1. The controller shall bear the burden of proof for the data subject's consent to the processing of their personal data for specified purposes.</p>	<p><i>Deleted.</i></p>

Justification

There is no justification for a burden of proof for the controller only, especially in cases where the data subject has the consent in his personal documents.



Amendment 17

Article 7(3)

Original wording	Proposed amendment
<p>3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.</p>	<p>3. The data subject shall have the right to withdraw his or her consent at any time. Without prejudice to Article 6(1), the withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.</p>

Justification

Data controllers will need to process data even after the withdrawal of consent by the data subject, in order to, for example, continue the contractual relationship that may exist between the controller and the subject, as well as allowing for the fulfillment of any obligation on the part of the controller incurred at the request of or under a contract with the data subject.

Therefore, where consent has been withdrawn, the continued processing in accordance with another legal basis, as set out in Article 6(1) of the Proposal should be permitted.

Amendment 18

Article 7 (4)

Original wording	Proposed amendment
<p>4. Consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller.</p>	<p>Deleted.</p>

Justification

What can be considered as a “significant imbalance” or “free” consent will be subject to differing national interpretations. It is essential that this provision does not result in the inability for businesses to process data because an automatic presumption of an imbalance between the positions of the consumer and business within every relationship between the two parties.

To avoid legal uncertainty, paragraph 4 should be deleted or at least amended to ensure that where consent cannot provide a legal basis due to an imbalance, the controller can process the data in accordance with another legal basis, as set out in Article 6(1) of the Proposal.



Amendment 19

Recital 34 – the accompanying recital to Article 7

Original wording	Proposed amendment
<p>(34) Consent should not provide a valid legal ground for the processing of personal data, where there is a clear imbalance between the data subject and the controller. This is especially the case where the data subject is in a situation of dependence from the controller, among others, where personal data are processed by the employer of employees' personal data in the employment context. Where the controller is a public authority, there would be an imbalance only in the specific data processing operations where the public authority can impose an obligation by virtue of its relevant public powers and the consent cannot be deemed as freely given, taking into account the interest of the data subject.</p>	<p>(34) Consent should not provide a valid legal ground for the processing of personal data, where there is a clear imbalance between the data subject and the controller. This is especially the case where the data subject is in a situation of dependence from the controller, among others, where personal data are processed by the employer of employees' personal data in the employment context. Where the controller is a public authority, there would be an imbalance only in the specific data processing operations where the public authority can impose an obligation by virtue of its relevant public powers and the consent cannot be deemed as freely given, taking into account the interest of the data subject. These processors and controllers should instead rely on another legal ground for processing data.</p>

<p><i>Justification</i></p> <p>What can be considered as a “significant imbalance” or “free” consent will be subject to differing national interpretations. It is essential that this provision does not result in the inability for businesses to process data because an automatic presumption of an imbalance between the positions of the consumer and business within every relationship between the two parties.</p> <p>Where consent cannot provide a legal basis due to an imbalance, the controller should be permitted to process the data in accordance with another legal basis, as set out in Article 6(1) of the Proposal.</p>
--

Amendment 20

Article 9(1)

Original wording	Proposed amendment
<p>1. The processing of personal data, revealing race or ethnic origin, political opinions, religion or beliefs, trade-union membership, and the processing of genetic data or data concerning health or sex life or criminal convictions or related security measures shall be prohibited.</p>	<p>1. The processing of personal data, revealing race or ethnic origin, political opinions, religion or beliefs, trade-union membership, and the processing of genetic data or data concerning health or sex life shall be prohibited.</p>



Justification

In some Member States credit and financial institutions can set up databases which contain data on fraud committed against consumer credit providers. Processing and sharing of this data with other providers is permitted in order to allow credit providers to prevent fraud and minimise risks.

To ensure that these databases, whose existence is essential to protect both consumers and businesses, can continue to exist and operate, this provision should reflect the rules currently in place (Article 8(7) of Directive 95/46/EC).



CHAPTER III – Rights of the Data Subject

Section 1 – Transparency and Modalities

Amendment 21

Article 12(1)

Original wording	Proposed amendment
<p>1. The controller shall establish procedures for providing the information referred to in Article 14 and for the exercise of the rights of data subjects referred to in Article 13 and Articles 15 to 19. The controller shall provide in particular mechanisms for facilitating the request for the actions referred to in Article 13 and Articles 15 to 19. Where personal data are processed by automated means, the controller shall also provide means for requests to be made electronically.</p>	<p>1. The controller shall establish procedures for providing the information referred to in Article 14 and for the exercise of the rights of data subjects referred to in Article 13 and Articles 15 to 19. The controller shall provide in particular mechanisms for facilitating the request for the actions referred to in Article 13 and Articles 15 to 19.</p>

Justification

The requirement to provide information in electronic form raises concerns about the security of the data. It is not current practice in credit markets. An email request does not enable a lender to validate that the request is from the data subject as there is no guarantee that it will be secure. It would also be a considerable challenge to take appropriate technological measures to ensure security of the data in a way that would work for every customer.

Amendment 22

Article 12(2)

Original wording	Proposed amendment
<p>2. The controller shall inform the data subject without delay and, at the latest within one month of receipt of the request, whether or not any action has been taken pursuant to Article 13 and Articles 15 to 19 and shall provide the requested information. This period may be prolonged for a further month, if several data subjects exercise their rights and their cooperation is necessary to a reasonable extent to prevent an unnecessary and disproportionate effort on the part of the controller. The information shall be given in writing. Where the data subject makes the request in electronic form, the information shall be provided in electronic form, unless otherwise requested by the data subject.</p>	<p>2. The controller shall inform the data subject without delay and, at the latest within one month of receipt of the request, whether or not any action has been taken pursuant to Article 13 and Articles 15 to 19 and shall provide the requested information. This period may be prolonged for another eight weeks, if several data subjects exercise their rights and their cooperation is necessary to a reasonable extent to prevent an unnecessary and disproportionate effort on the part of the controller. The information shall be given in writing.</p>



Justification

Where the validity of contested data has to be verified with third parties it seems appropriate to extend this period by another eight weeks.

The requirement to provide information in electronic form raises concerns about the security of the data. It is not current practice in credit markets. An email request does not enable a lender to validate that the request is from the data subject as there is no guarantee that it will be secure. It would also be a considerable challenge to take appropriate technological measures to ensure security of the data in a way that would work for every customer.

Amendment 23

Article 12(4)

Original wording	Proposed amendment
<p>4. The information and the actions taken on requests referred to in paragraph 1 shall be free of charge. Where requests are manifestly excessive, in particular because of their repetitive character, the controller may charge a fee for providing the information or taking the action requested, or the controller may not take the action requested. In that case, the controller shall bear the burden of proving the manifestly excessive character of the request.</p>	<p>4. The information and the actions taken on requests referred to in paragraph 1 shall be free of charge. Where requests are manifestly excessive, in particular because of their repetitive character, their complexity or the total number of requests, the controller may charge an appropriate fee for providing the information or taking the action requested, or the controller may not take the action requested. In that case, the controller shall bear the burden of proving the manifestly excessive character of the request.</p>

Justification

The provision of data held within a database has a cost. Requesting an appropriate (not for profit) contribution from data subjects for data access is critical in deterring fraudsters from obtaining high volumes of consumers’ credit data. If data access upon request were to become free of charge then consumers would face an increased risk of frauds (e.g. ‘account takeover’) with its attendant detrimental consequences.

Amendment 24

Recital 47 – the accompanying recital to Article 12

Original wording	Proposed amendment
<p>Modalities should be provided for facilitating the data subject’s exercise of their rights provided by this Regulation, including mechanisms to request, free of charge, in particular access to</p>	<p>Modalities should be provided for facilitating the data subject’s exercise of their rights provided by this Regulation, including mechanisms to request in particular access to data, rectification, erasure</p>



<p>data, rectification, erasure and to exercise the right to object. The controller should be obliged to respond to requests of the data subject within a fixed deadline and give reasons, in case he does not comply with the data subject's request.</p>	<p>and to exercise the right to object. The controller should be obliged to respond to requests of the data subject within a fixed deadline and give reasons, in case he does not comply with the data subject's request.</p>
--	---

Justification

The provision of data held within a database has a cost. Requesting an appropriate (not for profit) contribution from data subjects for data access is critical in deterring fraudsters from obtaining high volumes of consumers' credit data. If data access upon request were to become free of charge then consumers would face an increased risk of frauds (e.g. 'account takeover') with its attendant detrimental consequences.



Section 2 – Information and Access to Data

Amendment 25

Article 14(1)(b)

Original wording	Proposed amendment
<p>1. Where personal data relating to a data subject are collected, the controller shall provide the data subject with at least the following information:</p> <p>(b) the purposes of the processing for which the personal data are intended, including the contract terms and general conditions where the processing is based on point (b) of Article 6(1) and the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);</p>	<p>1. Where personal data relating to a data subject are collected, the controller shall provide the data subject with the following information:</p> <p>(b) the purposes of the processing for which the personal data are intended, including the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);</p>

Justification

The information to be provided to data subjects shall be an exhaustive list, to ensure that controllers have legal certainty with regard to their information obligations.

Data subjects will already have been provided the contract terms and conditions when they signed this contract. The duplication of such a requirement would lead to overloading consumers with information.

Amendment 26

Article 14(1)(c)

Original wording	Proposed amendment
<p>1. Where personal data relating to a data subject are collected, the controller shall provide the data subject with at least the following information:</p> <p>(c) the period for which the personal data will be stored;</p>	<p>1. Where personal data relating to a data subject are collected, the controller shall provide the data subject with the following information:</p> <p>Deleted;</p>

Justification

Periods for data storage are often not known at the time the data is collected, especially in highly regulated sectors such as financial services where anti-money laundering requires the collection and storage of data throughout the relationship with the client, which may be of an indeterminate period of time.



Amendment 27

Article 14(5)(b)

Original wording	Proposed amendment
5. Paragraphs 1 to 4 shall not apply, where: (b) the data are not collected from the data subject and the provision of such information proves impossible or would involve a disproportionate effort; or	5. Paragraphs 1 to 4 shall not apply, where: (b) the data are not collected from the data subject and the provision of such information proves impossible or would involve a disproportionate effort, such as substantial manual work ; or

Justification

The term “disproportionate effort” is open to various interpretations and should be clarified.

Amendment 28

Article 14(5)(e) - new

Original wording	Proposed amendment
-	5. Paragraphs 1 to 4 shall not apply, where: (e) the data are not collected from the data subject and are publicly available .

Justification

As the data is already publicly available, such a warranty is not necessary to ensure the protection of fundamental rights. The data has already been published and the data subject already knows this and that his or her data may be processed by third parties.

Amendment 29

Recital 48 – the accompanying recital to Article 14

Original wording	Proposed amendment
The principles of fair and transparent processing require that the data subject should be informed in particular of the existence of the processing operation and its purposes, how long the data	The principles of fair and transparent processing require that the data subject should be informed in particular of the existence of the processing operation and its purposes, on the existence of



<p>will be stored, on the existence of the right of access, rectification or erasure and on the right to lodge a complaint. Where the data are collected from the data subject, the data subject should also be informed whether they are obliged to provide the data and of the consequences, in cases they do not provide such data.</p>	<p>the right of access, rectification or erasure and on the right to lodge a complaint. Where the data are collected from the data subject, the data subject should also be informed whether they are obliged to provide the data and of the consequences, in cases they do not provide such data.</p>
---	--

Justification

Periods for data storage are often not known at the time the data is collected, especially in highly regulated sectors such as financial services where anti-money laundering requires the collection and storage of data throughout the relationship with the client, which may be of an indeterminate period of time.

Amendment 30
Article 15(1)(d)

Original wording	Proposed amendment
<p>1. The data subject shall have the right to obtain from the controller at any time, on request, confirmation as to whether or not personal data relating to the data subject are being processed. Where such personal data are being processed, the controller shall provide the following information:</p> <p>d) the period for which the personal data will be stored;</p>	<p>1. The data subject shall have the right to obtain from the controller at any time, on request, confirmation as to whether or not personal data relating to the data subject are being processed. Where such personal data are being processed, the controller shall provide the following information:</p> <p>d) Deleted.</p>

Justification

Periods for data storage are often not known at the time the data is collected, especially in highly regulated sectors such as financial services where anti-money laundering requires the collection and storage of data throughout the relationship with the client, which may be of an indeterminate period of time.



Section 3 – Rectification and Erasure

Amendment 31

Article 17(1)(a)

Original wording	Proposed amendment
<p>1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child, where one of the following grounds applies:</p> <p>(a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;</p>	<p>1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child, where one of the following grounds applies:</p> <p>(a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed and when the data controller has no legal or regulatory ground to retain the data;</p>

Justification

The article is designed to protect internet social media users. However, it is difficult to execute for example in the financial sector. The data controllers in, for example, the financial sector are obliged to store some data and therefore they are not able to erase all the data processed on the request of the data subject.

Amendment 32

Article 17(3)

Original wording	Proposed amendment
<p>3. The controller shall carry out the erasure without delay, except to the extent that the retention of the personal data is necessary:</p> <p>(a) for exercising the right of freedom of expression in accordance with Article 80;</p> <p>(b) for reasons of public interest in the area of public health in accordance with Article 81;</p> <p>(c) for historical, statistical and scientific research purposes in accordance with Article 83;</p> <p>(d) for compliance with a legal obligation to retain the personal data by Union or Member State law to which the controller is subject; Member State</p>	<p>3. The controller shall carry out the erasure without unreasonable delay, except to the extent that the retention and dissemination of the personal data is necessary:</p> <p>(a) for exercising the right of freedom of expression in accordance with Article 80;</p> <p>(b) for reasons of public interest in the area of public health in accordance with Article 81;</p> <p>(c) for historical, statistical and scientific research purposes in accordance with Article 83;</p> <p>(d) for compliance with a legal obligation to retain the personal data by Union or Member State law</p>



<p>laws shall meet an objective of public interest, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued;</p> <p>(e) in the cases referred to in paragraph 4.</p>	<p>to which the controller is subject;</p> <p>(e) in the cases referred to in paragraph 4.</p>
--	--

Justification

Where controllers are subject to a legal obligation to retain and process data, they may also be obliged to transfer this data to relevant supervisory authorities, such as suspicious transaction reports to financial intelligence units in the context of anti-money laundering rules. Therefore further dissemination should be possible. The “without delay” requirement must be qualified to ensure that it is realistic.

Whilst it is the responsibility of the Member States to ensure that their national legislation meets the above requirements, data controllers would bear the risks when processing data in accordance with a potentially non-conforming law. This should be avoided to increase legal certainty for controllers and processors.

Amendment 33
Article 17(9)

Original wording	Proposed amendment
<p>9. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying:</p> <p>(a) the criteria and requirements for the application of paragraph 1 for specific sectors and in specific data processing situations;</p> <p>(b) the conditions for deleting links, copies or replications of personal data from publicly available communication services as referred to in paragraph 2;</p> <p>(c) the criteria and conditions for restricting the processing of personal data referred to in paragraph 4.</p>	<p><i>Deleted</i></p>

Justification

Delegated acts would leave the Regulation to be changed substantially over time, likely resulting in business as well as legal uncertainty. In accordance with the provisions of the Treaty delegated acts can only be applied to “non-essential” aspects of the Regulation. Laying down a new body of detailed rules for specific sectors cannot be considered as non-essential.



Amendment 34

Article 18(1)

Original wording	Proposed amendment
<p>1. The data subject shall have the right, where personal data are processed by electronic means and in a structured and commonly used format, to obtain from the controller a copy of data undergoing processing in an electronic and structured format which is commonly used and allows for further use by the data subject.</p>	<p>Deleted.</p>

Justification

Article 15 of the Regulation already provides the right of data subjects to access personal data and to obtain communication thereon, i.e. to obtain a copy. Article 18(1) is therefore a repetition and redundant.

Amendment 35

Article 18(2)

Original wording	Proposed amendment
<p>2. Where the data subject has provided the personal data and the processing is based on consent or on a contract, the data subject shall have the right to transmit those personal data and any other information provided by the data subject and retained by an automated processing system, into another one, in an electronic format which is commonly used, without hindrance from the controller from whom the personal data are withdrawn.</p>	<p>Deleted</p>

Justification

Data portability could be open to abuse, as an ill-intended applicant borrower may alter the data in between receiving, for example, his credit history from one processor and presenting it to a lender. The receiving processor would thus not be able to rely on the accuracy of the data.

Data may not be stored or processed in the same language, according to the same categories or procedures. This may render data portability of little value.

There is also a risk that this provision could require organisations to disclose trade secrets, internal know-how or information on other customers. We are also concerned that data portability may



increase the risk of disclosure of personal data to third parties.

In the specific context of credit data, the European Commission’s Expert Group on Credit Histories decided that it should be left to each individual lender to decide which data access model offers the most convenient and cost-effective solution to data portability. The obligation for data portability would not be in line with these findings.

Perhaps there may also be the risk that the receiving processor will require the data subject to provide all his data (history) before offering services. This could be disproportionate.

Where data is made portable, the requirements and obligations for the receiving controller are unclear. For example, does the retention period start again at zero?

If deletion is not possible, the scope of the article should be narrowed down to only those sectors where this could appropriately be implemented, e.g. social networks.

Amendment 36
Article 18(3)

Original wording	Proposed amendment
<p>3. The Commission may specify the electronic format referred to in paragraph 1 and the technical standards, modalities and procedures for the transmission of personal data pursuant to paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>	<p>Deleted</p>

Justification

Standardisation of IT solutions and technical systems used by controllers to process data should not be the aim of the new data protection framework. The imposition of technical requirements to enable personal data to become portable, would come at a significant cost for businesses.

In the specific context of credit data, the European Commission’s Expert Group on Credit Histories decided that it should be left to each individual lender to decide which data access model offers the most convenient and cost-effective solution to data portability.

Amendment 37
Recital 55 – the accompanying recital to Article 18

Original wording	Proposed amendment
<p>To further strengthen the control over their own data and their right of access, data subjects should have the right, where personal data are</p>	<p>Deleted</p>



<p>processed by electronic means and in a structured and commonly used format, to obtain a copy of the data concerning them also in commonly used electronic format. The data subject should also be allowed to transmit those data, which they have provided, from one automated application, such as a social network, into another one. This should apply where the data subject provided the data to the automated processing system, based on their consent or in the performance of a contract.</p>	
---	--

<p style="text-align: center;"><i>Justification</i></p> <p>See justification in amendments 34-36.</p>



Section 4 – Right to Object and Profiling

Amendment 38

Article 19(1)

Original wording	Proposed amendment
<p>1. The data subject shall have the right to object, on grounds relating to their particular situation, at any time to the processing of personal data which is based on points (d), (e) and (f) of Article 6(1), unless the controller demonstrates compelling legitimate grounds for the processing which override the interests or fundamental rights and freedoms of the data subject.</p>	<p>1. The data subject shall have the right to object, on grounds relating to their particular situation, at any time to the processing of personal data which is based on points (d), (e) and (f) of Article 6(1), unless the controller demonstrates compelling legitimate grounds for the processing which override the interests or fundamental rights and freedoms of the data subject, such as the processing of data for the prevention of fraud and for credit reports.</p>

<p><i>Justification</i></p> <p>See justification amendment 11.</p>
--

Amendment 39

Article 20 - Title

Original wording	Proposed amendment
<p>Measures based on profiling</p>	<p>Measures based on automated processing</p>

<p><i>Justification</i></p> <p>Art. 20 concerns automated processing. The title of this article should therefore be amended to “Measures based on automated processing.”</p>
--

Amendment 40

Article 20(1)

Original wording	Proposed amendment
<p>1. Every natural person shall have the right not to be subject to a measure which produces legal effects concerning this natural person or significantly affects this natural person, and</p>	<p>1. Every natural person shall have the right not to be subject to a measure which produces legal effects concerning this natural person or significantly affects this natural person, and</p>



<p>which is based solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour.</p>	<p>which is based solely on automated processing intended to evaluate certain personal aspects relating to this natural person, such as his creditworthiness, or to analyse or predict in particular the natural person's performance at work, location, health, personal preferences, reliability or behaviour.</p>
--	---

Justification

Art. 20(1) should retain the reference to “creditworthiness” introduced under Directive 95/46/EC and is preferable to “economic situation.”

Amendment 41
Article 20(2)(a)

Original wording	Proposed amendment
<p>2. Subject to the other provisions of this Regulation, a person may be subjected to a measure of the kind referred to in paragraph 1 only if the processing:</p> <p>(a) is carried out in the course of the entering into, or performance of, a contract, where the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or where suitable measures to safeguard the data subject's legitimate interests have been adduced, such as the right to obtain human intervention; or</p>	<p>2. Subject to the other provisions of this Regulation, a person may be subjected to a measure of the kind referred to in paragraph 1 if the processing:</p> <p>(a) is carried out in the course of the entering into, or performance of, a contract, where suitable measures to safeguard the data subject's legitimate interests have been adduced, such as the right to obtain human intervention; or</p>

Justification

A customer may enquire as to the terms and conditions for entering into, for example, a consumer credit contract. In order for the consumer credit provider to provide information on the APRC, it will assess the consumer's creditworthiness, a legal obligation. Requiring a formal request for the entering into a contract to be proven, would essentially render service and goods providers unable to respond to information requests.



Amendment 42

Article 20(2)(b)

Original wording	Proposed amendment
<p>2. Subject to the other provisions of this Regulation, a person may be subjected to a measure of the kind referred to in paragraph 1 only if the processing:</p> <p>[...]</p> <p>(b) is expressly authorized by a Union or Member State law which also lays down suitable measures to safeguard the data subject's legitimate interests; or</p> <p>[...]</p>	<p>2. Subject to the other provisions of this Regulation, a person may be subjected to a measure of the kind referred to in paragraph 1 if the processing:</p> <p>[...]</p> <p>(b) is necessary to comply with a Union or Member State law; or</p> <p>[...]</p>

Justification

It cannot be the task of data controllers to check, whether the Member State law “lays down suitable measures to safeguard the data subject's legitimate interests”. On the contrary, firms have to be able to rely on the law.

Amendment 43

Article 20(4)

Original wording	Proposed amendment
<p>4. In the cases referred to in paragraph 2, the information to be provided by the controller under Article 14 shall include information as to the existence of processing for a measure of the kind referred to in paragraph 1 and the envisaged effects of such processing on the data subject.</p>	<p>4. In the cases referred to in paragraph 2, the information to be provided by the controller under Article 14 shall include information as to the existence of processing for a measure of the kind referred to in paragraph 1.</p>

Justification

It may not always be possible to determine in advance the envisaged effects, in particular where automated processing is subject to subsequent human intervention. An explanation of the existence of this measure will adequately inform and protect data subjects.



Amendment 44

Article 20(5)

Original wording	Proposed amendment
<p>5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for suitable measures to safeguard the data subject's legitimate interests referred to in paragraph 2.</p>	<p><i>Deleted</i></p>

<p><i>Justification</i></p> <p>Delegated acts would leave the Regulation to be changed substantially over time, likely resulting in business as well as legal uncertainty. In accordance with the provisions of the Treaty delegated acts can only be applied to “non-essential” aspects of the Regulation. Laying down a new body of detailed rules for specific sectors cannot be considered as non-essential.</p> <p>Furthermore, similar provisions on automated processing have been in place since Directive 95/46/EC. Controllers and processors have built systems which rely on the interpretations of these rules already in place. Laying down new rules without any specific justification would create legal uncertainty.</p>
--

Amendment 45

Recital 58 – the accompanying recital to Article 20

Original wording	Proposed amendment
<p>Every natural person should have the right not to be subject to a measure which is based on profiling by means of automated processing. However, such measure should be allowed when expressly authorised by law, carried out in the course of entering or performance of a contract, or when the data subject has given his consent. In any case, such processing should be subject to suitable safeguards, including specific information of the data subject and the right to obtain human intervention and that such measure should not concern a child.</p>	<p>Every natural person should have the right not to be subject to a measure which is based solely on automated processing. Such measure should be allowed when expressly authorised by law, carried out in the course of entering or performance of a contract, or when the data subject has given his consent. In any case, such processing should be subject to suitable safeguards, including specific information of the data subject and the right to obtain human intervention and that such measure should not concern a child.</p>

<p><i>Justification</i></p> <p>This recital should reflect the corresponding article with regard to the content.</p>
--



Amendment 46

Recital 51

Original wording	Proposed amendment
<p>Any person should have the right of access to data which has been collected concerning them, and to exercise this right easily, in order to be aware and verify the lawfulness of the processing. Every data subject should therefore have the right to know and obtain communication in particular for what purposes the data are processed, for what period, which recipients receive the data, what is the logic of the data that are undergoing the processing and what might be, at least when based on profiling, the consequences of such processing. This right should not adversely affect the rights and freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of these considerations should not be that all information is refused to the data subject.</p>	<p>Any person should have the right of access to data which has been collected concerning them, and to exercise this right easily, in order to be aware and verify the lawfulness of the processing. Every data subject should therefore have the right to know and obtain communication in particular for what purposes the data are processed, for what period, which recipients receive the data and what is the logic of the data that are undergoing the processing. This right should not adversely affect the rights and freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of these considerations should not be that all information is refused to the data subject.</p>

<p><i>Justification</i></p> <p>See justification to amendment 43.</p>

Amendment 47

Recital 59

Original wording	Proposed amendment
<p>Restrictions on specific principles and on the rights of information, access, rectification and erasure or on the right to data portability, the right to object, measures based on profiling, as well as on the communication of a personal data breach to a data subject and on certain related obligations of the controllers may be imposed by Union or Member State law, as far as necessary and proportionate in a democratic society to safeguard public security, including the protection of human life especially in response to natural or man made disasters, the prevention, investigation and prosecution of criminal offences or of breaches of ethics for regulated professions, other public interests of the Union or</p>	<p>Restrictions on specific principles and on the rights of information, access, rectification and erasure or on the right to data portability, the right to object, measures based on automated processing, as well as on the communication of a personal data breach to a data subject and on certain related obligations of the controllers may be imposed by Union or Member State law, as far as necessary and proportionate in a democratic society to safeguard public security, including the protection of human life especially in response to natural or man made disasters, the prevention, investigation and prosecution of criminal offences or of breaches of ethics for regulated professions, other public interests of</p>



<p>of a Member State, in particular an important economic or financial interest of the Union or of a Member State, or the protection of the data subject or the rights and freedoms of others. Those restrictions should be in compliance with requirements set out by the Charter of Fundamental Rights of the European Union and by the European Convention for the Protection of Human Rights and Fundamental Freedoms.</p>	<p>the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, or the protection of the data subject or the rights and freedoms of others. Those restrictions should be in compliance with requirements set out by the Charter of Fundamental Rights of the European Union and by the European Convention for the Protection of Human Rights and Fundamental Freedoms.</p>
--	---

Justification

See justification to amendment 39.



CHAPTER IV – Controller and Processor

Section 1 – General Obligations

Amendment 48

Article 22(3)

Original wording	Proposed amendment
<p>3. The controller shall implement mechanisms to ensure the verification of the effectiveness of the measures referred to in paragraphs 1 and 2. If proportionate, this verification shall be carried out by independent internal or external auditors.</p>	<p>3. The controller shall implement mechanisms to ensure the verification of the effectiveness of the measures referred to in paragraphs 1 and 2. Controllers may have this verification carried out by independent internal or external auditors.</p>

<p><i>Justification</i></p> <p>Introducing an obligation to have the verification carried out by internal/external auditors would introduce an unnecessary duplication of the measures taken by controllers to ensure compliance and an unjustified expense. It should be left to controllers to decide and assess what steps need to be taken to verify adherence to the Regulation.</p>

Amendment 49

Article 23(2)

Original wording	Proposed amendment
<p>2. The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals.</p>	<p>2. The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals.</p>

<p><i>Justification</i></p> <p>See justification amendment 6.</p>



Amendment 50

Article 23(3)

Original wording	Proposed amendment
<p>3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures and mechanisms referred to in paragraph 1 and 2, in particular for data protection by design requirements applicable across sectors, products and services.</p>	<p><i>Deleted.</i></p>

Justification

Delegated acts would leave the Regulation to be changed substantially over time, likely resulting in business as well as legal uncertainty. In accordance with the provisions of the Treaty delegated acts can only be applied to “non-essential” aspects of the Regulation. Laying down a new body of detailed rules for specific sectors cannot be considered as non-essential.

Amendment 51

Article 23(4)

Original wording	Proposed amendment
<p>4. The Commission may lay down technical standards for the requirements laid down in paragraph 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>	<p><i>Deleted</i></p>

Justification

The aim of the Proposal is to introduce a new European framework for data protection that ensures protection of individual’s rights and the free movement of data (Article 1), not to standardise processing systems, as proposed in Article 23(4). We strongly oppose any standardisation of IT solutions and technical systems used by controllers to process data, through the adoption of implementing measures.



Amendment 52

Article 26(2)(a)

Original wording	Proposed amendment
<p>2. The carrying out of processing by a processor shall be governed by a contract or other legal act binding the processor to the controller and stipulating in particular that the processor shall:</p> <p>(a) act only on instructions from the controller, in particular, where the transfer of the personal data used is prohibited;</p>	<p>2. The carrying out of processing by a processor shall be governed by a contract or other legal act binding the processor to the controller and stipulating in particular that the processor shall:</p> <p>(a) Deleted</p>

<p><i>Justification</i></p> <p>The scope of this provision is unclear.</p>
--

Amendment 53

Article 26(2)(f)

Original wording	Proposed amendment
<p>2. The carrying out of processing by a processor shall be governed by a contract or other legal act binding the processor to the controller and stipulating in particular that the processor shall:</p> <p>(f) assist the controller in ensuring compliance with the obligations pursuant to Articles 30 to 34;</p>	<p>2. The carrying out of processing by a processor shall be governed by a contract or other legal act binding the processor to the controller and stipulating in particular that the processor shall:</p> <p>(f) Deleted</p>

<p><i>Justification</i></p> <p>Obligations to adhere to these respective articles is already contained in other parts and there is thus no need to repeat these.</p>
--



Amendment 54

Article 26(3)

Original wording	Proposed amendment
3. The controller and the processor shall document in writing the controller's instructions and the processor's obligations referred to in paragraph 2.	<i>Deleted</i>

<p><i>Justification</i></p> <p>Obligations of the processor regarding the instructions of the controller and the obligations of the processor are already contained in other sections, so it is repetitive.</p>

Amendment 55

Article 27

Original wording	Proposed amendment
The processor and any person acting under the authority of the controller or of the processor who has access to personal data shall not process them except on instructions from the controller, unless required to do so by Union or Member State law.	The processor and any person acting under the authority of the controller or of the processor who has access to personal data shall not process them except on instructions from the controller, unless authorised to do so by Union or Member State law.

<p><i>Justification</i></p> <p>The exemption should not only cover situations where the data processor or the person acting under the authority of the controller or of the processor who has access to personal data is required to process personal data, but also situations where they have the right to process data under the national or EU legislation.</p>



Section 2 – Data Security

Amendment 56

Article 31(1)

Original wording	Proposed amendment
<p>1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 24 hours after having become aware of it, notify the personal data breach to the supervisory authority. The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within 24 hours.</p>	<p>1. In the case of a personal data breach <i>which is likely to substantially adversely affect the personal data or privacy of the data subject</i>, the controller shall notify the personal data breach to the supervisory authority <i>within a reasonable period of time</i>. The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within <i>a reasonable period of time</i>.</p> <p><i>For regulated activities, where a duty already exists to notify a personal data breach to sectoral supervisory authorities, the latter shall communicate the personal data breach to the data protection supervisory authority.</i></p>

Justification

An appropriate time period should be foreseen for notifying the supervisory authority of the substantial amount of information required in Article 31(3) regarding data breaches which are likely to substantially adversely affect data subjects.

In some Member States, credit and financial institutions shall notify the Financial Services Authority where substantial disruptions in services provided to the customers and in payment and IT systems occur. Where such an obligation already exists in national law, this should not be duplicated by an additional obligation to also notify the data protection supervisor. This sectoral supervisor should instead notify the data protection supervisor.

Amendment 57

Article 32(1)

Original wording	Proposed amendment
<p>1. When the personal data breach is likely to adversely affect the protection of the personal data or privacy of the data subject, the controller shall, after the notification referred to in Article 31, communicate the personal data breach to the data subject without undue delay.</p>	<p>1. When the personal data breach is likely to <i>substantially</i> adversely affect the protection of the personal data or privacy of the data subject, the controller shall, after the notification referred to in Article 31, communicate the personal data breach to the data subject without undue delay.</p>



Justification

Data subjects should be informed of a breach where there could be a significant impact on them.

Amendment 58

Article 32(5)

Original wording	Proposed amendment
<p>5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements as to the circumstances in which a personal data breach is likely to adversely affect the personal data referred to in paragraph 1.</p>	<p>Deleted</p>

Justification

The establishment by the Commission at a later stage of the requirements for these circumstances is likely to create substantial legal uncertainty.

Amendment 59

Recital 67 – the accompanying recital to Article 31 & 32

Original wording	Proposed amendment
<p>A personal data breach may, if not addressed in an adequate and timely manner, result in substantial economic loss and social harm, including identity fraud, to the individual concerned. Therefore, as soon as the controller becomes aware that such a breach has occurred, the controller should notify the breach to the supervisory authority without undue delay and, where feasible, within 24 hours. Where this cannot be achieved within 24 hours, an explanation of the reasons for the delay should accompany the notification. The individuals whose personal data could be adversely affected by the breach should be notified without undue delay in order to allow them to take the necessary precautions. A breach should be considered as adversely affecting the personal data or privacy of a data subject where it could result in, for example, identity theft or fraud, physical harm, significant humiliation or damage to reputation. The</p>	<p>A personal data breach may, if not addressed in an adequate and timely manner, result in substantial economic loss and social harm, including identity fraud, to the individual concerned. Therefore, as soon as the controller becomes aware that such a breach, which substantially adversely affects the personal data or privacy of the data subject, has occurred, the controller should notify the breach to the supervisory authority within a reasonable period of time. Where this cannot be achieved within a reasonable period of time, an explanation of the reasons for the delay should accompany the notification. The individuals whose personal data could be substantially adversely affected by the breach should be notified without undue delay in order to allow them to take the necessary precautions. A breach should be considered as adversely affecting the personal data or privacy of a data</p>



<p>notification should describe the nature of the personal data breach as well as recommendations as well as recommendations for the individual concerned to mitigate potential adverse effects. Notifications to data subjects should be made as soon as reasonably feasible, and in close cooperation with the supervisory authority and respecting guidance provided by it or other relevant authorities (e.g. law enforcement authorities). For example, the chance for data subjects to mitigate an immediate risk of harm would call for a prompt notification of data subjects whereas the need to implement appropriate measures against continuing or similar data breaches may justify a longer delay.</p>	<p>subject where it could result in, for example, identity theft or fraud, physical harm, significant humiliation or damage to reputation. The notification should describe the nature of the personal data breach as well as recommendations as well as recommendations for the individual concerned to mitigate potential adverse effects. Notifications to data subjects should be made as soon as reasonably feasible, and in close cooperation with the supervisory authority and respecting guidance provided by it or other relevant authorities (e.g. law enforcement authorities). For example, the chance for data subjects to mitigate an immediate risk of harm would call for a prompt notification of data subjects whereas the need to implement appropriate measures against continuing or similar data breaches may justify a longer delay.</p>
--	--

Justification

See justification for amendment 56 & 57.



Section 3 – Data Protection Impact Assessment and Prior Authorisation

Amendment 60

Article 33(2)(a)

Original wording	Proposed amendment
<p>2. The following processing operations in particular present specific risks referred to in paragraph 1:</p> <p>(a) a systematic and extensive evaluation of personal aspects relating to a natural person or for analysing or predicting in particular the natural person's economic situation, location, health, personal preferences, reliability or behaviour, which is based on automated processing and on which measures are based that produce legal effects concerning the individual or significantly affect the individual;</p>	<p>2. The following processing operations in particular present specific risks referred to in paragraph 1:</p> <p>(a) a systematic and extensive evaluation of personal aspects relating to a natural person or for analysing or predicting in particular the natural person's economic situation, location, health, personal preferences, reliability or behaviour, which is based on automated processing and on which measures are based that produce legal effects concerning the individual or significantly affect the individual, except where this systematic and extensive evaluation is a legal obligation for the controller provided for by Union or Member State law;</p>

Justification

Data processors cannot and should not be asked to make the assessment as to whether or not a legal obligation placed upon them poses “a high degree of specific risks”. This is a consideration for the legislator and, at European level, through the opinion of the European Data Protection Supervisor, who advises the Institutions on legislation that affects privacy.

Amendment 61

Article 33(4)

Original wording	Proposed amendment
<p>4. The controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations.</p>	<p>4. The controller shall seek the views of the supervisory authority on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations.</p>

Justification

It will be impossible to implement in practice and data subjects’ representatives may not always have the expertise, qualifications or resources to respond to such imposed requests for their views. The



supervisory authority will be in better qualified to respond to such requests.

Amendment 62

Article 33(6)

Original wording	Proposed amendment
<p>6. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the processing operations likely to present specific risks referred to in paragraphs 1 and 2 and the requirements for the assessment referred to in paragraph 3, including conditions for scalability, verification and auditability. In doing so, the Commission shall consider specific measures for micro, small and medium-sized enterprises.</p>	<p>Deleted</p>

Justification

Delegated acts would leave the Regulation to be changed substantially over time, likely resulting in business as well as legal uncertainty. In accordance with the provisions of the Treaty delegated acts can only be applied to “non-essential” aspects of the Regulation.

Amendment 63

Article 35(7)

Original wording	Proposed amendment
<p>7. The controller or the processor shall designate a data protection officer for a period of at least two years. The data protection officer may be reappointed for further terms. During their term of office, the data protection officer may only be dismissed, if the data protection officer no longer fulfils the conditions required for the performance of their duties.</p>	<p>Deleted</p>

Justification

This provision will prevent someone being replaced in the normal course of the management of a company and its employees. This is particularly pertinent for smaller companies where the data protection officer may well be only part of the individual’s job designation. There has to be flexibility for the firm to be able to reorganise and reshape its employee resources. The officer should be no different position from any other person in a compliance function as far as these issues are concerned.



CHAPTER V – Transfer of Personal Data to Third Countries or International Organisations

Amendment 64

Article 42(1)

Original wording	Proposed amendment
<p>1. Where the Commission has taken no decision pursuant to Article 41, a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has adduced appropriate safeguards with respect to the protection of personal data in a legally binding instrument.</p>	<p>1. Where the Commission has taken no decision pursuant to Article 41, a controller or processor may transfer personal data to a third country or an international organisation or corporate group only if appropriate safeguards with respect to the protection of personal data in a legally binding instrument.</p>

Justification

The reference to the processor or controller restricts the authorisation to them as the only appropriate parties to provide guarantees for the performance of the international data transfer to a third country, eliminating others such as the importer of the data.

Amendment 65

Article 42(2)(e) - new

Original wording	Proposed amendment
<p>2. The appropriate safeguards referred to in paragraph 1 shall be provided for, in particular, by:</p>	<p>2. The appropriate safeguards referred to in paragraph 1 shall be provided for, in particular, by:</p> <p><i>(e) a legally binding statement by the international organisation or corporate group acting as a data importer, through which it is subjected to the fundamental principles of this Regulation, according to the models adopted by the Commission following Article 45(1).</i></p> <p>(NEW)</p>

Justification

We included as appropriate guarantees the binding declaration of the international organisation or corporate group acting as data importer as an alternative instrument to further facilitate international data flows, thereby avoiding directly subordinating the legality of the transfer to the signing of a



contract between the parties, and therefore, the development of multiple contract terms with each of the exporters.

Said declarations could incorporate such elements as the Commission deems necessary in order to safeguard the right to privacy of the citizens of the European Union, in addition to the development of the principle of international cooperation laid down in Article 45(1) of the Regulation.

Amendment 66

Article 42(3)

Original wording	Proposed amendment
3. A transfer based on standard data protection clauses or binding corporate rules as referred to in points (a), (b) or (c) of paragraph 2 shall not require any further authorisation.	3. A transfer based on standard data protection clauses or binding corporate rules as referred to in points (a), (b), (c) or (e) of paragraph 2 shall not require any further authorisation.

Justification

See justification amendment 65.

Amendment 67

Article 44(1)(h)

Original wording	Proposed amendment
<p>1. In the absence of an adequacy decision pursuant to Article 41 or of appropriate safeguards pursuant to Article 42, a transfer or a set of transfers of personal data to a third country or an international organisation may take place only on condition that:</p> <p>(h) the transfer is necessary for the purposes of the legitimate interests pursued by the controller or the processor, which cannot be qualified as frequent or massive, and where the controller or processor has assessed all the circumstances surrounding the data transfer operation or the set of data transfer operations and based on this assessment adduced appropriate safeguards with respect to the protection of personal data, where necessary.</p>	<p>1. In the absence of an adequacy decision pursuant to Article 41 or of appropriate safeguards pursuant to Article 42, a transfer or a set of transfers of personal data to a third country or an international organisation may take place only on condition that:</p> <p>(h) the transfer is necessary for the purposes of the legitimate interests pursued by the controller or the processor, and where the controller or processor has assessed all the circumstances surrounding the data transfer operation or the set of data transfer operations</p>



Justification

The article presents legal concepts -frequent and massive legitimate interests- whose interpretation may result in greater legal uncertainty than what the wording aims to provide.

Furthermore, regardless of this uncertainty, there is no legal basis for applying a different solution in the event that there is a frequent legitimate interest as opposed to an infrequent legitimate interest, considering the impact on the protection of data transfer depends not frequency or size, but rather on the types of processing and data affected.

Amendment 68

Article 44(1)(j) - New

Original wording	Proposed amendment
<p>1. In the absence of an adequacy decision pursuant to Article 41 or of appropriate safeguards pursuant to Article 42, a transfer or a set of transfers of personal data to a third country or an international organisation may take place only on condition that:</p>	<p>1. In the absence of an adequacy decision pursuant to Article 41 or of appropriate safeguards pursuant to Article 42, a transfer or a set of transfers of personal data to a third country or an international organisation may take place only on condition that:</p> <p><i>j) When the transfer is made to a processor following the instructions of a controller located in the European Union. In this case, Articles 26 to 28 and Article 30 concerning the security of the processing will apply; or (new)</i></p>

Justification

Given the new regime for data processors, which includes:

- (i) A written contract between the parties governing the mandated processing of personal data.
- (ii) The obligation of the controller to select a processor that offers sufficient guarantees that the processing will be tailored to the provisions of these rules,
- (iii) The documentation of the entire process (art. 28) with details of processing, transfers, documentation, guarantees adopted in the event of transfers, and
- (iv) The requirement that this documentation is made available to the supervisory authority,

It should be possible to transfer data in these cases.

Amendment 69

Article 44(1)(j) - new

Original wording	Proposed amendment
<p>1. In the absence of an adequacy decision pursuant to Article 41 or of appropriate</p>	<p>1. In the absence of an adequacy decision pursuant to Article 41 or of appropriate</p>



<p>safeguards pursuant to Article 42, a transfer or a set of transfers of personal data to a third country or an international organisation may take place only on condition that:</p>	<p>safeguards pursuant to Article 42, a transfer or a set of transfers of personal data to a third country or an international organisation may take place only on condition that:</p> <p><i>j) When the international transfer is made within the framework of the development of an activity subject to specific regulation and supervision by a recognised or established regulator in the European Union, provided that the transfer is performed in accordance with said legislation and within the scope of the activity being supervised. (new)</i></p>
--	---

Justification

Where an activity is conducted subject to specific regulation and supervision, including financial and banking or insurance services, the approval process in these cases should also be exempted given the guarantee that the processing in such activities is subject to regulation and the legitimacy thereof.



CHAPTER VI – Independent Supervisory Authorities

Section 2 – Duties and powers

Amendment 70

Article 51(2)

Original wording	Proposed amendment
<p>2. Where the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union, and the controller or processor is established in more than one Member State, the supervisory authority of the main establishment of the controller or processor shall be competent for the supervision of the processing activities of the controller or the processor in all Member States, without prejudice to the provisions of Chapter VII of this Regulation.</p>	<p>2. Where the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union, and the controller or processor, or any subsidiary or affiliate thereof is established in more than one Member State, the supervisory authority of the main establishment or parent company of the controller or processor shall be competent for the supervision of the processing activities of the controller or the processor in all Member States, without prejudice to the provisions of Chapter VII of this Regulation.</p>

Justification

The principle of concentration of functions preached by this article should apply in the case of branches and subsidiary companies, affiliates and investees of a parent company, since they share the same foundation.

Amendment 71

Article 52(3)

Original wording	Proposed amendment
<p>3. The supervisory authority shall, upon request, advise any data subject in exercising the rights under this Regulations and, if appropriate, co-operate with the supervisory authorities in other Member States to this end.</p>	<p>3. The supervisory authority shall, upon request, advise any data subject in exercising the rights under this Regulations and, if appropriate, co-operate with the supervisory authorities in other Member States to this end. The supervisory authority shall advise controllers and processors regarding the obligations thereof, and especially the Data Protection Officers, promoting cooperation, training and permanent contact with them for a better understanding and enforcement of data protection.</p>



Justification

We understand that it is essential that the supervisory authority support those responsible for compliance with the rules and most especially the Data Protection Officers, in terms of training, information and cooperation to increase the level of compliance with the regulation.

Amendment 72

Article 53(5)

Original wording	Proposed amendment
<p>5. The performance of the duties of the supervisory authority shall be free of charge for the data subject.</p>	<p>5. The performance of the duties of the supervisory authority shall be free of charge for the data subject, <i>data controller, data processor and Data Protection Officers and be included in the budgets of the supervisory authority.</i></p>

Justification

The free services of the supervisory authority must exist regardless of the party requesting it.



CHAPTER VII – Co-Operation and Consistency

Section 2 – Consistency

Amendment 73

Article 58(3)

Original wording	Proposed amendment
<p>3. Any supervisory authority or the European Data Protection Board may request that any matter shall be dealt with in the consistency mechanism, in particular where a supervisory authority does not submit a draft measure referred to in paragraph 2 or does not comply with the obligations for mutual assistance in accordance with Article 55 or for joint operations in accordance with Article 56.</p>	<p>3. Any supervisory authority or the European Data Protection Board and any third party with accredited legitimate interest may request that any matter shall be dealt with in the consistency mechanism, in particular where a supervisory authority does not submit a draft measure referred to in paragraph 2 or does not comply with the obligations for mutual assistance in accordance with Article 55 or for joint operations in accordance with Article 56.</p>

Justification

We understand that the consistency mechanism should also be able to be activated by a controller or processor directly or indirectly affected by the measure on which the request applies or any other accredited third party with a legitimate interest in confirming the adequacy of country-level measures applied by a supervisory authority.



CHAPTER VIII – Remedies, Liability and Sanctions

Amendment 74

Article 76(1)

Original wording	Proposed amendment
1. Any body, organisation or association referred to in Article 73(2) shall have the right to exercise the rights referred to in Articles 74 and 75 on behalf of one or more data subjects.	Deleted

Justification

We are opposed to the introduction of class action mechanisms at European level, especially through sector specific legislation. It has not been shown that the absence of such mechanisms has prevented data subjects from exercising their rights.

Amendment 75

Recital 112 – the accompanying recital to Article 76

Original wording	Proposed amendment
Any body, organisation or association which aims to protect the rights and interests of data subjects in relation to the protection of their data and is constituted according to the law of a Member State should have the right to lodge a complaint with a supervisory authority or exercise the right to a judicial remedy on behalf of data subjects, or to lodge, independently of a data subject's complaint, an own complaint where it considers that a personal data breach has occurred.	Deleted

Justification

See justification for amendment 74.



Amendment 76

Article 79(2)

Original wording	Proposed amendment
<p>2. The administrative sanction shall be in each individual case effective, proportionate and dissuasive. The amount of the administrative fine shall be fixed with due regard to the nature, gravity and duration of the breach, the intentional or negligent character of the infringement, the degree of responsibility of the natural or legal person and of previous breaches by this person, the technical and organisational measures and procedures implemented pursuant to Article 23 and the degree of cooperation with the supervisory authority in order to remedy the breach.</p>	<p>2. Where the supervisory authority decides to impose an administrative sanction, this sanction shall in each individual case be effective, proportionate and dissuasive. The amount of an administrative fine shall be fixed with due regard to the nature, gravity and duration of the breach, the intentional or negligent character of the infringement, the degree of responsibility of the natural or legal person and of previous breaches by this person, the technical and organisational measures and procedures implemented pursuant to Article 23 and the degree of cooperation with the supervisory authority in order to remedy the breach.</p>

Justification

Supervisory authorities should not be obliged to impose sanctions, instead they should only impose sanctions after taking into account all circumstances of each individual case.

Amendment 77

Article 79(3)

Original wording	Proposed amendment
<p>3. In case of a first and non-intentional non-compliance with this Regulation, a warning in writing may be given and no sanction imposed, where:</p> <p>(a) a natural person is processing personal data without a commercial interest; or</p> <p>(b) an enterprise or an organisation employing fewer than 250 persons is processing personal data only as an activity ancillary to its main activities.</p>	<p>3. In case of a non-intentional non-compliance with this Regulation, or in the event that the breach of an obligation under this Regulation has not caused actual harm or impairment of the principles and rights set out in Chapters II and III of this Regulation, a warning in writing may be given and no sanction imposed.</p>

Justification

The written warning is a persuasive tool which must be used by the supervisory authority the times



and where it deems appropriate.

In keeping with the spirit and purpose of the Regulation, only intentional non-compliance or impairment of the principles and rights set forth in the Regulation should be subject to financial penalty.

Amendment 78
Article 79(4)

Original wording	Proposed amendment
4. The supervisory authority shall impose a fine up to 250 000 EUR, or in case of an enterprise up to 0,5 % of its annual worldwide turnover, to anyone who, intentionally or negligently: [...]	4. The supervisory authority may impose a fine up to 250 000 EUR, or in case of an enterprise up to 0,5 % of its annual worldwide turnover, to anyone who, intentionally or negligently: [...]

Justification

Supervisory authorities should not be obliged to impose sanctions, instead they should only impose sanctions after taking into account all circumstances of each individual case.

Amendment 79
Article 79(5)

Original wording	Proposed amendment
5. The supervisory authority shall impose a fine up to 500 000 EUR, or in case of an enterprise up to 1 % of its annual worldwide turnover, to anyone who, intentionally or negligently: [...]	5. The supervisory authority may impose a fine up to 500 000 EUR, or in case of an enterprise up to 1 % of its annual worldwide turnover, to anyone who, intentionally or negligently: [...]

Justification

Supervisory authorities should not be obliged to impose sanctions, instead they should only impose sanctions after taking into account all circumstances of each individual case.



Amendment 80

Article 79(6)

Original wording	Proposed amendment
<p>6. The supervisory authority shall impose a fine up to 1 000 000 EUR or, in case of an enterprise up to 2 % of its annual worldwide turnover, to anyone who, intentionally or negligently:</p> <p>[...]</p>	<p>6. The supervisory authority may impose a fine up to 1 000 000 EUR or, in case of an enterprise up to 2 % of its annual worldwide turnover, to anyone who, intentionally or negligently:</p> <p>[...]</p>

Justification

Supervisory authorities should not be obliged to impose sanctions, instead they should only impose sanctions after taking into account all circumstances of each individual case.

Amendment 81

Recital 119 – the accompanying recital to Article 76

Original wording	Proposed amendment
<p>Penalties should be imposed to any person, whether governed by private or public law, who fails to comply with this Regulation. Member States should ensure that the penalties should be effective, proportionate and dissuasive and should take all measures to implement the penalties.</p>	<p><i>Supervisory authorities shall be empowered to impose administrative sanctions</i> to any person, whether governed by private or public law, who fails to comply with this Regulation. Member States should ensure that the penalties should be effective, proportionate and dissuasive and should take all measures to implement the penalties.</p>

Justification

See justification for amendment 76-80.



CHAPTER X – Delegated Acts and Implementing Acts

Amendment 82

Article 86(2)

Original wording	Proposed amendment
<p>2. The delegation of power referred to in Article 6(5), Article 8(3), Article 9(3), Article 12(5), Article 14(7), Article 15(3), Article 17(9), Article 20(6), Article 22(4), Article 23(3), Article 26(5), Article 28(5), Article 30(3), Article 31(5), Article 32(5), Article 33(6), Article 34(8), Article 35(11), Article 37(2), Article 39(2), Article 43(3), Article 44(7), Article 79(6), Article 81(3), Article 82(3) and Article 83(3) shall be conferred on the Commission for an indeterminate period of time from the date of entry into force of this Regulation.</p>	<p>2. The delegation of power referred to in Article 8(3), Article 9(3), Article 12(5), Article 14(7), Article 15(3), Article 17(9), Article 22(4), Article 26(5), Article 28(5), Article 30(3), Article 31(5), Article 34(8), Article 35(11), Article 37(2), Article 39(2), Article 43(3), Article 44(7), Article 79(6), Article 81(3), Article 82(3) and Article 83(3) shall be conferred on the Commission for an indeterminate period of time from the date of entry into force of this Regulation.</p>

Justification

Delegated acts would leave the Regulation to be changed substantially over time, likely resulting in business as well as legal uncertainty. In accordance with the provisions of the Treaty delegated acts can only be applied to “non-essential” aspects of the Regulation, rather than, as in the Proposal, on all essential aspects of the Regulation.

The Regulation should therefore not be subject to change in particular on the following issues:

- Lawfulness of processing (Article 6(5));
- Right to be forgotten (Article 17(9));
- Measures based on profiling (Article 20(5));
- Design (Article 23(4));
- Communication of personal data breach (Article 32(5));
- Data protection impact assessment (Article 33(6)).

Amendment 83

Article 86(3)

Original wording	Proposed amendment
<p>3. The delegation of power referred to in Article 6(5), Article 8(3), Article 9(3), Article 12(5), Article 14(7), Article 15(3), Article 17(9), Article 20(6), Article 22(4), Article 23(3), Article 26(5), Article 28(5), Article 30(3), Article 31(5), Article 32(5), Article 33(6), Article 34(8), Article 35(11), Article 37(2), Article 39(2), Article 43(3), Article 44(7), Article 79(6), Article 81(3), Article 82(3) and Article 83(3) may be revoked at any time by the</p>	<p>3. The delegation of power referred to in Article 8(3), Article 9(3), Article 12(5), Article 14(7), Article 15(3), Article 17(9), Article 22(4), Article 26(5), Article 28(5), Article 30(3), Article 31(5), Article 34(8), Article 35(11), Article 37(2), Article 39(2), Article 43(3), Article 44(7), Article 79(6), Article 81(3), Article 82(3) and Article 83(3) may be revoked at any time by the European Parliament or by the Council. A decision of</p>



<p>European Parliament or by the Council. A decision of revocation shall put an end to the delegation of power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.</p>	<p>revocation shall put an end to the delegation of power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.</p>
--	---

Justification

See justification for amendment 82.

Amendment 84
Article 86(5)

Original wording	Proposed amendment
<p>5. A delegated act adopted pursuant to Article 6(5), Article 8(3), Article 9(3), Article 12(5), Article 14(7), Article 15(3), Article 17(9), Article 20(6), Article 22(4), Article 23(3), Article 26(5), Article 28(5), Article 30(3), Article 31(5), Article 32(5), Article 33(6), Article 34(8), Article 35(11), Article 37(2), Article 39(2), Article 43(3), Article 44(7), Article 79(6), Article 81(3), Article 82(3) and Article 83(3) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or the Council.</p>	<p>5. A delegated act adopted pursuant to Article 8(3), Article 9(3), Article 12(5), Article 14(7), Article 15(3), Article 17(9), Article 22(4), Article 26(5), Article 28(5), Article 30(3), Article 31(5), Article 34(8), Article 35(11), Article 37(2), Article 39(2), Article 43(3), Article 44(7), Article 79(6), Article 81(3), Article 82(3) and Article 83(3) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or the Council.</p>

Justification

See justification for amendment 82.



Amendment 85

Recital 129 – the accompanying recital to Article 86

Original wording	Proposed amendment
<p>In order to fulfil the objectives of this Regulation, namely to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data and to ensure the free movement of personal data within the Union, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the Commission. In particular, delegated acts should be adopted in respect of lawfulness of processing; specifying the criteria and conditions in relation to the consent of a child; processing of special categories of data; specifying the criteria and conditions for manifestly excessive requests and fees for exercising the rights of the data subject; criteria and requirements for the information to the data subject and in relation to the right of access; the right to be forgotten and to erasure; measures based on profiling; criteria and requirements in relation to the responsibility of the controller and to data protection by design and by default; a processor; criteria and requirements for the documentation and the security of processing; criteria and requirements for establishing a personal data breach and for its notification to the supervisory authority, and on the circumstances where a personal data breach is likely to adversely affect the data subject; the criteria and conditions for processing operations requiring a data protection impact assessment; the criteria and requirements for determining a high degree of specific risks which require prior consultation; designation and tasks of the data protection officer; codes of conduct; criteria and requirements for certification mechanisms; criteria and requirements for transfers by way of binding corporate rules; transfer derogations; administrative sanctions; processing for health purposes; processing in the employment context and processing for historical, statistical and scientific research purposes. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level. The Commission, when preparing and drawing-up delegated acts, should ensure a simultaneous, timely and appropriate transmission of relevant documents to the European Parliament and Council.</p>	<p>In order to fulfil the objectives of this Regulation, namely to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data and to ensure the free movement of personal data within the Union, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the Commission. In particular, delegated acts should be adopted in respect of specifying the criteria and conditions in relation to the consent of a child; processing of special categories of data; specifying the criteria and conditions for manifestly excessive requests and fees for exercising the rights of the data subject; criteria and requirements for the information to the data subject and in relation to the right of access; criteria and requirements in relation to the responsibility of the controller and a processor; criteria and requirements for the documentation and the security of processing; criteria and requirements for establishing a personal data breach and for its notification to the supervisory authority; the criteria and conditions for processing operations requiring a data protection impact assessment; the criteria and requirements for determining a high degree of specific risks which require prior consultation; designation and tasks of the data protection officer; codes of conduct; criteria and requirements for certification mechanisms; criteria and requirements for transfers by way of binding corporate rules; transfer derogations; administrative sanctions; processing for health purposes; processing in the employment context and processing for historical, statistical and scientific research purposes. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level. The Commission, when preparing and drawing-up delegated acts, should ensure a simultaneous, timely and appropriate transmission of relevant documents to the European Parliament and Council.</p>



Justification

See justification for amendment 82.

Amendment 86

Recital 130

Original wording	Proposed amendment
<p>In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission for: specifying standard forms in relation to the processing of personal data of a child; standard procedures and forms for exercising the rights of data subjects; standard forms for the information to the data subject; standard forms and procedures in relation to the right of access; the right to data portability; standard forms in relation to the responsibility of the controller to data protection by design and by default and to the documentation; specific requirements for the security of processing; the standard format and the procedures for the notification of a personal data breach to the supervisory authority and the communication of a personal data breach to the data subject; standards and procedures for a data protection impact assessment; forms and procedures for prior authorisation and prior consultation; technical standards and mechanisms for certification; the adequate level of protection afforded by a third country or a territory or a processing sector within that third country or an international organisation; disclosures not authorized by Union law; mutual assistance; joint operations; decisions under the consistency mechanism. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers. In this context, the Commission should consider specific measures for micro, small and medium-sized enterprises.</p>	<p>In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission for: specifying standard forms in relation to the processing of personal data of a child; standard procedures and forms for exercising the rights of data subjects; standard forms for the information to the data subject; standard forms and procedures in relation to the right of access; specific requirements for the security of processing; the standard format and the procedures for the notification of a personal data breach to the supervisory authority and the communication of a personal data breach to the data subject; standards and procedures for a data protection impact assessment; forms and procedures for prior authorisation and prior consultation; technical standards and mechanisms for certification; the adequate level of protection afforded by a third country or a territory or a processing sector within that third country or an international organisation; disclosures not authorized by Union law; mutual assistance; joint operations; decisions under the consistency mechanism. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers. In this context, the Commission should consider specific measures for micro, small and medium-sized enterprises.</p>

Justification

See justification for amendment 36 and 51.

Eurofinas observations and proposal for amendments on the ITRE draft opinion on the Proposal for a General Data Protection Regulation

Eurofinas, the voice of consumer credit providers at European level, believes that the Commission Proposal for a General Data Protection Regulation provides a good starting point to further discussions and debate on the EU framework for the protection of personal data. We have taken note of the draft opinion of the Industry, Research and Energy Committee and would like to share our views on this document with you. The below should be read in light of the Eurofinas observations on the Proposal.¹

The draft ITRE opinion on this Proposal addresses the concerns of the industry in a number of areas. **In particular we support the following amendments incorporated in the draft opinion:**

- **Amendment 6 and 30: Recital 38, Article 6(1)(f) – Legitimate interests**
These amendments ensures that data can be processed for the legitimate interests pursued by the controller and the third party/parties to whom the data are communicated, in line with the currently applicable Directive 95/46/EC
- **Amendment 34: Article 7(1) - Consent**
There is no justification for a burden of proof for the controller only, especially in cases where the data subject has the consent in his personal documents. We support the deletion of this provision.
- **Amendment 29: Article 6(1)(a) – Specific purposes**
In some Member States, consumers give consent for the processing of their data for general purposes. If consent were to be required for each separate purpose, this would be disproportionately time-consuming, resource-intensive and costly.
- **Amendment 47, 48, 49, 50, 56: Article 14(1)(b), Article 14(1)(c), Article 14(1)(e), Article 14(1)(h), Article 15(1)(f) – Information to be provided to data subjects**
We support the amendments put forward in this area. Data subjects will already have been provided the contract terms and conditions when they signed this contract and there is no reason for duplications. Periods for data storage are often not known at the time the data is collected, especially in highly regulated sectors such as financial services where anti-money laundering requires the collection and storage of data throughout the relationship with the client, which may be of an indeterminate period of time.
- **Amendment 52: Article 14(3) – Publicly available data**
As the data is already publicly available, such a warranty is not necessary to ensure the protection of fundamental rights. The data has already been published and the data subject already knows this and that his or her data may be processed by third parties.

¹ See <http://www.eurofinas.org/uploads/documents/positions/Eurofinas%20observations%20-%20final.pdf>.

- **Amendment 62: Article 17(3)(d) – Erasure**
The amendment would increase legal certainty for controllers who are obliged to process data in accordance with legal obligations.
- **Amendment 93: Article 33(4) – Impact Assessments**
We support deletion of this provision as it will be impossible to implement in practice for controllers to seek the views of data subjects’ representatives and they may not always have the expertise, qualifications or resources to respond to such imposed requests for their views;
- **Amendment 125 - 153: Article 79(3) – Article 79(7) – Sanctions**
Supervisory authorities should not be obliged to impose sanctions, they should only impose sanctions after taking into account all circumstances of each individual case.
- **Amendments 20, 33, 40, 45, 46, 57, 64, 73, 77, 79, 80 85, 87, 89, 91, 9, 114, 156, 157: Recital 129, Article 6(5), Article 8(3), Article 9(3), Article 12(5), Article 15(3), Article 17(9), Article 20(5), Article 22(4), Article 23(3), Article 23(4), Article 28(5), Article 30(3), Article 31(5), Article 32(5), Article 34(8), Article 44(7), Article 81(3), Article 82(3) – Delegated and implementing acts**
Delegated and implementing acts would leave the Regulation to be changed substantially over time, likely resulting in business as well as legal uncertainty, we therefore fully support a reduction in the number of delegated acts.
- **Amendment 28, 44, 71 and 158: Article 4(19a) (new), Article 9(2)(j), Article 20(2)(cb) (new) and Article 83 (a) (new) – Processing of criminal convictions data for the purpose of the prevention of financial crime**
We support these provisions, as it enables financial institutions to detect and prevent fraud. However, this is only one of many measures that we feel should be taken in this area.

Therefore, in addition, we would also like to suggest a number of further amendments:

Amendment 1 – Data minimisation
Article 5(c)

Original wording	Proposed amendment
Personal data must be: (c) adequate, relevant, and limited to the minimum necessary in relation to the purposes for which they are processed; they shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data;	Personal data must be: (c) adequate, relevant, and not excessive in relation to the purposes for which they are processed; they shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data;

Justification

The obligation to process the minimum data necessary would contradict with legal provisions which require, e.g. lending institutions, to process personal data such as the Consumer Credit Directive and the Capital Requirements Package. Therefore wording of Directive 95/46/EC which permits “not excessive” processing is more appropriate.

Amendment 2 – Lawfulness of processing

Article 6(1)(c)

Original wording	Proposed amendment
<p>1. Processing of personal data shall be lawful only if and to the extent that at least one of the following applies:</p> <p>(c) processing is necessary for compliance with a legal obligation to which the controller is subject;</p>	<p>1. Processing of personal data shall be lawful only if and to the extent that at least one of the following applies:</p> <p>(c) processing is necessary for compliance with a legal obligation, regulatory rule, guidance, industry code of practice, either domestically or internationally to which the controller is subject including the requirements of supervisory authorities;</p>

Justification

Article 6(1)(c) should be widened-up to ensure that domestic financial regulation or codes of conduct are included, in particular the requirements of supervisory authorities.

Amendment 3 – Legitimate interest

Article 6(1)(f)

Original wording	Proposed amendment
<p>1. Processing of personal data shall be lawful only if and to the extent that at least one of the following applies:</p> <p>(f) processing is necessary for the purposes of the legitimate interests pursued by a controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks.</p>	<p>1. Processing of personal data shall be lawful only if and to the extent that at least one of the following applies:</p> <p>(f) processing is necessary for the purposes of the legitimate interests pursued by a controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks. It is within the controller's legitimate interests to prevent and detect fraud.</p> <p>OR</p> <p>(f) processing is necessary for the purposes of the legitimate interests pursued by a controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to</p>

	<p>processing carried out by public authorities in the performance of their tasks.</p> <p><i>It is within the controller's legitimate interests to prevent and detect fraud, to consult and input into a database for the purpose of the approval, monitoring and recovery of risks, credit transactions and recurring billing services, through the sharing of both positive information and information on defaults. This processing may be managed by service providers with capital and credit solvency subject to compliance with these rules.</i></p>
--	--

<p><i>Justification</i></p> <p>Experience in practice has shown that these provisions often do not permit the processing of data for fraud prevention and detection purposes. Detecting and preventing fraud is of paramount importance for data controllers. Not only for the controller in question but also to protect data subjects from, for example, falling victim to a loan fraudulently being taken out in their name. Fraud prevention and detection should be explicitly recognised as a legitimate purpose for data processing.</p> <p>Credit reports should also be explicitly recognised as a legitimate purpose for data processing. The Judgement of the Court of Justice of the European Union in joined Cases C 468/10 and C 469/10 established the presumption in favour of the legitimate interest in cases where the data come from public sources when considering the possible violation of fundamental rights. With regard to fraud prevention files and credit reports, the prevention of fraud, defaults, and over-indebtedness of families are legitimate interests of operators, most notably in the cases of compliance with the rules on responsible lending. Each country has regulated these purposes differently. The above points legitimise the need to include these assumptions within the cases of data processing based on legitimate interest.</p>
--

Amendment 4 – Significant imbalance
Article 7 (4)

Original wording	Proposed amendment
<p>4. Consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller.</p>	<p><i>Deleted.</i></p>

<p><i>Justification</i></p> <p>What can be considered as a “significant imbalance” or “free” consent will be subject to differing national interpretations. It is essential that this provision does not result in the inability for businesses to process data because an automatic presumption of an imbalance between the positions of the consumer and business within every relationship between the two parties.</p> <p>To avoid legal uncertainty, paragraph 4 should be deleted or at least amended to ensure that where consent cannot provide a legal basis due to an imbalance, the controller can process the data in accordance with another legal basis, as set out in Article 6(1) of the Proposal.</p>
--

Amendment 5 – Right to be forgotten

Article 17(3) introduction

Original wording	Proposed amendment
3. The controller shall carry out the erasure without delay, except to the extent that the retention of the personal data is necessary:	3. The controller shall carry out the erasure without unreasonable delay, except to the extent that the retention and dissemination of the personal data is necessary:

Justification

Where controllers are subject to a legal obligation to retain and process data, they may also be obliged to transfer this data to relevant supervisory authorities, such as suspicious transaction reports to financial intelligence units in the context of anti-money laundering rules. Therefore further dissemination should be possible. The “without delay” requirement must be qualified to ensure that it is realistic.

Amendment 6 – Data portability

Article 18

Original wording	Proposed amendment
1. [...] 2. [...] 3. [...]	Deleted.

Justification

Article 15 of the Regulation already provides the right of data subjects to access personal data and to obtain communication thereon, i.e. to obtain a copy. Article 18(1) is therefore a repetition and redundant.

Data portability could be open to abuse, as an ill-intended applicant borrower may alter the data in between receiving, for example, his credit history from one processor and presenting it to a lender. The receiving processor would thus not be able to rely on the accuracy of the data. Data may not be stored or processed in the same language, according to the same categories or procedures. This may render data portability of little value. There is also a risk that this provision could require organisations to disclose trade secrets, internal know-how or information on other customers. We are also concerned that data portability may increase the risk of disclosure of personal data to third parties.

In the specific context of credit data, the European Commission’s Expert Group on Credit Histories decided that it should be left to each individual lender to decide which data access model offers the most convenient and cost-effective solution to data portability. The obligation for data portability would not be in line with these findings. Perhaps there may also be the risk that the receiving processor will require the data subject to provide all his data (history) before offering services. This could be disproportionate.

Where data is made portable, the requirements and obligations for the receiving controller are unclear. For example, does the retention period start again at zero? If deletion is not possible, the scope of the article should be narrowed down to only those sectors where this could appropriately be implemented, e.g. social networks.

Amendment 7 – Automated processing

Article 20(2)(a)

Original wording	Proposed amendment
<p>2. Subject to the other provisions of this Regulation, a person may be subjected to a measure of the kind referred to in paragraph 1 only if the processing:</p> <p>(a) is carried out in the course of the entering into, or performance of, a contract, where the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or where suitable measures to safeguard the data subject's legitimate interests have been adduced, such as the right to obtain human intervention; or</p>	<p>2. Subject to the other provisions of this Regulation, a person may be subjected to a measure of the kind referred to in paragraph 1 if the processing:</p> <p>(a) is carried out in the course of the entering into, or performance of, a contract, where suitable measures to safeguard the data subject's legitimate interests have been adduced, such as the right to obtain human intervention; or</p>

Justification

A customer may enquire as to the terms and conditions for entering into, for example, a consumer credit contract. In order for the consumer credit provider to provide information on the APRC, it will assess the consumer's creditworthiness, a legal obligation. Requiring a formal request for the entering into a contract to be proven, would essentially render service and goods providers unable to respond to information requests.

Amendment 8 – Automated processing
Article 20(2)(b)

Original wording	Proposed amendment
<p>2. Subject to the other provisions of this Regulation, a person may be subjected to a measure of the kind referred to in paragraph 1 only if the processing:</p> <p>(b) is expressly authorized by a Union or Member State law which also lays down suitable measures to safeguard the data subject's legitimate interests; or</p>	<p>2. Subject to the other provisions of this Regulation, a person may be subjected to a measure of the kind referred to in paragraph 1 if the processing:</p> <p>(b) is necessary to comply with a Union or Member State law; or</p>

Justification

It cannot be the task of data controllers to check, whether the Member State law "lays down suitable measures to safeguard the data subject's legitimate interests". On the contrary, firms have to be able to rely on the law.

We would be pleased to answer any question you may have on these elements or to provide you with further information. Please do not hesitate to contact Eurofinas legal adviser Anke Delava (a.delava@eurofinas.org, T: +32 2 778 05 73).

Facebook recommendations on the Internal Market and Consumer Affairs draft opinion on the European Commission’s proposal for a General Data Protection Regulation “on the protection of individuals with regard to the processing of personal data and on the free movement of such data”

1. Jurisdiction/One-stop shop/Consistency mechanism

The core principle of a single Data Protection Authority (DPA) having jurisdiction over organisations that operate across multiple European countries is a sensible and positive development in the draft Regulation. The 'one-stop shop' principle has the potential of creating the right incentives for international organisations to establish and invest in Europe. However there are some aspects of the drafting of the draft Regulation which need to be improved if this principle is to be realised. This will in turn provide better protection for European citizens who will be able to seek redress in the European Union (the "EU").

In particular, for citizens and international organisations with a presence in the EU to reap the full benefits of the one-stop shop principle, it must be clear how the law applies in the case of group companies. Where if there is already an EU based controller within a corporate group, that controller should be responsible for compliance with the relevant EU data protection obligations and accountable to the competent supervisory authority.

Further, many provisions of the draft Regulation undermine the intent of the one-stop shop principle and create legal uncertainty for businesses. These provisions should be revised to maintain the robustness of the changes that are proposed.

Drafting recommendations:

Article 3 (Territorial scope): If there is already an EU-based controller processing the same personal data as a non-EU based controller within a corporate group, the EU-based controller should be responsible for compliance in respect of the relevant data processing (as per Article 3(1)).

As further explained in section 4 “profiling” of this document, the draft Regulation as it is currently worded is set to apply to non-EU controllers when the processing relates to the 'monitoring of an individual's behaviour'. It is our view that the express reference to 'monitoring' undermines the principle of technology neutrality. *Article 55 (Mutual Assistance):* The draft Regulation should reflect the practical viability and resources affecting mutual assistance duties between supervisory authorities. We therefore propose:

- deleting the mutual assistance obligations regarding prior authorisations (Article 55(1)) and the ability to take a provisional measure and submit the matter the EDPB where a request for assistance is not actioned within 1 month (Article 55(8) and (9));

FACEBOOK

- the measures required to reply to a request of another supervisory authority must be "reasonable". Further, requests made by another supervisory authority for general "enforcement measures" should be specifically limited to requests for the communication of any enforcement decision which relates to processing operations that have been proven to be contrary to the Regulation (Article 55(2)).
- the mutual assistance provisions should only apply:
 - where individuals in several member states are likely to be affected by the processing to operations that "produce adverse legal effects concerning the fundamental rights and freedoms of the individual or affect them in a significantly negative manner" (Article 55(1));
 - unless complying with request for assistance would "involve disproportionate effort" (Article 55(4)(b)).

Article 58 (Consistency Mechanism - Opinion by the European Data Protection Board):

The consistency mechanism should only apply in limited circumstances to avoid a potentially massive and damaging bureaucratisation of the decision making process by the data protection authorities.

Drafting suggestions:

<p>Recital 27</p> <p>The main establishment of a controller or a processor in the Union should be determined according to objective criteria and should imply the effective and real exercise of management activities determining the main decisions as to the purposes, conditions and means of processing through stable arrangements. This criterion should not depend whether the processing of personal data is actually carried out at that location; the presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute such main establishment and are therefore no determining criteria for a main establishment.</p>	<p>Recital 27</p> <p>The main establishment of a controller or a processor in the Union should be determined according to objective criteria and should imply the effective and real exercise of management activities determining the main decisions as to the purposes, conditions and means of processing through stable arrangements. This criterion should not depend whether the processing of personal data is actually carried out at that location; the presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute such main establishment and are therefore no determining criteria for a main establishment. <i>The main establishment of the processor should be the place of its central administration in the Union.</i></p>
---	--

Justification

Retain the European Commission’s text. The proposed additions do not work given the different definitions between controller and processor in the draft Regulation.

<p>Recital 97 (EC proposal)</p> <p>Where the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union takes place in more than one Member State, one single supervisory authority should be competent for monitoring the activities of the controller or processor throughout the Union and taking the related decisions, in order to increase the consistent application, provide legal certainty and reduce administrative burden for such controllers and processors.</p>	<p>Recital 97</p> <p>Where the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union takes place in more than one Member State, one single supervisory authority should be competent for monitoring the activities of the controller or processor throughout the Union and taking the related decisions, in order to increase the consistent application, provide legal certainty and reduce administrative burden for such controllers and processors.</p>
--	---

Justification

The draft Regulation should be clear about how the law applies in the case of group companies. Where an EU-based controller and a non-EU based controller within the same corporate group process the same personal data, the EU controller should be responsible for compliance with the relevant EU data protection obligations and accountable to the competent supervisory authority. It is important that the position regarding territorial scope is sufficiently clear to ensure that the rules concerning the competent data protection supervisory authority are not seriously compromised. International companies and individuals must have certainty as to which competent supervisory authority will have authority to supervise a non-EU controller.

<p>Recital 105</p> <p>In order to ensure the consistent application of this Regulation throughout the Union, a consistency mechanism for co-operation between the supervisory authorities themselves and the Commission should be established. This mechanism should in particular apply where a supervisory authority intends to take a measure as regards processing</p>	<p>Recital 105</p> <p>In order to ensure the consistent application of this Regulation throughout the Union, a consistency mechanism for co-operation between the supervisory authorities themselves and the Commission should be established. This mechanism should in particular apply where a the competent supervisory authority intends to take a measure as</p>
--	---

FACEBOOK

<p>operations that are related to the offering of goods or services to data subjects in several Member States, or to the monitoring of such data subjects, or that might substantially affect the free flow of personal data. It should also apply where any supervisory authority or the Commission requests that the matter should be dealt with in the consistency mechanism. Furthermore, the data subjects should have the right to obtain consistency, if they deem a measure by a Data Protection Authority of a Member State has not fulfilled this criterion. This mechanism should be without prejudice to any measures that the Commission may take in the exercise of its powers under the Treaties.</p>	<p>regards processing operations that are related to the fundamental rights and freedoms of a data subject the offering of goods or services to data subjects in several Member States, or to the monitoring of such data subjects, or that might substantially affect the free flow of personal data. It should also apply where those factors are present and any supervisory authority or the Commission requests that the matter should be dealt with in the consistency mechanism. This mechanism should be without prejudice to any measures that the Commission may take in the exercise of its powers under the Treaties.</p>
--	--

<p style="text-align: center;"><i>Justification</i></p> <p>The consistency mechanism should only apply in limited circumstances (and where there is a substantial public interest) to avoid a potentially massive and very damaging bureaucratisation of the decision making process by the data protection authorities. The range of instances that trigger that mechanism, the ability of the Commission to launch it, and the process to be followed need to be carefully worded so that they can reflect the practical viability and resources required. References to the 'supervisory authority' should be consistent with the regime set out in the 'competence' provisions in Article 51.</p> <p>Further, the express reference to 'monitoring' violates the principle of technology neutrality. In any event, any adverse effects to the data subject that may result from the 'monitoring of an individual's behavior' are already adequately protected by the provisions of this regulation.</p>	
---	--

<p>Recital 108 (EC proposal) There may be an urgent need to act in order to protect the interests of data subjects, in particular when the danger exists that the enforcement of a right of a data subject could be considerably impeded. Therefore, a supervisory authority should be able to adopt provisional measures with a specified</p>	<p>Recital 108 There may be an urgent need to act in order to protect the interests of data subjects, in particular when the danger exists that the enforcement of a right of a data subject could be considerably impeded. Therefore, a the competent supervisory authority should be able to adopt provisional measures with a</p>
--	---

FACEBOOK

period of validity when applying the consistency mechanism	specified period of validity when applying the consistency mechanism.
<i>Justification</i>	
References to the 'supervisory authority' should be consistent with the regime set out in the 'competence' provisions in Article 51.	

Recital 109 (EC proposal) The application of this mechanism should be a condition for the legal validity and enforcement of the respective decision by a supervisory authority. In other cases of cross-border relevance, mutual assistance and joint investigations might be carried out between the concerned supervisory authorities on a bilateral or multilateral basis without triggering the consistency mechanism.	Recital 109 The application of this mechanism should be a condition for the legal validity and enforcement of the respective decision by the competent supervisory authority. In other cases of cross-border relevance, mutual assistance and joint investigations might be carried out between the concerned supervisory authorities on a bilateral or multilateral basis without triggering the consistency mechanism.
<i>Justification</i>	
References to the 'supervisory authority' should be consistent with the regime set out in the 'competence' provisions in Article 51.	

Recital 111 Every data subject should have the right to lodge a complaint with a supervisory authority in any Member State and have the right to a judicial remedy if they consider that their rights under this Regulation are infringed or where the supervisory authority does not react on a complaint or does not act where such action is necessary to protect the rights of the data subject. <i>If the data subject deems consistency is not fulfilled, a complaint to the European Data Protection Board can be filed</i>	Recital 111 Every data subject should have the right to lodge a complaint with a supervisory authority in any Member State and have the right to a judicial remedy if they consider that their rights under this Regulation are infringed or where the supervisory authority does not react on a complaint or does not act where such action is necessary to protect the rights of the data subject. <i>If the data subject deems consistency is not fulfilled, a complaint to the European Data Protection Board can be filed.</i>
<i>Justification</i>	
Retain the European Commission's text. It is unclear what power the European Data Protection Board (the 'EDPB') has in such a situation. If an opinion is issued, the draft Regulation does not empower the EDPB to force a supervisory authority to abide by that	

opinion. Such powers should ultimately lie with the courts, not the EDPB.

<p>Recital 113 Each natural or legal person should have the right to a judicial remedy against decisions of a supervisory authority concerning them. Proceedings against a supervisory authority should be brought before the courts of the Member State, where the supervisory authority is established, or before the European Data Protection Board on grounds of inconsistency with the application of the present Regulation in other Member States</p>	<p>Recital 113 Each natural or legal person should have the right to a judicial remedy against decisions of a supervisory authority concerning them. Proceedings against a supervisory authority should be brought before the courts of the Member State, where the supervisory authority is established.</p>
<p><i>Justification</i></p> <p>Retain the European Commission’s text. It is unclear what power the European Data Protection Board (the 'EDPB') has in such a situation. If an opinion is issued, the draft Regulation does not empower the EDPB to force a supervisory authority to abide by that opinion. Such powers should ultimately lie with the courts, not the EDPB.</p>	

<p>Article 3 1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union. 2. This Regulation applies to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are related to: (a) the offering of goods and services to such data subjects in the Union, including services provided without financial costs to the individual, or; (b) the monitoring of their behaviour. 3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place</p>	<p>Article 3 1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union. 2. This Regulation applies to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are related to: (a) the offering of goods or services to such data subjects in the Union; or (b) the monitoring of their behaviour except where the processing of personal data is carried out by a controller within the same corporate group of a controller to which paragraph 1 applies.</p>
---	---

FACEBOOK

<p>where the national law of a Member State applies by virtue of public international law.</p>	<p>3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where the national law of a Member State applies by virtue of public international law..</p>
<p style="text-align: center;"><i>Justification</i></p> <p>The draft Regulation should be clear about how the law applies in the case of group companies. Where an EU-based controller and a non-EU based controller within the same corporate group process the same personal data, the EU controller should be responsible for compliance with the relevant EU data protection obligations and accountable to the competent supervisory authority. It is important that the position regarding territorial scope is sufficiently clear to ensure that the rules concerning the competent data protection supervisory authority are not seriously compromised. International companies and individuals must have certainty as to which competent supervisory authority will have authority to supervise a non-EU controller.</p> <p>Any adverse effects to the data subject that may result from the ‘monitoring of an individual’s behavior’ is adequately covered by the provisions of this regulation. It is unclear why an express reference to this should be made under the territorial scope provisions – such reference could jeopardise the technologically neutral nature of the proposal.</p>	

<p>Article 4(1)(13) ‘main establishment’ means the place where the controller or the processor has its establishment in the Union where the main decisions as to the purposes, conditions and means of the processing of personal data are taken; if no decisions as to the purposes, conditions and means of the processing of personal data are taken in the Union, the main establishment is the place where the main processing activities in the context of the activities of an establishment of a controller or a processor in the Union take place.</p>	<p>Article 4(1)(13) ‘main establishment’ means as regards the place where the controller, the place of or the processor has its establishment in the Union where the main decisions as to the purposes, conditions and means of the processing of personal data are taken; if no decisions as to the purposes, conditions and means of the processing of personal data are taken in the Union, the main establishment is the place where the main processing activities in the context of the activities of an establishment of a controller or a processor in the Union take place. As regards the processor, ‘main establishment’ means the place of its central administration in the Union;</p>
<p style="text-align: center;"><i>Justification</i></p>	

Retain the European Commission’s text. The proposed additions do not work given the different definitions between controller and processor in the draft Regulation.

	<p>Article 4(1)(20)new</p> <p><i>'competent supervisory authority' means the supervisory authority of the controller in accordance with the Article 51(2) &(3)</i></p>
<p style="text-align: center;">Justification</p> <p>'Competent supervisory authority' should be clearly defined to assist with certainty as to which supervisory authority will have authority to supervise a controller. Further, the reference to 'competent' reinforces one of the key principles of the Regulation that one single authority will be competent in respect of the scrutiny of the controller, even if the other supervisory authorities can play a role in terms of safeguarding the data subjects within their jurisdictions.</p>	

<p>Article 51 (EC proposal)</p> <p>1. Each supervisory authority shall exercise, on the territory of its own Member State, the powers conferred on it in accordance with this Regulation.</p> <p>2. Where the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union, and the controller or processor is established in more than one Member State, the supervisory authority of the main establishment of the controller or processor shall be competent for the supervision of the processing activities of the controller or the processor in all Member States, without prejudice to the provisions of Chapter VII of this Regulation.</p>	<p>Article 51</p> <p>1. Each supervisory authority shall exercise, on the territory of its own Member State, the powers conferred on it in accordance with this Regulation.</p> <p>2. Where the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor <i>of a controller within the same corporate group not established in the Union or where</i> the controller or processor is established in more than one Member State, the supervisory authority of the main establishment of the controller or processor shall be competent for the supervision of the processing activities of the controller or the processor in all Member States, without prejudice to the provisions of Chapter VII of this Regulation. <i>All references to the competent supervisory authority shall be</i></p>
--	---

<p>3. The supervisory authority shall not be competent to supervise processing operations of courts acting in their judicial capacity.</p>	<p><i>interpreted in accordance with this Article 51(2).</i> 4. The supervisory authority shall not be competent to supervise processing operations of courts acting in their judicial capacity.</p>
<p style="text-align: center;"><i>Justification</i></p> <p>The draft Regulation should be clear about how the law applies in the case of group companies. Where an EU-based controller and a non-EU based controller within the same corporate group process the same personal data, the EU controller should be responsible for compliance with the relevant EU data protection obligations and accountable to the competent supervisory authority. It is important that the position regarding territorial scope is sufficiently clear to ensure that the rules concerning the competent data protection supervisory authority are not seriously compromised. International companies and individuals must have certainty as to which competent supervisory authority will have authority to supervise a non-EU controller.</p> <p>'Competent supervisory authority should be clearly defined to assist with certainty as to which supervisory authority will have authority to supervise a controller. Further. the reference to competent reinforces one of the key principles of the Regulation that one single authority will be competent in respect of the scrutiny of the controller, even if the other supervisory authorities can play a role in terms of safeguarding the data subjects within their jurisdictions.</p> <p>Processors should not be subject to the same administrative obligations and regulatory scrutiny as controllers as per our position in relation to Recital 65 / Article 28 (Documentation) / Article 9.</p>	

<p>Article 55 (EC proposal)</p> <p>1. Supervisory authorities shall provide each other relevant information and mutual assistance in order to implement and apply this Regulation in a consistent manner, and shall put in place measures for effective co-operation with one another. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out prior authorisations and consultations, inspections and prompt information on the opening of cases and ensuing developments where data</p>	<p>Article 55</p> <p>1. Supervisory authorities shall provide each other relevant information and mutual assistance in order to implement and apply this Regulation in a consistent manner, and shall put in place measures for effective co-operation with one another. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out prior authorisations and consultations, inspections and prompt information on the opening of cases and ensuing developments where data</p>
--	---

<p>subjects in several Member States are likely to be affected by processing operations.</p> <p>2. Each supervisory authority shall take all appropriate measures required to reply to the request of another supervisory authority without delay and no later than one month after having received the request. Such measures may include, in particular, the transmission of relevant information on the course of an investigation or enforcement measures to bring about the cessation or prohibition of processing operations contrary to this Regulation.</p> <p>3. The request for assistance shall contain all the necessary information, including the purpose of the request and reasons for the request. Information exchanged shall be used only in respect of the matter for which it was requested.</p> <p>4. A supervisory authority to which a request for assistance is addressed may not refuse to comply with it unless: (a) it is not competent for the request; or (b) compliance with the request would be incompatible with the provisions of this Regulation.</p> <p>5. The requested supervisory authority shall inform the requesting supervisory authority of the results or, as the case may be, of the progress or the measures taken in order to meet the request by the requesting supervisory authority.</p>	<p>subjects in several Member States are likely to be affected by processing operations that produce adverse legal effects concerning the fundamental rights and freedoms of the individual or affect them in a significantly negative manner;</p> <p>2. Each supervisory authority shall take all appropriate reasonable measures required to reply to the request of another supervisory authority without delay and no later than one month after having received the request. Such measures may include, in particular, the transmission of relevant information on the course of an investigation or enforcement measures communicating any enforcement decision taken to bring about the cessation or prohibition of processing operations that have been proven contrary to this Regulation.</p> <p>3. The request for assistance shall contain all the necessary information, including the purpose of the request and reasons for the request. Information exchanged shall be used only in respect of the matter for which it was requested.</p> <p>4. A supervisory authority to which a request for assistance is addressed may not refuse to comply with it unless: (a) it is not competent for the request; or (b) compliance with the request would be incompatible with the provisions of this Regulation or would involve disproportionate effort.</p> <p>5. The requested supervisory authority shall inform the requesting supervisory authority of the results or, as the case may be, of the progress or the measures taken in order to meet the request by the requesting supervisory authority.</p> <p>6. Supervisory authorities shall supply the</p>
--	---

<p>6. Supervisory authorities shall supply the information requested by other supervisory authorities by electronic means and within the shortest possible period of time, using a standardised format.</p> <p>7. No fee shall be charged for any action taken following a request for mutual assistance.</p> <p>8. Where a supervisory authority does not act within one month on request of another supervisory authority, the requesting supervisory authorities shall be competent to take a provisional measure on the territory of its Member State in accordance with Article 51(1) and shall submit the matter to the European Data Protection Board in accordance with the procedure referred to in Article 57.</p> <p>9. The supervisory authority shall specify the period of validity of such provisional measure. This period shall not exceed three months. The supervisory authority shall, without delay, communicate those measures, with full reasons, to the European Data Protection Board and to the Commission.</p> <p>10. The Commission may specify the format and procedures for mutual assistance referred to in this article and the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the European Data Protection Board, in particular the standardised format referred to in paragraph 6. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>	<p>information requested by other supervisory authorities by electronic means and within the shortest possible period of time, using a standardised format.</p> <p>7. No fee shall be charged for any action taken following a request for mutual assistance.</p> <p>8. Where a supervisory authority does not act within one month on request of another supervisory authority, the requesting supervisory authorities shall be competent to take a provisional measure on the territory of its Member State in accordance with Article 51(1) and shall submit the matter to the European Data Protection Board in accordance with the procedure referred to in Article 57.</p> <p>9. The supervisory authority shall specify the period of validity of such provisional measure. This period shall not exceed three months. The supervisory authority shall, without delay, communicate those measures, with full reasons, to the European Data Protection Board and to the Commission.</p> <p>10. The Commission may specify the format and procedures for mutual assistance referred to in this article and the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the European Data Protection Board, in particular the standardised format referred to in paragraph 6. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>
<p><i>Justification</i></p> <p>The draft Regulation should reflect the practical viability and resources affecting mutual assistance duties between supervisory authorities.</p>	

<p>Article 58 (EC proposal)</p> <p>1. Before a supervisory authority adopts a measure referred to in paragraph 2, this supervisory authority shall communicate the draft measure to the European Data Protection Board and the Commission.</p> <p>2. The obligation set out in paragraph 1 shall apply to a measure intended to produce legal effects and which:</p> <p>(a) relates to processing activities which are related to the offering of goods or services to data subjects in several Member States, or to the monitoring of their behaviour; or</p> <p>(b) may substantially affect the free movement of personal data within the Union; or</p> <p>(c) aims at adopting a list of the processing operations subject to prior consultation pursuant to Article 34(5); or</p> <p>(d) aims to determine standard data protection clauses referred to in point (c) of Article 42(2); or</p> <p>(e) aims to authorise contractual clauses referred to in point (d) of Article 42(2); or</p> <p>(f) aims to approve binding corporate rules within the meaning of Article 43.</p> <p>3. Any supervisory authority or the</p>	<p>Article 58</p> <p>1. Before a the competent supervisory authority adopts a measure referred to in paragraph 2, this competent supervisory authority shall communicate the draft measure to the European Data Protection Board and the Commission.</p> <p>2. The obligation set out in paragraph 1 shall apply to a measure intended to produce legal effects concerning the fundamental rights and freedoms of a data subject and which:</p> <p>(a) relates to processing activities which are likely to produce adverse legal effects concerning the fundamental rights and freedoms of the individual or affect the individual in a significantly negative manner related to the offering of goods or services to data subjects in several Member States, or to the monitoring of their behaviour; or</p> <p>(b) may substantially affect the free movement of personal data within the Union; or</p> <p>(c) aims at adopting a list of the processing operations subject to prior consultation pursuant to Article 34(5); or</p> <p>(d) aims to determine standard data protection clauses referred to in point (c) of Article 42(2); or</p> <p>(e) aims to authorise contractual clauses referred to in point (d) of Article 42(2); or</p> <p>(f) aims to approve binding corporate rules within the meaning of Article 43.</p> <p>3. Any supervisory authority or the</p>
---	--

<p>European Data Protection Board may request that any matter shall be dealt with in the consistency mechanism, in particular where a supervisory authority does not submit a draft measure referred to in paragraph 2 or does not comply with the obligations for mutual assistance in accordance with Article 55 or for joint operations in accordance with Article 56.</p> <p>4. In order to ensure correct and consistent application of this Regulation, the Commission may request that any matter shall be dealt with in the consistency mechanism.</p> <p>5. Supervisory authorities and the Commission shall electronically communicate any relevant information, including as the case may be a summary of the facts, the draft measure, and the grounds which make the enactment of such measure necessary, using a standardised format.</p> <p>6. The chair of the European Data Protection Board shall immediately electronically inform the members of the European Data Protection Board and the Commission of any relevant information which has been communicated to it, using a standardised format. The chair of the European Data Protection Board shall provide translations of relevant information, where necessary.</p> <p>7. The European Data Protection Board shall issue an opinion on the matter, if the European Data Protection Board so decides by simple majority of its members or any supervisory authority or the Commission so requests within one week after the relevant information has been provided according to paragraph 5. The</p>	<p>European Data Protection Board may request that any matter shall be dealt with in the consistency mechanism,in particular where the competent supervisory authority does not submit a draft measure referred to in paragraph 2 or does not comply with the obligations for mutual assistance in accordance with Article 55 or for joint operations in accordance with Article 56.</p> <p>4. In order to ensure correct and consistent application of this Regulation, the Commission may request that any matter related to the category of measures referred to in paragraph 2 shall be dealt with in the consistency mechanism.</p> <p>5. Supervisory authorities and the Commission shall electronically communicate any relevant information, including as the case may be a summary of the facts, the draft measure, and the grounds which make the enactment of such measure necessary, using a standardised format.</p> <p>6. The chair of the European Data Protection Board shall immediately electronically inform the members of the European Data Protection Board and the Commission of any relevant information which has been communicated to it, using a standardised format. The chair of the European Data Protection Board shall provide translations of relevant information, where necessary.</p> <p>7. The European Data Protection Board shall issue an opinion on the matter, if the European Data Protection Board so decides by simple majority of its members or any supervisory authority or the Commission so requests within one week after the relevant information has been provided according to paragraph 5. The</p>
---	--

FACEBOOK

<p>opinion shall be adopted within one month by simple majority of the members of the European Data Protection Board. The chair of the European Data Protection Board shall inform, without undue delay, the supervisory authority referred to, as the case may be, in paragraphs 1 and 3, the Commission and the supervisory authority competent under Article 51 of the opinion and make it public.</p> <p>8. The supervisory authority referred to in paragraph 1 and the supervisory authority competent under Article 51 shall take account of the opinion of the European Data Protection Board and shall within two weeks after the information on the opinion by the chair of the European Data Protection Board, electronically communicate to the chair of the European Data Protection Board and to the Commission whether it maintains or amends its draft measure and, if any, the amended draft measure, using a standardised format.</p>	<p>opinion shall be adopted within one month by simple majority of the members of the European Data Protection Board. The chair of the European Data Protection Board shall inform, without undue delay, the supervisory authority referred to, as the case may be, in paragraphs 1 and 3, the Commission and the competent supervisory authority competent under Article 51 of the opinion and make it public.</p> <p>8. The supervisory authority referred to in paragraph 1 and The competent supervisory authority competent under Article 51 shall take utmost account of, but not be bound by, the opinion of the European Data Protection Board and shall within two weeks after the information on the opinion by the chair of the European Data Protection Board, electronically communicate to the chair of the European Data Protection Board and to the Commission whether it maintains or amends its draft measure and, if any, the amended draft measure, using a standardised format.</p>
<p><i>Justification</i></p> <p>The consistency mechanism should only apply in limited circumstances to avoid a potentially massive and very damaging bureaucratisation of the decision making process by the data protection authorities. The range of instances that trigger that mechanism (paragraph 2), the ability of the Commission to launch it (paragraph 4), and the process to be followed (paragraphs 7 and 8) need to be carefully worded so that they can reflect the practical viability and resources required. With regard to the process to be followed, experience shows that despite their best efforts, supervisory authorities are not organized and resourced in a way that allows them to meet strict timeframes. Therefore, it is very likely that the timeframes set out will be routinely missed and, as a result, any decisions or measures subject to the consistency mechanism will be unnecessarily and unjustifiably delayed. In view of this, the consistency mechanism should only be engaged in a minority of situations and where there is a substantial public interest.</p>	
<p>Article 59 (EC proposal)</p>	<p>Article 59</p>

FACEBOOK

<p>1. Within ten weeks after a matter has been raised under Article 58, or at the latest within six weeks in the case of Article 61, the Commission may adopt, in order to ensure correct and consistent application of this Regulation, an opinion in relation to matters raised pursuant to Articles 58 or 61.</p> <p>2. Where the Commission has adopted an opinion in accordance with paragraph 1, the supervisory authority concerned shall take utmost account of the Commission’s opinion and inform the Commission and the European Data Protection Board whether it intends to maintain or amend its draft measure.</p> <p>3. During the period referred to in paragraph 1, the draft measure shall not be adopted by the supervisory authority.</p> <p>4. Where the supervisory authority concerned intends not to follow the opinion of the Commission, it shall inform the Commission and the European Data Protection Board thereof within the period referred to in paragraph 1 and provide a justification. In this case the draft measure shall not be adopted for one further month.</p>	<p>1. Within ten weeks after a matter has been raised under Article 58, or at the latest within six weeks in the case of Article 61, the Commission may adopt, in order to ensure correct and consistent application of this Regulation, an opinion in relation to matters raised pursuant to Articles 58 or 61.</p> <p>2. Where the Commission has adopted an opinion in accordance with paragraph 1, the competent supervisory authority concerned shall take utmost account of the Commission’s opinion and inform the Commission and the European Data Protection Board whether it intends to maintain or amend its draft measure.</p> <p>3. During the period referred to in paragraph 1, the draft measure shall not be adopted by the supervisory authority.</p> <p>4. Where the competent supervisory authority concerned intends not to follow the opinion of the Commission, it shall inform the Commission and the European Data Protection Board thereof within the period referred to in paragraph 1 and provide a justification. In this case the draft measure shall not be adopted for one further month.</p>
---	---

Justification

References to the 'supervisory authority' should be consistent with the regime set out in the 'competence' provisions in Article 51.

<p>Article 60 (EC proposal)</p> <p>1. Within one month after the communication referred to in Article 59(4), and where the Commission has serious doubts as to whether the draft measure would ensure the correct application of this Regulation or would otherwise result in its inconsistent application, the Commission may adopt a reasoned</p>	<p>delete</p>
---	----------------------

FACEBOOK

<p>decision requiring the supervisory authority to suspend the adoption of the draft measure, taking into account the opinion issued by the European Data Protection Board pursuant to Article 58(7) or Article 61(2), where it appears necessary in order to:</p> <ul style="list-style-type: none"> (a) reconcile the diverging positions of the supervisory authority and the European Data Protection Board, if this still appears to be possible; or (b) adopt a measure pursuant to point (a) of Article 62(1). <p>2. The Commission shall specify the duration of the suspension which shall not exceed 12 months.</p> <p>3. During the period referred to in paragraph 2, the supervisory authority may not adopt the draft measure.</p>	
--	--

Justification

The power granted to the European Commission to adopt interpretive opinions and draft measures undermines the principle of independent data protection supervision. Such powers should lie with the data protection supervisory authorities and ultimately the courts, not the Commission. Where an issue arises in relation to an opinion or draft measure issued by the European Data Protection Board (under Article 58) this would be most appropriately dealt with by the European Court of Justice whose primary function is to interpret the law, rather than the Commission.

<p>Article 61 (EC proposal)</p> <p>1. In exceptional circumstances, where a supervisory authority considers that there is an urgent need to act in order to protect the interests of data subjects, in particular when the danger exists that the enforcement of a right of a data subject could be considerably impeded by means of an alteration of the existing state or for averting major disadvantages or for other reasons, by way of derogation from the</p>	<p>Article 61</p> <p>1. In exceptional circumstances, where a the competent supervisory authority considers that there is an urgent need to act in order to protect the interests of data subjects, in particular when the danger exists that the enforcement of a right of a data subject could be considerably impeded by means of an alteration of the existing state or for averting major disadvantages or for other reasons, by way</p>
--	---

<p>procedure referred to in Article 58, it may immediately adopt provisional measures with a specified period of validity. The supervisory authority shall, without delay, communicate those measures, with full reasons, to the European Data Protection Board and to the Commission.</p> <p>2. Where a supervisory authority has taken a measure pursuant to paragraph 1 and considers that final measures need urgently be adopted, it may request an urgent opinion of the European Data Protection Board, giving reasons for requesting such opinion, including for the urgency of final measures.</p> <p>3. Any supervisory authority may request an urgent opinion where the competent supervisory authority has not taken an appropriate measure in a situation where there is an urgent need to act, in order to protect the interests of data subjects, giving reasons for requesting such opinion, including for the urgent need to act.</p> <p>4. By derogation from Article 58(7), an urgent opinion referred to in paragraphs 2 and 3 of this Article shall be adopted within two weeks by simple majority of the members of the European Data Protection Board.</p>	<p>of derogation from the procedure referred to in Article 58, it may immediately adopt provisional measures with a specified period of validity. The competent supervisory authority shall, without delay, communicate those measures, with full reasons, to the European Data Protection Board and to the Commission.</p> <p>2. Where a competent supervisory authority has taken a measure pursuant to paragraph 1 and considers that final measures need urgently be adopted, it may request an urgent opinion of the European Data Protection Board, giving reasons for requesting such opinion, including for the urgency of final measures.</p> <p>3. Any supervisory authority may request an urgent opinion of the European Data Protection Board where the competent supervisory authority has not taken an appropriate measure in a situation where there is an urgent need to act, in order to protect the interests of data subjects, giving reasons for requesting such opinion, including for the urgent need to act.</p> <p>4. By derogation from Article 58(7), an urgent opinion referred to in paragraphs 2 and 3 of this Article shall be adopted within two weeks by simple majority of the members of the European Data Protection Board.</p>
<p><i>Justification</i></p> <p>References to the 'supervisory authority' should be consistent with the regime set out in the 'competence' provisions in Article 51. The specific reference to the European Data Protection Board creates certainty about the relevant body that the Supervisory authority can submit a request for an urgent opinion to.</p>	

<p>Article 63 (EC proposal)</p> <p>1. For the purposes of this Regulation, an enforceable measure of the supervisory</p>	<p>Article 63</p> <p>1. For the purposes of this Regulation, an enforceable measure of the competent</p>
--	---

FACEBOOK

<p>authority of one Member State shall be enforced in all Member States concerned.</p> <p>2. Where a supervisory authority does not submit a draft measure to the consistency mechanism in breach of Article 58(1) to (5), the measure of the supervisory authority shall not be legally valid and enforceable.</p>	<p>supervisory authority of one Member State shall be enforced in all Member States concerned.</p> <p>2. Where a competent supervisory authority does not submit a draft measure to the consistency mechanism in breach of Article 58(1) to (5), the measure of the competent supervisory authority shall not be legally valid and enforceable.</p>
<p><i>Justification</i></p> <p>References to the 'supervisory authority' should be consistent with the regime set out in the 'competence' provisions in Article 51.</p>	

<p>Article 63a new Appealing procedures</p> <p>Without prejudice to the competences of the judiciary system of the Member States and of the Union, the European Data Protection Board can issue binding opinions if:</p> <p>(a) a data subject or data controller appeals on ground of inconsistent application of the present Regulation across the Member States and</p> <p>(b) the Consistency Mechanism described in Article 58 to 63 has failed to ensure that a simple majority of the members of the European Data Protection Board agrees on a measure.</p> <p>Before issuing such opinion, the European Data Protection Board shall take into consideration every information the competent Data Protection Authority knows, including the point of view of the interested parties.</p>	<p><i>delete</i></p>
<p><i>Justification</i></p> <p>The EDPB should not be granted the power to adopt binding opinions. The primary function of interpreting the law should lie with the data protection supervisory authorities and ultimately the European Court of Justice whose primary function is to</p>	

interpret the law.

Article 66(1)(d) issue opinions on draft decisions of supervisory authorities pursuant to the consistency mechanism referred to in Article 57 and in Article 63a ;	Article 66(1)(d) issue opinions on draft decisions of supervisory authorities pursuant to the consistency mechanism referred to in Article 57 and in Article 63a ;
--	--

<i>Justification</i>	
This amendment relates to the proposed new Article 63(a) above.	

Article 73(2) Any body, organisation or association which aims to protect citizens' rights and interests shall have the right to lodge a complaint with a supervisory authority in any Member State on behalf of one or more data subjects if it considers that a data subject's rights under this Regulation have been infringed as a result of the processing of personal data.	Article 73(2) Any body, organisation or association which aims to protect data subjects' citizens' rights and interests concerning the protection of their personal data and has been properly constituted according to the law of a Member State shall have the right to lodge a complaint with a supervisory authority in any Member State on behalf of one or more data subjects if it considers that a data subject's rights under this Regulation have been infringed as a result of the processing of personal data.
---	--

<i>Justification</i>	
The reference to 'citizen' rights' is inconsistent with the draft Regulation which refers to 'data subjects' throughout. Further, it creates a suggestion that consumer organisations or claim foundations could bundle claims of consumers and class action could be used by some as a mechanism to litigate against corporate groups. The potential scale of such collective actions, time, cost and outcome - on top of penalties - might have severe financial implications for companies. The effect of this judicial remedy would be disproportionate to the aims of deterrence and effective enforcement of the data protection provisions in the proposed Regulation.	

2. Consent

Individuals should be able to exercise control over what personal data organisations collect from them and how they use it, but the highly prescriptive nature of the requirements for consent contained in Articles 4(8) and 7(2) could potentially require more intrusive mechanisms to ask for consent for specific activities. This carries the risk

FACEBOOK

of inundating users with tick boxes and warnings and may result in an overly disrupted or disjointed internet experience. This will inevitably lead to a potential 'devaluation' of the principle, and may make it harder for users to make judgments about when it is appropriate to give consent or withhold it. It may also prevent organisations from being innovative about the way they interact with individuals.

Unambiguous consent should be a valid means of legitimizing data processing. Everyday practice shows that in many instances individuals' consent may be obvious from the context in which they are using the service, provided that any such implied consent meets the standards of being a "freely given, specific and informed" indication of the individual's wishes. This is recognized by the Opinion of the Article 29 Working Party on the definition of consent which states that "unambiguous consent may be inferred from certain actions (...) when the actions lead to an unmistakable conclusion that consent is given".

It is important to keep in mind that there are many services, such as social networks, which are expressly designed for people to be able to connect and share information.

A great amount of privacy best practice has been developed, especially in the online environment, to provide users with transparency and control. We are seeing great innovation (including granular and sophisticated control tools) from many players in the market to empower users to understand how their information is used and how services work when they choose to share information online. Equally many internet players are incorporating 'privacy by design' into their privacy programmes. These practices must not be hampered by over-prescriptive and often meaningless consent requirements.

Drafting recommendations:

Recital 25, Article 4(8) (Definition of Consent): The reference "explicit" in the definition of consent is counterproductive and unrealistic in the majority of processing situations. We therefore propose that the reference that consent must be given "explicitly" and "silence and inactivity should not constitute consent" should be deleted from Recital 25. We have suggested language that makes clear that "other conduct that leads to an unmistakable conclusion that consent is given" is valid consent. We also recommend that there should be some flexibility in the way that this is provided i.e. "either by a statement or by a clear affirmative action or by any other method" (see Recital 25 and the definition of Consent contained in Article 4(8)).

The controller is in the best position to decide the appropriate level of information to provide individuals about specific processing activities. Therefore, we propose adding wording to Article 4(8) to state that the information to be provided for the purposes of obtaining the data subject's consent may be determined by the data controller in accordance with the controller's obligations as regards the general data processing principles (as contained in Article 5).

Article 7 (Conditions for Consent): We propose that:

FACEBOOK

- The controller should only bear the 'burden of proof' in cases where the need for consent is in connection with the processing of sensitive personal data. This position is reflected in the proposed changes to Article 7(1).
- The Regulation shall provide common and practical examples of how processing activities can be communicated to individuals for the purposes of obtaining consent for a range of activities in a single step. This position is reflected in the proposed changes to Recital 32 and Article 7(2).
- Controllers should not be obliged to continue to offer services where individuals decline to provide their personal data. We have therefore suggested that the controller shall be entitled to suspend or terminate services where such provision of services relies on consent to the processing which has been withdrawn by the individual (see Article 7(3)).
- Controllers should be able to make consent to the processing a condition of access to a service which may not be otherwise free. This position is reflected in our amendments to Recital 34 and Article 7(4).

Drafting suggestions:

<p>Recital 25 (EC proposal)</p> <p>Consent should be given explicitly by any appropriate method enabling a freely given specific and informed indication of the data subject's wishes, either by a statement or by a clear affirmative action by the data subject, ensuring that individuals are aware that they give their consent to the processing of personal data, including by ticking a box when visiting an Internet website or by any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data. Silence or inactivity should therefore not constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. If the data subject's consent is to be given following an electronic request, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is</p>	<p>Recital 25</p> <p>Consent should be given explicitly by any appropriate method enabling a freely given specific and informed indication of the data subject's wishes, either by a statement or by a clear affirmative action by the data subject, by taking some other conduct that leads to an unmistakable conclusion that consent is given, ensuring that individuals are aware that they give their consent to the processing of personal data including by ticking a box. Consent may be given by taking an action when visiting an Internet website or by any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data. Silence or inactivity should therefore not constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. If the data subject's consent is to be given following an electronic request, the request</p>
--	--

FACEBOOK

<p>provided.</p>	<p>must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.</p>
<p style="text-align: center;"><i>Justification</i></p> <p>Unambiguous consent shall be a valid means of legitimizing data processing. Everyday practice shows that in many instances individuals' consent may be obvious from the context in which they are using the service, provided that any such implied consent meets the standards of being a "freely given, specific and informed" indication of the individual's wishes. This is recognized by the Opinion of the Article 29 Working Party on the definition of consent which states that "unambiguous consent may be inferred from certain actions (...) when the actions lead to an unmistakable conclusion that consent is given".</p> <p>Individuals should be able to exercise control over what personal data organisations collect from them and how they use it, but the proposed requirement for consent may lead to an overly disrupted or disjointed internet experience and may also prevent organisations from being innovative about the way they interact with individuals.</p> <p>The highly prescriptive nature of the requirements for consent could potentially require more intrusive mechanisms to ask for consent for specific activities. This carries the risk of inundating users with tick boxes and warnings. As well as affecting the user experience, this inevitably will lead to a potential 'devaluation' of the principle, and may make it harder for users to make judgments about when it is appropriate to give consent or withhold it.</p> <p>Furthermore, controllers should be allowed some technical flexibility as to the way that data subjects' consent is obtained.</p>	

<p>Recital 32 (EC proposal)</p> <p>Where processing is based on the data subject's consent, the controller should have the burden of proving that the data subject has given the consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware that and to what extent consent is given.</p>	<p>Recital 32</p> <p>Where processing is based on the data subject's consent, the controller should have the burden of proving that the data subject has given the consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware that and to what extent consent is given, <i>including by identifying and explaining the relevant data processing activities in a data protection statement or privacy policy</i></p>
--	---

FACEBOOK

	<i>made available to the data subject at the time of obtaining his or her consent.</i>
<p style="text-align: center;"><i>Justification</i></p> <p>The draft Regulation should provide common and practical examples of how processing activities can be communicated to individuals for the purposes of obtaining consent for a range of activities in a single step. It should also allow controllers to define the most appropriate channel and level of information to be provided to data subjects for each processing activity. The information to be provided for the purposes of obtaining the data subject's consent shall be determined by the data controller in accordance with the controller's obligations as regards the general data processing principles (considered below in the justification for the proposed changes to Article 4(8)).</p>	

<p>Recital 34 (EC proposal)</p> <p>Consent should not provide a valid legal ground for the processing of personal data, where there is a clear imbalance between the data subject and the controller. This is especially the case where the data subject is in a situation of dependence from the controller, among others, where personal data are processed by the employer of employees' personal data in the employment context. Where the controller is a public authority, there would be an imbalance only in the specific data processing operations where the public authority can impose an obligation by virtue of its relevant public powers and the consent cannot be deemed as freely given, taking into account the interest of the data subject.</p>	<p>Recital 34</p> <p>Consent should not provide a valid legal ground for the processing of personal data, where there is a clear imbalance between the data subject and the controller. This is especially the case where the data subject is in a situation of dependence from the controller, among others, where personal data are processed by the employer of employees' personal data in the employment context. <i>However, a data controller may legitimately make consent to the processing a condition of access to a service, particularly when the service is free of charge to the data subject.</i> Where the controller is a public authority, there would be an imbalance only in the specific data processing operations where the public authority can impose an obligation by virtue of its relevant public powers and the consent cannot be deemed as freely given, taking into account the interest of the data subject.</p>
<p style="text-align: center;"><i>Justification</i></p> <p>Controllers should be able to make consent to the processing a condition of access to a</p>	

service which may not be otherwise free. See also the proposed changes to Article 7(4).

<p>Article 4(8) (EC proposal)</p> <p>'the data subject's consent' means any freely given specific, informed and explicit indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed;</p>	<p>Article 4(8)</p> <p>'the data subject's consent' means any freely given specific, informed and explicit unambiguous indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action or by any other method, signifies agreement to personal data relating to them being processed. The information to be provided for the purposes of obtaining the data subject's consent may be determined by the data controller in accordance with Article 5;</p>
<p style="text-align: center;"><i>Justification</i></p> <p>Unambiguous consent should be a valid means of legitimizing data processing. Everyday practice shows that in many instances individuals' consent may be obvious from the context in which they are using the service, provided that any such implied consent meets the standards of being a "freely given, specific and informed" indication of the individual's wishes. This is recognized by the Opinion of the Article 29 Working Party on the definition of consent which states that "unambiguous consent may be inferred from certain actions (...) when the actions lead to an unmistakable conclusion that consent is given".</p> <p>The highly prescriptive nature of the requirements for consent could potentially require more intrusive mechanisms to ask for consent for specific activities. This carries the risk of inundating users with tick boxes and warnings. As well as affecting the user experience, this inevitably will lead to a potential 'devaluation' of the principle, and may make it harder for users to make judgments about when it is appropriate to give consent or withhold it. The controller is in the best position to decide the appropriate level of information to provide individuals about specific processing activities. The information to be provided for the purposes of obtaining the data subject's consent may be determined by the data controller in accordance with the controller's obligations as regards the general data processing principles under Article 5.</p>	

<p>Article 7 (EC proposal)</p> <p>1. The controller shall bear the burden of</p>	<p>Article 7</p> <p>1. For the purposes of Article 9(2)(a), the</p>
--	--

<p>proof for the data subject's consent to the processing of their personal data for specified purposes.</p> <p>2. If the data subject's consent is to be given in the context of a written declaration which also concerns another matter, the requirement to give consent must be presented distinguishable in its appearance from this other matter.</p> <p>3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.</p> <p>4. Consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller.</p>	<p>controller shall bear the burden of proof for the data subject's consent to the processing of their personal data for specified purposes.</p> <p>2. If the data subject's consent is to be given in the context of a written declaration which also concerns another matter, the requirement to give consent must be presented distinguishable in its appearance from this other matter. <i>The data subject's consent may be exercised by a single step provided that all relevant matters to which the consent relates are made clearly available.</i></p> <p>3. The data subject shall have the right to withdraw his or her consent at any time <i>and the data controller shall be entitled to suspend or terminate the provision of services to the data subject where such provision relies on the consent to the processing withdrawn by the data subject.</i> The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.</p> <p>4. Consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller, <i>except where consent to the processing may legitimately constitute a condition of access to a service by the data subject.</i></p>
<p><i>Justification</i></p> <p>The controller should only bear the 'burden of proof' in cases where the need for consent is in connection with the processing of sensitive personal data.</p> <p>Controllers should be entitled to obtain consent for a range of data processing activity in a single step as long as they provide them the appropriate level of information for each processing activity.</p> <p>Controllers should not be obliged to continue to offer services where individuals decline to provide their personal data. The controller shall be entitled to suspend or terminate</p>	

services where such provision of services relies on consent to the processing which has been withdrawn by the individual.

Controllers should also be able to make consent to the processing a condition of access to a service which may not be otherwise free.

3. Right to be forgotten

The right to erasure is a key data protection principle which already exists under the current data protection directive and should naturally be reaffirmed in the draft Regulation. However, the right to be forgotten needs very careful consideration. As drafted, apart from not harmonising national laws, it raises major concerns with regard to the right of others to remember and of freedom of expression. There is also a risk that it could result in measures which are technically impossible to apply in practice and therefore make for bad law. A right balance should be found between data subject's right to get their data deleted, the fundamental rights of other individuals and the reality of the online environment. The proposal prescribes a right for people to have their data deleted and also requires data controllers to take all reasonable steps to obtain erasure of content copied to a third party website or application.

It is important to differentiate between three challenges presented by the 'right to be forgotten':

The *first* is in relation to people who have posted personal information about themselves online and later wish to delete that information.

The *second* is in relation to the practical difficulty to identify the necessary information to ensure compliance with the right to be forgotten. This challenge arises in two specific situations:

- The first situation concerns the deletion of personal data of an individual made available online by another individual. In practice, the operator of a website or hosting platform is unlikely to know in many cases which information available on the platform constitutes the personal data that should be deleted. It is virtually impossible to control what information millions of users may make available about other individuals – many of whom will not be users themselves – and to determine where all of the information is and whether that information is the personal data of the person making the request. Therefore a broad obligation to delete any information made available by users upon request of other individuals would be likely to present major implementation challenges to the extent that it would be practically unworkable.
- The second situation concerns the specific provision under Article 17(2), which requires informing third parties of the request for deletion of links to or copies of

FACEBOOK

an individual's personal data. This would involve identifying any such links or copies of the information elsewhere on the Internet and communicating with those responsible for placing the links or copying the information to request such links or information to be deleted. Again, we do not see any practicable means for services like social networking to control which links to or copies of someone's personal data exist in other places on the Internet, let alone communicate with the third parties responsible for their dissemination.

In order to meet such obligations, service providers would in practice be obliged to 'monitor' peoples' activities across the Internet. There is concern in the Internet community that it could also lead to the interpretation that intermediary services could be considered responsible for erasing any content related to the data subject that requests it. The erasure of data hosted by other services is not within the technical power of the intermediary and directly conflicts with the way the Internet works and how the current liability status of intermediaries is designed.

The *third* is in relation to any personal data made publicly available and the fact that there may be strong grounds to justify under certain circumstances the right of others to know certain facts concerning individuals, as this is closely linked to the right to freedom of expression and other democratic values. It is clear that there is a potential conflict between the right for people to express themselves and the privacy rights of others. It is important to consider fully the implications on the open Internet and personal expression as we determine the right balance. The scope of freedom of expression contained in Article 80 and further clarified in Recital 121 is defined quite narrowly and should be extended to cover for example mere expressions of opinion, user generated content and more generally recognise the nature of new forms of communication such as blogging and social networking.

Finally, the debate on the "right to be forgotten" affects a number of Internet services, which rely on user-generated content. This issue is not unique to social networking. Policy makers should take into account the "right of others to remember" and reach a balanced conclusion which respects freedom of expression.

Drafting recommendations:

Recital 53 / Article 17 (Right to be forgotten and to erasure): The right to erasure in Article 17(1) is welcome, but the wording should be amended to ensure that it balances the competing interests set out above. As such, we propose that:

- Where a third party makes information about another individual available online, it is not always possible for a controller to identify all of the related personal data. Therefore we have suggested that the right of an individual to require erasure when it is 'impossible or involves a disproportionate effort' (Article 17(1)(e)).

FACEBOOK

- The right of erasure may be overridden by the interests or fundamental rights and freedoms of others (Article 17(1)(f) and Recital 53).
- The right to be forgotten, as drafted, raises major concerns with regard both to the right of others to remember and to freedom of expression. Moreover, it is technically impossible or involves a disproportionate effort for a data controller in the context of the online environment, to identify the data that have been copied or replicated on other platforms. We therefore resist the wording contained in Article 17(2) and Recital 54.
- An exemption should apply when a controller wishes to process the information for a certain legitimate purpose (such as the provision of system, network or information security). This position should be limited to circumstances where the interests of the controller are not outweighed by those of the individual and we have therefore proposed changes to Recital 53 in this regard.

Drafting suggestions:

<p>Recital 53</p> <p>Any person should have the right to have personal data concerning them rectified and the right to <i>have such personal data erased</i> where the retention of such data is not in compliance with this Regulation. In particular, data subjects should have the right that their personal data are erased and no longer processed, where the data are no longer necessary in relation to the purposes for which the data are collected or otherwise processed, where data subjects have withdrawn their consent for processing or where they object to the processing of personal data concerning them or where the processing of their personal data otherwise does not comply with this Regulation. This right is particularly relevant, when the data subject has given their consent as a child, when not being fully aware of the risks involved by the processing, and later wants to remove such personal data especially on the Internet. However, the further retention of the data should be</p>	<p>Recital 53</p> <p>Any person should have the right to have personal data concerning them rectified the right to have such personal data erased where the retention of such data is not in compliance with this Regulation. In particular, data subjects should have the right that their personal data are erased and no longer processed, where the data are no longer necessary in relation to the purposes for which the data are collected or otherwise processed, where data subjects have withdrawn their consent for processing or where they object to the processing of personal data concerning them or where the processing of their personal data otherwise does not comply with this Regulation. <i>This right is particularly relevant, when the data subject has given their consent as a child, when not being fully aware of the risks involved by the processing, and later wants to remove such personal data especially on the Internet.</i> However, certain exemptions should apply, particularly when</p>
---	--

FACEBOOK

<p>allowed where it is necessary for historical, statistical and scientific research purposes, for reasons of public interest in the area of public health, for exercising the right of freedom of expression, when required by law or where there is a reason to restrict the processing of the data instead of erasing them.</p>	<p><i>identifying all relevant personal data in question proves impossible or involves a disproportionate effort and when in relation to personal data made publicly available by the data subject himself or herself, such right is overridden by the interests or fundamental rights and freedoms of others. An exemption should also apply to enable the data controller to process data for their legitimate interest, as for instance for the purpose of providing system, network or information security.</i> and The further retention of the data should be allowed where it is necessary for historical, statistical and scientific research purposes, for reasons of public interest in the area of public health, for exercising the right of freedom of expression, when required by law or where there is a reason to restrict the processing of the data instead of erasing them.</p>
<p><i>Justification</i></p> <p>The right to erasure is a key data protection principle which already exists under the current data protection directive and should naturally be reaffirmed in the draft Regulation. However, certain exemptions should apply to recognise that:</p> <ul style="list-style-type: none"> • Where a third party makes information about another individual available online, it is not always possible for a controller to identify all of the related personal data; • Where an individual makes information their information publicly available, there is a potential conflict between the right of others to know and the right of others to remember (including where the data subject has given their consent as a child); • The right to know is closely linked to the right to freedom of expression and other democratic values; and • An exemption to the right to be forgotten should apply when a controller wishes to process the information for a certain legitimate purpose such as for the purpose of providing system, network or information security. 	
<p>Recital 54 To strengthen the right to <i>erasure</i> in the online environment, <i>such</i> right should also be extended in such a way that a</p>	<p><i>delete</i></p>

FACEBOOK

<p>controller who has transferred the personal data or made them public without being instructed to do so by the data subject should be obliged to inform third parties which are processing such data that a data subject requests them to erase any links to, or copies or replications of that personal data. To ensure this information, the controller should take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible. In relation to a third party publication of personal data, the controller should be considered responsible for the publication, where the controller has authorised the publication by the third party.</p>	
--	--

Justification

It is technically impossible or involves a disproportionate effort for a data controller in the context of the online environment, to identify the data that have been copied or replicated on other platforms. Furthermore, these provisions might generate negative unintended consequences in the online environment whereby, in order to meet such obligations, service providers would in practice be obliged to ‘monitor’ peoples’ activities across the internet. It could also lead to the interpretation that intermediary services could be considered responsible for erasing any content related to the data subject that requests it. The erasure of data hosted by other services is not within the technical power of the intermediary and directly conflicts with the way the Internet works and how the current liability status of intermediaries is designed.

<p>Article 6 (EC proposal)</p> <p>1. Processing of personal data shall be lawful only if and to the extent that at least one of the following applies:</p> <p>(a) the data subject has given consent to the processing of their personal data for one or more specific purposes;</p> <p>(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take</p>	<p>Article 6</p> <p>1. Processing of personal data shall be lawful only if and to the extent that at least one of the following applies:</p> <p>(a) the data subject has given consent to the processing of their personal data for one or more specific purposes;</p> <p>(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take</p>
--	--

<p>steps at the request of the data subject prior to entering into a contract;</p> <p>(c) processing is necessary for compliance with a legal obligation to which the controller is subject;</p> <p>(d) processing is necessary in order to protect the vital interests of the data subject;</p> <p>(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;</p> <p>(f) processing is necessary for the purposes of the legitimate interests pursued by a controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks.</p> <p>2. Processing of personal data which is necessary for the purposes of historical, statistical or scientific research shall be lawful subject to the conditions and safeguards referred to in Article 83.</p> <p>3. The basis of the processing referred to in points (c) and (e) of paragraph 1 must be provided for in:</p> <p>(a) Union law, or</p> <p>(b) the law of the Member State to which the controller is subject.</p> <p>The law of the Member State must meet an objective of public interest or must be necessary to protect the rights and freedoms of others, respect the essence of</p>	<p>steps at the request of the data subject prior to entering into a contract;</p> <p>(c) processing is necessary for compliance with a legal obligation to which the controller is subject;</p> <p>(d) processing is necessary in order to protect the vital interests of the data subject;</p> <p>(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;</p> <p>(f) processing is necessary for the purposes of the legitimate interests pursued by a controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks. <i>The processing of data to the extent necessary for the purpose of providing system, network or information security constitutes a legitimate interest of the data controller.</i></p> <p>2. Processing of personal data which is necessary for the purposes of historical, statistical or scientific research shall be lawful subject to the conditions and safeguards referred to in Article 83.</p> <p>3. The basis of the processing referred to in points (c) and (e) of paragraph 1 must be provided for in:</p> <p>(a) Union law, or</p> <p>(b) <i>a legally binding obligation to</i></p>
--	---

<p>the right to the protection of personal data and be proportionate to the legitimate aim pursued.</p> <p>4. Where the purpose of further processing is not compatible with the one for which the personal data have been collected, the processing must have a legal basis at least in one of the grounds referred to in points (a) to (e) of paragraph 1. This shall in particular apply to any change of terms and general conditions of a contract.</p> <p>5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the conditions referred to in point (f) of paragraph 1 for various sectors and data processing situations, including as regards the processing of personal data related to a child.</p>	<p>which a controller is subject.</p> <p>The legally binding obligation must meet an objective of public interest or must be necessary to protect the rights and freedoms of others, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued.</p> <p>4. Where the purpose of further processing is not compatible with the one for which the personal data have been collected, the processing must have a legal basis at least in one of the grounds referred to in points (a) to (e) of paragraph 1. This shall in particular apply to any change of terms and general conditions of a contract.</p>
<p><i>Justification</i></p> <p>An exemption to the right to be forgotten should apply when a controller wishes to process the information for a certain legitimate purpose such as for the purpose of providing system, network or information security.</p>	

<p>Article 13(1) Any rectification or erasure carried out in accordance with Articles 16 and 17 is extended to each recipient to whom the data have been disclosed without the control of the data subject.</p>	<p>Article 13(1) Any rectification or erasure carried out in accordance with Articles 16 and 17 is extended to each recipient to whom the data have been disclosed without the control of the data subject, unless this proves impossible or involves a disproportionate effort.</p>
<p><i>Justification</i></p> <p>Retain the European Commission’s proposal to the extent that this obligation should not apply where compliance would be impossible or involve a disproportionate effort in addition to the language proposed by the rapporteur.</p>	

<p>Article 17 – Right to erasure</p> <p>1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child, where one of the following grounds applies:</p> <p>(a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;</p> <p>(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data;</p> <p>(c) the data subject objects to the processing of personal data pursuant to Article 19;</p> <p>(d) the processing of the data does not comply with this Regulation for other reasons.</p> <p>2. Where the controller referred to in paragraph 1 has transferred the personal data, or has made such data public without being clearly instructed by the data subject to do so, it shall take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible, to inform third parties which are processing such data, that a data</p>	<p>Article 17 – Right to erasure</p> <p>1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child, where one of the following grounds applies:</p> <p>(a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;</p> <p>(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data;</p> <p>(c) the data subject objects to the processing of personal data pursuant to Article 19;</p> <p>(d) the processing of the data does not comply with this Regulation for other reasons.</p> <p>except where:</p> <p>(e) identifying all relevant personal data in question proves impossible or involves a disproportionate effort;</p> <p>(f) such right is overridden by the interests or fundamental rights and freedoms of others.</p> <p>2. Where the controller referred to in paragraph 1 has transferred the personal data, or has made such data public without being clearly instructed by the data subject to do so, it shall take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible, to inform third parties which are processing such data, that a data subject requests them to erase any links to,</p>
--	--

<p>subject requests them to erase any links to, or copy or replication of that personal data. Where the controller has authorised a third party publication of personal data, the controller shall be considered responsible for that publication.</p> <p>3. The controller shall carry out the erasure without delay, except to the extent that the retention of the personal data is necessary:</p> <p>(a) for exercising the right of freedom of expression in accordance with Article 80;</p> <p>(b) for reasons of public interest in the area of public health in accordance with Article 81;</p> <p>(c) for historical, statistical and scientific research purposes in accordance with Article 83;</p> <p>(d) for compliance with a legal obligation to retain the personal data by Union or Member State law to which the controller is subject; Member State laws shall meet an objective of public interest, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued;</p> <p>(e) in the cases referred to in paragraph 4.</p> <p>4. Instead of erasure, the controller shall restrict processing of personal data where:</p> <p>(a) their accuracy is contested by the data subject, for a period enabling the controller to verify the accuracy of the data;</p> <p>(b) the controller no longer needs the personal data for the accomplishment of its task but they have to be maintained for purposes of proof;</p> <p>(c) the processing is unlawful and the data subject opposes their erasure and requests the restriction of their use instead;</p> <p>(d) the data subject requests to transmit</p>	<p>or copy or replication of that personal data. Where the controller has authorised a third party publication of personal data, the controller shall be considered responsible for that publication.</p> <p>3. The controller shall carry out the erasure without delay, except to the extent that the retention of the personal data is necessary:</p> <p>(a) for exercising the right of freedom of expression in accordance with Article 80;</p> <p>(b) for reasons of public interest in the area of public health in accordance with Article 81;</p> <p>(c) for historical, statistical and scientific research purposes in accordance with Article 83;</p> <p>(d) for compliance with a legal obligation to retain the personal data by Union or Member State law to which the controller is subject; Member State laws shall meet an objective of public interest, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued;</p> <p>(e) in the cases referred to in paragraph 4.</p> <p>4. Instead of erasure, the controller shall restrict processing of personal data where:</p> <p>(a) their accuracy is contested by the data subject, for a period enabling the controller to verify the accuracy of the data;</p> <p>(b) the controller no longer needs the personal data for the accomplishment of its task but they have to be maintained for purposes of proof;</p> <p>(c) the processing is unlawful and the data subject opposes their erasure and requests the restriction of their use instead;</p> <p>(d) the data subject requests to transmit the personal data into another automated</p>
---	--

FACEBOOK

<p>the personal data into another automated processing system in accordance with Article 18(2).</p> <p>5. Personal data referred to in paragraph 4 may, with the exception of storage, only be processed for purposes of proof, or with the data subject's consent, or for the protection of the rights of another natural or legal person or for an objective of public interest.</p> <p>6. Where processing of personal data is restricted pursuant to paragraph 4, the controller shall inform the data subject before lifting the restriction on processing.</p> <p>7. The controller shall implement mechanisms to ensure that the time limits established for the erasure of personal data and/or for a periodic review of the need for the storage of the data are observed.</p> <p>8. Where the erasure is carried out, the controller shall not otherwise process such personal data.</p> <p>9. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying:</p> <p>(a) the criteria and requirements for the application of paragraph 1 for specific sectors and in specific data processing situations;</p> <p>(b) the conditions for deleting links, copies or replications of personal data from publicly available communication services as referred to in paragraph 2;</p> <p>(c) the criteria and conditions for restricting the processing of personal data referred to in paragraph 4.</p>	<p>processing system in accordance with Article 18(2).</p> <p>5. Personal data referred to in paragraph 4 may, with the exception of storage, only be processed for purposes of proof, or with the data subject's consent, or for the protection of the rights of another natural or legal person or for an objective of public interest.</p> <p>6. Where processing of personal data is restricted pursuant to paragraph 4, the controller shall inform the data subject before lifting the restriction on processing.</p> <p>7. The controller shall implement mechanisms to ensure that the time limits established for the erasure of personal data and/or for a periodic review of the need for the storage of the data are observed.</p> <p>8. Where the erasure is carried out, the controller shall not otherwise process such personal data.</p> <p>9. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying:</p> <p>(a) the criteria and requirements for the application of paragraph 1 for specific sectors and in specific data processing situations;</p> <p>(b) the conditions for deleting links, copies or replications of personal data from publicly available communication services as referred to in paragraph 2;</p> <p>(c) the criteria and conditions for restricting the processing of personal data referred to in paragraph 4.</p>
<p style="text-align: center;"><i>Justification</i></p> <p>The right to erasure is a key data protection principle which already exists under the current data protection directive and should naturally be reaffirmed in the draft</p>	

Regulation. The right to erasure in Article 17(1) should be reviewed to recognize that the right balance is struck between the rights of a data subject to get their data deleted, the rights of individuals to remember and the right to freedom of expression. The practical difficulties associated with identifying the necessary information to ensure compliance with this provision must also be taken into account. Certain exemptions should apply to recognise that:

- It is not always possible for a controller to identify all of the related personal data (for instance, where a third party makes information about another individual available online);
- The right of erasure may be overridden by the interests or fundamental rights and freedoms of others;
- An exemption should apply when a controller wishes to process the information for a certain legitimate purpose such as for the purpose of providing system, network or information security

Moreover, the right to be forgotten in Article 17(2) needs very careful consideration. It is technically impossible or involves a disproportionate effort for a data controller in the context of the online environment, to identify the data that have been copied or replicated on other platforms.

Furthermore, this provision might generate negative unintended consequences in the online environment whereby, in order to meet such obligations, service providers would in practice be obliged to 'monitor' peoples' activities across the internet. It could also lead to the interpretation that intermediary services could be considered responsible for erasing any content related to the data subject that requests it. The erasure of data hosted by other services is not within the technical power of the intermediary and directly conflicts with the way the Internet works and how the current liability status of intermediaries is designed.

For the reasons above and because the right to erasure is sufficient to give data subjects control over their personal data, Article 17(2) should be deleted.

4. Profiling

The specific provisions on "profiling" contained in the draft Regulation are unnecessary, over-broad, and legally vague. Profiling techniques are used in a variety of sectors ranging from banking to health and retail and for various purposes that include the fight against fraud, service improvement or marketing. Therefore a 'one size fits all' approach to profiling is not adequate and is likely to produce unintended consequences to the detriment of consumers, business and the society as a whole.

FACEBOOK

Article 20 extends the scope of the 95/46/EC Directive provisions relating to automated individual decisions to cover a range of new factors including location, personal preferences and behaviour. It also introduces a new and undefined test of “significant effect”. Failure to adequately distinguish between processing with legal or significant effect and content customization could indiscriminately subject a potentially enormous range of activity (and yet-to-be-invented applications) across every industry sector to the stricter consent provisions of Article 7 and the provisions relating to prior authorization as defined in Article 33 and 34. As well as being burdensome on data protection authorities, this fails to strike an appropriate balance between protecting the rights of individuals and safeguarding innovation and commerce. Customization is an essential element in a competitive online marketplace, and such broadly-framed provisions are likely to have unintended consequences and affect many legitimate practices in the process negatively.

Measures on profiling do not distinguish between the technology and its use. The current drafting of the Regulation shows that there is no recognition of positive uses of profiling and no differentiation is made between the technology and its uses. Article 20 clearly violates the principle of technology neutrality which is alluded to in Recital 13, and which is critically important in crafting future-proof regulation. Given the numerous other safeguards in this draft Regulation, profiling techniques do not need be treated differently to any other type of personal data processing.

The legitimate interests of the data controller should provide a legal basis for “profiling”. The legitimate interests pursued by a controller should be an additional legal ground for lawful profiling, along with consent, in order to ensure that profiling techniques and technologies that do not aim at identifying data subjects but at extracting aggregate baseline data that can be used to manage, improve or customize services for similar customers are not prohibited under the draft Regulation. It is important that this be the case here as with other sections of the draft Regulation, to ensure that the use of profiling techniques for legitimate purposes such as security, anti-fraud, accounting are not prohibited.

Drafting recommendations:

Recital 51 / Recital 58 / Recital 59 / Article 20 (Measures based on Profiling): Prohibiting or severely restricting profiling is not adequate for a technique that is enabled by various technologies, is used across sectors for various purposes and, whilst potentially presenting risks in certain cases, also has benefits for consumers, business and the economy.

Recital 13 recognises that, in order to avoid a serious risk of circumvention, “the protection of individuals should be technologically neutral and not depend on the techniques used”. Article 20 clearly violates this principle of technology neutrality, which should be core to any laws that deal with technology if they are to withstand the test of time and technology evolution.

FACEBOOK

Given the likely evolution of technology as a tool to help make decisions, it is no longer justifiable to treat profiling techniques differently from other types of processing, particularly taking into account all other safeguards introduced by the draft Regulation.

Therefore, it is proposed that Recital 51, Recital 58 and Article 20 be entirely deleted, as well as a reference in Recital 59.

Drafting suggestions:

<p>Recital 51 (EC proposal)</p> <p>Any person should have the right of access to data which has been collected concerning them, and to exercise this right easily, in order to be aware and verify the lawfulness of the processing. Every data subject should therefore have the right to know and obtain communication in particular for what purposes the data are processed, for what period, which recipients receive the data, what is the logic of the data that are undergoing the processing and what might be, at least when based on profiling, the consequences of such processing. This right should not adversely affect the rights and freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of these considerations should not be that all information is refused to the data subject.</p>	<p><i>delete</i></p>
<p style="text-align: center;"><i>Justification</i></p> <p>Profiling techniques are used in a variety of sectors ranging from banking to health and retail and for various purposes that include the fight against fraud, service improvement or marketing. Therefore a 'one size fits all' approach to profiling is not adequate and is likely to produce unintended consequences to the detriment of consumers, business and the society as a whole.</p> <p>Given the likely evolution of technology as a tool to help make decisions, it is no longer justifiable to treat profiling techniques differently from other types of processing, particularly taking into account all other safeguards introduced by the draft Regulation.</p>	

FACEBOOK

<p>Recital 58</p> <p>Every natural person should have the right not to be subject to a measure which is based on profiling by means of automated processing. However, such measure should be forbidden only when expressly stated by law, not carried out in the course of entering or performance of a contract, or when the data subject has withdrawn his consent. In any case, such processing should be subject to suitable safeguards, including specific information of the data subject and the right to obtain human intervention and that such measure should not concern a child. The data subject, when this profiling is not necessary for entering or performing a contract, should always have the possibility to opt-out.</p>	<p>delete</p>
<p style="text-align: center;"><i>Justification</i></p> <p>Profiling techniques are used in a variety of sectors ranging from banking to health and retail and for various purposes that include the fight against fraud, service improvement or marketing. Therefore a 'one size fits all' approach to profiling is not adequate and is likely to produce unintended consequences to the detriment of consumers, business and the society as a whole.</p> <p>Given the likely evolution of technology as a tool to help make decisions, it is no longer justifiable to treat profiling techniques differently from other types of processing, particularly taking into account all other safeguards introduced by the draft Regulation.</p>	

<p>Recital 59 (EC proposal)</p> <p>Restrictions on specific principles and on the rights of information, access, rectification and erasure or on the right to data portability, the right to object, measures based on profiling, as well as on the communication of a personal data breach to a data subject and on certain related obligations of the controllers may be imposed by Union or Member State law, as far as necessary and proportionate in a democratic society to safeguard public security, including the protection of</p>	<p>Recital 59</p> <p>Restrictions on specific principles and on the rights of information, access, rectification and erasure or on the right to data portability, the right to object, measures based on profiling, as well as on the communication of a personal data breach to a data subject and on certain related obligations of the controllers may be imposed by Union or Member State law, as far as necessary and proportionate in a democratic society to safeguard public security, including the protection of</p>
--	---

FACEBOOK

<p>human life especially in response to natural or man made disasters, the prevention, investigation and prosecution of criminal offences or of breaches of ethics for regulated professions, other public interests of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, or the protection of the data subject or the rights and freedoms of others. Those restrictions should be in compliance with requirements set out by the Charter of Fundamental Rights of the European Union and by the European Convention for the Protection of Human Rights and Fundamental Freedoms.</p>	<p>human life especially in response to natural or man made disasters, the prevention, investigation and prosecution of criminal offences or of breaches of ethics for regulated professions, other public interests of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, or the protection of the data subject or the rights and freedoms of others. Those restrictions should be in compliance with requirements set out by the Charter of Fundamental Rights of the European Union and by the European Convention for the Protection of Human Rights and Fundamental Freedoms.</p>
<p style="text-align: center;"><i>Justification</i></p> <p>Profiling techniques are used in a variety of sectors ranging from banking to health and retail and for various purposes that include the fight against fraud, service improvement or marketing. Therefore a 'one size fits all' approach to profiling is not adequate and is likely to produce unintended consequences to the detriment of consumers, business and the society as a whole.</p> <p>Given the likely evolution of technology as a tool to help make decisions, it is no longer justifiable to treat profiling techniques differently from other types of processing, particularly taking into account all other safeguards introduced by the draft Regulation.</p>	

<p>Article 20</p> <p>1. Every natural person shall have the right not to be subject to a measure which produces legal effects concerning this natural person or significantly affects this natural person, and which is based solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour.</p>	<p><i>delete</i></p>
--	-----------------------------

<p>2. Subject to the other provisions of this Regulation, a <i>measure which produces legal effects on a person or significantly affects this person, based solely on automated processing intended to evaluate certain personal aspects relating to this person or to analyse or predict in particular the person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour, is lawful</i> only if the processing:</p> <p>(a) is carried out in the course of the entering into, or performance of, a contract, where the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or where suitable measures to safeguard the data subject's legitimate interests have been adduced, such as the right to obtain human intervention; or</p> <p>(b) expressly authorized by a Union or Member State law which also lays down suitable measures to safeguard the data subject's legitimate interests; or</p> <p>(c) is based on the data subject's consent, subject to the conditions laid down in <i>Article 7 in Article 15 and Article 16.</i></p> <p>3. Automated processing of personal data intended to evaluate certain personal aspects relating to a natural person shall not be based solely on the special categories of personal data referred to in Article 9.</p> <p>4. In the cases referred to in paragraph 2, the information to be provided by the controller under Article 14 shall include information as to the existence of processing for a measure of the kind referred to in paragraph 1 and the envisaged effects of such processing on the data subject.</p> <p>5. The Commission shall be empowered to</p>	
--	--

FACEBOOK

adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for suitable measures to safeguard the data subject's legitimate interests referred to in paragraph 2.	
<i>Justification</i>	
<p>Profiling techniques are used in a variety of sectors ranging from banking to health and retail and for various purposes that include the fight against fraud, service improvement or marketing. Therefore a 'one size -fits all' approach to profiling is not adequate and is likely to produce unintended consequences to the detriment of consumers, business and the society as a whole.</p> <p>Given the likely evolution of technology as a tool to help make decisions, it is no longer justifiable to treat profiling techniques differently from other types of processing, particularly taking into account all other safeguards introduced by the draft Regulation.</p>	

5. Controller/Processor

The concepts of data processor and data controller have been appropriately defined in the existing data protection legislation (i.e. Directive 95/46/EC). In the draft Regulation, the concept of data processor is not clearly defined and, as a result, there may be situations where a data processor may unjustifiably be regarded as a data controller. For example, under Article 26(4), if a processor is considered to be taking independent decisions then that processor will be deemed as a controller. In practice, the interaction between the two concepts might raise practical difficulties when a data controller and a data processor are part of the same company group and both parts of the group collaborate on a daily basis. The policies and protocols will be defined by the data controller, but often implemented independently by the data processor.

Drafting recommendations:

Recital 62 / Article 4(5) (Definition of Controller) / Article 4(6) (Definition of Processor) / Article 24 (Joint Controllers) / Article 26 (Processor): Proposals regarding the definition of the data controller need to be narrowed down to ensure that organisations can operate efficiently with legal certainty. The definition of data processor should also be modified to allow certain elements of co-decision-making.

Article 22 (Responsibility of the Controller): This provision introduces new accountability provisions on controllers. These include requirements to demonstrate compliance with the draft Regulation through the adoption of internal policies, assignment of internal responsibilities and verification of compliance. Even though these provisions are sound, there may be some difficulty in situations where the level of prescription in the draft Regulation is such that they may not reflect practices that are otherwise appropriate to safeguard personal data. To this end the Article would requires further consideration.

FACEBOOK

Recital 65 / Article 28 (Documentation) / Article 9 (Co-operation with the supervisory authority): Processors should not be subject to the same administrative obligations as controllers. The administrative obligations on processors to keep the same documentation as controllers are unduly burdensome. We have therefore suggested that the obligations placed on controllers as regards documentation (Article 28(1), (3) and (4)) and co-operation with the competent supervisory authority (Article 29(1)) should not extend to processors.

Drafting suggestions:

<p>Recital 62 (EC proposal) The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processor, also in relation to the monitoring by and measures of supervisory authorities, requires a clear attribution of the responsibilities under this Regulation, including where a controller determines the purposes, conditions and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller.</p>	<p>Recital 62 The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processor, also in relation to the monitoring by and measures of supervisory authorities, requires a clear attribution of the responsibilities under this Regulation, including where a controller determines the purposes conditions and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller.</p>
<p><i>Justification</i></p> <p>The definition of controller as set out in the draft Regulation creates uncertainty. The definition contained in existing data protection legislation (i.e. Directive 95/46/EC) works well in practice and should be maintained. The draft Regulation should focus on the real factor that determines controllership of the personal data (i.e. the purposes of the processing).</p>	

<p>Recital 65 (EC proposal) In order to demonstrate compliance with this Regulation, the controller or processor should document each processing operation. Each controller and processor should be obliged to co-operate with the supervisory authority and make this documentation, on request, available to it, so that it might serve for monitoring those processing operations.</p>	<p>Recital 65 In order to demonstrate compliance with this Regulation, the controller or processor should document each processing operation. Each The controller and processor should be obliged to co-operate with the competent supervisory authority and make this documentation, on request, available to it, so that it might serve for monitoring those processing operations.</p>
<p><i>Justification</i></p>	

FACEBOOK

Processors should not be subject to the same administrative obligations as controllers. The administrative obligations on processors to keep the same documentation as controllers are unduly burdensome.

<p>Article 4(5) (EC proposal) 'controller' means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes, conditions and means of the processing of personal data; where the purposes, conditions and means of processing are determined by Union law or Member State law, the controller or the specific criteria for his nomination may be designated by Union law or by Member State law;</p>	<p>Article 4(5) 'controller' means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes, conditions and means of the processing of personal data; where the purposes, conditions and means of processing are determined by Union law or Member State law, the controller or the specific criteria for his nomination may be designated by Union law or by Member State law;</p>
<p style="text-align: center;"><i>Justification</i></p> <p>The definition of controller as set out in the draft Regulation creates uncertainty. The definition contained in existing data protection legislation (i.e. Directive 95/46/EC) works well in practice and should be maintained. The draft Regulation should focus on the real factor that determines controllership of the personal data (i.e. the purposes of the processing).</p>	

<p>Article 4(6) (EC proposal) 'processor' means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;</p>	<p>Article 4(6) 'processor' means a natural or legal person, public authority, agency or any other body which processes personal data, including making decisions with regard to the processing, on behalf of the controller;</p>
<p style="text-align: center;"><i>Justification</i></p> <p>The definition of processor as it is worded in the draft Regulation does not reflect current practices. It would be consistent with current practices to allow processors to undertake certain decision making responsibilities without losing their processor status, as long as such processing continues to take place on behalf of a controller.</p>	

<p>Article 15(d) the period for which the personal data will be stored and the time of collection;</p>	<p>Article 15(d) the period for which the personal data will be stored and the time of collection;</p>
--	--

Justification

Retain the European Commission’s proposal. The obligation added by the rapporteur has the potential of being administratively burdensome for the controller.

<p>Article 22 The controller shall adopt policies and implement appropriate measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation.</p> <p>2. The measures provided for in paragraph 1 shall in particular include: (a) keeping the documentation pursuant to Article 28; (b) implementing the data security requirements laid down in Article 30; (c) performing a data protection impact assessment pursuant to Article 33; (d) complying with the requirements for prior authorisation or prior consultation of the supervisory authority pursuant to Article 34(1) and (2); (e) designating a data protection officer pursuant to Article 35(1).</p> <p>3. The controller shall implement mechanisms to ensure the verification of the effectiveness of the measures referred to in paragraphs 1 and 2. If proportionate, this verification shall be carried out by independent internal or external auditors.</p>	<p>Article 22 The controller shall adopt policies and implement appropriate and reasonable measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation. For the purpose of this Regulation, appropriate and reasonable measures will mean measures that are proportional to the risks involved, the administrative burdens and costs of the implementation, and the state of and availability of the technology.</p> <p>2. The measures provided for in paragraph 1 shall in particular include: (a) keeping the documentation pursuant to Article 28; (b) implementing the data security requirements laid down in Article 30; (c) performing a data protection impact assessment pursuant to Article 33; (d) complying with the requirements for prior authorisation or prior consultation of the competent supervisory authority pursuant to Article 34(1) and (2); (e) designating a data protection officer pursuant to Article 35(1).</p> <p>3. The controller shall implement mechanisms to ensure for the verification of the effectiveness of the measures referred to in paragraphs 1 and 2. If proportionate, this verification shall be carried out by independent internal or external auditors.</p>
<p><i>Justification</i></p>	

The obligations on controllers to adopt policies and appropriate measures should be clear. Such policies and measures should be "appropriate and reasonable" and proportional to the "risks involved, the administrative burdens and costs of the implementation, and the state of and availability of the technology".

Article 24

Where a controller determines the purposes, conditions and means of the processing of personal data jointly with others, the joint controllers shall determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the procedures and mechanisms for exercising the rights of the data subject, by means of an arrangement between them. **Where such determination is lacking or is not sufficiently clear, the data subject can exercise his rights with any of the controllers and they shall be equally liable.**

Article 24

Where a controller determines the purposes, ~~conditions~~ and means of the processing of personal data jointly with others, the joint controllers shall determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the procedures and mechanisms for exercising the rights of the data subject, by means of an arrangement between them.

Justification

The definition of controller as set out in the draft Regulation creates uncertainty. The definition contained in existing data protection legislation (i.e. Directive 95/46/EC) works well in practice and should be maintained. The draft Regulation should focus on the real factor that determines controllership of the personal data (i.e. the purposes of the processing).

Article 26

1. Where a processing operation is to be carried out on behalf of a controller, the controller shall choose a processor providing sufficient guarantees to implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject, in particular in respect of the technical security measures and organizational measures governing the

Article 26

1. Where a processing operation is to be carried out on behalf of a controller, the controller shall choose a processor providing sufficient guarantees to implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject, in particular in respect of the technical security measures and organizational measures governing the

<p>processing to be carried out and shall ensure compliance with those measures.</p> <p>2. The carrying out of processing by a processor shall be governed by a contract or other legal act binding the processor to the controller and stipulating in particular that the processor shall:</p> <p>(a) act only on instructions from the controller, in particular, where the transfer of the personal data used is prohibited;</p> <p>(b) employ only staff who have committed themselves to confidentiality or are under a statutory obligation of confidentiality;</p> <p>(c) take all required measures pursuant to Article 30;</p> <p>(d) enlist another processor only with the prior permission of the controller;</p> <p>(e) insofar as this is possible given the nature of the processing, create in agreement with the controller the necessary technical and organisational requirements for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;</p> <p>(f) assist the controller in ensuring compliance with the obligations pursuant to Articles 30 to 34;</p> <p>(g) hand over all results to the controller after the end of the processing and not process the personal data otherwise;</p> <p>(h) make available to the controller and the supervisory authority all information necessary to control compliance with the obligations laid down in this Article.</p> <p>3. The controller and the processor shall document in writing the controller's instructions and the processor's obligations referred to in paragraph 2.</p>	<p>processing to be carried out and shall ensure compliance with those measures.</p> <p>2. The carrying out of processing by a processor shall be governed by a contract or other legal act binding the processor to the controller and stipulating in particular that the processor shall:</p> <p>(a) act only on instructions from the controller, in particular, where the transfer of the personal data used is prohibited;</p> <p>(b) employ only staff who have committed themselves to confidentiality or are under a statutory obligation of confidentiality;</p> <p>(c) take all required measures pursuant to Article 30;</p> <p>(d) enlist another processor only with the prior permission of the controller; not conflict with the instructions given by the controller when enlisting another processor;</p> <p>(e) insofar as this is possible given the nature of the processing, create in agreement with the controller the necessary technical and organisational requirements for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;</p> <p>(f) assist the controller in ensuring compliance with the obligations pursuant to Articles 30-29 to 34;</p> <p>(g) hand over all results to the controller after the end of the processing and not process the personal data otherwise; not process the personal data further after the end of the agreed processing;</p> <p>(h) make available to the controller and the supervisory authority all information necessary to control compliance with the obligations laid down in this Article.</p> <p>3. The controller and the processor shall document in writing the controller's instructions and the processor's obligations referred to in paragraph 2.</p>
---	---

FACEBOOK

<p>4. If a processor processes personal data other than as instructed by the controller, the processor shall be considered to be a controller in respect of that processing and shall be subject to the rules on joint controllers laid down in Article 24.</p>	<p>4. If a processor processes personal data other than as instructed by the controller, the processor shall be considered to be a controller in respect of that processing and shall be subject to the rules on joint controllers laid down in Article 24.</p>
<p style="text-align: center;"><i>Justification</i></p> <p>The definition of processor as it is worded in the draft Regulation does not reflect current practices. It would be consistent with current practices to allow processors to undertake certain decision making responsibilities without losing their processor status, as long as such processing continues to take place on behalf of a controller. In particular:</p> <p>Processors should be able to enlist sub-processors that enable the requirements of the Regulation to be met (rather than only with the prior permission of the controller (Article 26(2)(d)).</p> <p>Processors should not be able to process personal data after the end of the agreed processing (rather than being required to hand over all results to the controller after the end of the processing and not process the personal data otherwise (Article 26(2)(g)).</p> <p>Processors should provide information to the controller necessary to control compliance with the obligations laid down in the Article but not to the supervisory authority (Article 26(2)(h)).</p>	

<p>Article 28</p> <p>1. Each controller and processor and, if any, the controller’s representative, shall maintain documentation of all processing operations under its responsibility.</p> <p>2. The documentation shall contain at least the following information:</p> <p>(a) the name and contact details of the controller, or any joint controller or processor, and of the representative, if any;</p> <p>(b) the name and contact details of the data protection officer, if any;</p> <p>(c) the purposes of the processing, including the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);</p> <p>(d) a description of categories of data</p>	<p>Article 28</p> <p>1. Each controller and processor and, if any, the controller’s representative, shall maintain documentation of all processing operations under its responsibility.</p> <p>2. The documentation shall contain at least the following information:</p> <p>(a) the name and contact details of the controller, or any joint controller or processor, and of the representative, if any;</p> <p>(b) the name and contact details of the data protection officer, if any;</p> <p>(c) the purposes of the processing, including the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);</p> <p>(d) a description of categories of data</p>
--	---

FACEBOOK

<p>subjects and of the categories of personal data relating to them;</p> <p>(e) the recipients or categories of recipients of the personal data, including the controllers to whom personal data are disclosed for the legitimate interest pursued by them;</p> <p>(f) where applicable, transfers of data to a third country or an international organisation, including the identification of that third country or international organisation and, in case of transfers referred to in point (h) of Article 44(1), the documentation of appropriate safeguards;</p> <p>(g) a general indication of the time limits for erasure of the different categories of data;</p> <p>(h) the description of the mechanisms referred to in Article 22(3).</p> <p>3. The controller and the processor and, if any, the controller's representative, shall make the documentation available, on request, to the supervisory authority and, in an electronic format, to the data subject.</p> <p>4. The obligations referred to in paragraphs 1 and 2 shall not apply to the following controllers and processors:</p> <p>(a) a natural person processing personal data without a commercial interest; or</p> <p>(b) an enterprise or an organisation that is processing personal data only as an activity ancillary to its main activities.</p> <p>6. The Commission may lay down standard forms for the documentation referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>	<p>subjects and of the categories of personal data relating to them;</p> <p>(e) the recipients or categories of recipients of the personal data, including the controllers to whom personal data are disclosed for the legitimate interest pursued by them;</p> <p>(f) where applicable, transfers of data to a third country or an international organisation, including the identification of that third country or international organisation and, in case of transfers referred to in point (h) of Article 44(1), the documentation of appropriate safeguards;</p> <p>(g) a general indication of the time limits for erasure of the different categories of data;</p> <p>(h) the description of the mechanisms referred to in Article 22(3).</p> <p>3. The controller and the processor and, if any, the controller's representative, shall make the documentation available, on request, to the competent supervisory authority.</p> <p>4. The obligations referred to in paragraphs 1 and 2 shall not apply to the following controllers and processors:</p> <p>(a) a natural person processing personal data without a commercial interest; or</p> <p>(b) an enterprise or an organisation employing fewer than 250 persons that is processing personal data only as an activity ancillary to its main activities.</p> <p>6. The Commission may lay down standard forms for the documentation referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>
<p style="text-align: center;"><i>Justification</i></p> <p>Processors should not be subject to the same administrative obligations as controllers. The administrative processor related obligations to keep the same documentation as</p>	

FACEBOOK

controllers is unduly burdensome. The obligations placed on controllers as regards documentation (Article 28(1), (3) and (4)) should not extend to processors.

References to the 'supervisory authority' should be consistent with the regime set out in the 'competence' provisions (Article 51).

Article 29 (EC proposal)

1. The controller and the processor and, if any, the representative of the controller, shall co-operate, on request, with the supervisory authority in the performance of its duties, in particular by providing the information referred to in point (a) of Article 53(2) and by granting access as provided in point (b) of that paragraph.
 2. In response to the supervisory authority's exercise of its powers under Article 53(2), the controller and the processor shall reply to the supervisory authority within a reasonable period to be specified by the supervisory authority. The reply shall include a description of the measures taken and the results achieved, in response to the remarks of the supervisory authority.

Article 29

1. The controller ~~and the processor~~ and, if any, the representative of the controller, shall co-operate, on request, with the **competent** supervisory authority in the performance of its duties, in particular by providing the information referred to in point (a) of Article 53(2) and by granting access as provided in point (b) of that paragraph.
 2. In response to the **competent** supervisory authority's exercise of its powers under Article 53(2), the controller and the processor shall reply to the supervisory authority within a reasonable period to be specified by the **competent** supervisory authority. The reply shall include a description of the measures taken and the results achieved, in response to the remarks of the **competent** supervisory authority.

Justification

References to the 'supervisory authority' should be consistent with the regime set out in the 'competence' provisions (Article 51).

Processors should not be subject to the same administrative obligations as controllers. The administrative obligations on processors to keep the same documentation as controllers is unduly burdensome. Therefore the obligations placed on controllers as regards co-operation with the competent supervisory authority (Article 29(1)) should not extend to processors.

International Transfers

Article 41(2)(a)

Article 41(2)(a)

FACEBOOK

the rule of law, relevant legislation in force, both general and sectoral, including concerning public security, defence, national security and criminal law, the professional rules and security measures which are complied with in that country or by that international organisation, <i>jurisprudential precedents</i> as well as effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects residing in the Union whose personal data are being transferred;	the rule of law, relevant legislation in force, both general and sectoral, including concerning public security, defence, national security and criminal law, the professional rules and security measures which are complied with in that country or by that international organisation, <i>jurisprudential precedents</i> as well as effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects residing in the Union whose personal data are being transferred;
<i>Justification</i>	
The European Commission should not be granted the power to give consideration to judicial precedents. This would be most appropriately dealt with by the European Court of Justice whose primary function is to interpret the law, rather than the Commission.	



FEDERATION
BANCAIRE
FRANCAISE

**PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE
COUNCIL ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING
OF PERSONAL DATA AND ON THE FREE MOVEMENT OF SUCH DATA
(GENERAL DATA PROTECTION REGULATION)**

August 2012

The French Banking Federation (FBF) is the professional body representing the interests of the banking industry in France. Its membership is composed of all credit institutions authorised as banks and doing business in France, i.e. more than 450 commercial and cooperative banks. FBF member banks have 40,000 permanent branches in France. They employ 400,000 people, and service 60 million customers.

The FBF is in favour of the choice of legal form made by the European Commission: regulations would indeed establish a harmonised body of rules relative to the protection of personal data for all member countries.

The FBF is also in favour of the Commission's position concerning the application of the regulation to those in charge of processing who are not established in the Union, in order to avoid distortions of competition related to regulatory restrictions.

The FBF draws the Commission's attention to the necessary connection to be established between regulation on data protection and other regulations, particularly those relative to the fight against money-laundering and the financing of terrorism, in order to reconcile the growing requirements in terms of security with the key principles of the protection of personal data and personal privacy in a context of the globalisation of the economy and technologies. To this end, a study should be made on the abolition of administrative formalities with the data protection authorities concerning processing imposed by a legal obligation, as well as improved institutional cooperation between European or international bank regulators and data protection authorities, with the idea of promoting consultation and discussions so that common interpretations can be widely spread.

Key points:

- **Delegated acts:** the FBF considers that the number of delegated acts is too large and a factor in legal uncertainty.
The FBF would like delegated acts to be abolished or incorporated into the text of the regulation itself in order to allow its immediate application through specific provisions. A delegated act may not cover an essential subject (art. 290 of the Treaty on the functioning of the European Union) with regard to the subject of the regulation. This is the case of the acts specified in articles 6, 8, 17, 18 paragraph 3, 26, 33.
Also, a delegated act does not appear necessary when draft regulation measures are of a general nature: it is for those responsible for processing to demonstrate responsibility and to determine the appropriate resources to comply with these measures. The regulations are not intended to interfere in the organisation of companies. This is

particularly the case concerning articles 22, 23 and 31 paragraph 6 of the draft regulation.

- **Existence of sectorial provisions** (art. 17 and 18): the draft regulation is a horizontal instrument intended to apply to all sectors of activity. Yet, it transforms into general measures those that should only concern the Internet and social networks (particularly the right to data portability and the right to be digitally forgotten). The consequences of such measures, in terms of technical costs, competition risks and data-transmission security risks have not given rise to any audit or impact study.
A limitation of the scope of the right to data portability and the right to be digitally forgotten would not weaken the protection of people who already have access and objection rights, whatever the sector of activity concerned.
- **Explicit consent** (art. 4 and 7): when the lawfulness of the processing is based on collecting consent, the draft regulation specifies that the consent must be free, specific, informed and **explicit** (which requires a positive action from the person concerned). This addition of the definition of consent is unrealistic and difficult to apply for all companies, as they have to retain their freedom and the option of setting up innovative resources concerning the procedures for collecting consent according to the vectors used (paper media, Internet and telephone) and the type of relationships established with people. It is thus necessary to come back to the definition of consent as set forth in Directive 46/95, i.e. *“any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed”*
Also, consent may be withdrawn by the person concerned, which has consequences that are not controlled by companies.
- **Notification of breaches of personal data** (art 4, 31 and 32): the draft regulation extends to all sectors of activity, the principle of the notification of breaches of personal data introduced by directive 2002/58/CE for the operators of electronic communications and modified in 2009, known as the "privacy and electronic communications" directive.

All breaches of data (even the most minor) cannot be notified to the people concerned, otherwise this will create an unjustified and disproportionate climate of insecurity, confusion and anxiety. What is more, this risks generating significant costs for those responsible for processing. It is therefore necessary for any communication to people concerned, about a breach of data, to be measured and researched and not systematic.
Also, the notification without undue delay, and if possible within 24 hours, is technically impossible to comply with and in any case would only make sense for notifications presenting a serious problem requiring quick intervention to limit the risks.

- **Data-protection officer** (art. 35): the draft regulation specifies the mandatory appointment of a data-protection officer. Creating a specific protective status of "data-protection officer" would be a source of constraints and difficulties. As a result, it is necessary to delete the following provision of article 35.7 : *“During their term of office, the data protection officer may only be dismissed, if the data protection officer no longer fulfils the conditions required for the performance of their duties”*. However, in order to ensure his/her independence, it would be necessary to associate him/her with a sufficient hierarchical level, as is the case, for example, under French law for the person responsible for compliance.
- **The one-stop shop** (art. 51): we fear that the wording of the article, if it remains unchanged, obliges groups established in several countries of the European Union to review their personal-data-protection organisation, particularly if the result of this is that the competent national data-protection authority is necessarily the one of the country where the person responsible for processing has their main establishment located. Even

for groups that have chosen to designate a single person in charge of processing for the entire group, it should not be the case that the concept of the one-stop shop necessarily results in the data-protection authority of the main establishment becoming competent to check and possibly impose penalties for any breach committed in any of the group's entities located in the European Union. Everything should depend on the nature of the shortcoming and whether or not it is related to the way the processing has been designed, when it concerns a process common to the whole of the group.

It would be more appropriate to leave international groups to decide, for each of the processes common to the whole of the group, whether they prefer to have a single person in charge of processing for the whole group or a person in charge of processing in each of the countries where the group is established.

- **Administrative sanctions** (art. 79): the draft regulation specifies the application of heavy administrative sanctions calculated from a company's worldwide revenue (until 2%), equivalent to those already existing in matters of competition. The latter are based on the negative impact of anti-competitive practices on the markets, which justifies the calculation of sanctions based on revenue.

Such criteria of the revenue to calculate the amount of the sanctions is not relevant because non-compliance with data protection regulations harms private interests, together with individual rights, and do not harm the market.

As a result, it is necessary that administrative pecuniary sanctions be purely standard, as it is the case for natural person responsible for the data processing in a non-commercial way (sanctions between 250,000 euros and 1 million euros maximum) and to delete the criteria of percentage of revenue.

Other general comments

- **Definitions** (art. 4): some concepts used are susceptible to interpretation because they do not correspond to legal concepts that are consistently shared at the European level. For example, it is the case with the concepts of: main establishment, enterprise, group of undertakings.

In particular, it would be necessary to review the definition of enterprise, so that subsidiaries that do not have a corporate status are considered as companies.

In the definition of "Group of undertakings", the concept of control should be defined by an objective criterion that is easy to determine.

- **Excessively-strict control of profiling** (art. 20): the rules proposed on profiling go far beyond those specified by the 1995 directive, which aim to reduce discriminatory behaviour having a negative impact, such as the use of automatic profiling to refuse a product or service.

The draft regulation extends the restrictions of 1995 to practices that do not necessarily have a negative effect for people if they are intended to make information more relevant and more useful for the individual. By encompassing all forms of personalisation, whatever the possible impact on users, the new rules could compromise the effort made by companies to offer their customers "customised" products and services and degrade the quality of services offered to European citizens.

- **Reduction in formalities, but increase in obligations for those in charge of processing** (art. 28, 33 and 34): the draft regulation imposes very detailed obligations concerning the documentation of all processing performed by a person in charge of processing. These obligations appear disproportionate because they cover all processes, which will entail high costs, including for processes for which the risks are low. It would therefore be necessary to propose exceptions for this type of processing.

It does not appear necessary for the Commission to establish model forms for the documentation, because at the IT level, such documentation may be constituted in different forms left to the responsibility of those in charge of processing.

Also, the draft regulations require those in charge of processing to measure the risks presented by certain processes and to consult the data-protection authorities in case of at-risk processes.

These provisions, far from reducing administrative burden, increase them without necessarily taking into account the best practices concerning the organisation and assessment of risks put in place by those in charge of processing.

There should be no obligation to consult the data-protection authorities as long as the company has taken the necessary measures to comply with the regulations on data protection. If the principle of consultation of the data-protection authorities, and/or authorisation by them, is retained, the mechanisms should be simplified and clarified so as not to be interpreted differently by national data-protection authorities.

Furthermore, the obligation to consult the people concerned (art 33.4) should be deleted because this may harm the confidentiality of information and business secrecy. What is more, it is impossible to consult people concerning all processing or large-scale processing.

- **Class actions** (art. 73, 75 and 76): The draft regulation is not the appropriate vehicle for dealing with the question of class actions which, moreover, are the subject of general work within the European Commission in order to study the option of a Common European framework for class actions. This framework would contain a set of principles that all future EU initiatives on class actions must comply with, whatever the sector concerned.



27 November 2012

Proposed FEAM amendments to EC Proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (COM(2012)0011)

Amendments to Article 4(20) (new), Article 6(1)(g) (new) and Article 9(2)(k) (new) should be included as a group.

Recital 23

Text from the Commission	Proposed Amendment
<p>The principles of protection should apply to any information concerning an identified or identifiable person. To determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the individual. The principles of data protection should not apply to data rendered anonymous in such a way that the data subject is no longer identifiable.</p>	<p>The principles of protection should apply to any information concerning an identified or identifiable person. To determine whether a person is identifiable, account should be taken of all the means <u>reasonably likely</u> to be used either by the controller or by any other person to identify the individual. <u>Identification shall not be deemed “reasonably likely” in respect of data held for historical, statistical and scientific purposes, if information that enables the identification of a data subject is kept separately from the data that is the object of the historical, statistical and scientific purposes. Keeping separately can be achieved where appropriate safeguards are in place to prevent the risk of unnecessary identification and that any key enabling such identification is kept securely. A single data controller can achieve keeping separately for these purposes. The data controller need not engage a third party to hold any key if such appropriate safeguards are in place and the key is kept securely by that data controller.</u></p> <p>The principles of data protection should not apply to data rendered anonymous in such a way that the data subject is no longer identifiable. <u>Anonymisation is a valuable means of protecting data subjects that is promoted by this Regulation.</u></p>

Justification

Some forms of historical, statistical and scientific analysis require that data is attributable to an individual, without requiring the individual to be identifiable by the researchers. Pseudonymisation or key-coding is often used to enable such analysis while protecting the privacy of the research subjects. This amendment would clarify that key-coded data used for historical, statistical and scientific purposes are intended to be out of scope of the Regulation where appropriate safeguards are in place to protect the privacy of individuals, with reference to the approach used in Article 83. The amendment also clarifies that in specified circumstances a single data controller can hold key-coded data outside the scope of the Regulation and that this can be achieved without needing to send the key to a third party to hold. Further, separate parts of a single organisation should be able to process key-coded data in the same way as those outside the organisation.

Recital 26

Text from the Commission	Proposed Amendment
<p>Personal data relating to health should include in particular all data pertaining to the health status of a data subject; information about the registration of the individual for the provision of health services; information about payments or eligibility for healthcare with respect to the individual; a number, symbol or particular assigned to an individual to uniquely identify the individual for health purposes; any information about the individual collected in the course of the provision of health services to the individual; information derived from the testing or examination of a body part or bodily substance, including biological samples; identification of a person as provider of healthcare to the individual; or any information on e.g. a disease, disability, disease risk, medical history, clinical treatment, or the actual physiological or biomedical state of the data subject independent of its source, such as e.g. from a physician or other health professional, a hospital, a medical device, or an in vitro diagnostic test.</p>	<p>Personal data relating to health should include in particular all personal data pertaining to the health status of a data subject; information about the registration of the individual for the provision of health services; information about payments or eligibility for healthcare with respect to the individual; a number, symbol or particular assigned to an individual to uniquely identify the individual for health purposes; any information about the individual collected in the course of the provision of health services to the individual; information personal data derived from the testing or examination of a body part or, bodily substance, including or biological samples; identification of a person as provider of healthcare to the individual; or any information on e.g. a disease, disability, disease risk, medical history, clinical treatment, or the actual physiological or biomedical state of the data subject independent of its source, such as e.g. from a physician or other health professional, a hospital, a medical device, or an in vitro diagnostic test.</p>

Justification

Recital 26 must be consistent with definition of “data concerning health” in Article 4. This amendment would clarify that data concerning health includes personal data obtained from testing biological samples, rather than biological samples *per se*.

Recital 40

Text from the Commission	Proposed Amendment
<p>The processing of personal data for other purposes should be only allowed where the processing is compatible with those purposes for which the data have been initially collected, in particular where the processing is necessary for historical, statistical or scientific research purposes. Where the other purpose is not compatible with the initial one for which the data are collected, the controller should obtain the consent of the data subject for this other purpose or should base the processing on another legitimate ground for lawful processing, in particular where provided by Union law or the law of the Member State to which the controller is subject. In any case, the application of the principles set out by this Regulation and in particular the information of the data subject on those other purposes should be ensured.</p>	<p>The processing of personal data for other purposes should be only allowed where the processing is compatible with those purposes for which the data have been initially collected, in particular such as where the processing is necessary for historical, statistical or scientific research purposes. Where the other purpose is not compatible with the initial one for which the data are collected, the controller should obtain the consent of the data subject for this other purpose or should base the processing on another legitimate ground for lawful processing, in particular where provided by Union law or the law of the Member State to which the controller is subject. In any case, the application of the principles set out by this Regulation and in particular the information of the data subject on those other purposes should be ensured.</p>

Justification

This amendment clarifies that historical, statistical and scientific purposes are intended to be deemed ‘not incompatible’ purposes. While this appears to have been the intention of the original draft in order to be consistent with the 1995 Data Protection Directive, the use of “in particular” is ambiguous. This amendment is supported by the proposal to introduce a new paragraph 2 in Article 83.

There are a range of scientific activities, such as audit, that support research, but are not research *per se*. This proposal would also provide greater clarity by removing the word “research” to indicate that all such scientific activities are included in the scope of Article 83. [Note: this amendment is consistent with the Council Presidency’s proposed changes in the version dated 22 June 2012.]

**Article 4 – Paragraph 10
Definitions**

Text from the Commission	Proposed Amendment
(10) 'genetic data' means all data, of whatever type, concerning the characteristics of an individual which are inherited or acquired during early prenatal development;	(10) 'genetic data' means <u>information on the hereditary characteristics, or alteration thereof, of an identified or identifiable person, obtained through nucleic acid analysis.</u>

Justification

Not all “genetic data” contain sufficient information to identify an individual. The proposed definition of “genetic data” should therefore be clarified to ensure that it only relates to “personal data”. The definition should also be amended to relate specifically to information obtained by the analysis of nucleic acids to make it consistent with other widely used definitions. [Note: this amendment is consistent with the Council Presidency’s proposed changes released on 22 June 2012.]

**Article 4 – Paragraph 12
Definitions**

Text from the Commission	Proposed Amendment
(12) 'data concerning health' means any information which relates to the physical or mental health of an individual, or to the provision of health services to the individual;	(12) 'data concerning health' means <u>any information personal data</u> which relates to the physical or mental health of an individual, or to the provision of health services to the individual;

Justification

The proposed definition of “data concerning health” should be clarified to ensure that it only relates to “personal data”.

**Article 4 – Paragraph 20 (new)
Definitions**

Text from the Commission	Proposed Amendment
	<u>(20) 'Anonymisation' means processing personal data in such a manner that it can subsequently no longer be considered identifiable.</u>

Justification

Anonymous data falls outside of the scope of the Regulation and anonymisation is an important means to protect the privacy of data subjects. However, the act of removing identifiers to ensure that data are no longer personal – anonymisation – is an act of processing and must comply with the Regulation. This amendment establishes a definition of anonymisation to support the clarification of the legal basis for anonymisation in the amendments to Articles 6(1) and 9(2) below.

**Article 5 – Paragraph 10
Principles relating to personal data processing**

Text from the Commission	Proposed Amendment
Personal data must be: (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the data will be processed solely for historical, statistical or scientific research purposes in accordance with the rules and conditions of Article 83 and if a periodic review is carried out to assess the necessity to continue the storage;	Personal data must be: (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the data will be processed solely for historical, statistical or scientific research purposes in accordance with the rules and conditions of Article 83 and if a periodic review is carried out to assess the necessity to continue the storage until it becomes <u>apparent that continued storage is no longer necessary;</u>

Justification

This amendment would replace the proposal for periodic review of data stored solely for historical, statistical or scientific purposes with requirement more suited to the nature of these activities. For example, it is a characteristic of research that certain data may not be used for a long time until they become significant in the future. The future uses of data for research are also difficult to predict.

**Article 6 – Paragraph 1(g) (new)
Lawfulness of processing**

Text from the Commission	Proposed Amendment
	<u>(g) Processing is conducted for the purpose of anonymisation.</u>

Justification

Anonymous data falls outside of the scope of the Regulation and anonymisation is an important means to protect the privacy of individuals. However, the act of removing identifiers to ensure that data are no longer personal – anonymisation – is an act of processing. This amendment provides a legal basis for anonymisation of personal data in its own right, to clarify that this can be achieved without consent of the data subject. This amendment is complementary to the amendment in Article 9(2) below and also requires a definition of “anonymisation” to be included in Article 4.

**Article 9 – Paragraph 2(k) (new)
Processing of special categories of personal data**

Text from the Commission	Proposed Amendment
	<u>(k) Processing is conducted for the purpose of anonymisation.</u>

Justification

Anonymous data falls outside of the scope of the Regulation and anonymisation is an important means to protect the privacy of data subjects. However, the act of removing identifiers to ensure that data are no longer personal – anonymisation – is an act of processing. This amendment provides a legal basis for anonymisation of sensitive categories of personal data in its own right, to clarify that this can be achieved without consent of the data subject. This amendment is complementary to the amendment in Article 6(1) above and also requires a definition of “anonymisation” to be included in Article 4.

**Article 14 – Paragraph 5 – point (e) (new)
Right of the data subject to information**

Text from the Commission	Proposed Amendment
Paragraphs 1 to 4 shall not apply, where: a) the data subject has already the information referred to in paragraphs 1, 2 and 3; or (b) the data are not collected from the data subject and the provision of such information proves impossible or would involve a disproportionate effort; or (c) the data are not collected from the data subject and recording or disclosure is expressly laid down by law; or (d) the data are not collected from the data subject and the provision of such information will impair the rights and freedoms of others, as defined in Union law or Member State law in accordance with Article 21.	Paragraphs 1 to 4 shall not apply, where: (a) the data subject has already the information referred to in paragraphs 1, 2 and 3; or (b) the data are not collected from the data subject and the provision of such information proves impossible or would involve a disproportionate effort; or (c) the data are not collected from the data subject and recording or disclosure is expressly laid down by law; or (d) the data are not collected from the data subject and the provision of such information will impair the rights and freedoms of others, as defined in Union law or Member State law in accordance with Article 21; <u>or (e) the data are processed for historical, statistical or scientific purposes subject to the conditions and safeguards referred to in Article 83 and the provision of such information proves impossible or would involve a disproportionate effort.</u>

Justification

The right of the data subject to information could be problematic for research in situations where notifying participants would create a disproportionate burden that could prevent the research from proceeding. The Regulation includes a 'disproportionate effort' provision where the data are not collected from the data subject. However, in research studies where data *are* collected from the data subject, it may not always be possible or may be prohibitively burdensome for researchers to provide information to data subjects.

**Article 83 – Paragraph 1
Processing for historical, statistical and scientific research purposes**

Text from the Commission	Proposed Amendment
Within the limits of this Regulation, personal data may be processed for historical, statistical or scientific research purposes only if:	Within the limits of this Regulation, personal data may be processed for historical, statistical or scientific research purposes <u>under paragraph 2 of Article 6 and point (i) of Article 9(2)</u> only if:

Justification

Article 83 establishes an independent legal basis for the processing of personal data for historical, statistical and scientific purposes, provided the criteria in Article 83(1) (a) and (b) are met. This proposed amendment clarifies that data controllers may rely on an alternative legal basis, such as consent of the data subject, for processing of personal data for historical, statistical and scientific purposes rather than relying on paragraph 1 of Article 83.

**Article 83 – Paragraph 1 (a) and (b)
Processing for historical, statistical and scientific research purposes**

Text from the Commission	Proposed Amendment
Within the limits of this Regulation, personal data may be processed for historical, statistical or scientific research purposes only if: (a) these purposes cannot be otherwise fulfilled by processing data which does not permit or not any longer permit the identification of the data subject; (b) data enabling the attribution of information to an identified or identifiable data subject is kept separately from the other information as long as these purposes can be fulfilled in this manner.	Within the limits of this Regulation, personal data may be processed for historical, statistical or scientific research purposes only if: (a) these purposes cannot be otherwise fulfilled <u>reasonably be achieved</u> by processing data which does not permit or not any longer permit the identification of the data subject; and (b) data enabling the attribution of information to an identified or identifiable data subject is kept separately from the other information as long as these purposes can be fulfilled in this manner.

Justification

This amendment retains the safeguard that anonymised data should be used in place of personal data wherever possible. However, this amendment provides for a test based on what can reasonably be achieved, rather than the very strict test in the current draft that may prove prohibitive to research. This amendment also provides a conjunction between points (a) and (b) for clarity.

**Article 83 – Paragraph 2 (new)
Processing for historical, statistical and scientific research purposes**

Text from the Commission	Proposed Amendment
	<u>2. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible under point (b) of Article 5(1) provided that the processing:</u> <u>(a) is subject to the conditions and safeguards of this Article; and</u> <u>(b) complies with all other relevant legislation.</u>

Justification

This amendment clarifies that historical, statistical and scientific research purposes are intended to be not incompatible purposes, by relating Article 5(1)(b) to Article 83. The proposal would ensure that the Regulation is

consistent with the previous 1995 Data Protection Directive, which states that “Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards.” (Art. 6(1)(b)). [Note: this amendment is consistent with the Council Presidency’s proposed changes in the version dated 22 June 2012.]

For further information please contact:

Laurence Legros: laurence.legros@feam.eu.com; +32 2 550 2268

Beth Thompson : b.thompson@wellcome.ac.uk; +44 20 7611 7303

The FEAM statement is available from: www.feam.eu.com

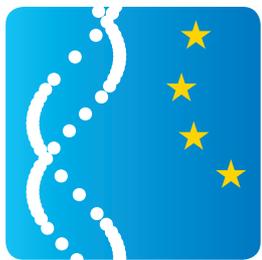
FEAM – Federation of European Academies of Medicine

Palais des Académies

Rue Ducale 1 Hertogstraat

B-1000 Brussels

www.feam.eu.com



FEAM

Federation of European
Academies of Medicine

Data Protection Regulation

A FEAM Statement

June 2012

The Federation of European Academies of Medicine (FEAM)

FEAM was founded in 1993 in Brussels with the objective of promoting cooperation between the national Academies of Medicine and of extending to the political and administrative authorities of the European Union the advisory role that the Academies exercise in their own countries on matters concerning medical sciences and public health. Since 31 March 1995, FEAM has enjoyed the civil status of an international association with a scientific objective. As an umbrella organization, it brings together national Academies of fourteen European member states (Austria, Belgium, Czech Republic, France, Germany, Greece, Hungary, Ireland, Italy, Portugal, the Netherlands, Romania, Spain and the United Kingdom) and aims to reflect the European diversity by seeking the involvement of additional Academies and experts in its scientific activities and by collaborating with other networks on scientific matters of common interest.

The FEAM Office:

President:	Prof. Jesus A.F. Tresguerres (Spain)
Vice-President:	Prof. Dermot Kelleher (Ireland)
General Secretary:	Prof. Paul-Pierre Pastoret (Belgium)
Treasurer:	Prof. Francisco Rubia Vila (Spain)
Past President:	Prof. Hubert E. Blum (Germany)
Deputy Secretary:	Prof. Paolo Villari (Italy)
Scientific Advisers:	Prof. Luigi Frati (Italy) Prof. János Frühling (Belgium) Prof. Cyril Höschl (Czech Republic) Sir Peter Lachmann (United Kingdom) Prof. Charles Pilet (France) Prof. Robert Souhami (United Kingdom)
Executive Director:	Mrs. Laurence Legros

Acknowledgements

This FEAM Statement was endorsed by the FEAM Officers, the national Academies listed on page 11 and the European Medical Research Councils (EMRC).

FEAM warmly thanks Professor Robert Souhami for undertaking this study and the UK Academy of Medical Sciences for its support and advice; the members of the FEAM Working Group and independent experts (listed on page 10) for their input and instructive comments; the national Academies for reviewing and endorsing this Statement; and Dr. Robin Fears and Mr. Laurie Smith for its preparation.

Data Protection Regulation

A FEAM Statement

June 2012

Content

Summary	4
1. Why patient data is important to health research	5
2. How is the use of patient data in research governed?	6
3. Ensuring the Data Protection Regulation facilitates research	7
Appendix: FEAM procedures and contributing individuals	12
This Statement was endorsed by the FEAM member Academies	13
Acknowledgements	14

Summary

We welcome the provisions in the European Data Protection Regulation to support health research that is vital to improve the health of people in the European Union (EU). To ensure that the Regulation does not inhibit ground-breaking medical science it is now necessary to clarify certain points and to address current barriers to health research. In particular:

- it is essential that Article 83 and the associated derogations that facilitate research are maintained as the Regulation moves through the legislative process;
- amendments are needed to clarify and strengthen the research provisions to ensure these achieve their intended purpose; and
- amendments are needed to clarify the scope of the Regulation and ensure that the use of pseudonymised data in health research is regulated proportionately.

1

Why patient data is important to health research

Health research is essential for better public health and health care. The EU has a strong, productive health research base¹: in 2008 the EU was responsible for around 37% of world biomedical research publications and 44% of clinical research publications². According to the Eurobarometer survey of opinion across the EU, a majority of the public (71%) is interested in medical and health research³.

Individual patient records provide a vital resource for this health research for the benefit of society. These records form the basis, for example, for observational studies of the factors underpinning health and disease. Observational studies have led to breakthroughs such as understanding the association between smoking and lung cancer, and the association between high blood pressure and cardiovascular disease.

Access to patient records also helps researchers identify suitable participants to invite to take part in studies, such as clinical trials that test how

well new treatments or diagnostic screening programmes work. Increasingly, these trials also include genetic analysis of participants, for example to study the factors that determine how an individual responds to a specific treatment. This is a crucial component of stratified (personalized) medicine.

By supporting patient recruitment, the use of patient data has an important role to play in creating a facilitative environment in the EU for public, charitable and commercial collaboration on clinical trials and other studies that promote economic growth.

To capitalise on these benefits, it is vital that the EU strikes an appropriate balance between facilitating the safe and secure use of patient data for health research and the rights and interests of individuals.

1 EMRC (2011), White Paper II, A stronger biomedical research for a better European future, http://www.esf.org/uploads/media/emrc_wpII.pdf.

2 UNESCO (2010), UNESCO science report, 2010, <http://www.unesco.org/new/en/natural-sciences/science-technology/prospective-studies/unesco-science-report/unesco-science-report-2010>.

3 Eurobarometer (2007), Medical and health research: a special Eurobarometer public survey. http://ec.europa.eu/public_opinion/archives/ebs/ebs_265_en.pdf.

2

How is the use of patient data in research governed?

Generally, researchers use anonymised patient data wherever possible. However, sometimes it is necessary to access information that can, directly or indirectly, identify a specific individual (Box 1).

Box 1: Health data can be accessed by researchers in different forms

Identifiable data – these include information in patient records such as names, addresses, dates of birth. There are also aspects of health data that could become identifiable when they relate to a diagnosis of a rare condition or when combined with other data. Identifiable data are needed when future contact is established with the participant, for example to contact them to take part in a study, or to link information across different data sets.

Key-coded or pseudonymised data - these cannot directly identify an individual, but are provided with an identifier that enables the patient's identity to be re-connected to the data by reference to separate databases containing the identifiers and identifiable data. Pseudonymised data can often, but not always, be used in place of identifiable data.

Anonymised data – these data cannot be connected to the original patient record. Anonymised data are suitable when no contact is needed with the participant or where the data do not need to be linked to any other data sources.

In the EU, the use of patient data is currently governed by the EU Data Protection Directive, transposed into Member State legislation. This data protection framework has been criticized for being overly complex and sometimes ambiguous and, in some Member States, has been an obstacle to epidemiological and other research⁴. Furthermore, variability in the implementation of the Directive in different countries has been an impediment in the collection and use of complete, accurate and homogenous data in multi-centre studies, for example using diabetes registries⁵.

The Directive is now being revised, as a Data Protection Regulation, with the objective further to harmonise data protection across the EU, facilitate the flow of data across borders and enhance privacy protection. A Regulation is a legislative act of the European Union that becomes immediately enforceable as law in all member states simultaneously, unlike a Directive that needs to be transposed into national law. However, discussion of the revisions has paid rather little attention to the value of data in health research; imposing more restrictive rules on how data should be handled might jeopardize the use of personal data in health research⁶.

4 Academy of Medical Sciences (2010), A new pathways for the regulation and governance of health research, <http://www.acmedsci.ac.uk/p47prid88.html>.

5 Di Zorio, CT & Carinci, F (2010), Cross-border flow of health information: is "privacy by design" sufficient to obtain complete and accurate data for public health in Europe? The case of BIRO/EUBIROD diabetes registers. *Eur J Public Health* 20 (Suppl 1) 101-102.

6 Verschuuren, M, Badeyer, G, Carnicero, J, Sisler, M, Asciak, RP, Sakkeus, L, Stenbeck, M & Deville, W (2008), The European data protection legislation and its consequences for public health monitoring: a plea for action. *Eur J Public Health* 18 550-551; Stenbeck, M & Allebeck, P (2011), Do the planned changes to European data protection threaten or facilitate important health research? *Eur J Public Health* 21 682-683; Hakulinen, T, Arbyn, M, Brewster, DH, Coebergh, JW, Coleman, MP, Crocetti, E, Forman, D, Gissler, M, Katalinic, A, Luostarinen, T, Pukkala, E, Rahu, M, Storm, H, Sund, R, Tornberg, S & Tryggvadottir, L (2011), Harmonization may be counterproductive – at least for parts of Europe where public health research operates effectively. *Eur J Public health* 21 686-687.

3

Ensuring the Data Protection Regulation facilitates research

In previous work, FEAM has expressed concern about the impact of other EU legislation on health research, in particular the problems associated with the Clinical Trials Directive⁷. In the present Statement, we focus on specific points in the proposed draft of the Data Protection Regulation. Our Statement draws on the work of the UK Medical Research Funders⁸ that formed the basis for discussion by a group of experts nominated by FEAM member Academies, and the Academies themselves, during the period March-May 2012.

Outlined below are specific suggestions that we ask to be taken into consideration during the discussion of the Regulation by the European Commission, European Parliament and Council of Ministers.

The proposed Regulation clarifies some of the previously ambiguous areas while attempting to maintain a proportionate mechanism for protecting privacy and enabling health research to continue. We are, therefore, broadly supportive of the intention to strengthen the safeguards for the processing of personal data within the EU as long as balancing protection for health research remains in place.

(i) Article 83 and associated research derogations

The draft Regulation appears to provide a number of derogations – or exceptions – from particular requirements for the use of “personal data” for scientific research. To qualify for these derogations, personal data must be processed in accordance with the conditions set out in Article 83: personal data should not be used if anonymous data would be sufficient and, if possible, any identifying information should be kept separately from other information. The derogations do not exempt research studies from all the requirements set out in the Regulation. However, the derogations do, for example, enable the processing of personal data without consent and for personal data

to be held for extended periods for research purposes. We warmly welcome this approach since it provides a framework that balances the facilitation of research and its associated benefits, with the protection of the interests of research participants (see UK case study in Box 2).

We call on the EU Institutions to prioritise the protection of Article 83 and ensure that the associated derogations for research are maintained as the Regulation moves through the legislative process.

Box 2: UK case study of where it is not practical or possible to obtain consent for the use of patient data in research – Power lines and the risk of childhood leukaemia

Cancer registries were used to identify 33,000 children with cancer, aged up to 14 years. The study showed that, compared with children who lived more than 600 metres from a power line at birth, those who lived within 200 metres had an increased risk of leukaemia (relative risk: 1.69). This study involved information that a child of a particular age lived in a specific postcode. These two pieces of information alone could enable the identification of an individual child. However, it would not have been feasible – or proportionate – to seek individual consent from all 33,000 children.

This shows the importance of protecting Article 83 and the associated derogations for research.

There are a number of issues around Article 83 and the associated derogations that would benefit from clarification. Generally, the lack of clarity in the current Directive has contributed to a risk-averse culture among those sharing and using data for research. Misinterpretation of the current regulatory and governance framework has led in some Member States to delays to, and even halted, research that would otherwise be

in the public interest. To avoid replicating these difficulties, it is essential that any lack of clarity is minimized in the new Regulation, including:

- clarifying that the reference to Article 83 (processing for historical, statistical and scientific research purposes) within Article 81 (processing of personal data concerning health) is intended to link the two sections, rather than to impose an additional restriction on research;
- clarifying that Recital 40 and Article 6.4 about processing of personal data for other purposes intends scientific research to be viewed as a compatible purpose in itself;
- clarifying that Article 83 is intended to allow individuals and organisations to use identifiable data in research where this is necessary and subject to appropriate standards of confidentiality. For example those responsible for on-site monitoring of clinical trials would not be able to use pseudonymised data and will require identifiable information.

We call on the EU Institutions to seek clarification of Article 83 and the associated derogations to ensure that these provide the intended support for research.

(ii) Scope of the Regulation

It is important that the research community is clear about how “personal data” relate to the different types of data used in research (Box 1), since the scope determines which research studies are brought within the remit of the Regulation and, therefore, must comply with its requirements.

The Regulation is not explicit on whether pseudonymised data are intended to be included within its scope. Under current data protection legislation in some Member States, pseudonymised (key-coded) data are treated the same as fully identifiable data and this presents an obstacle to health research. Pseudonymised or

key-coded data underpin a substantial amount of research, for example in genetic studies, when using Biobanks or other large-scale, population-based studies (Box 3).

Box 3: Example of the importance of pseudonymised data in health research – the Collaborative Oncological Gene-environment Study

There are 440,000 cases and 190,000 deaths annually in Europe from breast, ovarian and prostate cancer. The Collaborative Oncological Gene-environment Study (COGS) is a European Commission Framework Programme 7-funded project involving 140 groups worldwide and a total of 200,000 individual participants, that seeks to study these cancers. It incorporates many existing consortia into one large project and, so, adding value to money already spent on research. The project analyzes the genetic variation associated with developing these cancers together with information on environmental and lifestyle factors. The project combines genotyping, statistical modeling and examination of ethical, legal and social issues to develop a comprehensive understanding of how knowledge of genetic factors can enable better tailoring of interventions to individuals in the prevention and treatment of these cancers. Individual participant's data will be pseudonymised so that it can be shared securely between researchers. An overly restrictive approach to pseudonymisation has the potential to compromise the genetic analysis of samples and use of data by the research groups because of the strict regulatory requirements this would impose. Excessive restriction would delay the translation of the findings into more effective interventions for patients.

Further details of the project can be found at <http://cogseu.org>.

It is vital that pseudonymised data are handled proportionately by the Regulation.

Inclusion of pseudonymised data within the scope of the Regulation would dramatically

3 Ensuring the Data Protection Regulation facilitates research

increase the regulatory burden on health research. If pseudonymised data are intended to be included in the scope, we suggest that amendments will be needed to protect the status of well-established uses of pseudonymised data in health research and to ensure that the regulatory burden is proportionate to risk. For example, international transfers of pseudonymised data between collaborators play an essential role in research and must be treated appropriately to ensure that they are not unduly inhibited by the legislation. This should reflect the fact that although re-identification from pseudonymised data may be technically possible, conditions have been established in health research to minimize the opportunity of re-identification. It is important for the European health research community to share this best practice in ensuring confidentiality.

Anonymised data fall outside the scope of the Regulation. However, the act of removing identifiers to ensure that data are no longer personal – anonymisation – could fall within the definition of processing. This would mean that the process of anonymisation itself would have to comply with the requirements of the Regulation to be lawful. We suggest that the Regulation should be revised expressly to permit anonymisation while prohibiting re-identification of data that has been anonymised.

Clarification is also needed about “genetic data” to ensure that the definition is only intended to apply to personal data that falls within this category, rather than all related data. That is, the definition of genetic data used within the Regulation should exclude genetic data not capable of identifying a subject – it should be defined in terms of it being personal data.

We call on the EU Institutions to seek clarification of the scope of the Regulation and to ensure that the use of pseudonymised data in health research is handled proportionately by the Regulation.

(iii) Biological samples

The definition of “data concerning health” must be consistent with the related Recital. Recital 26 includes “information derived from the testing or examination of a body part or bodily substance, including biological samples” in its description of data relating to health. However, no reference is made to biological samples in the definition of Article 4.12.

We ask for this inconsistency to be rectified to clarify that data concerning health does not include biological samples per se but rather to personal data obtained from testing such material.

(iv) Increases in the regulatory burden for health research

Apart from the potential increases in scope, the Regulation increases the regulatory burden in other ways compared to the current Data Protection Directive. If implemented, these additional burdens will make it increasingly difficult for Member States to conduct important research. The following issues present particular problems:

- Article 5(e) on **data storage** provides a welcome derogation that enables data to be held for extended, potentially indefinite, periods for research purposes. However, this derogation imposes a requirement to undertake periodic review to assess the necessity to continue storage. These reviews would be impractical since data are routinely held over long periods and it can be difficult to predict future uses or need for the data. Furthermore, these reviews would create a substantial burden for research institutions that currently hold valuable data and research resources, which may not be sustainable for the sector. We recommend amending Article 5 to remove the need for such review.

-
- The **right of the data subject to information** (Article 14) could be problematic for research in situations where notifying the participants would create a disproportionate burden that could prevent research from proceeding. The Regulation includes a “disproportionate effort” provision (Article 14.5(b)), but this only applies where the data are not collected from the data subject. **It would be helpful to clarify the situation for research by amending this Article to create a specific “disproportionate effort” provision for research, in line with the current Data Protection Directive.**
 - The **right to rectification** (Article 16) is inherently problematic for health research since researchers routinely hold data generated through their studies that cannot be guaranteed to be accurate. For example, data generated by genetic sequencing in the laboratory environment will rarely meet diagnostic standards used in a clinical setting. As a result, such data cannot be considered analytically accurate. In addition, a person’s health status changes over time, for example pregnancy. The Regulation does not contain any guidance as regards practical means for researchers to assess or rectify such “inaccuracies”. **The Regulation should be amended to take this reality of health research into account, that is to propose limits as regards the steps that researchers should be required to take to assess, or to rectify, any potential inaccuracies.**
 - Articles 33-34 require the **impact assessment** of operations presenting specific risks and the need for an approval of this assessment by the Data Protection authority. **We recommend that in the highly regulated area of health research, such authorization need not be required on a project by project basis when assessment has already been undertaken by another suitable national authority (Ethics Committee or National Competent Authority for Clinical Trials of Investigational Medicinal Products).**

(v) Transfer to third countries

Sharing data within international consortia is particularly important in studying rare diseases or for analyzing information across a wide range of different circumstances, for example in the global study represented by the International Childhood Cancer Cohort , pooling data to study various modifiable and genetic factors in relation to cancer risk. Article 45 recognizes the importance of facilitating international collaboration. However, currently there are difficulties in transferring pseudonymised (key-coded) data to countries outside the EU, for example the USA. Even though international research collaborators in these other countries lack the key and are unable to identify subjects, this is often not regarded as a sufficient safeguard. We suggest that, to address this obstacle, the recipients sign a legally binding document that they will not seek access to the key in any attempt to identify the individual, or communicate or transfer the individual’s raw data.

Appendix: FEAM procedures and contributing individuals

The scope and content of this Statement were developed by a FEAM Working Group chaired by Professor Robert Souhami and the draft Statement was reviewed by independent experts and the FEAM membership.

Members of the Working Group

Professor Robert Souhami (Chair)
Foreign Secretary of the UK Academy of Medical Sciences
Scientific Adviser at FEAM
Emeritus Professor of Medicine at University College London (FEAM)

Professor Adelin Albert
Medical informatics and biostatistics, University of Liège
French Belgian Royal Academy of Medicine

Professor Bernard Charpentier
Department of Nephrology, Dialysis and Transplantation, University Hospital of Bicêtre
French National Academy of Medicine

Professor Sandor Kerpel-Fronius
Department of Pharmacology and Pharmacotherapy, Semmelweis University, Budapest, Hungary

Professor Françoise Meunier
Director of the European Organisation for Research and Treatment of Cancer (EORTC)
French Belgian Royal Academy of Medicine

Professor Duarte Nuno Vieira
Instituto Nacional de Medicina Legal,
Universidade de Coimbra
Portuguese National Academy of Medicine

Professor Dragos Vinereanu
University of Medicine and Pharmacy Carol Davila, Bucharest, Romania
Romanian Academy of Medical Sciences

Professor Hans-Peter Zenner
Universitäts Hals-Nasen-Ohren-Klinik, Tübingen
German National Academy of Sciences
Leopoldina

Scientific secretariat

Dr. Robin Fears (FEAM)
Mr. Laurie Smith (UK Academy of Medical Sciences)

We are extremely grateful for the advice of **Professor Carol Dezateux**, **Professor Kay-Tee Khaw**, **Professor Simon Wessely**, **Dr. Beth Thompson** and **Dr. Stéphane Berghmans**.

**This statement was endorsed
by the FEAM member
Academies:**

Austria

Austrian Academy of Sciences

Dr. Ignaz Seipel-Platz 2
1010 Vienna
Website: www.oeaw.ac.at

Belgium

French Belgian Royal Academy of Medicine

Palais des Académies
Rue Ducale 1
1000 Brussels
Website: www.armb.be

Flemish Belgian Royal Academy of Medicine

Paleis der Academiën
Hertogsstraat 1
1000 Brussel
Website: www.academiegeneeskunde.be

Czech Republic

Czech Medical Academy

Řehořova 10
130 00 Praha 3
Website: www.medical-academy.cz

France

French National Academy of Medicine

16, rue Bonaparte
75006 Paris
Website: www.academie-medecine.fr

Germany

German National Academy of Sciences Leopoldina

Jägerberg 1 (formerly Moritzburgring 10)
06108 Halle (Saale)
Website: www.leopoldina-halle.de

Greece

Academy of Athens

28 Panepistimiou Street
10679 Athens
Website: www.academyofathens.gr

Hungary

Hungarian Academy of Sciences

Széchenyi István tér 9.
1051 Budapest
Postal address: Pf. 1000, Budapest, H-1245
Website: www.mta.hu

Ireland

Irish Academy of Medical Sciences

Italy

Italian National Academy of Medicine

Via Martin Piaggio 17/6
16122 Genoa
Website: www.acmed.org

Portugal

Portuguese National Academy of Medicine

Faculdade de Medicina
Av. Prof. Egas Moniz
1649-028 Lisboa
Website: www.academianacionalmedicina.pt

Romania

Romanian Academy of Medical Sciences

Splaiul Independentei N°99-101
Sector 5, Bucuresti
Website: www.adsm.ro

Spain

Spanish Royal National Academy of Medicine

Calle Arrieta 12
28013 Madrid
Website: www.ranm.es

The Netherlands

Royal Netherlands Academy of Arts and Sciences

Het Trippenhuis
Kloveniersburgwal 29
1011 JV Amsterdam
Website: www.knaw.nl

The United Kingdom

The UK Academy of Medical Sciences

41 Portland Place
London W1B 1QH
Website: www.acmedsci.ac.uk

**by the following national
Academies:**

Finland

Council of Finnish Academies

Mariankatu 7 C 1
00170 Helsinki
www.tsv.fi/international/akatemiati

Lithuania

Lithuanian Academy of Sciences

3 Gedimino Ave
01103 Vilnius
Website: www.lma.lt

Poland

Polish Academy of Sciences

Palace of Culture and Science
PO. Box 24
00-901 Warsaw
Website: www.pan.pl

by the following network:

**European Medical
Research Councils
(EMRC)**

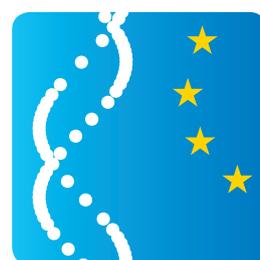


efpia

European Federation of Pharmaceutical
Industries and Associations

**EGAN**
European Genetic Alliances' Network

NHS European Office



FEAM

Federation of European
Academies of Medicine

Palais des Académies
Rue Ducale 1
B-1000 Bruxelles
Tel: 0032 (0) 2 550 22 68
Fax: 0032 (0) 2 550 22 65
E-mail : info@feam.eu.com
Web : www.feam.eu.com

A Summary of the FEAM Statement on the Data Protection Regulation

With the support of :



**EMRC – European
Medical Research
Councils**



NHS European Office



Summary of key points

This is a summary of the FEAM statement on the European Data Protection Regulation. A full copy of the FEAM statement can be found: www.feam.eu.com

FEAM welcomes the provisions in the European Data Protection Regulation to support health research that are vital to improve the health of people in the EU. To ensure that the Regulation does not inhibit groundbreaking medical science it is now necessary to clarify certain points and to address current barriers to health research that are outlined in this summary. In particular:

1. it is essential that Article 83 and the associated derogations that facilitate research are maintained as the Regulation moves through the legislative process;
2. amendments are needed to clarify and strengthen the research provisions to ensure these achieve their intended purpose; and
3. amendments are needed to clarify the scope of the Regulation and ensure that the use of pseudonymised data in health research is regulated proportionately.

Draft amendments that take forward the thinking in this summary are annexed.

Patient data is vital for health research

Patient data provides a vital resource for health research. Observational studies using patient records can be used to determine factors underpinning health and disease, for example information from patient records was used to demonstrate the association between smoking and lung cancer. Patient records can also help identify suitable participants for clinical trials, including those for stratified (personalised) medicine.

Health research is important to the EU, which is responsible for 44% of clinical research publications¹. A majority of the EU public (71%) is interested in medical and health research².

The Data Protection Regulation should facilitate ground breaking medical research

In the EU, the use of patient data is currently governed by the EU Data Protection Directive (DPD). Many believe that the DPD is overly complex and sometimes ambiguous and, in some Member States, has been an obstacle to health research³.

¹ UNESCO (2010), UNESCO science report, 2010, <http://www.unesco.org/new/en/natural-sciences/science-technology/prospective-studies/unesco-science-report/unesco-science-report-2010>

² Eurobarometer (2007), Medical and health research: a special Eurobarometer public survey. http://ec.europa.eu/public_opinion/archives/ebs/ebs_265_en.pdf

The DPD is now being revised, as the Data Protection Regulation (DPR), to further to harmonise data protection across the EU, facilitate the flow of data across borders and enhance privacy protection. It is vital that health research is taken into account as the draft Regulation passes through the legislative process, to reflect the importance of health research to society as a whole.

Ensuring the Data Protection Regulation facilitates research

It is vital that the EU strikes an appropriate balance between facilitating the safe and secure use of patient data for health research and the rights and interests of individuals. Outlined below are specific suggestions that we ask to be taken into consideration during the discussion of the proposals for the DPR.

Article 83 and associated derogations

The draft DPR provides several exceptions from particular requirements for the use of “personal data” for scientific research, provided the conditions set out in Article 83 are fulfilled. We warmly welcome this approach that facilitates research and its associated benefits whilst protecting the interests of research participants. We call on the EU Institutions to prioritise the protection of Article 83 and ensure the associated derogations for research are maintained as the DPR moves through the legislative process;

To ensure that misinterpretation of the DPR does not lead to a risk-averse culture that inhibits medical research, we ask for clarification that:

- the reference to Article 83 (processing for historical, statistical and scientific research purposes) within Article 81 (processing of personal data concerning health) is intended to link the two sections, rather than to impose an additional restriction on research;
- Recital 40 and Article 6.4 about processing of personal data for other purposes intends scientific research to be viewed as a compatible purpose in itself;
- Article 83 is intended to allow individuals and organisations to use identifiable data in research where this is necessary and subject to appropriate standards of confidentiality. For example those responsible for on-site monitoring of clinical trials would not be able to use pseudonymised data and will require identifiable information.

Scope

The DPR is not explicit on whether pseudonymised (key-coded) data, is within its scope. Pseudonymised data replaces personal identifiers with a code, thus concealing the identity of the patient. The key identifying the patient is kept separately from the pseudonymised data to protect the identity of individuals. Pseudonymised data underpins a substantial amount of research, and its inclusion will increase the regulatory burden on health research. We call for clarification of the scope of the DPR and for the use of pseudonymised data in health research to be handled proportionately by the DPR.

Although anonymised data falls outside the scope of the DPR, the process of anonymisation could fall within the DPR. We suggest that the DPR should be revised expressly to permit anonymisation while prohibiting re-identification of data that has been anonymised.

Genetic data

Clarification is needed about the use of the term “genetic data” in the DPR to ensure that the definition is only intended to apply to personal data that falls within this category, rather than all related data.

³ Academy of Medical Sciences (2010), A new pathways for the regulation and governance of health research, <http://www.acmedsci.ac.uk/p47prid88.html>

Biological Samples

There is currently an inconsistency between Recital 26 and Article 4.12, with reference to biological samples. We ask for clarification that data concerning health does not include biological samples per se but rather to personal data obtained from testing such material.

Increases in the regulatory burden for health research

The DPR has the potential to increase the regulatory burden on health research with limited benefit for patients. We believe that the DPR should not require periodic review of research data, data subjects should only have the right to information if this would not require disproportionate effort to obtain, there should be a limit to the extent to which researchers should be required to rectify data, and impact assessments should not be required when assessment has already been undertaken by a suitable national authority.

These include: a requirement for periodic review of stored research data, the right of the data subject to information not including a clause to ensure proportionality, the right to rectification when health status may change over time or when diagnostic tests used for research would not be suitable for the clinic and the requirement for impact assessment in an already highly regulated field.

Transfer to third countries

Article 45 recognizes the importance of facilitating international collaboration. However, there are current difficulties in transferring pseudonymised data to countries outside the EU, for example the USA. Despite collaborators in these other countries lacking the key that identifies subjects, this is often not regarded as a sufficient safeguard. To overcome these difficulties, we suggest that the Regulation is amended to facilitate data transfers to third countries for research while continuing with appropriate safeguards to protect individuals.

For further information please contact:

Laurence Legros: laurence.legros@feam.eu.com; tel : +32 2 550 2268

Beth Thompson: b.thompson@wellcome.ac.uk; tel: +44 20 7611 7303

The FEAM statement is available from: www.feam.eu.com

FEAM – Federation of European Academies of Medicine
Palais des Académies
Rue Ducale 1 Hertogstraat
B-1000 Brussels
www.feam.eu.com



27 November 2012

Annex: Proposed FEAM amendments to EC Proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (COM(2012)0011)

Amendments to Article 4(20) (new), Article 6(1)(g) (new) and Article 9(2)(k) (new) should be included as a group.

Recital 23

Text from the Commission	Proposed Amendment
<p>The principles of protection should apply to any information concerning an identified or identifiable person. To determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the individual. The principles of data protection should not apply to data rendered anonymous in such a way that the data subject is no longer identifiable.</p>	<p>The principles of protection should apply to any information concerning an identified or identifiable person. To determine whether a person is identifiable, account should be taken of all the means <u>reasonably likely</u> to be used either by the controller or by any other person to identify the individual. <u>Identification shall not be deemed “reasonably likely” in respect of data held for historical, statistical and scientific purposes, if information that enables the identification of a data subject is kept separately from the data that is the object of the historical, statistical and scientific purposes. Keeping separately can be achieved where appropriate safeguards are in place to prevent the risk of unnecessary identification and that any key enabling such identification is kept securely. A single data controller can achieve keeping separately for these purposes. The data controller need not engage a third party to hold any key if such appropriate safeguards are in place and the key is kept securely by that data controller.</u></p> <p>The principles of data protection should not apply to data rendered anonymous in such a way that the data subject is no longer identifiable. <u>Anonymisation is a valuable means of protecting data subjects that is promoted by this Regulation.</u></p>

Justification

Some forms of historical, statistical and scientific analysis require that data is attributable to an individual, without requiring the individual to be identifiable by the researchers. Pseudonymisation or key-coding is often used to enable such analysis while protecting the privacy of the research subjects. This amendment would clarify that key-coded data used for historical, statistical and scientific purposes are intended to be out of scope of the Regulation where appropriate safeguards are in place to protect the privacy of individuals, with reference to the approach used in Article 83. The amendment also clarifies that in specified circumstances a single data controller can hold key-coded data outside the scope of the Regulation and that this can be achieved without needing to send the key to a third party to hold. Further, separate parts of a single organisation should be able to process key-coded data in the same way as those outside the organisation.

Recital 26

Text from the Commission	Proposed Amendment
<p>Personal data relating to health should include in particular all data pertaining to the health status of a data subject; information about the registration of the individual for the provision of health services; information about payments or eligibility for healthcare with respect to the individual; a number, symbol or particular assigned to an individual to uniquely identify the individual for health purposes; any information about the individual collected in the course of the provision of health services to the individual; information derived from the testing or examination of a body part or bodily substance, including biological samples; identification of a person as provider of healthcare to the individual; or any information on e.g. a disease, disability, disease risk, medical history, clinical treatment, or the actual physiological or biomedical state of the data subject independent of its source, such as e.g. from a physician or other health professional, a hospital, a medical device, or an in vitro diagnostic test.</p>	<p>Personal data relating to health should include in particular all personal data pertaining to the health status of a data subject; information about the registration of the individual for the provision of health services; information about payments or eligibility for healthcare with respect to the individual; a number, symbol or particular assigned to an individual to uniquely identify the individual for health purposes; any information about the individual collected in the course of the provision of health services to the individual; information personal data derived from the testing or examination of a body part or, bodily substance, including or biological samples; identification of a person as provider of healthcare to the individual; or any information on e.g. a disease, disability, disease risk, medical history, clinical treatment, or the actual physiological or biomedical state of the data subject independent of its source, such as e.g. from a physician or other health professional, a hospital, a medical device, or an in vitro diagnostic test.</p>

Justification

Recital 26 must be consistent with definition of “data concerning health” in Article 4. This amendment would clarify that data concerning health includes personal data obtained from testing biological samples, rather than biological samples *per se*.

Recital 40

Text from the Commission	Proposed Amendment
<p>The processing of personal data for other purposes should be only allowed where the processing is compatible with those purposes for which the data have been initially collected, in particular where the processing is necessary for historical, statistical or scientific research purposes. Where the other purpose is not compatible with the initial one for which the data are collected, the controller should obtain the consent of the data subject for this other purpose or should base the processing on another legitimate ground for lawful processing, in particular where provided by Union law or the law of the Member State to which the controller is subject. In any case, the application of the principles set out by this Regulation and in particular the information of the data subject on those other purposes should be ensured.</p>	<p>The processing of personal data for other purposes should be only allowed where the processing is compatible with those purposes for which the data have been initially collected, in particular such as where the processing is necessary for historical, statistical or scientific research purposes. Where the other purpose is not compatible with the initial one for which the data are collected, the controller should obtain the consent of the data subject for this other purpose or should base the processing on another legitimate ground for lawful processing, in particular where provided by Union law or the law of the Member State to which the controller is subject. In any case, the application of the principles set out by this Regulation and in particular the information of the data subject on those other purposes should be ensured.</p>

Justification

This amendment clarifies that historical, statistical and scientific purposes are intended to be deemed ‘not incompatible’ purposes. While this appears to have been the intention of the original draft in order to be consistent with the 1995 Data Protection Directive, the use of “in particular” is ambiguous. This amendment is supported by the proposal to introduce a new paragraph 2 in Article 83.

There are a range of scientific activities, such as audit, that support research, but are not research *per se*. This proposal would also provide greater clarity by removing the word “research” to indicate that all such scientific activities are included in the scope of Article 83. [Note: this amendment is consistent with the Council Presidency’s proposed changes in the version dated 22 June 2012.]

**Article 4 – Paragraph 10
Definitions**

Text from the Commission	Proposed Amendment
(10) 'genetic data' means all data, of whatever type, concerning the characteristics of an individual which are inherited or acquired during early prenatal development;	(10) 'genetic data' means <u>information on the hereditary characteristics, or alteration thereof, of an identified or identifiable person, obtained through nucleic acid analysis.</u>

Justification

Not all “genetic data” contain sufficient information to identify an individual. The proposed definition of “genetic data” should therefore be clarified to ensure that it only relates to “personal data”. The definition should also be amended to relate specifically to information obtained by the analysis of nucleic acids to make it consistent with other widely used definitions. [Note: this amendment is consistent with the Council Presidency’s proposed changes released on 22 June 2012.]

**Article 4 – Paragraph 12
Definitions**

Text from the Commission	Proposed Amendment
(12) 'data concerning health' means any information which relates to the physical or mental health of an individual, or to the provision of health services to the individual;	(12) 'data concerning health' means <u>any information personal data</u> which relates to the physical or mental health of an individual, or to the provision of health services to the individual;

Justification

The proposed definition of “data concerning health” should be clarified to ensure that it only relates to “personal data”.

**Article 4 – Paragraph 20 (new)
Definitions**

Text from the Commission	Proposed Amendment
	<u>(20) 'Anonymisation' means processing personal data in such a manner that it can subsequently no longer be considered identifiable.</u>

Justification

Anonymous data falls outside of the scope of the Regulation and anonymisation is an important means to protect the privacy of data subjects. However, the act of removing identifiers to ensure that data are no longer personal – anonymisation – is an act of processing and must comply with the Regulation. This amendment establishes a definition of anonymisation to support the clarification of the legal basis for anonymisation in the amendments to Articles 6(1) and 9(2) below.

**Article 5 – Paragraph 10
Principles relating to personal data processing**

Text from the Commission	Proposed Amendment
Personal data must be: (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the data will be processed solely for historical, statistical or scientific research purposes in accordance with the rules and conditions of Article 83 and if a periodic review is carried out to assess the necessity to continue the storage;	Personal data must be: (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the data will be processed solely for historical, statistical or scientific research purposes in accordance with the rules and conditions of Article 83 and if a periodic review is carried out to assess the necessity to continue the storage until it becomes <u>apparent that continued storage is no longer necessary;</u>

Justification

This amendment would replace the proposal for periodic review of data stored solely for historical, statistical or scientific purposes with requirement more suited to the nature of these activities. For example, it is a characteristic of research that certain data may not be used for a long time until they become significant in the future. The future uses of data for research are also difficult to predict.

**Article 6 – Paragraph 1(g) (new)
Lawfulness of processing**

Text from the Commission	Proposed Amendment
	<u>(g) Processing is conducted for the purpose of anonymisation.</u>

Justification

Anonymous data falls outside of the scope of the Regulation and anonymisation is an important means to protect the privacy of individuals. However, the act of removing identifiers to ensure that data are no longer personal – anonymisation – is an act of processing. This amendment provides a legal basis for anonymisation of personal data in its own right, to clarify that this can be achieved without consent of the data subject. This amendment is complementary to the amendment in Article 9(2) below and also requires a definition of “anonymisation” to be included in Article 4.

**Article 9 – Paragraph 2(k) (new)
Processing of special categories of personal data**

Text from the Commission	Proposed Amendment
	<u>(k) Processing is conducted for the purpose of anonymisation.</u>

Justification

Anonymous data falls outside of the scope of the Regulation and anonymisation is an important means to protect the privacy of data subjects. However, the act of removing identifiers to ensure that data are no longer personal – anonymisation – is an act of processing. This amendment provides a legal basis for anonymisation of sensitive categories of personal data in its own right, to clarify that this can be achieved without consent of the data subject. This amendment is complementary to the amendment in Article 6(1) above and also requires a definition of “anonymisation” to be included in Article 4.

**Article 14 – Paragraph 5 – point (e) (new)
Right of the data subject to information**

Text from the Commission	Proposed Amendment
Paragraphs 1 to 4 shall not apply, where: a) the data subject has already the information referred to in paragraphs 1, 2 and 3; or (b) the data are not collected from the data subject and the provision of such information proves impossible or would involve a disproportionate effort; or (c) the data are not collected from the data subject and recording or disclosure is expressly laid down by law; or (d) the data are not collected from the data subject and the provision of such information will impair the rights and freedoms of others, as defined in Union law or Member State law in accordance with Article 21.	Paragraphs 1 to 4 shall not apply, where: (a) the data subject has already the information referred to in paragraphs 1, 2 and 3; or (b) the data are not collected from the data subject and the provision of such information proves impossible or would involve a disproportionate effort; or (c) the data are not collected from the data subject and recording or disclosure is expressly laid down by law; or (d) the data are not collected from the data subject and the provision of such information will impair the rights and freedoms of others, as defined in Union law or Member State law in accordance with Article 21; <u>or (e) the data are processed for historical, statistical or scientific purposes subject to the conditions and safeguards referred to in Article 83 and the provision of such information proves impossible or would involve a disproportionate effort.</u>

Justification

The right of the data subject to information could be problematic for research in situations where notifying participants would create a disproportionate burden that could prevent the research from proceeding. The Regulation includes a 'disproportionate effort' provision where the data are not collected from the data subject. However, in research studies where data *are* collected from the data subject, it may not always be possible or may be prohibitively burdensome for researchers to provide information to data subjects.

**Article 83 – Paragraph 1
Processing for historical, statistical and scientific research purposes**

Text from the Commission	Proposed Amendment
Within the limits of this Regulation, personal data may be processed for historical, statistical or scientific research purposes only if:	Within the limits of this Regulation, personal data may be processed for historical, statistical or scientific research purposes <u>under paragraph 2 of Article 6 and point (i) of Article 9(2)</u> only if:

Justification

Article 83 establishes an independent legal basis for the processing of personal data for historical, statistical and scientific purposes, provided the criteria in Article 83(1) (a) and (b) are met. This proposed amendment clarifies that data controllers may rely on an alternative legal basis, such as consent of the data subject, for processing of personal data for historical, statistical and scientific purposes rather than relying on paragraph 1 of Article 83.

**Article 83 – Paragraph 1 (a) and (b)
Processing for historical, statistical and scientific research purposes**

Text from the Commission	Proposed Amendment
Within the limits of this Regulation, personal data may be processed for historical, statistical or scientific research purposes only if: (a) these purposes cannot be otherwise fulfilled by processing data which does not permit or not any longer permit the identification of the data subject; (b) data enabling the attribution of information to an identified or identifiable data subject is kept separately from the other information as long as these purposes can be fulfilled in this manner.	Within the limits of this Regulation, personal data may be processed for historical, statistical or scientific research purposes only if: (a) these purposes cannot be otherwise fulfilled <u>reasonably be achieved</u> by processing data which does not permit or not any longer permit the identification of the data subject; <u>and</u> (b) data enabling the attribution of information to an identified or identifiable data subject is kept separately from the other information as long as these purposes can be fulfilled in this manner.

Justification

This amendment retains the safeguard that anonymised data should be used in place of personal data wherever possible. However, this amendment provides for a test based on what can reasonably be achieved, rather than the very strict test in the current draft that may prove prohibitive to research. This amendment also provides a conjunction between points (a) and (b) for clarity.

**Article 83 – Paragraph 2 (new)
Processing for historical, statistical and scientific research purposes**

Text from the Commission	Proposed Amendment
	<u>2. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible under point (b) of Article 5(1) provided that the processing:</u> <u>(a) is subject to the conditions and safeguards of this Article; and</u> <u>(b) complies with all other relevant legislation.</u>

Justification

This amendment clarifies that historical, statistical and scientific research purposes are intended to be not incompatible purposes, by relating Article 5(1)(b) to Article 83. The proposal would ensure that the Regulation is

consistent with the previous 1995 Data Protection Directive, which states that “Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards.” (Art. 6(1)(b)). [Note: this amendment is consistent with the Council Presidency’s proposed changes in the version dated 22 June 2012.]

For further information please contact:

Laurence Legros: laurence.legros@feam.eu.com; tel : +32 2 550 2268

Beth Thompson: b.thompson@wellcome.ac.uk; tel: +44 20 7611 7303

The FEAM statement is available from: www.feam.eu.com

FEAM – Federation of European Academies of Medicine
Palais des Académies
Rue Ducale 1 Hertogstraat
B-1000 Brussels



Business Federation
Luxembourg

Fedil – Business Federation Luxembourg

Comments on the Commission Proposal for a Regulation on the Protection of Personal Data in the EU and on the free Movement of such Data

Table of Contents

Introduction	3
1. Territorial scope, DPA jurisdiction and one-stop-shop feature.....	4
a. Clarification of the “main establishment” concept	4
b. Clarification of the extra-territorial reach of the Regulation	5
c. Clarification of the one-stop-shop concept & cooperation mechanisms between DPAs	6
2. Definition of personal data	7
3. Consent requirement.....	9
4. Introduction of a new set of rights for data subjects	10
a. Right to be forgotten	10
b. Right to data portability	11
c. Profiling.....	12
5. Data breach notification obligations.....	13
6. General administrative obligations of controller and processor	14
a. Documentation, privacy impact assessments, prior consultations and authorisations.	14
b. Data protection officers.....	15
7. International data transfers	15
8. Provisions relevant to cloud computing – Definition, responsibility and liability of controller and processor	17
a. Controller/processor concept.....	17
b. Allocation of responsibilities and liabilities between controller and processor	18
Conclusion.....	20
About Fedil-Business Federation www.fedil.lu	21

Introduction

Fedil-Business Federation Luxembourg acting as a multi-sector business federation in Luxembourg welcomes the European Commission's proposal for a General Data Protection Regulation published on 25th of January 2012 as it has the potential to ensure a consistently high level of data protection throughout the EU while at the same time facilitating the free flow of information in the Internal Market. In particular, we believe that the approach chosen by the Commission to introduce a fully harmonised single set of data protection rules applicable throughout the EU, coupled with a one-stop-shop enforcement mechanism, is fundamental in solving existing problems and creating a consistent regulatory level playing field across all EU Member States. Furthermore, it will help reduce administrative burdens and improve the level of trust and legal certainty to the benefit of consumers and businesses, a prerequisite for a well-functioning Digital Single Market.

The review of the EU's Data Protection Framework (the Framework) provides a unique opportunity to update and modernise the rules as well as to strengthen individuals' privacy rights while promoting the continued growth of the Internet economy, fostering innovation and trade. Striking the appropriate balance here will be critical to Europe's economy.

However, achieving the right balance will require a much more pragmatic and results-oriented approach, which truly embraces principles such as accountability, the context in which data is processed as well as the actual risks involved for individuals. Instead, the proposed Regulation pursues an over-regulatory and prescriptive approach which we fear will not only place additional unnecessary burdens and costs on companies without any benefit for individuals, but more importantly risk stifling innovation and economic growth in Europe.

We believe that the review should be guided by a fundamental principal of the EU, namely the notion of the rational and informed consumer. Any over-protective regulation will convey a perception of a consumer who is vulnerable and ultimately unable to navigate through life without the encompassing protection of the government. We are certain that such extensive notion is not intended by the EU. However, in our understanding of the proposed Regulation there are traces implying this perception. Furthermore, the far reaching powers that the proposal attributes to the European Commission through the instrument of "delegated acts", which would apply in a number of key areas, will entail legal uncertainty.

Given the direct impact of data protection rules on the information and communication technologies (ICT) sector, which is a well-established industry in Luxembourg, we would like to comment on some key issues under discussion, which we feel need to be clarified and refined to allow the new Framework to achieve its objectives and be workable in practice.

1. Territorial scope, DPA jurisdiction, one-stop-shop feature

Fedil strongly supports the introduction of a “one-stop-shop” approach with respect to the competence of the Data Protection Authorities (DPA), which is particularly crucial for multi-national companies with separate legal entities and different business lines operating in several Member States. This will reduce complexity and administrative burden for companies as they will have to interact with only one single DPA - the authority in the country where they have their main establishment. Coupled with the so-called “consistency mechanism”, this will help ensuring a consistent application of data protection rules across Europe. However, we feel that in order to achieve a true one-stop-shop and avoid confusion over the determination of the “lead DPA”, proposed definitions of the “main establishment” need to be clarified further. This concerns also the mutual cooperation aspects between DPAs.

a. Clarification of the “main establishment” concept

A clear understanding of the term “main establishment” is crucial as it is the decisive factor for determining which DPA should be the lead authority. We take the view that the proposed terminology is too vague, leaving too much room for diverging interpretation. In this respect, we concur with the Article 29 Working Party, which in its recent opinion 01/2012 on the data protection reform proposals has emphasised that the proposed rules require clarification.

Under the proposed definition, the term „establishment“ could be interpreted differently and therefore result in an inconsistent or more burdensome application of the one-stop-shop feature than intended. In order to avoid unnecessary confusion for businesses and DPAs as well as satisfy the need for legal certainty, the establishment definition should be interpreted based on a limited set of objective criteria. Article 54 TFEU should be the relevant starting point for determining the location of an establishment, and this term should then be narrowed further in the Regulation to determine the “main establishment” for data protection purposes. In any case, it should be clarified that the designation of establishment for data protection compliance purposes should be without prejudice to such designation for other purposes of EU law (e.g., tax, insolvency, other compliance purposes).

The Regulation introduces different terms in relation to business operations (e.g. „management activities determining the processing purposes“, „central administration“, „economic activity“, „controlling undertaking“), which particularly for groups of undertakings makes it difficult to determine which of their entities is the „main establishment“ and may lead to several DPAs claiming jurisdiction over companies. For the sake of consistency and legal clarity for multinational groups of companies, we take the view that the Regulation should provide for a single uniform definition of „main establishment“, applicable across borders to controller and processor. Ideally, this definition should be based on a set of relevant objective criteria, which a group of undertakings can choose from in order to officially designate its location of „main establishment“ as regards to the Data Protection Law. The affirmative obligation for businesses to self-assess their structures and declare the main establishment on the basis of objective criteria is essential for eliminating disputes over main establishment.

A similar concept has already been developed under current EU Data Protection Law, namely in relation to Binding Corporate Rules (BCRs), where the „lead“ DPA responsible for the evaluation and approval of BCRs is determined on the basis of objective criteria¹. Having set a precedent and for the sake of consistency, this concept could perfectly lend itself for the purpose of determining the place of „main establishment“ as regards to the data protection legal framework.

¹ European Commission’s DG Justice Guidance on how to designate the lead authority in the framework of BCRs, accessible here: http://ec.europa.eu/justice/policies/privacy/binding_rules/designation_authority_en.htm

The objective criteria for the determination of the „lead DPA“ should primarily be the location of a group’s designated European headquarter, which we understand to be the entity in the Union in which are placed certain corporate services, which for group purposes is typically considered as “shared corporate services” centre whose costs are charged to the line of businesses or borne by the parent group. They could also include, for instance, the entity within the group with delegated data protection responsibilities, the entity which is best placed, in terms of management, administrative functions etc., to deal with data protection matters, or the entity where most decisions in terms of processing operations are taken.

On the basis of such criteria, businesses should officially designate their place of „main establishment“ in the Union and such designation should apply to all entities that are part of the group established in the Union. The Regulation should also clarify that the lead DPA for the company’s main establishment should be competent to supervise all the processing operations carried out by all entities of the group as far as they are subject to the Regulation.

We propose designation of the main establishment to be accomplished through a regular filing by the controller or processor with the relevant DPA. In order to ensure legal certainty and transparency, such designation should have binding effects for a specific period (e.g. three years) with exceptions and transitional rules for changes in the main establishment due to events that are unrelated to data protection compliance jurisdiction, e.g., takeovers, mergers, acquisitions and/or insolvencies. Such information would be available in real-time on a database shared by DPAs.

We do not believe that the proposed approach would lead to forum shopping for data protection purposes given all the other factors which are related to the group’s decision where to locate its headquarters entity. On the contrary, we believe that such a single, consistent definition of „main establishment“, to be used for all situations, would provide the required level of legal certainty to the benefit of individuals, companies and DPAs alike. Furthermore, as the legal instrument proposed by the Commission is a regulation, the rules regarding data protection will be fully harmonised across the EU and there will be no space for regime shopping.

Fedil’s recommendation:

We suggest aligning the „main establishment“ concept for the determination of the „lead DPA“ to the one developed in relation to Binding Corporate Rules. We propose that (1) groups of companies should be allowed to designate their location of „main establishment“ based on a set of objective criteria, particularly the location of the group’s EU headquarters; (2) such designation should apply to all entities that are part of the group established in the Union, and (3) a transparent and binding process should be established for such designation with dispute resolution mechanism for regulators and appeal possibilities for companies.

b. Clarification of the extra-territorial reach of the Regulation

According to Article 3(2), the scope of the Regulation extends to controllers established outside of the EU where the processing activities relate to goods/services offered to EU citizens or where their behaviour is monitored. We acknowledge that it is desirable to have companies based outside of the EU respect EU data protection standards when processing personal data of EU citizens. However, we would recommend clarifying the criteria determining the scope of application of the Regulation for companies not established in the EU.

The term “offering” of goods and services cannot in our view constitute a valid legal notion in the context of cross-border activities to determine the applicable law and jurisdiction. Companies may not know that their customers are European residents and if the mere fact of “offering” goods and services was the determining criteria, then they would be obliged to process even more personal data to identify whom of their customers are EU citizens. The EU jurisprudence² rather suggests that applicable jurisdiction needs to be determined based on the question whether a service is intentionally addressed to EU consumers or not, and that the terms „targeting” or „directing” carry more legal certainty. According to the ECJ, these notions involve objective criteria such as the use of a language or a currency other than the language or currency generally used in the country in which the trader is established with the possibility of making and confirming the reservation in that other language, the mention of telephone numbers with an international code, the use of a top-level domain name with the .eu suffix or other than that, of the country in which the trader is established.

Fedil’s recommendation:

We suggest clarifying that the Regulation applies to non-EU established controllers only when they have envisaged processing personal data of data subjects residing in the Union by amending Article 3.2. (a) to replace the word „offering” by „targeting” or „directing” goods or services and by clarifying in corresponding recitals that the mere accessibility of the controller’s website by a data subject residing in the Union is insufficient.

c. Clarification of “one-stop-shop” concept and DPA cooperation mechanisms

While Fedil explicitly welcomes the Commission’s proposals with respect to DPAs competence, we believe that further clarification is needed to ensure that the „lead DPA” can truly function and operate as a one-stop-shop. Contrary to the Commission’s declared objective, the enforcement system as currently designed would not allow for such a one-stop-shop and companies are put in difficult legal situations in case of a conflict between DPAs claiming competence for a specific case.

This is particularly true in the event of a conflict between DPAs as to a DPA’s lead role. In such cases, a dispute resolution mechanism should be implemented allowing the controller to put forward its viewpoint and arguments. With a view to reduce the legal uncertainty resulting from such situation, neither DPA should be able to issue or enforce decisions (including fines) against the controller until the conflict is cleared. The controller should have the right to appeal any decision taken with respect to a DPA’s lead role as the result of the conflict resolution mechanism.

Furthermore, the Regulation seems to limit the role of the „lead DPA” to the supervision of all cross-border processing activities of the controller and, where individuals in several Member States are affected, to the cooperation with the DPAs of those Member States as well as the coordination and the execution of joint investigations and enforcement actions. The role of the lead authority is unclear when another Member State’s DPA makes use of the powers granted by the Regulation (see Article 51 (1), 52, 53) and, for instance, based on a complaint conducts an investigation against a controller, whose main establishment is outside of this DPA’s territory. The Regulation is silent about any involvement of the lead authority in such cases and it is also not clear how far such a case would trigger the application of the consistency mechanism.

² Judgment of the Court (Grand Chamber) of 7 December 2010, Peter Pammer v Reederei Karl Schlüter GmbH & Co. KG ([C-585/08](#)) and Hotel Alpenhof GesmbH v Oliver Heller (C-144/09); Judgment of the Court (Grand Chamber) of 12 July 2011, L’Oréal SA and Others v eBay International AG and Others (Case C-324/09)

We take the view that the Regulation should clarify and strengthen the one-stop-shop concept by providing an obligation which would ensure that DPAs, who receive a complaint or wish to launch investigations for other reasons, are required to refer such matters to the lead authority and merely act as point of liaison. A real-time data base (accessible at least by all DPAs) should refer the lead DPA for each company. In any case, a DPA - not being the lead DPA- should not be able to launch actions against a company for which another Member State DPA acts as lead DPA. In such situation, the former should refer the matter to the lead DPA and hand over competence to the latter. The company should refer the matter to its lead DPA and should in no event be bound by actions or decisions taken by non-leading DPAs. As the case may be, the dispute resolution mechanism referred to in this section 1. c should apply.

Furthermore, we note that the „lead DPA“ and one-stop-shop concept as currently provided for in the draft Regulation does not apply to controllers who are not established in the EU, but would fall within the scope of the Regulation. The Regulation lacks rules on which DPA should be the lead in such cases, and consequently, such companies could be required to interact with any (or all) of the 27 DPAs depending on whether their processing operations concern individuals in their territory. In line with our proposal above, we would suggest closing this gap by granting non-EU established companies the right to designate a „lead DPA“, based on objective criteria to be further defined.

Fedil's recommendation:

1. Introduce a single uniform definition of „main establishment“, which is aligned with the concept used for the determination of the „lead DPA“ for Binding Corporate Rules and is based on a set of relevant objective criteria – particularly the location of a company's EU headquarter. Allow groups of undertakings to officially designate their location of „main establishment“ in terms of Data Protection Laws based on these criteria and ensure that such designation applies to all processing of all entities that are part of the group established in the European Union.
2. Make sure that the Regulation applies to non-EU established controllers only when they have envisaged processing personal data of data subjects residing in the EU by amending Article 3.2. (a) to replace the word „offering“ by „targeting“ or „directing“ goods or services.
3. Clarify and strengthen the “one-stop-shop” concept by providing for an obligation which would ensure that DPAs, who receive a complaint or wish to launch investigations for other reasons, are required to refer such matters to the lead authority and merely act as point of liaison.

2. Definition of personal data

The definition of personal data is a key concept triggering the application and enforcement of EU data protection law and entailing a number of obligations and liabilities for controllers and processors. Therefore, it is crucial that the definition is clear and future-proof.

The draft Regulation substantially extends the scope of data covered by it by defining personal data as “any information relating to a data subject who can be identified by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data or online identifier...”. As a result of this very broad definition, the Regulation is likely to apply to the majority of all processing operations, irrespective of the context of the data processing, the risk of identification and the risk of harm for individuals. Specifically, this broad approach raises concerns in several respects.

Firstly, the extension to “any other person” as a relevant reference point to determine whether an individual is identifiable means that any information relating to a data subject will be covered. As such, even anonymised data would have to be considered personal data as theoretically there may always be somebody who may have additional knowledge allowing for de-anonymisation, even if this is only the data subject who has encrypted its data. As there will be no secure way to anonymise data any longer, this effectively removes any incentive for privacy-enhancing measures such as encryption or hashing. Consequently, this broad approach to personal data runs counter the intended objective of the Regulation, effectively reducing individuals’ privacy protection, rather than increasing it, as companies might abstain from using or investing into privacy-friendly measures which are encouraged under Article 23 on data protection by design and by default.

This downside of the broad definition of personal data also becomes apparent in the context of consent. If every piece of information was to be considered personal data, then data subjects would continuously be confronted with extensive consent requirements and lengthy privacy policies. In consequence, granting consent would become an automatic reflex as hardly any service could be provided without the data subject dealing with data protection issues. The line between relevant and irrelevant aspects of data protection issues would become increasingly blurred, thus rendering the whole concept ineffective.

Secondly, the fact that Article 4(1) enumerates factors such as identification numbers, location data, online identifiers etc. as examples of personal data, suggests that these are deemed per se as relating to a data subject, thus qualifying automatically as personal data. By contrast, Recital 24 rightly clarifies that identification numbers, location data, online identifiers etc. cannot categorically be considered as personal data rather that it is dependent on the circumstances whether an individual can be identified on the basis of such factors, and where it cannot, these should not be considered personal data. We concur with this clarification as it recognises the inherent nature of such identifiers. For example, while website operators are generally not able to identify a person on the basis of the IP address, ISPs usually are. Similarly, if IP addresses are processed in combination with other personal data for certain purposes (anti-money laundering for example), they may be collected in an isolated fashion for advertising purposes. If all identifiers were to be qualified automatically as personal data, this would likely lead to a situation where a multitude of harmless processing operations would be subject to the requirements of the Regulation, causing additional administrative burden for businesses and supervisory authorities with no additional benefit for data subjects.

We urge EU decision-makers to abstain from such a broad „one-size-fits-all“ approach. Instead, the focus should be placed on the context and risk of processing to ensure that only those processing operations are captured, when there is a realistic risk of identification, and which involve a risk of harm to individuals. We suggest deleting reference to „any other person“ and clarifying that data will be considered personal if it is reasonably likely, given the context of processing, the means available to the controller as well as his intention to identify an individual, and that the controller is able to use the information for personal identification purposes. If there is only a remote, highly theoretical risk of identification, particularly because appropriate technical and organisational measures have been taken to minimise the risk of identification, then such data should not be treated as 'personal data'. Further criteria to be taken into consideration are the degree of risk of harm to individuals and the likely extent of that harm. More sensitive situations, with greater risk of harm and/or greater impact of this harm, would require greater precautionary measures in relation to the data than less sensitive ones. The introduction of such combined criteria, i.e. a subjective intentionality criteria coupled with the objective element of the context of processing, will allow focus on the really relevant data processing operations and will incentivise businesses to continue investing in privacy-friendly techniques and procedures. Furthermore, we believe that further clarification is needed regarding the status of anonymised, pseudonymised and encrypted data as non-personal data, particularly where appropriate industry standards and best practices or

recognised certifications are used to secure data. At a minimum, the ideas reflected in recitals 23 and 24 that the context is a relevant factor and that anonymised data is not personal data, should be expressly reflected in Article 4.

Fedil's recommendation:

Limit the scope of "personal data" by deleting reference to "by any other natural or legal person" from the definition and by introducing a reference to the context of the data processing, the risk of identification and the risk of harm for individuals. Amend Article 4 to reflect that anonymized and pseudonymized data are not to be considered personal data.

3. Consent requirement

Consent is one out of six legal grounds for processing personal data. Fedil considers that this important principle needs to be implemented in ways that are both appropriate for data subjects and companies and do not unnecessarily disrupt the use of a service. However, the current text proposed in the draft Regulation heightens consent requirements and introduces additional burden and more ambiguity.

More specifically and taking account of the specificities of online businesses, we consider that the requirement for consent to always be "explicit", irrespective of the context for which consent is being obtained or the risks involved in the processing operation for data subjects, is too formalistic and rigid, creating practical problems in the off-and online environment without adding anything to users' data protection. We take the view that the "explicit" consent requirement should instead be replaced by a context-based approach, which has the benefit of being more flexible as it takes into account the content and risks of a specific data processing operation. In light of the notion of an informed consumer we also deem it more relevant to focus on transparency with respect to the usage of personal data. A formalistic check-box approach would generally only result in an automatic reflex by the consumer, which ultimately does not lead to an increase in awareness, rather to the contrary.

Consent can in fact be inferred or implied from the action of requesting a service. For example, this is the case when a mobile user gives consent for being geo-located when requesting restaurant recommendations nearby. Yet, even if such action or behaviour is clear, it may not meet the threshold of "explicit" consent insofar as consent which is implied from behaviour is by definition "implicit": if we consider the situation of requesting a service based on geo-location data, the user's consent for processing such data is informed and implicitly given at the time of the request. The insistence on explicit consent for such a broad range of situations is also likely to lead to a "trivialisation" of the experience for data subjects. If they are asked to take affirmative action too frequently, they are likely to have trouble differentiating between the relative importance of different situations. The best way to guarantee meaningful consent is therefore in our opinion to allow for context-based consent.

Fedil would also like to question the notion of "significant imbalance" between data subject and controller in the context of consent (Article 7(4)) as it leads to significant legal uncertainty. We consider that the language proposed by the Commission is too broad and could actually miss its target. There is the risk that the utility of consent will be significantly restricted, as there is rarely an equal bargaining power between individuals and businesses. For instance, one could claim that there is significant imbalance where an individual relies upon the usage of a service for his business, therefore leading to some kind of dependency to this relationship. It would be excessive

to qualify such common examples as imbalanced and prevent usage of consent as a legal ground for processing personal data. As there are too many situations where one could claim an imbalance between the data subject and the controller, we believe this objective is better addressed on a case-by-case basis through the requirement that consent shall only be valid if it is “freely given”, in the definition of consent (Article 4(8)).

Fedil’s recommendation:

1. Guarantee meaningful consent by replacing „explicit“ consent requirement by a “context based approach” which takes into account the content and risks of a specific data processing operation.
2. Delete Article 7(4) which forbids the use of consent as a legal ground for processing personal data in case of „significant imbalance“ between data subject and controller.

4. Introduction of a new set of rights for data subjects

Fedil supports the idea that in order to guarantee trust and security in the Digital Single Market and to take into account new technological trends, the current set of data protection rules needs to be modernised. This should be done in a way that can be easily implemented by companies, that is technologically neutral and that does not create unnecessary obstacles for future innovation in the EU to the benefit of citizens.

In that respect, we would like to comment briefly on some of the key changes proposed by the Commission.

a. Right to be forgotten

While Fedil is generally supportive of a right to be forgotten as such, we believe a certain number of safeguards should be put in place in order to make it meaningful for users, workable for data controllers and enforceable by supervisory authorities.

We understand the term has been designed primarily for users of online services, particularly social network services. We do not want to put into question the relevance of a general deletion right in the “offline” world if such an obligation is compatible with other EU or national legislative instruments that companies have to comply with.

The Regulation should however not create false expectations for European citizens by making them believe that there are no risks involved in sharing or publishing information about themselves, as they can always revert to the right to be forgotten mechanism at a later stage. This may eventually prove counter-productive for the protection of data subjects considering that deletion of information published on the web is not always technically feasible. In addition, we believe that this right should not be designed as an absolute right given that other legitimate interests are often at stake which must be balanced with the right to be forgotten. Data controllers may indeed have many perfectly legitimate reasons “not to forget” users’ personal data, including for fraud detection, anti-money laundering purposes or other legal retention obligations. Many regulatory and best practice requirements compel preservation of records. As an example, banks are required to retain identification documents (which include, amongst others, the customer’s surname and first name, date of birth, full address, profession and reference number and date of the official identity document) for a period of at least five years beginning at the end of the business relationship with

the customer³. We therefore welcome the safeguards listed in Article 17(3) and (4), which rightfully limit the scope of its application to data that are not required to be retained by controllers for compliance purposes. However, we suggest clarifying the scope of the right to be forgotten by specifying that the controller's obligation to "forget":

- applies only where "forgetting" is technically feasible and does not involve disproportionate efforts from the controller;
- is technology neutral and may be complied with by appropriate means and protection techniques equalling deletion (e.g. rendering data anonymous or otherwise unusable, unreadable, indecipherable).

We appreciate the precautions surrounding the application of the right to be forgotten. However, in addition to the above, we are concerned by the requirement for controllers to take all reasonable steps to inform third parties about the request to erase any links to, copies or replications of the data. Article 17(2) does not seem to take account of the nature of the Internet and the ICT sector in general. When operating online, our member companies do not grant any kind of formal authorisation to third parties to publish information that has been made public on their website; once it is publicly available, they do not have any control on how this data are treated by third parties (they may be transferred, duplicated etc.). For the great majority of online services, this requirement would mean that controllers would have to look for every potential copy of any data that has been published on its website, which would practically amount to an obligation to police the Internet. Eventually, there are no obligations whatsoever for third parties that have been informed of the data subject's request to be forgotten to take any action for deleting his/her data. Article 17(2) does not bring any meaningful value to the right to be forgotten, on the contrary, the lack of clarity may lead to enforcement discrepancies, difference in the way users are treated from one platform to another and of course to a high degree of legal uncertainty for companies trying to translate this into practice.

Fedil's recommendation:

1. Clarify in Article 17(1) that the controller's obligation to "forget" only applies where this is technically feasible and does not involve disproportionate efforts, and may be complied with by appropriate means and protection techniques with equivalent effect to deletion.
2. Delete Article 17(2). At a minimum, it should be clarified that this requirement only applies when the controller has proactively made the data available to third parties, with which he has a contractual relationship.

b. Right to data portability

Article 18 of the proposed Regulation requires controllers to make data portable so that it can be transmitted from one controller to another "without hindrance from the controller from whom the personal data are withdrawn" (Article 18(2)). Fedil supports the rationale underlying the portability provision, which is to give individuals control over their data. However, we are concerned that due to its wide scope and in particular the requirement to make the data transferrable, this provision may have detrimental effects to both data subjects and data controllers.

³Directive 2005/60/CE on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing

Firstly, we believe that data which has to be retained by the controller for compliance reasons should be excluded from the scope of the portability provision. Article 18 does not foresee any safeguards limiting the right to request transmission of such data to another service. Article 18(2) even explicitly mentions that the personal data must be “withdrawn” from the initial controller. We take the view that Article 18 should include a paragraph limiting the applicability of the right to data portability in situations where the data concerned must be retained for compliance reasons with a legal obligation by EU or Member State law to which the controller is subject.

Secondly, while we appreciate the Commission’s intention to allow users to switch from one service to another as easily as possible, we take the view that data protection legislation is the wrong place to address such an issue. More important, imposing standards for electronic format, modalities and procedures for the transmission of personal data through EU legislation would both hinder competition and innovation in the online industry, which develops and uses many different kinds of mechanisms and formats for data export. Fedil acting as a multi-sector business association also wonders what would be the impact of these provisions on offline companies.

Finally, imposing the right to data portability for any type of personal data risks killing any incentive for economic operators to create new algorithms and offer innovative services to their users. The end result would be a homogeneous landscape of services combined with a decrease in research and innovation, hence less functionality and service quality, thereby frustrating user experience. Our proposed solution would be to differentiate between user-generated data that are uploaded by data subjects themselves (such as name, date of birth, email address and so on), and data that are the result of their interaction with the service providers. Such information carries significant commercial value and is being created by algorithms that are proprietary assets of the data controller. If this was perfectly transferable on a standard basis, there would be a risk that service providers would lose important competitive leverage.

Fedil’s recommendation:

1. Clarify that the scope of Article 18(1) does not cover situations where data has to be kept by data controllers for compliance purposes.
2. Delete Article 18(2). At a minimum, restrict the scope of Article 18(2) to user-generated data only.
3. Refrain from imposing standards for data transmission by deleting reference to „electronic format which is commonly used“.

c. Profiling

We appreciate the Commission’s proposal regarding profiling as expressed in Article 20 of the draft Regulation and understand this to be the regulatory response to recent debates and concerns generated by the increased use of profiling techniques, particularly in the online environment. However, we would caution against the attempt to entrench an overly negative perception of profiling by means of special regulatory treatment of all forms of profiling irrespective of the objectives pursued. Naturally, as with any business process, automated profiles can be used to achieve aims that are undesirable and that may not be in the interest of consumers. However, the proposal seems to neglect the fact that there are many positive uses of profiling, which are actually welcomed by users. The aim of most profiling techniques is in fact for businesses to better understand customers’ needs and provide them with better products and services. Profiling is therefore an important aspect of a competitive online marketplace. For instance, profiles are frequently used to satisfy consumer demand for technologies and services that remember their preferences, such as their native language or home country. Profiling is often the basis for a

customised shopping experience on online platforms, which is specifically tailored to the interests and needs of customers. It also helps to improve the services rendered to customers by online platforms. Furthermore, profiling is often part of a risk assessment process in certain industries, for instance to assess solvency/credit-worthiness of customers by online traders and financial institutions or to detect and prevent fraudulent behaviour in electronic payment systems. Profiling is an important tool to guide consumer behaviour as regards to energy efficiency and energy savings and hence contribute to achieve environmental goals, for instance through smart metering and smart grids.

We fear that Article 20, as currently drafted, will subject a number of legitimate practices with little privacy impact to overly strict obligations, for which there is no real need given the many safeguards that are already contained in the draft Regulation.

Consequently, rather than discouraging the use of profiling mechanisms as such, the focus of rules regulating profiling should be based on the purposes for which profiles are used and the degree of impact/consequence for the individual of such purpose. The Regulation should be amended to clarify that the controller's legitimate interest can provide a valid legal basis for the use of profiling techniques, particularly where it concerns fraud prevention, security purposes etc. Profiling should also be acceptable for beneficial purposes such as providing personalised and customised Internet experiences to users, while the strict requirements of the profiling provision should be reserved particularly to special categories of data (i.e. sensitive data). Such clarification would satisfy the need for legal clarity and consistency, ensure that the Regulation lives up to its objective of providing technologically neutral data protection, and strike an appropriate balance between protecting the rights of individuals and safeguarding innovation and commerce.

Fedil's recommendation:

Clarify that the controller's legitimate interest can provide a valid legal basis for the use of profiling and limit strict requirements of the profiling provision to special categories of sensitive data.

5. Data breach notification obligations

Data breaches and cybercrime are growing challenges for society. In that respect, a system that allows DPAs to be better informed about breaches is a key element in protecting personal information.

The proposed Regulation introduces new provisions on data breach notifications. All industry sectors are obliged to notify all data breaches to the DPA without undue delay and, where feasible, no later than 24 hours after having become aware of the breach. Controllers must also notify data subject where the breach is likely to adversely affect the protection of their personal data or privacy.

Fedil is concerned that the current wording may lead to over-notification to DPAs and will overall prevent effective implementation of rules by controllers and DPAs alike.

A mandatory notification requirement to DPAs for all breaches, even minor ones, will significantly increase the number of notifications as controllers will report every breach. The 24-hour deadline is problematic as it does not provide sufficient time to fully assess the nature of the breach, its impact as well as the most appropriate solution to tackle the effects of the breach. There is a risk that the

provision as proposed will impose significant compliance burdens not only on controllers but also on DPAs and trigger “notification fatigue” amongst consumers.

The aim of data breach notification rules should be to promote best practices in raising data subjects’ awareness about a breach, providing them assurance that their personal data is handled in a secure and safe fashion and to propose appropriate solutions. A workable system should therefore be based on a threshold that is itself based on the concept of “significant risk of serious harm” for the notification to data subjects and hence oblige companies to notify breaches to DPAs in a reasonable delay instead of a 24 hours’ notice (thereby ensuring consistency with the breach notification requirement stipulated in the e-Privacy Directive). The notification obligation should only apply in limited cases, e.g., where disclosure concerns sensitive data, data covered by a professional secrecy or where a significant number of data subjects are concerned. Furthermore, breach notification rules should allow for an exemption to notify breaches when technical protection measures have been implemented to render the data unintelligible. We believe that such a system, as it is currently in effect in e.g. Germany, leads to a more risk-adequate balance.

Fedil’s recommendation:

Introduce a workable system for data breach notification based on a threshold that is itself based on the concept of “significant risk of serious harm” and that obliges companies to notify breaches to DPAs in a reasonable delay. Delete reference to the 24 hour notice deadline.

6. Administrative obligations for controller and processor

Fedil considers that the accountability principle is a very useful concept that can have a positive impact on companies’ behaviour as it encourages controllers and processors to put consumers’ privacy high up on the agenda, be responsible and accountable with respect to existing privacy risks and put in place policies and processes to mitigate those risks. Accountability can be effectively implemented by taking an ex ante rather than an ex post control approach, thereby reducing the burden on businesses and DPAs, and by granting benefits to companies demonstrating a responsible approach to privacy, which will incentivise the use of privacy enhancing measures (“Privacy by design”).

However, we are not convinced by the manner the accountability principle has been incorporated into the Regulation. Indeed, Fedil regrets to see that the Commission proposal is very prescriptive and lacks flexibility. Instead of encouraging the use of privacy enhancing measures, thereby reducing the administrative obligations on controllers and processors, it introduces new and onerous requirements that will substantially increase disproportionate administrative burden for businesses without any regard to the potential privacy risks.

This concerns in particular controller obligations regarding:

a. Documentation, privacy impact assessments and prior consultations and authorisations

The proposed Regulation replaces the current obligation to notify all processing operations to the DPA with a requirement for detailed documentation as well as requirements to conduct privacy impact assessments and obtain prior clearance from DPAs, thereby creating a system that is

significantly more burdensome for both controllers and processors than the initial notification requirement.

The proposed documentation obligations are very detailed and the Commission is mandated to lay down standard forms for the documentation. We stress that data processing can be documented well in many ways and no specific method should be mandated. The obligation is disproportionate since it covers almost all processes. Documenting will be a very extensive process, especially when joint responsibility is introduced. The obligation will trigger high costs, also for low-risk processes. Therefore, Fedil asks for the introduction of exceptions for low-risk processes, as they may be encountered in many business sectors and activities.

Furthermore, prescriptive provisions on privacy impact assessments risk create a rigid approach to data protection without any consideration of the risk associated. The proposed provisions on privacy impact assessments and prior consultations increase the administrative burden on businesses and supervisory authorities alike but also on consumers without reflecting the good practice of planning and assessment work done by companies. There should be no prior consultation obligation for data processing, which according to the assessment is in compliance with data protection legislation. Also the obligation to consult data subjects or their representatives should be deleted as it could e.g. risk the confidentiality of information and trade secrets.

b. Data protection officers

The proposed Regulation introduces an obligation for controllers and processors to designate a data protection officer (DPO) for companies employing more than 250 persons or where the core activities of the controller consist of processing requiring regular and systematic monitoring of data subjects.

While Fedil recognises that compliance with data protection rules is of utmost importance, these prescriptive and detailed provisions will be costly and burdensome, in particular for organisations (online and offline) where data processing forms only a marginal part of their activities,

In order to limit the cost of compliance and the administrative burden on companies, the appointment of a DPO could be linked with the benefit of an exemption from detailed documentation, impact assessment and pre-clearance requirements. An incentive for accountable controllers could also be a simplified system for international data transfer.

Fedil's recommendation:

Achieve a more efficient approach by balancing administrative obligations and companies' accountability, encouraging the use of "privacy enhancing measures" instead of introducing prescriptive new administrative measures.

7. International data transfers

We appreciate that, in recognition of the international dimension of many businesses, the proposal contains a number of key improvements that are aimed at making international data transfers easier for companies. These are essential elements in positioning Europe in a globalised economy based on a growing number of data exchanges. In that regard, Fedil welcomes the formal recognition of

Binding Corporate Rules (BCR) in the proposed Regulation as a means for complying with data protection rules in international data transfers within organisations.

Nonetheless, Fedil members feel that the new rules as proposed are a missed opportunity. Data transfers are still, except in the case of BCRs and standard contractual clauses, subject to prior authorisation from the lead DPA. A notification system would have been a much more efficient way to regulate data transfers by still providing appropriate safeguards for data subjects.

Moreover, we believe that it is necessary to revise and further simplify the regime of standard contractual clauses, which are an important instrument particularly in the context of cloud computing, where international data transfers occur on a regular basis. Where contractual clauses have been approved by the lead DPA in accordance with Article 42.2(d) no further authorisation from the DPA should be required, if the approved clauses are used by the controller as "model clauses" for further data transfers to other processors or recipients. Furthermore, we deplore that standard contractual clauses as currently designed in Commission decision 2010/87/EU can only be used in constellations when an EU-based cloud customer/user (i.e. the controller) makes use of processors (i.e. cloud providers) that are based outside of the EU, whereas these cannot be relied upon when a European cloud provider (i.e. processor), as the data exporter, wishes to enlist a sub-contractor who is based outside of the EU (for instance in order to make use of their storage capacity). In addition, agreements which are based on those standard contractual clauses are only effective if directly signed by the controller and the processor established in the third country. This does not take account situations where there is more than one provider involved in the delivery of cloud solutions. In fact, in today's reality, a growing number of cloud solutions made available by cloud service providers are bundled products of services delivered by multiple, globally located independent vendors of service solutions. This ever-increasing globalisation of product delivery processes requires an adaptation of the legal framework for standard contractual clauses allowing for a "sub-contractor" regime that also applies to the export of personal data in third countries without the direct involvement/consent of the controller.

In addition, we believe that international data transfers could be further facilitated by means of the data protection officer, an instrument that has been introduced in the draft Regulation as a mandatory requirement for larger companies with a view to reinforce accountability of those processing personal data. We believe that companies, who live up to these enhanced accountability requirements by nominating a data protection officer, should be rewarded by relieving them from any further administrative requirements for data transfers. For instance, they should be allowed to transfer data without any further authorisation from or notification to the lead DPA.

Considering all the strict safeguards that the draft Regulation imposes on controllers, notably in terms of accountability, we believe that a more self-regulatory system for data transfers to non-EU/EEA or assimilated countries would be justified and appropriate. It is our firm belief that data protection goals are best served if adequate data security measures are in place in order to technically prevent most, if not all of the risks that texts and contracts also seek to avoid.

Fedil's recommendation:

Further simplify administrative constraints on international data transfers through better use of instruments such as the regime of standard contractual clauses or a more self-regulatory system for companies who have reinforced their accountability.

8. Cloud computing – Definition, responsibility and liability

Data protection is one of the main reasons why many companies are hesitant to make use of cloud services. The uptake of new technologies such as cloud computing in Europe will therefore depend very much on whether the new EU Data Protection Framework is sufficiently clear, workable in practice and designed to accommodate the realities of the cloud business environment. For the development of cloud services and the promotion of new cloud business models, it is crucial that actors operating in the cloud know if and to what extent they are subject to EU data protection obligations, how responsibilities and liabilities in terms of privacy protection are to be allocated between them and that the burden placed on the different parties is appropriate to their respective roles in the business ecosystem.

We take the view that the proposed Data Protection Regulation, particularly the rules relating to the controller/processor concept and the respective distribution of responsibilities and liabilities, structurally do not cater for many types of cloud computing services and we are therefore concerned that it will impede rather than promote their further development in Europe.

a. Controller/processor concept

The draft Regulation maintains the traditional controller/processor concept, defining a controller as the entity which determines the purposes, conditions and means of processing of personal data, while the processor is understood to be the entity that processes personal data on behalf of the controller. This concept is critical as it determines the obligations and liabilities in terms of data protection compliance. The status of a cloud service provider (CSP) as controller or processor will depend on the context and the nature of his relation with data subjects. However, as a general rule, CSPs tend to be commonly characterized as processors, while cloud customers/users are usually qualified as controllers.

Considering today's sophisticated cloud environment with many different business models, multiple actors and layered arrangements between providers, this static categorisation is unsuitable and therefore very difficult to apply in practice. In fact, a number of CSPs should not even be qualified as processors given that their services are fundamentally different to those of a standard processor. Indeed, depending on the nature of the service offering, CSPs host and give access to infrastructure facilities (IaaS), such as processing power, storage, networking equipment and other basic computing resources, to software development tools for the creation and deployment of customised applications (PaaS), or to software solutions (SaaS), which are used by the cloud customer/user for purposes that are usually unknown to the CSP. The processing of data happens in a fully automated way, within the limits of the offered cloud solution and under the sole and full control of the cloud customer/user, as most cloud solutions are delivered with the required management tools.

Unlike traditional processors who access and manage data for the controllers, CSPs are ultimately data-agnostic. Their view on the data is restricted to an absolute minimum and usually their access possibilities are strictly limited to the system data in order to be able to manage the user accounts and provide a proper support service. For example, a provider of an online web hosting solution manages and bills the subscriptions of his customers. He does not supervise the type of user content uploaded and published on the website. Particularly IaaS providers regularly do not know whether information stored on or processed through their infrastructure is "personal data" and they usually have no control over or ability to access that data, nor do they require such knowledge or access to provide their services. This is also obvious with respect to the emerging cloud broker business, where cloud service brokers are just reselling access rights without being involved in the

hosting and/or management of the cloud solution they give access to. Furthermore, a growing number of cloud solutions include encryption tools that encrypt the user content even before being submitted to the CSP or feature other appropriate technical and organisational measures in order to prevent access to the data by anyone other than the cloud customer/user. In these situations, nobody besides the cloud customer/user himself can process, access or even display his content. Hence, assuming that the CSP is always directly involved in the processing and has access to or even has a view on the data processed via the cloud solution he is providing, is not reflecting the realities of today's cloud industry.

The examples listed above show that CSPs, particularly where they do not have knowledge as to the nature of the data on their infrastructure and/or do not have the practical ability to access such data, cannot reasonably be considered as processor. They should rather be qualified as neutral intermediaries, unless the CSP takes measures to accessing or using the personal data in breach with its contractual obligations or in excess of its authority in relation to that data (in which case it is justified to consider such provider a controller who should be liable as such).

We therefore suggest revision of the definitions of "controller" and „processor" so as to allow for a more nuanced and balanced approach with a view to accommodate the specificities of new technologies and business models. The draft regulation should provide for different actors with varying degrees of obligations and liabilities under the data protection law.

b. Allocation of responsibilities and liabilities between controller and processor

EU data protection law has so far always been governed by the basic principle that the controller has primary responsibility for complying with legal privacy obligations and faces primary liability for any data protection law breaches. The controller may use another entity to process personal data on his behalf. However, he remains the exclusive point of contact for data issue related claims and vis-à-vis DPAs. Conversely, with a view to enable the controller to comply with his privacy obligations, the processor is required to act on the controller's instructions only and the controller's obligations need to be laid down in a written controller-processor contract. Processors are not normally directly subject to the data protection regulatory framework; their responsibilities and liability is strictly limited to what has been contractually agreed with the controller.

While the draft Regulation continues to place the onus for compliance primarily on the controller, it considerably extends the responsibilities of data processors (see Articles 24, 26, 27 and 28), thereby further blurring the initial distinction between controller and processor, ignoring the complex contractual set-up between these players and the limited access/control possibilities processors often have over the data they process. Newly introduced obligations for the processor are for instance the requirement to assist the controller in carrying out data protection impact assessments, to obtain prior authorization or to consult DPAs, and to maintain, in addition to the controller, detailed documentation of all processing operations. This increase in direct obligations imposed on processors is coupled with a new liability provision, whereby the processor is jointly and severally liable with the controller for damages, unless it can prove it is not responsible for the event giving rise to the damage.

We take the view that this extension of the processor's responsibilities and liability unnecessarily interferes in the contractual relationship between controller and processor, the aim of which is to ensure that processors undertake the required measures so that the controller can comply with his obligations. It further complicates the already complex relationship between controller and processor, leading to additional confusion and uncertainty and is even less compatible with new business models such as the cloud than the existing legal solutions. Many CSPs will not be in a position to comply with many of these additional obligations, because, as explained in previous paragraphs, they usually do not have access to the data or processing strategies, are not aware of

the nature of the data in their infrastructure, its importance to the cloud customer or the risks linked to it, and are hence unable to comply with detailed information requirements, conduct data impact assessments or make any determination as to the treatment of the personal data.

Furthermore, even if the CSP assists the controller at the moment of the service subscription, things might change over time, without the CSP being involved or being aware. This risk is greater when the cloud solution provides the option to store the user content outside of the hosting environment of the cloud solution. The user content only remains within the area of influence of the CSP for a very short period of time and can change from one login to the next. Any extension of the CSP's responsibilities regarding user content will expose him to unpredictable and unmanageable risks. As a result, CSPs will not be able to guarantee continual compliance with any regulation that allows the controller to transfer any kind of responsibility and accountability to the CSP.

In light of the above, Fedil would urge the EU legislator to revisit the controller/processor concept as well as the chosen allocation of responsibilities between them, and amend Articles 2.3, 4(5), 4(6) and Chapter IV of the draft Regulation accordingly. We suggest opting for a more flexible and nuanced approach, recognising that there may be different entities involved in the treatment of personal data and ensuring that each entity is only responsible and liable to the extent it has reasonable means of access to or control of the data. Providers, who do not have any knowledge as to the nature of the data they process or store on their network and/or who do not have any meaningful access to it, should not be classified as controller nor processor, but should rather be considered neutral intermediaries, and as such, they should benefit from the liability "defense" provisions as stipulated in Articles 12 to 15 of the E-Commerce Directive. For the rest, the parties should be free to allocate risks and responsibilities amongst them contractually.

Fedil's recommendation:

1. Revisit the controller/processor concept in Articles 4(5) and 4(6) and introduce other categories of actors with varying levels of responsibility and liability, in particular the category of „neutral intermediary“ for actors without any meaningful access to or control of data (with additional link to Article 2(3)).
2. Revisit the chosen allocation of responsibilities between controller and processor in Chapter IV. In particular, delete all reference to „processor“ in all provisions concerning the controller's obligations (Articles 28 – 34, 53, 75, 77 and corresponding recitals) and amend Article 26(2) to clarify that the obligations in this Article only apply where the processor is able to assist with reasonable effort and insofar as this is possible given the nature of processing.

Conclusion

As highlighted above, Fedil supports the approach chosen by the Commission to facilitate the free flow of information in the Internal Market, namely a fully harmonized single set of data protection rules applicable throughout the EU, coupled with a one-stop-shop enforcement mechanism. However, we urge EU legislators to revisit the rules on how to comply with general principles and consider providing for a true accountability-based approach that lives up to its name. Rather than being detailed and prescriptive, the Regulation should introduce real incentives for companies to act responsibly.

Fedil looks forward to working with the EU Institutions and Member States and to sharing our experience and expertise when it comes to the protection of personal data in the European Union and abroad. We would be happy to discuss these points and the broader revision of Directive 95/46/EC in more detail.

Luxembourg, 17th of July 2012

About Fedil-Business Federation www.fedil.lu

Founded in 1918, Fedil – Business Federation Luxembourg is today a multi-sector business federation representing the industry, construction and business services sectors among which the ICT industry. On a national level, Fedil’s objectives are to protect the professional rights and interests of its members, and provide analysis on any related economic, social and legal questions arising. On a community level, Fedil is associated with the Confederation of European businesses BUSINESSEUROPE (www.businesseurope.eu), and has a representative office in Brussels.



Insurance Europe comments on the ITRE draft opinion report

1. Consent

Insurance Europe welcomes the Rapporteur's proposed changes (AM 4 and 7) encouraging the appropriate use of consent as equal to the other grounds for lawful processing of personal data. Insurance Europe also supports changes proposed in relation to the withdrawal of consent, as outlined in AM 38.

However, Insurance Europe does not support the (new) Recital 33a (AM 5): This amendment unhelpfully introduces an implied hierarchy in the conditions of processing. It also includes references to terms that are legally uncertain, such as the "right context" and the "inappropriate context". Above all, the recital would restrict the consumers' ability to own their data and be able to give consent freely in order to enter into contracts or access services.

2. Significant imbalance

Insurance Europe believes that a high level of legal uncertainty surrounding the concept of "significant imbalance" remains in the text. Despite the proposed changes, the term could still be open to interpretation. The introduction of this term is not necessary, as existing contract law provides adequate safeguards for consumers.

Therefore, Insurance Europe asks for the deletion of Article 7par.4 of the proposed Regulation.

3. Profiling

Insurance Europe supports the Rapporteur's proposed changes to Article 20 (AM 71) to permit profiling when necessary in order to protect the right of other data subjects, such as for the purposes of fraud detection.

However, Insurance Europe further suggests that profiling should also be allowed when carried out at pre-contractual stage. The ability to access and process personal data through automated processing is central to the ability of insurers to determine at pre-contractual stage the level of cover consumers need, assess the risk and hence propose appropriate and fairly-priced products and services to consumers that reflect their needs.

4. Data Portability

Insurance Europe believes the Rapporteur's proposed amendments (AMs 66, 67 and 68) take into consideration the legitimate interests of businesses to protect their trade secrets. These amendments are a step in the right, giving businesses the flexibility to determine the most appropriate format for the transmission of personal data.

However, Insurance Europe believes that article 18 would have competition implications by unintentionally forcing insurers to disclose commercially sensitive information to competitors. The ability to change providers easily is a consumer and /or competition issue and should be dealt with under other relevant legislation at which point any data protection considerations can be take into account.

5. Administrative sanctions

Insurance Europe welcomes the Rapporteur's proposed changes (AMs 124 to 153) to Article 79 on administrative sanctions, in particular that sanctions are defined as a competence ("may impose") and not as an obligation ("shall impose") of Data Protection Authorities (DPAs).

Insurance Europe believes that sanctions for breaching the regulation as initially proposed by the European Commission are disproportionate. They do not leave any discretion to DPAs in relation to fines. For instance, DPAs are obliged to impose a fine even if the violation has not produced any damage to the data subject, or if it is a first violation without consideration of any other mitigating circumstances.

6. Delegated and implementing acts

Insurance Europe supports the Rapporteur's proposal to reduce the number of delegated and implementing acts in the draft Regulation (AM 20) as this will increase legal certainty.



Insurance Europe believes that a too high number of delegated and implementing acts creates legal uncertainty as it is impossible to predict the final content and interpretation of key provisions. The large number of delegated and implementing acts is even more worrying since the chosen legal instrument, a Regulation, is directly applicable.

7. Data breach notification

Insurance Europe welcomes the abolition of the 24-hours breach notification and the introduction of the notions of "reasonable time period" and "undue delay" when the breach seriously threatens the rights or legitimate interests of the data subject (AMs 14, 88 and 90).

Indeed, Insurance Europe believes that any excessive notification requirements, as proposed in the draft Regulation, could lead to consumer apathy. Excessive notification would also distract data protection authorities from their important role of investigating serious breaches and, where necessary, from taking action. This would not be in the public interest.

8. Additional comments

In addition to these comments, Insurance Europe would like to share again its key messages (see attachment) addressing the issues of fraud, the right to be forgotten, the right to withdraw consent and the definition and processing of health data.

A. *Data protection legislation needs to take into account that processing data is at the core of insurance business*

Processing data enables insurers to assess the risks appropriately and thereby provide consumers with the appropriate insurance cover at a premium reflecting fairly their needs and risks.

Restricting insurers' ability to process data will have negative unintended consequences for consumers and insurers, such as delays for car accidents' compensation or insurers' inability to determine the right amount of medical treatment reimbursements.

- Any changes to the EU data protection legislation should be proportionate, balancing the individual's Right of Privacy with data security and taking into consideration the insurance market realities.

B. *Rules on consent should be mutually beneficial: protecting consumers while permitting insurers to deliver necessary services*

Definition of consent

Based on insurers' experience across member states, consumers do not encounter problems with the current rules on consent in Article 2(h) of Directive 95/46/EC on data protection.

- The Directive 95/46/EC rules on consent should be maintained in the new proposal.

Right to withdraw consent

The proposed data subject's 'right to withdraw consent' will:

- (i) hinder the execution of the insurance contract
- (ii) lead to a cancellation of the contract not foreseen by the parties
- (iii) conflict with other legal instruments, eg the Anti-money Laundering Directive 2005/06/EC

- Article 7par.3 should take into account situations where data must be:

- (i) retained for the conclusion and execution of insurance contracts and
- (ii) processed for regulatory, anti-fraud or legal purposes.

Right to be forgotten

The proposed data subject's 'right to be forgotten' seems to be designed to apply to pure internet services (ie, social networking). However, exercising this right in an insurance contractual relationship will bring unintended consequences. Concretely, insurers will be obliged to delete the consumer's personal data upon her/his request, despite it being vital for insurers to hold consumers' data to fulfil their legal obligations and provide services reflecting consumers' needs and risks.

- Article 17 should clearly state that the right to be forgotten does not apply where:

- (i) there is a contractual relationship between an organisation, such as an insurer, and an individual
- (ii) data is needed for the contract's performance
- (iii) there are regulatory requirements to retain data
- (iv) there is a need to retain data for fraud prevention purposes.

C. *Insurers have to process health related data to provide consumers with certain insurance products and services*

The proposed definition of health data is too broad. Treating administrative data as sensitive is disproportionate and will add administrative burden on consumers and insurers for all insurance products requiring health data processing, such as health, travel or motor insurance.

- The health data definition should be restricted to clinical and medical information, excluding administrative information. Administrative information should be categorised as non-sensitive data. Therefore, the sentence “*or to the provisions of health services*” should be removed from Article 4(12).

Processing data for insurance purposes

Processing sensitive data is imperative for insurers. It is crucial to clarify that the conclusion and execution of insurance contracts, including the management of health care services and settling claims in the health insurance system, is permissible.

- It should be clarified that insurance does fall under either Article 81 or Article 9par.2 (h). Equally it should be clarified that the scope for collecting and processing health data applies to all insurance purposes, for example health, life, accident, third party liabilities insurance and reinsurance.

D. *Preventing and detecting insurance fraud is essential to protect honest consumers*

Restricting the use of data will also restrict insurers’ ability to process information needed for fraud prevention and detection. As a result, the honest consumers will have to pay the price.

- The proposed Regulation should explicitly recognise the need for organisations, including insurers, to process and share information to prevent fraud.



Uachtaránacht na hÉireann ar
Chomhairle an Aontais Eorpaigh
Irish Presidency of the Council
of the European Union
eu2013.ie



OIFIG AN AIRE DLÍ AGUS CIRT AGUS COMHIONANNAIS
OFFICE OF THE MINISTER FOR JUSTICE AND EQUALITY

Informal Justice and Home Affairs Ministers' Meeting

Dublin 17 - 18 January 2013

Discussion Paper – Session III (Justice)

Data Protection – certain key issues

Household exemption

A minority of EU citizens had access to personal computers, mobile phones and Internet when the Data Protection Directive was adopted in 1995. The opposite is now the case. In 1995, individuals were, by and large, passive subjects of the processing of their data in data bases. Today, they voluntarily supply large amounts of personal data when purchasing goods and services on the Internet and using other online services. And many of them, especially young people, actively publish and share personal data about themselves and, frequently, about other family members and friends on social networking sites.

These developments call into question the traditional concepts of data subject, data controller and data processor and blur the dividing lines between these traditional roles. The data protection implications of these developments pose a challenge for policy makers and regulatory authorities.

Under the 1995 Directive, the processing of personal data “by a natural person in the course of a purely personal or household activity” is excluded from its scope. The European Commission has recognised the need to continue to exempt certain types of domestic data processing from the proposed Regulation: article 2.2(d) provides that the Regulation will not apply to the processing of personal data by a natural person “without any gainful interest” in the course of his or her own “exclusively personal or household activity”.

This provision seeks to draw a line between those processing activities which are personal and those which are commercial in nature. The exemption will not apply, therefore, if an individual has a “gainful interest” or if the activity is not “exclusively” of a personal or household nature. For example, if an individual decided to sell a

musical instrument or rare book online, he or she would fall outside the scope of the household exemption and the provisions of the Regulation would apply.

Therefore the Presidency invites Ministers to discuss—

- whether the scope of the proposed household exemption is correctly or too narrowly defined in article 2.2(d);
 - if too narrowly defined, in what way the scope should be extended; for example, by replacing “gainful interest” with “professional gainful interest” and by taking into account the frequency or occasional nature of the activity.

Right to be forgotten

Building on the data subject’s existing right to erasure of personal data, article 17 of the Regulation provides for a new “right to be forgotten”. The objective is to ensure that individuals have the power to require controllers that store their personal data to erase them once they are no longer needed for any legitimate purpose. It will mean that if an individual no longer wants his or her personal data to be processed – especially data supplied while he or she was a child – and there is no legitimate reason for keeping them, the data must be erased from the controller’s system.

This new right takes account, in particular, of evolving technologies and practices and addresses the risks of possible financial, reputational or psychological detriment to data subjects in the context of social networking sites.

Where the data have been made public, the Regulation requires the controller to take “all reasonable steps, including technical measures” to inform third parties that may be processing the data of the data subject’s request to erase any link to, or copy of, the data concerned. This limited obligation takes account of the fact that in many cases the initial controller may have no power or influence over the third parties to whom the data have been disclosed or, in the online world and in particular in the context of social networking, may not know the identity of those to whom the data have been disclosed.

As recognised in article 17(3)(a), issues may also arise in relation to balancing this right against other rights, such as freedom of expression. And it is not entirely clear how this right is intended to apply where more than one data subject is involved, e.g. in the case of a photograph featuring several individuals.

Therefore the Presidency invites Ministers to discuss—

- whether they support a strengthening of the existing right to erasure in the form of the new “right to be forgotten”;
 - if so, whether the obligations imposed on data controllers arising from the “right to be forgotten” are reasonable and feasible.

Administrative sanctions

Apart from their liability to pay compensation to data subjects, article 79 contains detailed proposals for the imposition of fines on individuals and legal persons for intentional or negligent infringements of the Regulation. The intention is to ensure that the Regulation’s safeguards are implemented in an effective manner.

Three categories of fine, with progressively higher upper limits, are proposed:

- up to €250,000 or, in the case of an enterprise, up to 0.5% of its annual worldwide turnover;
- up to €500,000 or, in the case of an enterprise, up to 1% of its annual worldwide turnover;
- up to €1 million or, in the case of an enterprise, up to 2% of its annual worldwide turnover.

It appears, subject to limited exceptions, that the imposition of fines is intended to be mandatory and in each individual case “effective, proportionate and dissuasive”. Fines are to be determined by the supervisory authority on a case-by-case basis with due regard to “the nature, gravity and duration of the breach”. The factors to be taken into account when determining the level of fine also include:

- the intentional or negligent character of the infringement;
- the degree of responsibility of the individual or legal person and previous breaches;
- and
- the level of cooperation with the supervisory authority in order to remedy the breach.

Therefore the Presidency invites Ministers to discuss—

- whether the framework of fines set out in article 79 is appropriate;
 - if wider provision should be made for warnings or reprimands, thereby making fines optional or at least conditional upon a prior warning or reprimand;
 - if supervisory authorities should be permitted to take other mitigating factors, such as adherence to an approved code of conduct or a privacy seal or mark, into account when determining sanctions.

Leaseurope, the European Federation for leasing and car rental believes that the European Commission's proposal for a General Data Protection Regulation provides a good starting point to further discussions and debate on the EU framework for the protection of personal data. We have taken note of the draft opinion of the Industry, Research and Energy Committee and would like to share our views on this document with you. The commentary below should be read in light of the Leaseurope observations on the Proposal.¹

The draft ITRE opinion on this Proposal addresses the concerns of the industry in a number of areas. **In particular we support the following amendments incorporated in the draft opinion:**

- Amendment 6 (Recital 38): Introduces data processing for legitimate interests of third parties, as this is considered indispensable for the day-to-day business activities of many companies e.g. using the addresses of third parties to reach new customers.
- Amendment 14 (Recital 67): Deletion the 24 hour period for reporting personal data breaches to the supervisory. It is amended to reflect 'a reasonable time period' in an effort to prevent the creation of a culture of over-reporting. Alternatively the potential harm to the data subjects should determine whether reporting is required. This is in line with Leaseurope's position.
- Amendment 25 (Article 4(8)): The definition of 'data subject's consent' has been altered. The reference to explicit indication and a 'statement of clear and affirmative action' have been removed. This is in line with the Leaseurope position, although we also advocated for tacit consent.
- Amendment 28 (Article 4(19)(a) NEW): A definition has been added to the Draft Opinion defining 'financial crime', as derived from the recommendations of the Financial Action Task Force on combatting money laundering and terrorist financing.
- Amendment 29 (Article 6(1)(a)): This article has been amended strives to ensure that for the purposes of legal certainty, the conditions established for lawful processing do not conflict with the conditions for consent outlined in Article 7.
- Amendment 32 (Article 6(4)): This article has been amended and widened to allow the full range legitimizers contained in Article 6(1)(a-f) to serve as lawful grounds for processing.
- Amendment 33 (Article 6(5)), Amendment 45 (Article 9(3)), Amendment 46 (Article 12(5)), Amendment 64 (Article 17(9)), Amendment 79 (Article 23(3)), Amendment 80 (Article 23(4)), amendment 89 (Article 31(5)), Amendment 91 (Article 32(5)): The delegated and implementing acts for these provisions have been deleted. This is in line with the Leaseurope position.
- Amendment 34 (Article 7(1)): This provision which provided for the controller to bear the burden of proof for the data subjects consent for specified purposes has been deleted, due to the fact that it is superfluous as the burden of proof for normal procedural law currently applies. This is in line with the Leaseurope position.

¹ See <http://www.leaseurope.org/uploads/Leaseurope%20Observations%20DPR.pdf>

- Amendment 35 (Article 7(1)(a) NEW): This new addition allows for the consent to be proportionate to the type of data to be processed and the purposes for the processing and is to be conducted through a properly conducted data impact assessment as described in Article 33.
- Amendment 39 (Article 7(4)): This article has been expanded to further explain the ambiguous term 'significant imbalance', by providing a situation whereby the imbalance makes it unlikely that consent was freely given.
- Amendment 48 (Article 14(&)(c)): The requirement to inform the data subject as to the length of time the data will be stored has been deleted. This is in line with the Leaseurope position.
- Amendment 83 & 84 (Article 28): The provision providing for documentation to be kept on each data processing activity has been deleted and replaced by a provision requiring documentation to only contain the necessary information for the supervisory authority to ascertain that the controller/processor has complied with the said Regulation.
- Amendment 88 (Article 31(1)): This provision has been amended to reflected situations where personal data breaches can be constituted as serious enough to warrant being reported to the supervisory authorities. This is in line with the Leaseurope position.
- Amendment 126-153 (Article 79): The Draft Opinion advocates to delete the extensive prescribed administrative sanctions provision, and in place advocates that the supervisory authority should first issue a written warning without imposing a sanction and then administer fines for repeated or deliberate breaches pertaining. The Draft Opinion also considered the particular category of personal data relevant to the calculation of the gravity of the breach.

Therefore, in addition, we would also like to suggest a further amendment:

Article 3

<i>Original Wording</i>	<i>Proposed Amendment</i>
<p>1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union.</p> <p>2. This Regulation applies to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are related to:</p> <p>(a) the offering of goods or services to such data subjects in the Union; or</p> <p>(b) the monitoring of their behaviour.</p> <p>3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where the national law of a Member State applies by virtue of public international law.</p>	<i>Deleted</i>

Justification

This provision may have implications for enterprises that work within the framework of multiple jurisdictions and lead to legal uncertainty as data protection laws are not at the same rate of development worldwide. It is vital to avoid overlapping provisions which could lead to conflicting rules and result in major inefficiencies.

We would be pleased to answer any question you may have on these elements or to provide you with further information. Please do not hesitate to contact Leaseurope legal adviser Maeve Butler (m.butler@leaseurope.org, T: +32 2 778 05 62).

About Leaseurope

Leaseurope brings together 44 member associations representing the leasing, long term and/or short term automotive rental industries in the 32 European countries in which they are present. The scope of products covered by Leaseurope members' ranges from hire purchase and finance leases to operating leases of all asset categories (automotive, equipment and real estate). It also includes the short term rental of cars, vans and trucks.

The Federation's mission is to represent the European leasing and automotive rental industry, ensuring the sector's voice is heard by European and international policy makers.



**OBSERVATIONS ON THE COMMISSION'S PROPOSAL FOR A REGULATION OF
THE EUROPEAN PARLIAMENT AND OF THE COUNCIL ON THE PROTECTION
OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA
AND ON THE FREE MOVEMENT OF SUCH DATA (COM (2012) 11 final)**

Boulevard Louis Schmidt, 87
1040 Brussels
Email: m.butler@leaseurope.org
Tel: +32 2 778 05 62 Fax: +32 2 778 05 78
Leaseurope ID: 16013361508-12
04 September 2012

About Leaseurope

Leaseurope brings together 44 member associations representing the leasing, long term and/or short term automotive rental industries in the 32 European countries in which they are present. The scope of products covered by Leaseurope members' ranges from hire purchase and finance leases to operating leases of all asset categories (automotive, equipment and real estate). It also includes the short term rental of cars, vans and trucks.

The Federation's mission is to represent the European leasing and automotive rental industry, ensuring the sector's voice is heard by European and international policy makers.

INTRODUCTORY OBSERVATIONS

Leaseurope, the voice of leasing and automotive rental at European level, takes note of the publication of the European Commission's Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (COM(2012) 11 final). (Released in January 2012)

We believe the European Commission Proposal provides a good starting point to further discussions and debate on the EU framework for the protection of personal data. Although we appreciate that this proposed Regulation is a horizontal instrument applicable across sectors, we feel that a number of aspects are ill-suited for financial services, and in particular for the leasing industry.

1. The Regulation lays down the rules relating to the protection of **individuals** with regard to the processing of personal data and the rules relating to the free movement of that data. **Hence the Regulation will impact on B2C leasing transactions** and this document contains analysis of the projected impact.
2. It has also come to the attention of Leaseurope that **this Regulation will also be applicable in some B2B commercial dealings by virtue** of the fact that as part of its general checks, a leasing company will run checks on company directors to ensure that the company applying to obtain the lease is not insolvent. In addition, when a vehicle is leased to a company, the leasing company will handle personal driver data related to the individual that drives the vehicle. (Currently Data Protection legislation at national level in Austria, Italy, Denmark and Luxembourg protects legal entities as well as natural persons.)

SPECIFIC OBSERVATIONS

1. Chapter I – Article 3 – Territorial scope

Companies outside the EU

The proposed Regulation applies to companies that process the personal data of individuals residing in the EU, even if the company is established outside the EU. This may have implications for companies that work within the framework of multiple jurisdictions and lead to possible legal uncertainty as data protection laws are not at the same rate of development worldwide. Leaseurope feels that it is vital to avoid overlapping provisions which could lead to conflicting rules and result in major inefficiencies.

2. Chapter I – Article 4 – Definitions

Data subject – natural person

The scope of the proposed Regulation is explicitly aimed at the “protection of individuals with regard to the processing of personal data and rules relating to the free movement of personal data” (*Article 1(1)*). In *Article 4* which relays the definitions for the purposes of this proposed Regulation, it states that “personal data means any information relating to the data subject”, and the data subject is further defined as a natural person. **This provision raises much uncertainty as to whether a small and medium size enterprise (SME) could be considered as a natural person, and if so then SMEs would come within the scope of the proposed Regulation.** It is inevitable that this would lead to much administrative burden. Therefore clarity is required as to whom the scope of the proposed Regulation is intended to cover.

3. Chapter II – Article 5 – Principles relating to personal data processing

Data minimisation

Article 5 of the Proposal introduces the principle of ‘data minimisation’, whereby personal data must be limited to the minimum that is necessary.

Leasing companies *may* use many different types of data out of necessity on a daily basis.

Leasing companies need to use personal data in order to:

- i) Assess objectively the creditworthiness of their customers in a B2C leasing transaction by virtue of the Consumer Credit Directive;
- ii) Minimise the risk of fraud; and
- iii) Check if the customer is solvent in a B2B capacity.

Legislation currently in force, such as the Third Anti-Money Laundering Directive¹, places an obligation upon the leasing company to use data when conducting risk analysis and for identification purposes (*know your customer*). National legislation often also provides extensive detail on what data must be collected.

We believe that without further clarification, the introduction and subsequent interpretation of the principle of **data minimisation** would present an obstacle to leasing companies in their capacity of complying with the aforementioned legislation.

This provision would also cause companies globally to completely overhaul their internal systems in order to ensure compliance, due to the territorial application provision contained in *Article 3*. Is this really feasible in practice? Or be subject to the onerous administrative sanctions mentioned in *Article 79*.

Further processing

Article 5(b) and *Article 6(4)*, as they are currently worded, appear to be contradictory with regard to further processing of data for purposes incompatible with the actual purpose for which the data was

¹ Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing.

collected. To clarify the relation between the two *Articles* and to increase legal certainty, Leaseurope considers that *Article 5(b)* should be rephrased so as to specify that personal data must not be further processed in a way incompatible with the purposes for which it has been collected, **unless specific provisions of the Regulation provide otherwise.**

4. Chapter II – Article 6 - Lawfulness of processing

Criteria for lawfulness

Article 6 of the proposed Regulation broadly retains the provision contained in the 1995 Data Protection Directive, which lists the requirements under which data processing is to be considered lawful. However, there is a concern that these requirements listed in *Article 6* would not permit the processing of data for fraud prevention and detection purposes. Leaseurope therefore takes the view that fraud prevention and detection should be explicitly recognised as a legitimate purpose for data processing.

5. Chapter II – Article 7 – Conditions for consent

Specified purposes

The introduction of explicit consent (*Article 4(8)*) for “specified purposes” (*Article 7(1)*) could constitute a procedural or administrative change for the leasing industry, depending on how these aspects are to be interpreted in practice. If explicit consent were to be required for each separate purpose, this would be time-consuming, resource-intensive and costly. So to facilitate efficiency Leaseurope would like tacit consent to also be relied upon as a form of consent giving.

Significant imbalance

With regard to *Article 7(4)* we would like to remark that the proposed wording may create uncertainty as to what could be understood by “a significant imbalance”. This could result in differing national interpretations.

This could to some extent be resolved by explicitly clarifying that where consent cannot provide a legal basis due to an imbalance, and that the controller may process the data if this is subject to another legal basis, in accordance with *Article 6* of the proposed Regulation.

Withdrawal of consent

Article 7(3) provides that consumers may withdraw their consent at any time. This provision could have a detrimental impact on the data which leasing companies need to have in order to prevent fraud and to lease in a responsible manner. In our view, this provision should be amended to allow, where consent has been withdrawn, for the continued processing in accordance with another legal basis, as set out in *Article 6* of the proposed Regulation. This would permit the processing of data necessary for continuing the contractual relationship that may exist between the controller and the data subject.

6. Chapter II – Article 9 – Processing of special categories of personal data

Fraud databases

In some Member States leasing companies have set up databases which contain data on fraud, with the aim of prevention and minimize risks.²

Due to the restrictions in *Article 9* of the proposed Regulation on the processing of data related to criminal convictions and similar security measures, it is unclear whether these databases, whose existence is essential to protect against fraud, can be maintained in the future. In our view, this should be addressed so that these databases can continue to exist and operate.

7. Chapter II – Article 12 – Procedures and mechanisms for exercising the rights of the data subject

² Portuguese National leasing Association “ALF” has a database for non-compliance and litigation. The objective of which is to decrease the risk of concluding contracts with potential non-compliant lessees and to reduce levels of credit risk for lessors. They have attained special permission in Portugal to operate this due to the presence of individual’s personal data.

The first paragraph of *Article 12* is superfluous and should be deleted as the procedures to be established are outlined in the *Articles* that follow this. The conditions contained in *paragraph 2* in relation to making requests by electronic form should be deleted as safety aspects are threatened due to the fact it may not be possible to identify the person requesting the information, as they will also have requested it in an electronic manner.

Format for receiving the information

The provision of information in an electronic form involves highly advanced IT systems, hence this places further administration burdens on smaller leasing companies e.g. SMEs.

Refusal of data subjects request

Leaseurope believes that the data subject should be entitled to know the reasons for the refusal of a request that they have made for certain data. However, Leaseurope does not believe in this context that the data subject should be informed by the controller about lodging a complaint to the supervisory authorities as the controller would only be compelled to make a refusal if they have the proper grounds to do so.

Provision free of charge

Leaseurope supports the rights to access to data, rectification and completion of inaccurate and incomplete data for data subjects, as all of these actions contribute to the improved quality of the data used by leasing companies.

The proposed Regulation establishes that information and actions taken at the request of data subjects shall be free of charge. Regarding the right of access for the data subjects in *Article 15*, as well as the rectification and the completion of data in *Article 16*, Leaseurope would like to emphasise that the provision of holding data within a database comes at a cost.

Thus if leasing companies are to be obliged to allow access to data stored free of charge, this would increase administrative costs which would inevitably be passed on to the lessee.

In addition, it should also be recognised that requesting an appropriate contribution by consumers for data access is critical in deterring fraudsters from obtaining high volumes of consumers' data e.g. credit data. If data access upon request were to become free of charge then consumers would face an increased risk of fraud.

Finally, further specification of the criteria and conditions for the manifestly excessive requests and the fees should not, in our view, be transferred to the Commission, and - if necessary - should rather fall under the full-fledged legislative process. Leaseurope is also strongly opposed to standardization of forms and procedures, the development of which should remain with controllers.

8. Chapter III – *Article 14* – Information to the data subject

Categories of data

Article 14 sets out the information data controllers shall provide to data subjects. This Article has been substantially expanded compared to the provisions currently contained in the 1995 Directive. Leaseurope would like to warn against over-loading consumers with information and therefore asks that an appropriate balance be struck between the rights and duties of both parties.

In relation to the information requirements that the controller must disclose to the customer *Article 14(1)(c)* provides that the "*period for which the data will be stored*" must be provided to the data subject. Leaseurope believes this will not always be possible in practice to implement as this period can be difficult to determine depending on factors such as for example whether the lease is renewed. This provision deserves deletion as it clearly conflicts with *Article 30* of the 3rd AML Directive³.

³ Documents and information must be kept for a minimum of five years after the business relationship has ceased.

9. Chapter III – Article 15 – Right of access for the data subject

Categories of data:

Leaseurope believes that allowing the data subject access to this data at any time would be impossible to ensure in practice. The list of information aspects that the data subject has the right to request is too extensive and would lead to an overload for the customer. Yet again the period for which the data is to be stored is very difficult to determine as the nature of the contractual relationship can change overtime, hence this entitlement is impossible to guarantee.

Format for supplying/requesting the data:

The electronic format stipulated in the proposal for requesting the data yet again goes against safety standards. An electronic request makes it very difficult for the data subject requesting the data to be identified.

Delegated acts:

The presence of delegated acts in this article would provide conditions that would be too rigorous and a one-size-fits all approach would be inappropriate in this respect. A degree of flexibility must be maintained given the sectorial differences that exist.

10. Chapter III – Article 17 - Right to be forgotten and to erasure

Right to be forgotten

Leaseurope welcomes the fact that proposed Regulation does not introduce an absolute right to be forgotten. Access to historic data is critical for leasing companies to assess past performance in order to make sound leasing decisions, for portfolio management, for developing future underwriting strategies and for fulfilling their legal obligations in terms of Prudential Regulation and Anti-Money Laundering compliance.

In any case, the relevant provisions on the storage of data prevent data controllers from storing data for longer than required and national laws often lays down specific storage limits. Therefore, Leaseurope would like the exceptions in *Article 17(3)* to specifically include “processing of data for creditworthiness purposes” as this is a condition of the Consumer Credit Directive.

11. Chapter III – Article 18 – Right to data portability

Credit data

The provision of data portability is not suitable for the processing of personal data in a company's internal data base and should be inherently limited to the online sphere. Leaseurope feels that the system currently proposed in *Article 18* of the proposed Regulation would be open to abuse, as data could be easily altered in a fraudulent manner before being passed on to its intended destination. Additional difficulties could be that the data may be supplied in a different language and/or use differently defined terms.

Disclosure

Careful consideration should also be given as to whether or not this provision could require organisations to disclose confidential, for example business systems and/or its customers. In this context the obligation to bank secrecy should also be taken in account.

We are also concerned that data portability may increase the risk of disclosure of personal data to third parties. This may be in conflict with other obligations of the controller, such as for example security of processing (*Article 30*).

Implementing acts

We strongly oppose any standardisation of IT solutions and technical systems used by controllers to process data, as this would be very expensive to establish. The aim of the proposed Regulation is to introduce a new European framework for data protection that ensures protection of individual's rights and the free movement of data (*Article 1*), and not to standardise processing systems.

We would also like to add that the imposition of technical requirements to enable personal data to become portable comes at a significant cost for businesses, which they are likely to pass on to consumers.

12. Chapter III - Article 19 - Right to Object

Burden of proof on controller

Leaseurope has observed that this article has clearly been changed from its appearance in the Directive and now is adjusted in favour of the data subject. The burden of proof is now placed on the controller to prove they have compelling legitimate grounds for the processing that overrides the interests or fundamental rights and freedoms of the data subject. Leaseurope feels that this is disproportionate and could result in frivolous claims.

13. Chapter IV – Article 23 – Data protection by design and by default

Design of systems

Article 23 of the Proposal would require businesses to implement technical and organisational measures and procedures, so as to meet the requirements of the Regulation. In our view, this provision is unnecessary. Furthermore, the current wording is unclear, imposing an obligation to redesign internal systems to an undefined standard.

Leaseurope strongly opposes any standardisation of IT solutions and technical systems used by controllers to process data, through the adoption of implementing measures. The aim of the Proposal is to introduce a new European framework for data protection that ensures protection of individual's rights and the free movement of data (*Article 1*), not to standardise processing systems, as proposed in *Article 23(4)*.

14. Chapter IV - Article 28 – Documentation

Maintenance of documentation

The obligation to maintain documentation will entail a significant and unnecessary administrative burden on businesses. This is solely for the purpose of the supervisory authority performing a check, which the proposed Regulation does not confirm to be a certainty.

The Commission's empowerment to adopt delegated acts in relation specifying the criteria and requirements for the documentation is not adequate as sectorial differences must be accounted for. The retention of such documentation should in effect be limited in effect of the volume of data that is processed.

15. Chapter IV – Article 31 – Notification of a personal data breach to the supervisory authority

Notification period

The foreseen time period for notifying the supervisory authority (24 hours) of all the information required in *Article 31(1)* is in practice too short as it always takes time to assess what has happened, understand the amount and nature of the data, the potential risk etc.

Notification to supervisory authorities

An obligation exists to notify the supervisory authorities when a data breach occurs. Leaseurope is of the opinion that this report should only be filed when the breach is likely to adversely affect the protection of the data.

16. Chapter IV – Article 32 – Communication of a personal data breach to the data subject

Adverse effects

With regard to the communication of personal data breaches to data subjects where this is likely to affect the personal data or privacy of the data subject, Leaseurope would like to note that the establishment by the Commission via delegated and implementing acts at a later stage for applicable circumstances is likely to create substantial legal uncertainty. Data subjects should be informed where there could be a significant impact on them and we therefore feel that the current article is disproportionate.

17. Chapter IV – Article 33 – Data protection impact assessments

Consultation

The impact assessments that are prescribed in the proposed Regulation cause an onerous burden and would be rather time consuming, as consultation is required with either the data subject or their representative, thus in essence external consultation is required.

Specific risks

The impact assessments are only required if risky processing operations occur. It is not clear what benefit the data subject or the business would derive from conducting such assessments. Additionally, the presences of delegated acts is inappropriate for the further specifying of the criteria and processing that are likely to present specific risks, as each business sector will encounter differing risks.

18. Chapter IV – Article 35 – Designation of the data protection officer

Appointment

This article provides for the creation of the role of a Data Protection Officer (DPO). There are three conditions outlined, and if one is satisfied, it is necessary to appoint a DPO. According to the proposal, if the processing of data is carried out by an enterprise employing 250 people or more a data protection officer must be appointed. Nonetheless, the provision does state that for a group of undertakings a single data protection officer can be appointed.

Leaseurope would like to express its opposition to the benchmark outlined, and would like to advocate for a benchmark more related to the amount of data processing carried out, rather than one that is solely based on an employee headcount.

Independence

Article 35(8) provides that the DPO may be employed by the controller or processor, or alternatively should provide their tasks on the basis of a service contract. The inherent independence attached to their role could mean that they could take decisions against the company and be an independent force against the company. This could be potentially problematic.

19. Chapter IV – Article 36 – Tasks of the data protection officer

Independence

The independence of the DPO is again reiterated in *Article 36(2)*. Leaseurope believes that this wording should be amended as the DPO should be subject to some control by the company to which he is appointed.

20. Chapter X – Article 79 – Administrative sanctions

Level of sanctions

The proposed Regulation introduces severe administrative sanctions which supervisory authorities can impose on data controllers. We feel that the sanctions should be proportionate to a breach of the provisions of the Regulation.

It would also be more appropriate to amend the wording of *Article 79* from the “supervisory authority **shall** impose” to the “supervisory authority **may** impose”. This is to allow each authority to take into account all the circumstances of each individual case.

As a counterbalance to the sanctions, it is crucial that the obligations and duties of controllers and processors are clearly laid out.

21. Chapter X – Article 86 – Exercise of the delegation

Delegated acts

Leaseurope has serious concerns regarding the extensive power for the European Commission to adopt delegated acts. This would entail that the provisions of the Regulation would be liable to substantial changes over time, as well as legal uncertainty. The limited involvement of stakeholders in this process is also a concern.

We would like to recall that in accordance with the provisions of the Lisbon Treaty delegated acts can only be applied to “non-essential” aspects of the Regulation, rather than, as in the proposed Regulation, on all essential aspects of the Regulation.

Leaseurope therefore objects to the provisions of the Regulation being altered at a later stage by delegated acts in general and in particular on the following issues:

- Lawfulness of processing (*Article 6(5)*);
- Right to be forgotten (*Article 17(9)*); Communication of personal data breach (*Article 32(5)*);
and
- Data protection impact assessment (*Article 33(6)*).

Amazon EU Sarl

Proposed amendments to MEP Gallo's opinion on data protection

Amendment 1

Proposal for a regulation

Recital 20

Text proposed by the Commission

(20) In order to ensure that individuals are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects residing in the Union by a controller not established in the Union should be subject to this Regulation where the processing activities are related to the offering of goods or services to such data subjects, or to the monitoring of the behaviour of such data subjects.

Amendment

(20) In order to ensure that individuals are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects residing in the Union by a controller not established in the Union, **and where this Regulation would not otherwise apply**, should be subject to this Regulation where the processing activities are related to the offering of goods or services **that are specifically targeted at** such data subjects, or to the monitoring of the behaviour of such data subjects.

Or. en

Justification

This amendment is consistent with the amendment to Art. 3.2.

Amendment 2

Proposal for a regulation

Recital 23

Text proposed by the Commission

(23) The principles of protection should apply to any information concerning an identified or identifiable person. To determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used **either** by the controller **or by any other person** to identify the individual. The principles of data protection should not apply to **data rendered anonymous in such a way that the data subject is no longer identifiable**.

Amendment

(23) The principles of protection should apply to any information concerning and identified or identifiable person. To determine whether a person is identifiable, account should be taken of all the means **that are technically feasible, do not involve a disproportionate effort, and are** likely reasonably to be used by the controller **or the processor in the context of the specific processing activity and with the intention** to identify the individual. **Account shall also be taken of the technical and organizational measures put in place by the controller or processor to prevent identification of the individual.** The principles of data protection shall not apply to **processors when processors are not required to identify data subjects as part of their processing activities and where the use of such technical and organizational measures render it substantially unlikely for the processor to identify the data subject.**

Data that has been collected, altered or otherwise processed in such a way that its controller or processor can no longer attribute it to a data subject or that such attribution would require a disproportionate amount of time, cost and effort (anonymous data), shall not be considered as personal data for that controller or processor. This shall also apply in cases where the controller or processor has replaced any personal identifiers contained in the data with a code, provided and as long as the code does neither alone nor together with other data available to the controller or processor allow identification of the data subject.

Data that has been collected, altered or otherwise processed in such a way that the data subject's name and other identifying features have been replaced with another identifier so that identifiability of the data subject is considerably impeded (pseudonymous data) shall be considered as personal data.

The principles of data protection shall not apply to data that has been collected, altered or otherwise processed with the sole purpose of rendering it anonymous, pseudonymous or unable to be identified by the controller or processor.

Or. en

Justification

This amendment is consistent with the amendment to Art. 4.1. points (1), (2) and new (2a).

Amendment 3
Proposal for a regulation
Recital 24a (new)

Text proposed by the Commission

Amendment

Where service providers process data without being able to access personal data by means that are technically feasible, do not involve a disproportionate effort, and are reasonably likely to be used by a controller or a processor to take knowledge of the content of such data, such service providers shall be qualified as mere conduits pursuant to Article 12 of the Directive 2000/31/EC----- and shall not be responsible for any personal data transmitted or otherwise processed or made available through them.

Or. en

Justification

This amendment intends to take account of the fact that the traditional controller/processor concept structurally does not cater for many types of cloud computing services particularly where the cloud provider offers simple infrastructure services (processing power, storage, basic computing resources). Such providers are usually data agnostic. They regularly don't know whether information stored on or processed through their infrastructure is personal data and they usually have no control over or ability to access that data, nor do they require such

knowledge or access to provide their services. The reality shows that the relation of a number of cloud providers to data is fundamentally different from that of traditional processors. Recognition of such reality will help promote (rather than impede) the further development of cloud computing in Europe. The Regulation should provide for different actors with varying degrees of obligations and liabilities under the data protection laws.

Amendment 4

Proposal for a regulation

Recital 25

Text proposed by the Commission

Amendment

(25) Consent should be given **explicitly** by any appropriate method enabling a freely given specific and informed indication of the data subject's wishes, **either by a statement or by a clear affirmative action by the data subject**, ensuring that individuals are aware that they give their consent to the processing of personal data, **including by** ticking a box when visiting an Internet website or by any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data. **Silence or inactivity should therefore not constitute consent.** Consent should cover all processing activities carried out for the same purpose or purposes. If the data subject's consent is to be given following an electronic request, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.

(25) Consent should be given by any appropriate method, **commensurate to the context of and risk involved with the respective processing activity**, enabling a freely given specific, and informed indication of the data subject's wishes **and** ensuring that individuals are aware that they give their consent to the processing of personal data. **Consent may be given by a statement or an affirmative action by the data subject such as** ticking a box when visiting an Internet website or by any other statement, conduct or **measure** which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data. Consent should cover all processing activities carried out for the same purpose or purposes. If the data subject's consent is to be given following an electronic request, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.

Or. en

Justification

This amendment is consistent with the amendment to Art. 4.1(8).

Amendment 5

Proposal for a regulation

Recital 27

Text proposed by the Commission

Amendment

(27) The main establishment of **a controller** in the Union should be **determined according to objective criteria and should imply the effective and real exercise of management activities determining the main decisions as to the purposes, conditions and means of processing through stable arrangements. This criterion should not depend whether** the processing of personal data is actually carried out **at that location**; the presence and use of technical means

(27) The main establishment of **an undertaking or a group of undertakings, whether controller or processor**, in the Union should be **designated by the undertaking or group of undertakings and the competent authority should be informed of such designation, subject to the consistency mechanism set out in Article 57. The designation of the main establishment should be based upon the following optional objective criteria:**

and technologies for processing personal data or processing activities do not, in themselves, constitute such main establishment and are therefore no determining criteria for a main establishment. **The main establishment of the processor should be the place of its central administration in the Union.**

(1) location of the group's European headquarters;
(2) location of the entity within the group with delegated data protection responsibilities;
(3) location of the entity within the group which is best placed (in terms of management function, administrative burden etc.) to deal with and enforce the rules as set out in this Regulation;
(4) location where effective and real management activities are exercised determining the data processing through stable arrangements.

Priority shall be given to the criteria described under (1) above.

The location where the processing of personal data is actually carried out **shall not be a relevant criteria;** the presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute such main establishment and are therefore no determining criteria for a main establishment.

Or. en

Justification

This amendment is consistent with the amendment to Art. 4(13).

Amendment 6

Proposal for a regulation

Recital 33

Text proposed by the Commission

Amendment

(33) In order to ensure free consent, it should be clarified that consent does not provide a valid legal ground where the individual has no genuine and free choice and is subsequently not able to refuse or withdraw consent ***without detriment***.

(33) In order to ensure free consent, it should be clarified that consent does not provide a valid legal ground where the individual has no genuine and free choice and is subsequently not able to refuse or withdraw consent.

Or. en

Justification

The change clarifies that free consent, including the ability to refuse or withdraw consent, cannot be made dependent on whether the data subject may incur a detriment as the result of consent withdrawal. This is particularly the case where benefits and services that are provided in the context of a contractual relationship are dependent upon consent. Withdrawal of consent shall be possible, but only in accordance with the contract's terms and data subjects should be aware that they may not be able to withdraw consent and maintain these benefits or services. The new language emphasizes this point so consumers make a well-reasoned decision before choosing to withdraw consent.

Amendment 7

Proposal for a regulation

Recital 34

Text proposed by the Commission

Amendment

(34) Consent should not provide a valid legal ground for the processing of personal data, where ***there is a clear imbalance between*** the data subject ***and the controller***. This ***is especially*** the case where the data subject is in a situation of dependence from the controller, ***among others***, where personal data are processed by the employer of employees' personal data in the employment context. Where the controller is a public authority, there would be an imbalance only in the specific data processing operations where the public authority can impose an obligation by virtue of its relevant public powers and the consent cannot be deemed as freely given, taking into account the interest of the data subject.

(34) Consent should not provide a valid legal ground for the processing of personal data, where ***consent is not freely given by*** the data subject. This ***can be*** the case where the data subject is in a situation of ***fundamental economic*** dependence from the controller ***that is*** where personal data are processed by the employer of employees' personal data in the employment context. Where the controller is a public authority, there would be an imbalance only in the specific data processing operations where the public authority can impose an obligation by virtue of its relevant public powers and the consent cannot be deemed as freely given, taking into account the interest of the data subject.

Or. en

Justification

The notion of “significant imbalance” lacks clarity and will lead to confusion and legal uncertainty for both consumers and businesses. There is the risk that the utility of consent will be significantly restricted, as there is rarely an equal bargaining power between individuals and businesses. For instance, one could claim that there is significant imbalance where an individual relies upon the usage of a service for his business. Article 4(8) better addresses concerns about protecting consumers by mandating data subject’s consent must be “freely given”.

Amendment 8

Proposal for a regulation

Recital 62

Text proposed by the Commission

Amendment

(62) The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers ***and processor***, also in relation to the monitoring by and measures of supervisory authorities, requires a clear attribution of the responsibilities under this Regulation, including where a controller determines the purposes, conditions and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller.

(62) The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers, also in relation to the monitoring by and measures of supervisory authorities, requires a clear attribution of the responsibilities under this Regulation, including where a controller determines the purposes, conditions and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller.

Or. en

Justification

This amendment is meant to clarify wording in line with amendments to Article 26.1 and 26.2.

Amendment 9

Proposal for a regulation

Recital 63

(63) Where a controller not established in the Union is processing personal data of data subjects residing in the Union whose processing activities are related to the offering of goods or services **to** such data subjects, or to the monitoring their behaviour, the controller should designate a representative, unless the controller is established in a third country ensuring an adequate level of protection, or the controller is a small or medium sized enterprise or a public authority or body or where the controller is only occasionally offering goods or services to such data subjects. The representative should act on behalf of the controller and **may** be addressed by **any** supervisory authority.

(63) Where a controller not established in the Union is processing personal data of data subjects residing in the Union whose processing activities are related to the offering of goods or services **that are specifically targeted at** such data subjects, or to the monitoring **of** their behaviour, the controller should designate a representative, unless the controller is established in a third country ensuring an adequate level of protection, or the controller is a small or medium sized enterprise or a public authority or body or where the controller is only occasionally offering goods or services to such data subjects. The representative should act on behalf of the controller and **shall only** be addressed by **the** supervisory authority **of the establishment of the representative**.

Or. en

Justification

The inclusion of the term “targeting” is consistent with the amendment to Art. 3.2. The second change is intended to ensure respect of the EU principle of non-discrimination by affording the benefit of the one stop shop principle also to non-EU controllers who appoint an EU representative. They should benefit from one of the main anchors of the draft Regulation in the same way as EU established companies, given that they are subject to the same rights and obligations of the draft Regulation.

Amendment 10

Proposal for a regulation

Recital 64

(64) In order to determine whether **a controller is only occasionally** offering goods or services **to** data subjects residing in the Union, it should be ascertained whether it is apparent from the controller's overall activities that the offering of goods and services to such data subjects is **ancillary to those main activities**.

(64) In order to determine whether **the offering of** goods or services **is targeted at** data subjects residing in the Union, it should be ascertained whether it is apparent from the controller's overall activities that the offering of goods and services to such data subjects is **specifically and-intentionally directed at them, taking account of in particular the international nature of the activities, use of a language or a currency other than the language or currency generally used in the controller's country of establishment, the possibility of making and confirming a reservation in that other language, or the use of a top-level domain name with the .eu suffix or other than that of the country in which the controller is established. The mere accessibility of the controller's website by a data subject residing in the Union is insufficient**.

Or. en

Justification

This amendment is consistent with the amendment to Art. 3.2.

Amendment 11
Proposal for a regulation
Recital 65

Text proposed by the Commission

(65) In order to demonstrate compliance with this Regulation, the controller **or processor** should document **each** processing operation. Each controller **and processor** should be obliged to co-operate with the supervisory authority and make this documentation, on request, available to it, **so that it might serve for monitoring those processing operations.**

Amendment

(65) In order to demonstrate compliance with this Regulation, the controller should document **the main** processing operations. Each controller should be obliged to co-operate reasonably with the supervisory authority and make this documentation, on request, available to it.

Or. en

Justification

The proposed documentation obligation is disproportionate since it covers virtually every data processing activity. It risks defeating the objective of the draft Regulation to reduce administrative burdens. The changes aim to achieve effective data protection, by requiring organisations to document their main data processing activities. Processors should not be subject to the documentation requirement as they usually do not have access to data or other processing strategies which remain the remit of the controller. It should be left to the controller and processor to determine contractually who is best placed to adequately document the specific processing activities in compliance with this Regulation.

Amendment 12
Proposal for a regulation
Recital 70

Text proposed by the Commission

(70) Directive 95/46/EC provided for a general obligation to notify processing of personal data to the supervisory authorities. While this obligation produces administrative and financial burdens, it did not in all cases contribute to improving the protection of personal data. Therefore such indiscriminate general notification obligation should be abolished, and replaced by effective procedures and mechanism which focus instead on those processing operations which are likely to present **specific** risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes. In such cases, a data protection impact assessment should be carried out by the controller **or processor** prior to the processing, which should include in particular the envisaged measures, safeguards and mechanisms for ensuring the protection of personal data and for demonstrating the compliance with this Regulation.

Amendment

(70) Directive 95/46/EC provided for a general obligation to notify processing of personal data to the supervisory authorities. While this obligation produces administrative and financial burdens, it did not in all cases contribute to improving the protection of personal data. Therefore such indiscriminate general notification obligation should be abolished, and replaced by effective procedures and mechanism which focus instead on those processing operations which are likely to present **significant** risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes. In such cases, a data protection impact assessment should be carried out by the controller prior to the processing, which should include in particular the envisaged measures, safeguards and mechanisms for ensuring the protection of personal data and for demonstrating the compliance with this Regulation.

Or. en

Justification

The term “specific risk” is too vague and would open up to a seemingly infinite amount of criteria. The scope should be narrowed down to “significant risks” to be reflective of the real concerns. Processors should not be subject to the data impact assessment requirement as they usually do not have access to data or other processing strategies which remain the remit of the controller. In any case, it should be left to the controller and processor to determine contractually who is best placed to undertake an impact assessment, where required under this Regulation.

Amendment 13

Proposal for a regulation

Recital 105

Text proposed by the Commission

In order to ensure the consistent application of this Regulation throughout the Union, a consistency mechanism for co-operation between the supervisory authorities themselves and the Commission should be established. This mechanism should in particular apply where **a** supervisory authority intends to take a measure as regards processing operations that are related to the offering of goods or services **to** data subjects in several Member States, or to the monitoring such data subjects, that might substantially affect the free flow of personal data. ***It should also apply where any supervisory authority or the Commission requests that the matter should be dealt with in the consistency mechanism.*** This mechanism should be without prejudice to any measures that the Commission may take in the exercise of its powers under the Treaties.

Amendment

In order to ensure the consistent application of this Regulation throughout the Union, a consistency mechanism for co-operation between the supervisory authorities themselves and the Commission should be established. This mechanism should in particular apply where ***the competent*** supervisory authority intends to take a measure as regards processing operations that are related to the offering of goods or services ***specifically targeted at*** data subjects in several Member States, or to the monitoring such data subjects, ***and the controller not established in the Union, or as regards processing operations*** that might substantially affect the free flow of personal data. This mechanism should be without prejudice to any measures that the Commission may take in the exercise of its powers under the Treaties.

Or. en

Justification

Companies not established in the Union that are covered by the Regulation should not automatically be subject to the consistency mechanism in all circumstances. The competence of the data protection board with respect to such non- EU companies should be equivalent to that for EU companies. Only if the non-EU company does not appoint a representative is it justified to apply the consistency mechanism. This amendment is also consistent with the amendment to Article 58.1, Article 58.2 as well as Article 3.2 and Article 51.2.

Amendment 14

Proposal for a regulation

Recital 106

Text proposed by the Commission

In application of the consistency mechanism, the European Data Protection Board should, within a determined period of time, issue an opinion, if a ***simple*** majority of its members so decides or if so requested by any supervisory authority or the

Amendment

In application of the consistency mechanism, the European Data Protection Board should, within a determined period of time, issue an opinion, if a ***qualified*** majority of its members so decides or if so requested by any supervisory authority or the

Commission.

Commission.

Or. en

Justification

Majorities need to be substantial in accordance with current practice.

Amendment 15

Proposal for a regulation

Recital 108

Text proposed by the Commission

Amendment

There may be an urgent need to act in order to protect the interests of data subjects, in particular when the danger exists that the enforcement of a right of a data subject could be considerably impeded. Therefore, **a** supervisory authority should be able to adopt provisional measures with a specified period of validity when applying the consistency mechanism.

There may be an urgent need to act in order to protect the interests of data subjects, in particular when the danger exists that the enforcement of a right of a data subject could be considerably impeded. Therefore, **the competent** supervisory authority should be able to adopt provisional measures with a specified period of validity when applying the consistency mechanism.

Or. en

Justification

This amendment is consistent with the amendment to Article 51.2.

Amendment 16

Proposal for a regulation

Article 3 – paragraph 2

Text proposed by the Commission

Amendment

2. This Regulation applies to the processing of personal data of data subjects residing in the Union **by a controller not established in the Union, where** the processing activities are related to:
(a) the offering of goods or services **to** such data subjects in the Union; or
(b) the monitoring of their behaviour.

2. This Regulation applies to the processing of personal data of data subjects residing in the Union, **in circumstances when Article 3(1) does not apply, but when** the processing activities **of the controller** are related to:
(a) the offering of goods or services **which are specifically targeted at** such data subjects in the Union; or
(b) the monitoring of their behaviour.

Or. en

Justification

While it is desirable that non-EU companies respect EU data protection standards when processing EU citizens' data, the term "offering" is too broad and unpredictable and does not constitute a valid legal notion in the context of cross-border activities to determine the applicable law and jurisdiction. Companies may not know that their customers are European residents. The wording does not take into account that goods and services may be offered passively online with no clear way to determine the location of the purchaser or end user. The use of the additional term "targeting" can be evaluated by objective criteria, thereby carrying much more legal certainty. It also reflects current EU jurisprudence.

Amendment 17

Proposal for a regulation

Article 4 – paragraph 1 – point 1

Text proposed by the Commission

(1) '**data subject**' means an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or **by any other natural or legal person, in particular** by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;

Amendment

(1) '**Personal data**' means **any information concerning** an identified natural person or a natural person who can be identified ('**data subject**'), directly or indirectly, by means **that are technically feasible, do not involve a disproportionate effort, and are** reasonably likely to be used by the controller **or the processor in the context of the specific processing activity and with the intention to identify the data subject, including** by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person; **these factors as such need not necessarily be considered as personal data in all circumstances;**

Or. en

Justification

The proposed definition is very broad and will effectively result in the strict conditions of the Regulation applying to the vast majority of all processing operations, regardless of the context in which the data is processed, whether the data is attributable to a person, the realistic privacy risk and intention of identification. This all-encompassing approach risks leading to a disruptive consumer experience, particularly in the online environment, and risks removing any incentive for companies to invest in or make use of privacy-enhancing measures and processes as under such an approach any piece of information, even if anonymized, would have to be considered personal. This will, as a result, lead to less privacy protection rather than more, which would directly conflict with the intended objective of the Regulation. The suggested changes are intended to enhance protection of individuals' data by placing the focus on the most relevant data processing operations, on the parties who will have access to the data and by setting true incentives for industry to continuously invest in robust privacy-friendly technologies. In line with recital 24, it should be made clear in the Article 4 itself that it depends on the context whether identification numbers, location data, and online identifiers are to be considered personal data.

Amendment 18

Proposal for a regulation

Article 4 – paragraph 1 – point 2

Text proposed by the Commission

(2) '**personal data**' means any **information relating to a data subject**;

Amendment

(2) '**Anonymous data**' means any **data that has been collected, altered or otherwise processed in such a way that it can no longer be attributed to a data subject, including where any personally identifying features are replaced with a code so that the data subject can no longer be identified, or that such attribution would require a disproportionate amount of time, cost and effort; anonymous data shall not be**

considered personal data.

Or. en

Justification

Businesses should be incentivized to anonymize data, which will ultimately strengthen consumers' privacy protection. The changes aim at clarifying the meaning of anonymous data and, in line with recital 23, explicitly excluding such data from the scope of the Regulation.

Amendment 19

Proposal for a regulation

Article 4 – paragraph 1 – point 2a (new)

Text proposed by the Commission

Amendment

(2a) 'pseudonymous data' means any personal data that has been collected, altered or otherwise processed in such a way that the data subject's name and other identifying features are replaced with another identifier so that identifiability of the data subject is considerably impeded; pseudonymous data shall be considered as personal data.

Or. en

Justification

Businesses should be incentivized to invest in and use privacy-enhancing measures, such as pseudonymization, which will ultimately strengthen consumers' privacy protection. The changes aim at ensuring that the Regulation expressly recognises the existence and value of pseudonymous data. Similar approaches in existing data protection laws of some Member States (e.g. Germany) have proven successful.

Amendment 20

Proposal for a regulation

Article 4 – paragraph 1 – point 6

Text proposed by the Commission

Amendment

(6) 'processor' means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

6) 'processor' means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller ***and is able to access personal data by means that are technically feasible, do not involve a disproportionate effort, and are reasonably likely to be used by a controller or a processor to take knowledge of the content of such data;***

Or. en

Justification

This amendment is consistent with the amendment to Recital 24a (new).

Amendment 21

Proposal for a regulation

Article 4 – paragraph 1 – point 8

Text proposed by the Commission

(8) 'the data subject's consent' means any freely given specific, informed **and explicit** indication of his or her wishes by which the data subject, either by a statement or **by a clear affirmative** action, signifies agreement to personal data relating to them being processed;

Amendment

(8) 'the data subject's consent' means any freely given specific **and** informed indication of his or her wishes by which the data subject, either by a statement or clear action **or any other appropriate method commensurate to the context of and risk involved with the respective processing activity**, signifies agreement to personal data relating to them being processed;

Or. en

Justification

Requiring 'explicit' consent as the norm for every data use scenario, irrespective of the context of data processing and the privacy risks for data subjects, is overly formalistic and rigid. It risks inhibiting legitimate and innovative business practices in the off- and online environment and impacting user experience and expectations without adding anything to users' data protection. Consent as a means to gain user acceptance and protect fundamental rights may be devaluated as a consequence of consumers being overloaded with consent requests, making it difficult for them to understand the privacy impact of different data processing operations. The suggested changes aim at allowing for flexibility for businesses, avoiding confusing of consumers and ensuring that there is a role for implied consent in cases where a user's behaviour can safely be interpreted as a decision to accept certain uses of data.

Amendment 22

Proposal for a regulation

Article 4 – paragraph 1 – point 13

Text proposed by the Commission

(13) 'main establishment' means **as regards the controller, the place of its establishment in the Union where the main decisions as to the purposes, conditions and means of the processing of personal data are taken; if no decisions as to the purposes, conditions and means of the processing of personal data are taken in the Union, the main establishment is the place where the main processing activities in the context of the activities of an establishment of a controller in the Union take place. As regards the processor, 'main establishment' means the place of its central administration in the Union;**

Amendment

(13) 'main establishment' means **the location as designated by the undertaking or group of undertakings, whether controller or processor, subject to the consistency mechanism set out in Article 57, on the basis of, but not limited to, the following optional objective criteria:**

(1) the location of the European headquarters of a group of undertakings;

(2) the location of the entity within a group of undertakings with delegated data protection responsibilities;

(3) the location of the entity within the group which is best placed in terms of management functions and administrative responsibilities to deal with and enforce the rules as set out in this Regulation; or

(4) the location where effective and real management activities are exercised determining the data processing through stable arrangements.

The competent authority shall be informed by the undertaking or group of undertakings of the designation of the main establishment.

Or. en

Justification

The ‘one-stop-shop’ approach with respect to the jurisdiction of regulators is particularly crucial for corporate groups operating in several Member States as they require legal certainty as to one ‘lead’ regulator being their single point of contact and by whom they may be addressed, and it is also essential to allow businesses and consumers to fully reap the benefits of the EU Single Market. It also has the potential to cut red tape, provide legal certainty and ensure a consistent and more efficient application of data protection rules across Europe. The current system has led to confusion as to competency questions and to conflicting approaches by regulators as a result of this. However, the proposed ‘main establishment’ terminology is too vague and narrow to work in different situations and provides too much room for diverging interpretation. To take account of today’s business reality and provide for clear-cut and common sense criteria allowing for flexibility and predictability for all stakeholders, one uniform test for determining an organization’s “main establishment” should be applied to “undertakings/groups of undertakings” as the relevant reference point (rather than applying different tests for controller and processor) and based on a set of relevant objective criteria, which a business can choose from in order to officially designate its location of ‘main establishment’, with effects for all processing activities of all entities part of the group. A similar concept to determine the lead DPA exists in relation to Binding Corporate Rules (BCRs) and should for consistency reasons also apply for the purpose of determining the place of ‘main establishment’ in the context of the draft Regulation. This approach will provide for legal certainty required by business while preventing the risk of forum shopping as well as disputes over the place of main establishment.

Amendment 23

Proposal for a regulation

Article 4 – paragraph 1 – point 14

Text proposed by the Commission

Amendment

(14) ‘representative’ means any natural or legal person established in the Union who, explicitly designated by the controller, acts and **may** be addressed by **any** supervisory authority **and other bodies in the Union instead of the controller**, with regard to the obligations of the controller under this Regulation;

(14) ‘representative’ means any natural or legal person established in the Union who, explicitly designated by the controller, acts and **shall only** be addressed by **the supervisory authority of the establishment of the representative**, with regard to the obligations of the controller under this Regulation;

Justification

The change is intended to ensure respect of the EU principle of non-discrimination by affording the benefit of the one stop shop principle also to non-EU controllers who appoint an EU representative. They should benefit from one of the main anchors of the draft Regulation in the same way as EU established companies, given that they are subject to the same rights and obligations of the draft Regulation.

Amendment 24

Proposal for a regulation

Article 4 – paragraph 1 – point 20 (new)

Text proposed by the Commission

Amendment

(20) ‘erasure’ means deleting personal data or rendering it unusable, unreadable, anonymous or indecipherable through the use of appropriate technological protection measures which are widely accepted as effective industry practices or industry standards, when applicable.

Or. en

Justification

This change is aimed at providing flexibility for different technical capabilities. Whether the data is deleted, rendered unusable, unreadable, irreversibly anonymous, or indecipherable, the main goal is that the data subject’s information can no longer be accessed or identified to the extent practicable by the controller or processor. The change of language will also provide assurance and comfort to data subjects in situations where information cannot be fully erased for a variety of reasons. Similar clarifications contained in existing data protection laws of some Member States (e.g. Germany) have proven successful.

Amendment 25

Proposal for a regulation

Article 6 – paragraph 1 – point (g) (new)

Text proposed by the Commission

Amendment

(g) only pseudonymous data is processed.

Or. en

Justification

This amendment is consistent with the amendment to new Art. 4.1(2a)

Amendment 26

Proposal for a regulation

Article 6 – paragraph 4

Text proposed by the Commission

Amendment

4. Where the purpose of further processing is not compatible with the one for which the personal data have been collected, the processing must have a legal basis at least in one of the grounds referred to in points (a) to **(e)** of paragraph 1. This shall in particular apply to any change of terms and general conditions of a contract.

4. Where the purpose of further processing is not compatible with the one for which the personal data have been collected, the processing must have a legal basis at least in one of the grounds referred to in points (a) to **(g)** of paragraph 1. This shall in particular apply to any change of terms and general conditions of a contract.

Or. en

Justification

This amendment is consistent with the amendment to new Art. 4.1(2a)

Amendment 27

Proposal for a regulation

Article 7 – Paragraph 2

Text proposed by the Commission

Amendment

2. ***If the data subject's consent is to be given in the context of a written declaration which also concerns another matter, the requirement to give consent must be presented distinguishable in its appearance from this other matter.***

2. ***The controller shall select the method most appropriate to obtain meaningful consent from data subjects. The requirement to give consent must be presented in a manner distinguishable in its appearance.***

Or. en

Justification

The changes reflect the need to consider differences in the purpose and context for the collection of data. The goal to provide clear information to data subjects is preserved and strengthened. The current wording "distinguishable in its appearance" is vague, which could result in situations where the data subject may be confused as to the importance of each section of the matters. Further, some contractual arrangements are fully dependent upon the data subject providing consent and fully separating consent from other issues may confuse data subjects.

Amendment 28

Proposal for a regulation

Article 7 – Paragraph 3

Text proposed by the Commission

Amendment

3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

3. The data subject shall have the right to withdraw his or her consent at any time, ***without prejudice to applicable laws and contractual arrangements***. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

Or. en

Justification

It should be clarified in the Regulation that while data subjects may withdraw their consent at any time, such withdrawal needs to be in accordance with the contractual terms. Many benefits and services that are provided in the context of a contractual relationship are dependent on consent for processing of data. Therefore, when data subjects withdraw consent, they may not be able to maintain these benefits or services. The new language emphasizes this point so consumers make a well-reasoned decision before choosing to withdraw consent.

Amendment 29

Proposal for a regulation

Article 7 – Paragraph 4

Text proposed by the Commission

Amendment

4. ***Consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller.***

Deleted

Or. en

Justification

The notion of “significant imbalance” lacks clarity and will lead to confusion and legal uncertainty for both consumers and businesses. There is the risk that the utility of consent will be significantly restricted, as there is rarely an equal bargaining power between individuals and businesses. For instance, one could claim that there is significant imbalance where an individual relies upon the usage of a service for his business. Article 4(8) better addresses concerns about protecting consumers by mandating data subject’s consent must be “freely given”.

Amendment 30

Proposal for a regulation

Article 19 – Paragraph 1

Text proposed by the Commission

Amendment

1. The data subject shall have the right to object, on grounds relating to their particular situation, at any time to the processing of personal data which is based on points (d), (e) **and** (f) of Article 6(1), unless the controller demonstrates compelling legitimate grounds for the processing which override the interests or fundamental rights and freedoms of the data subject.

1. The data subject shall have the right to object, on grounds relating to their particular situation, at any time to the processing of personal data which is based on points (d), (e), (f) **and (g)** of Article 6(1), unless the controller demonstrates compelling legitimate grounds for the processing which override the interests or fundamental rights and freedoms of the data subject.

Or. en

Justification

This amendment is consistent with the amendment to new Art. 4.1 point 2a. Data subjects’ right to object to data processing shall be extended to the processing of pseudonymous data.

Amendment 31

Proposal for a regulation

Article 20 – Paragraph 2 – point (d) (new)

Text proposed by the Commission

Amendment

(d) is based on pseudonymous data.

Or. en

Justification

This amendment is consistent with the amendment to new Art. 4.1 point 2a. Since the aim of pseudonymous data is to prevent identification of an individual, processing of such data for profiling purposes should be permitted.

Amendment 32

Proposal for a regulation

Article 22 – Paragraph 2a (new)

Text proposed by the Commission

Amendment

2a. Paragraph 2(a), (c), (d) shall not apply to controllers who have appointed a data protection

Justification

The appointment of a data protection officer should result in the exemption from administrative burdens, such as the documentation requirement, the obligation to undertake a data impact assessment, prior authorization and consultation. This practice has been widely successful in other Member States (e.g. Germany), encouraging the appointment of DPOs and ultimately leading to increases in both business efficiency and consumer protections.

Amendment 33

Proposal for a regulation

Article 22 – Paragraph 3

Text proposed by the Commission

Amendment

3. The controller shall implement mechanisms to ensure the verification of the effectiveness of the measures referred to in paragraphs 1 and 2. If proportionate, this verification shall be carried out by independent internal or external auditors.

3. The controller shall implement mechanisms to ensure the verification of the effectiveness of the measures referred to in paragraphs 1 and 2. If proportionate, this verification shall be carried out by independent internal or external auditors. ***Measures adhered to by the controller pursuant to Articles 38 and 39 shall be accepted as valid tool to prove compliance with the respective requirements of this Regulation.***

Justification

The Regulation should offer clear regulatory incentives to controllers and processors to invest in security and privacy enhancing measures and making use of viable self-regulatory systems and certification schemes via waivers from administrative burdens and simplification mechanisms. Where controllers and processors propose additional safeguards to protect data, which are in line with or go beyond accepted industry standards and who can demonstrate this via conclusive certificates (e.g. via DPO, code of conduct, third party audit), they should benefit from less prescriptive requirements. This would allow for flexibility, legal certainty, less administrative burden, highest privacy and security standards for data subjects and transparency for regulators.

Amendment 34

Proposal for a regulation

Article 26 – Paragraph 1

Text proposed by the Commission

Amendment

1. Where a processing operation is to be carried out on behalf of a controller, the controller shall choose a processor providing sufficient guarantees to implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject, in particular in respect of the technical security measures and

1. Where a processing operation is to be carried out on behalf of a controller ***and which involves the processing of data that would permit the processor to reasonably identify the data subject***, the controller shall choose a processor providing sufficient guarantees to implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this

organizational measures governing the processing to be carried out and shall ensure compliance with those measures.

Regulation and ensure the protection of the rights of the data subject, in particular in respect of the technical security measures and organizational measures governing the processing to be carried out and shall ensure compliance with those measures. ***The controller remains solely responsible for ensuring compliance with the requirements of this Regulation.***

Or. en

Justification

Where it is technically not feasible for the processor to identify a data subject, e.g. due to the use of proper anonymization techniques, Article 26 shall not apply. The lessening of administrative burdens will incentivize investment in robust anonymisation technology and use of strong system of restricted access, ultimately strengthening data subject protections. The basic principle according to which primary and direct responsibility and liability for processing is incumbent upon the controller should be clearly stated in this Article. There should be no direct obligation and liability for processors beyond the existing status quo.

Amendment 35

Proposal for a regulation

Article 26 – Paragraph 2

Text proposed by the Commission

Amendment

2. The carrying out of processing by a processor shall be governed by a contract or other legal act binding the processor to the controller ***and stipulating in particular that the processor shall:***

2. The carrying out of processing by a processor shall be governed by a contract or other legal act binding the processor to the controller. ***The controller and processor shall be free to determine respective roles and responsibilities with respect to the requirements of this Regulation, and shall provide for the following:***

Or. en

Justification

Any regulatory allocation of responsibilities between controller and processor needs to take account of the contractual arrangements between the parties, in order to avoid potential contradictions, overlapping responsibilities, duplication of administrative burdens and inefficiencies in enforcement. It is important that the freedom and flexibility for controller-processor arrangements is preserved. Also, processors are often not in a position to automatically comply with all the requirements as stipulated in Article 26. Processors have limited and distinct obligations that do not simply mirror those of controllers. Independent obligations upon processors will create needless uncertainty in the controller-processor relationship, as processors will need to independently evaluate their obligations vis-à-vis controller instructions. Controller and processor should be free to determine the nature of their relationship to ensure proper levels of protection and best comply with the requirements while at the same time allowing sufficient flexibility for practical business solutions.

Amendment 36

Proposal for a regulation

Article 26 – Paragraph 2 – point a

Text proposed by the Commission

Amendment

(a) act only on instructions from the controller, in

(a) ***the processor shall*** act only on instructions from

particular, where the transfer of the personal data used is prohibited;

the controller, in particular, where the transfer of the personal data used is prohibited;

Or. en

Justification

This amendment serves clarification purposes in line with amendments to Article 26.2.

Amendment 37

Proposal for a regulation

Article 26 – Paragraph 2 – point b

Text proposed by the Commission

Amendment

(b) ***employ only*** staff who have committed themselves to confidentiality ***or are under a statutory obligation of confidentiality***;

(b) staff ***employed by the processor shall commit*** to confidentiality;

Or. en

Justification

This amendment is meant to clarify wording in line with amendments to Article 26.2.

Amendment 38

Proposal for a regulation

Article 26 – Paragraph 2 – point c

Text proposed by the Commission

Amendment

(c) ***take all*** required measures pursuant to Article 30;

(c) ***agreement with respect to the*** required measures pursuant to Article 30;

Or. en

Justification

This amendment is meant to clarify wording in line with amendments to Article 26.2.

Amendment 39

Proposal for a regulation

Article 26 – Paragraph 2 – point d

Text proposed by the Commission

Amendment

(d) enlist another processor only with the prior permission of the controller;

deleted

Or. en

Justification

The apportionment of responsibilities between the controller and processor should be left to the parties to agree on and should be appropriately embodied in the contract. The requirement to obtain prior authorization from the controller for the processor to enlist sub-processors imposes burdens with no clear benefit in terms of enhanced data protection. Also, it is not workable particularly in the cloud context and especially if interpreted to require

prior authorization to use specific sub-processors. This requirement should be removed.

Amendment 40

Proposal for a regulation

Article 26 – Paragraph 2 – point e

Text proposed by the Commission

Amendment

(e) insofar as this is possible given the nature of the processing, **create in** agreement **with the controller** the **necessary** technical and organizational requirements **for the fulfilment of** the controller's **obligation** to respond to requests for exercising the data subject's rights laid down in Chapter III;

(e) insofar as this is possible given the nature of the processing **and the processor's ability to assist with reasonable effort, an** agreement **as to** the **appropriate and relevant** technical and organizational requirements **which support the ability of the controller** to respond to requests for exercising the data subject's rights laid down in Chapter III;

Or. en

Justification

This amendment is consistent with the amendment to Article 26.2. Furthermore, it clarifies the wording to take account of the fact that particularly in the cloud context certain processors are not in a position to assist the controller in complying with information requirements nor to make any determination as to the handling of the personal data.

Amendment 41

Proposal for a regulation

Article 26 – Paragraph 2 – point f

Text proposed by the Commission

Amendment

(f) **assist the controller in ensuring compliance** with the obligations pursuant to Articles **30** to 34;

(f) **insofar as this is possible given the nature of the processing, the information available to the processor and his ability to assist with reasonable effort, an agreement on how compliance will be ensured** with the obligations pursuant to Articles **28** to 34;

Or. en

Justification

This amendment is consistent with the amendment to Article 26.2 and Article 26.2 point e.

Amendment 42

Proposal for a regulation

Article 26 – Paragraph 2 – point g

Text proposed by the Commission

Amendment

(g) **hand over all results to the controller after the end of the processing and** not process the personal data **otherwise**;

(g) **assurance from the processor that he will** not process the personal data **further after the end of the agreed processing**;

Justification

This amendment is consistent with the amendment to Article 26.2. It also takes account of the fact that there may be no results as such to hand over if the data minimisation principle has been effectively applied. Making data available to the supervisory authority should be handled by the controller. Processors typically do not provide due diligence materials to a controller or DPA.

Amendment 43**Proposal for a regulation****Article 26 – Paragraph 2 – point h***Text proposed by the Commission*

(h) make available to the controller **and the supervisory authority** all information necessary to control compliance with the obligations laid down in this Article.

Amendment

(h) **agreement that, upon request, the processor will** make available to the controller all **available, relevant and permissible** information necessary to control compliance with the obligations laid down in this Article.

Justification

This amendment is consistent with the amendment to Article 26.2 and Article 26.2 point g.

Amendment 44**Proposal for a regulation****Article 26 – Paragraph 3a (new)***Text proposed by the Commission**Amendment*

3a. The controller is deemed to have fulfilled the obligations set out in paragraph 1 when employing a processor who has voluntarily self-certified or voluntarily obtained a third party certification, seal or mark showing the implementation of appropriate standard technical and organizational measures in response to the requirements set out in this Regulation.

Justification

The Regulation should offer clear regulatory incentives to controllers and processors to invest in security and privacy enhancing measures and making use of viable self-regulatory systems and certification schemes via waivers from administrative burdens and simplification mechanisms. Where controllers and processors propose additional safeguards to protect data, which are in line with or go beyond accepted industry standards and who can demonstrate this via conclusive certificates (e.g. via DPO, code of conduct, third party audit), they should benefit from less prescriptive requirements. This would allow for flexibility, legal certainty, less administrative burden, highest privacy and security standards for data subjects and transparency for regulators.

Amendment 45

Proposal for a regulation

Article 28 – Paragraph 1

Text proposed by the Commission

Amendment

1. Each controller **and processor** and, if any, the controller's representative, shall maintain documentation of **all** processing operations under its responsibility.

1. Each controller and, if any, the controller's representative shall maintain **appropriate** documentation of **the main** processing operations under its responsibility.'

Or. en

Justification

The proposed documentation obligation is disproportionate since it covers virtually every data processing activity. It risks defeating the objective of the draft Regulation to reduce administrative burdens. The changes aim to achieve effective data protection, by requiring organisations to document their main data processing activities. Processors should not be subject to the documentation requirement as they usually do not have access to data or other processing strategies which remain the remit of the controller. This amendment is also consistent with the amendment to Article 26.2.

Amendment 46

Proposal for a regulation

Article 28 – Paragraph 2

Text proposed by the Commission

Amendment

2. The documentation shall contain **at least** the following information:...

2. The documentation shall contain the following information:...

Or. en

Justification

This amendment is consistent with the amendment to Article 28.1.

Amendment 47

Proposal for a regulation

Article 28 – Paragraph 3

Text proposed by the Commission

Amendment

3. The controller **and the processor** and, if any, the controller's representative, shall make the documentation available, on request, to the supervisory authority.

3. The controller and, if any, the controller's representative, shall make the documentation available, on request, to the supervisory authority.

Or. en

Justification

This amendment is consistent with the amendment to Article 26.2, Article 26.2 point g and h, and Article 28.1.

Amendment 48
Proposal for a regulation
Article 28 – Paragraph 4

Text proposed by the Commission

Amendment

4. The obligations referred to in paragraphs 1 and 2 shall not apply to the following controllers **and processors**:

4. The obligations referred to in paragraphs 1 and 2 shall not apply to the following controllers:

Or. en

Justification

This amendment is consistent with the amendment to Article 26.2.

Amendment 49
Proposal for a regulation
Article 33 – Paragraph 1

Text proposed by the Commission

Amendment

1. Where processing operations present **specific** risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller **or the processor acting on the controller's behalf** shall carry out an assessment of the impact of the envisaged processing operations on the **protection of personal data**.

1. Where processing operations **are likely to** present **significant** risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller shall carry out an assessment of the impact of the envisaged processing operations on the **fundamental rights and freedoms of the data subjects**.

Or. en

Justification

This amendment is consistent with the amendment to 26.2. Furthermore, it proposes to limit the requirement for impact assessments to situations involving significant risks for data subjects, in order to funnel the priority towards assuring effective privacy protection rather than fulfilling burdensome administrative requirements. This is in line with the ethos of the data protection reform, which was intended to instil a culture of accountability backed by ex-post oversight rather than perpetuate ex-ante 'box-ticking.

Amendment 50
Proposal for a regulation
Article 33 – Paragraph 2

Text proposed by the Commission

Amendment

2. The following processing operations in particular present **specific** risks referred to in paragraph 1:

2. The following processing operations in particular **are likely to** present **such significant** risks **as** referred to in paragraph 1:

Or. en

Justification

This amendment is consistent with the amendment to Article 33.1.

Amendment 51
Proposal for a regulation
Article 33 – Paragraph 4

Text proposed by the Commission

Amendment

4. The controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations.

Or. en

Justification

Considering the data subject's need to be informed of the data processing in accordance with Article 14, an obligation to consult data subjects as part of the data impact assessment appears misplaced and unnecessary. It could also likely result in compromising important trade secrets.

Amendment 52
Proposal for a regulation
Article 34 – Paragraph 1

Text proposed by the Commission

Amendment

1. The controller **or the processor as the case may be** shall obtain an authorisation from the supervisory authority prior to the processing of personal data, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where a controller or processor adopts contractual clauses as provided for in point (d) of Article 42(2) or does not provide for the appropriate safeguards in a legally binding instrument as referred to in Article 42(5) for the transfer of personal data to a third country or an international organisation.

1. The controller shall obtain an authorisation from the supervisory authority prior to the processing of personal data, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where a controller or processor adopts contractual clauses as provided for in point (d) of Article 42(2) or does not provide for the appropriate safeguards in a legally binding instrument as referred to in Article 42(5) for the transfer of personal data to a third country or an international organisation.

Or. en

Justification

This amendment is consistent with the amendment to Article 26.1 and Article 26.2.

Amendment 53
Proposal for a regulation
Article 34 – Paragraph 2

Text proposed by the Commission

Amendment

2. The controller shall consult the supervisory

2. The controller *or processor acting on the controller's behalf* shall consult the supervisory authority prior to the processing of personal data in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where:

authority prior to the processing of personal data in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where:

Or. en

Justification

This amendment is consistent with the amendment to Article 26.1 and Article 26.2.

Amendment 54

Proposal for a regulation

Article 34 – Paragraph 2 – point a

Text proposed by the Commission

Amendment

(a) a data protection impact assessment as provided for in Article 33 indicates that processing operations are by virtue of their nature, their scope or their purposes, likely to present a high degree of *specific* risks; or

(a) a data protection impact assessment as provided for in Article 33 indicates that processing operations are by virtue of their nature, their scope or their purposes, likely to present a high degree of *significant* risks; or

Or. en

Justification

This amendment is consistent with the amendment to Recital 70 and Article 33.1.

Amendment 55

Proposal for a regulation

Article 34 – Paragraph 6

Text proposed by the Commission

Amendment

6. The controller *or processor* shall provide the supervisory authority with the data protection impact assessment provided for in Article 33 and, on request, with any other information to allow the supervisory authority to make an assessment of the compliance of the processing and in particular of the risks for the protection of personal data of the data subject and of the related safeguards.

6. The controller shall provide the supervisory authority with the data protection impact assessment provided for in Article 33 and, on request, with any other information to allow the supervisory authority to make an assessment of the compliance of the processing and in particular of the risks for the protection of personal data of the data subject and of the related safeguards.

Or. en

Justification

This amendment is consistent with the amendment to Article 26.1 and Article 26.2.

Amendment 56

Proposal for a regulation

Article 35 – Paragraph 1

Text proposed by the Commission

Amendment

1. The controller **and** the processor shall designate a data protection officer in any case where:

1. The controller **or** the processor shall designate a data protection officer in any case where:

Or. en

Justification

Only one DPO should be required for all subsidiaries of a group established in the Union, regardless of size and activity, instead of a separate DPO for every Member State in which that entity operates. This allows for consistency and ease of communication for data subjects and supervisory authorities.

Amendment 57

Proposal for a regulation

Article 35 – paragraph 2

Text proposed by the Commission

Amendment

2. In the case referred to in point (b) of paragraph 1, a group of undertakings may appoint a single data protection officer.

2. In the case referred to in point (b) **and (c)** of paragraph 1, a group of undertakings may appoint a single data protection officer.

Or. en

Justification

Only one DPO should be required for all subsidiaries of a group established in the Union, regardless of size and activity, instead of a separate DPO for every Member State in which that entity operates. This allows for consistency and ease of communication for data subjects and supervisory authorities.

Amendment 58

Proposal for a regulation

Article 38 – paragraph 1

Text proposed by the Commission

Amendment

1. The Member States, the supervisory authorities and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various data processing sectors, in particular in relation to:

1. The Member States, the supervisory authorities and the Commission shall encourage the drawing up of **voluntary** codes of conduct **and self-regulatory schemes** intended to contribute to the proper application of this Regulation, taking account of the specific features of the various data processing sectors, in particular in relation to:

Or. en

Justification

This amendment aims to clarify the voluntary nature of self-regulation and to extend the scope of the Article to other self-regulatory mechanisms that have the same function and are hence as viable as codes of conducts.

Amendment 59

Proposal for a regulation

Article 38 – paragraph 2

Text proposed by the Commission

2. Associations and other bodies representing categories of controllers or processors in one Member State which intend to draw up codes of conduct or to amend or extend existing codes of conduct may submit them to an opinion of the supervisory authority in that Member State. The supervisory authority *may* give an opinion whether the draft **code of conduct** or the amendment is in compliance with this Regulation. The supervisory authority shall seek the views of data subjects or their representatives on these drafts.

Amendment

2. Associations and other bodies representing categories of controllers or processors in one Member State which intend to draw up codes of conduct, **self-regulatory schemes or self-certification mechanisms**, or to amend or extend existing codes of conduct, **self-regulatory schemes or self-certification mechanisms**, may submit them to an opinion of the supervisory authority in that Member State. The supervisory authority **shall** give a **binding** opinion whether the draft or the amendment **of such measure** is in compliance with this Regulation. The supervisory authority shall seek the views of data subjects or their representatives on these drafts.

Or. en

Justification

This amendment aims to extend the scope of the Article to other self-regulatory and self-certification mechanisms that have the same function and are hence as viable as codes of conducts.

Amendment 60

Proposal for a regulation

Article 38 – paragraph 3

Text proposed by the Commission

3. Associations and other bodies representing categories of controllers in several Member States may submit draft codes of conduct and amendments or extensions to existing **codes of conduct** to the Commission.

Amendment

3. Associations and other bodies representing categories of controllers **or processors** in several Member States may submit draft codes of conduct, **self-regulatory schemes or self-certification mechanisms**, and amendments or extensions to **such** existing **measures** to the Commission.

Or. en

Justification

This amendment is in line with the amendment proposed to Article 38.1 and 38.2. It also aims to clarify that the Article applies to processors, the omission of which seems to be a drafting error, as processors are included in Article 38.2.

Amendment 61

Proposal for a regulation

Article 39 – paragraph 1

Text proposed by the Commission

1. The Member States and the Commission shall encourage, in particular at European level, the

Amendment

1. The Member States and the Commission shall encourage, in particular at European level, the

establishment of data protection certification mechanisms and of data protection seals and marks, allowing data subjects to quickly assess the level of data protection provided by controllers and processors. The data protection certifications mechanisms shall contribute to the proper application of this Regulation, taking account of the specific features of the various sectors and different processing operations.

establishment of data protection certification mechanisms, **including self-certification mechanisms**, and of data protection seals and marks, allowing data subjects to quickly assess the level of data protection provided by controllers and processors. The data protection certifications mechanisms shall contribute to the proper application of this Regulation, taking account of the specific features of the various sectors and different processing operations. **They shall be elaborated based on industry-led efforts and in consultation with the supervisory authorities, and shall be capable of global application, affordable and technology neutral.**

Or. en

Justification

This amendment aims to clarify that certification mechanisms and data protection seals and marks should be voluntary, industry-driven, enable competition and allow for innovative solutions for consumers. Given the global nature of the internet and increasing internationalisation of data flows, such certification mechanisms should be open to companies both inside and outside the EEA and be elaborated in consultation with relevant stakeholders. Certification mechanisms can help to reduce compliance burdens and foster competitiveness.

Amendment 62

Proposal for a regulation

Article 51 – paragraph 2

Text proposed by the Commission

2. Where **the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union, and** the controller or processor is established in more than one Member State, the supervisory authority of the main establishment of the controller or processor shall be competent for the supervision of **the** processing activities of **the** controller or the processor in all Member States, **without prejudice to** the provisions of Chapter VII of this Regulation.

Amendment

2. **In situations referred to in Article 3(1) and** where the controller or processor is established in more than one Member State, the supervisory authority of the main establishment of the controller or processor shall be **solely** competent for the supervision of **all** processing activities **that are carried out by or on behalf of that** controller or processor in all Member States, **or in the case of a group of undertakings, by any member of the group, as far as they are subject to this Regulation. The competent supervisory authority of the main establishment shall cooperate with other supervisory authorities in accordance with** the provisions of Chapter VII of this Regulation.

Or. en

Justification

This amendment is consistent with the amendment to Article 4(13). It is intended to further strengthen the so-called one-stop shop concept, according to which the DPA of a company's main establishment is to be the lead for investigative actions and interpreting rules. Other DPAs should serve as liaison point when needed. This language will help to provide consumers and multinational companies with legal certainty as to which competent supervisory authority will have authority to supervise any data processing activities subject to the Regulation. It will also prevent multiple supervisory authorities from sanctioning the same company for the same incident.

Amendment 63
Proposal for a regulation
Article 51 – paragraph 2a (new)

Text proposed by the Commission

Amendment

2a. In situations referred to in Article 3(2) and where the controller has designated a representative in the Union pursuant to Article 25, the supervisory authority of the establishment of the representative shall be solely competent for the supervision, in all Member States, of all processing activities that are carried out by or on behalf of that controller.

Or. en

Justification

This amendment is consistent with the amendment to recital 63. It intends to ensure respect of the EU principle of non-discrimination by affording the benefit of the one stop shop principle also to non-EU controllers who appoint an EU representative. They should benefit from one of the main anchors of the draft Regulation in the same way as EU established companies, given that they are subject to the same rights and obligations of the draft Regulation.

Amendment 64
Proposal for a regulation
Article 52 – paragraph 1

Text proposed by the Commission

Amendment

1. The supervisory authority shall:

1. The **competent** supervisory authority **pursuant to Article 51** shall:

Or. en

Justification

This amendment is consistent with the amendment to Article 51.2.

Amendment 65
Proposal for a regulation
Article 52 – paragraph 3

Text proposed by the Commission

Amendment

3. The supervisory authority shall, upon request, advise any data subject in exercising the rights under this Regulation and, if appropriate, co-operate with the supervisory authorities in other Member States to this end.

3. The **competent** supervisory authority **pursuant to Article 51** shall, upon request, advise any data subject in exercising the rights under this Regulation and, if appropriate, co-operate with the supervisory authorities in other Member States to this end.

Or. en

Justification

This amendment is consistent with the amendment to Article 51.2.

Amendment 66

Proposal for a regulation

Article 53 – paragraph 1

Text proposed by the Commission

Amendment

1. Each supervisory authority shall have the power:

1. **The competent** supervisory authority **pursuant to Article 51** shall have the power:

Or. en

Justification

This amendment is consistent with the amendment to Article 51.2.

Amendment 67

Proposal for a regulation

Article 53 – paragraph 1 – point b

Text proposed by the Commission

Amendment

(b) to order the controller **or the processor** to comply with the data subject's requests to exercise the rights provided by this Regulation;

(b) to order the controller to comply with the data subject's requests to exercise the rights provided by this Regulation;

Or. en

Justification

This amendment is consistent with the amendment to Article 26.1 and 26.2.

Amendment 68

Proposal for a regulation

Article 53 – paragraph 1 – point c

Text proposed by the Commission

Amendment

(c) to order the controller **and the processor**, and, where applicable, the representative to provide any information relevant for the performance of its duties;

(c) to order the controller, and, where applicable, the representative to provide any information relevant for the performance of its duties;

Or. en

Justification

This amendment is consistent with the amendment to Article 26.1 and 26.2.

Amendment 69

Proposal for a regulation

Article 53 – paragraph 1 – point e

Text proposed by the Commission

Amendment

(e) to warn or admonish the controller **or the processor**;

(e) to warn or admonish the controller;

Or. en

Justification

This amendment is consistent with the amendment to Article 26.1 and 26.2.

Amendment 70

Proposal for a regulation

Article 53 – paragraph 2

Text proposed by the Commission

Amendment

2. **Each** supervisory authority shall have the investigative power to obtain from the controller **or the processor**:

2. **The competent** supervisory **authority pursuant to Article 51** shall have the investigative power to obtain from the controller:

Or. en

Justification

This amendment is consistent with the amendments to Article 26.1, 26.2 and 51.2.

Amendment 71

Proposal for a regulation

Article 53 – paragraph 3

Text proposed by the Commission

Amendment

3. **Each** supervisory authority shall have the power to bring violations of this Regulation to the attention of the judicial authorities and to engage in legal proceedings, in particular pursuant to Article 74(4) and Article 75(2).

3. **The competent** supervisory authority **pursuant to Article 51** shall have the power to bring violations of this Regulation to the attention of the judicial authorities and to engage in legal proceedings, in particular pursuant to Article 74(4) and Article 75(2).

Or. en

Justification

This amendment is consistent with the amendments to Article 51.2.

Amendment 72

Proposal for a regulation

Article 53 – paragraph 4

Text proposed by the Commission

Amendment

4. **Each** supervisory authority shall have the power to sanction administrative offences, in particular those referred to in Article 79(4), (5) and (6).

4. **The competent** supervisory authority **pursuant to Article 51** shall have the power to sanction administrative offences, in particular those referred to in Article 79(4), (5) and (6).

Or. en

Justification

This amendment is consistent with the amendments to Article 51.2.

Amendment 73

Proposal for a regulation

Article 53 – paragraph 4a (new)

Text proposed by the Commission

Amendment

4a. The competent supervisory authority pursuant to Article 51 shall serve as the primary contact and reference point for any action to be implemented in accordance with Chapter VII of this Regulation. Other supervisory authorities shall refer any matter concerning a controller under the jurisdiction of the competent supervisory authority to that authority.

Or. en

Justification

This amendment is consistent with the amendments to Article 51.2.

Amendment 74

Proposal for a regulation

Article 55 – paragraph 8

Text proposed by the Commission

Amendment

8. Where a supervisory authority does not act within one month on request of another supervisory authority, the requesting supervisory authorities **shall be competent to take a provisional measure on the territory of its Member State in accordance with Article 51(1) and** shall submit the matter to the European Data Protection Board in accordance with the procedure referred to in Article 57.

8. Where a supervisory authority does not act within one month on request of another supervisory authority, the requesting supervisory authorities shall submit the matter to the European Data Protection Board in accordance with the procedure referred to in Article 57.

Or. en

Justification

This amendment is consistent with the amendments to Article 51.2. The draft Regulation should reflect the practical viability and resources affecting mutual assistance duties between supervisory authorities.

Amendment 75
Proposal for a regulation
Article 55 – paragraph 9

Text proposed by the Commission

Amendment

9. The supervisory authority shall specify the period of validity of such provisional measure. This period shall not exceed three months. The supervisory authority shall, without delay, communicate those measures, with full reasons, to the European Data Protection Board and to the Commission.

deleted

Or. en

Justification

This amendment is consistent with the amendments to Article 51.2. The draft Regulation should reflect the practical viability and resources affecting mutual assistance duties between supervisory authorities.

Amendment 76
Proposal for a regulation
Article 58 – paragraph 1

Text proposed by the Commission

Amendment

1. Before **a** supervisory authority adopts a measure referred to in paragraph 2, this supervisory authority shall communicate the draft measure to the European Data Protection Board and the Commission.

1. Before **the competent** supervisory authority adopts a measure referred to in paragraph 2, this supervisory authority shall communicate the draft measure to the European Data Protection Board and the Commission.

Or. en

Justification

This amendment is consistent with the amendments to Article 51.2.

Amendment 77
Proposal for a regulation
Article 58 – paragraph 2 – point a

Text proposed by the Commission

Amendment

(a) relates to processing activities which are related to the offering of goods or services **to** data subjects in several Member States, or to the monitoring of their behaviour; or

(a) relates to processing activities which are related to the offering of goods or services **specifically targeted at** data subjects in several Member States, or to the monitoring of their behavior, **and where the controller not established in the Union has not appointed a representative in the territory of the Union**; or

Or. en

Justification

The first part of this amendment is consistent with the amendment to Article 3.2. The second part of this amendment aims to limit the scope of applicability of the consistency mechanism to those cases where consistency of data protection enforcement is truly at stake. It would seem unjustified to automatically apply the consistency mechanism to non-EU established companies that are subject to the Regulation in all circumstances, particularly where these have appointed a representative in the EU. The competence of the data protection board over non- EU established companies that are subject to the Regulation should be equivalent to that over EU companies.

Amendment 78

Proposal for a regulation

Article 58 – paragraph 2 – point c

Text proposed by the Commission

Amendment

(c) aims at adopting a list of the processing operations subject to prior consultation pursuant to Article 34(5);
or

deleted

Or. en

Justification

This amendment is consistent with the amendment to Article 58.2(a). The consistency mechanism should remain an exceptional mechanism and not a body of appeal of legitimate decisions of the competent Data Protection Authority. Otherwise there is the risk that the consistency mechanism becomes an appeal mechanism that slows down decision taking and becomes a bureaucratic step to the detriment of all actors.

Amendment 79

Proposal for a regulation

Article 58 – paragraph 3

Text proposed by the Commission

Amendment

3. Any supervisory authority or the European Data Protection Board may request that any matter shall be dealt with in the consistency mechanism, in particular where **a** supervisory authority does not submit a draft measure referred to in paragraph 2 or does not comply with the obligations for mutual assistance in accordance with Article 55 or for joint operations in accordance with Article 56.

3. Any supervisory authority or the European Data Protection Board may request that any matter shall be dealt with in the consistency mechanism, in particular where **the competent** supervisory authority does not submit a draft measure referred to in paragraph 2 or does not comply with the obligations for mutual assistance in accordance with Article 55 or for joint operations in accordance with Article 56.

Or. en

Justification

This amendment is consistent with the amendments to Article 51.2.

Amendment 80

Proposal for a regulation

Article 58 – paragraph 4

Text proposed by the Commission

Amendment

4. In order to ensure correct and consistent application of this Regulation, the Commission may request that any matter shall be dealt with in the consistency mechanism.

4. In order to ensure correct and consistent application of this Regulation, the Commission may request that any matter ***related to the category of measures referred to in paragraph 2*** shall be dealt with in the consistency mechanism.

Or. en

Justification

This amendment is consistent with the amendments to Article 51.2 point c.

Amendment 81

Proposal for a regulation

Article 58 – paragraph 7

Text proposed by the Commission

Amendment

7. The European Data Protection Board shall issue an opinion on the matter, if the European Data Protection Board so decides by ***simple*** majority of its members or any supervisory authority or the Commission so requests within one week after the relevant information has been provided according to paragraph 5. The opinion shall be adopted within one month by ***simple*** majority of the members of the European Data Protection Board. The chair of the European Data Protection Board shall inform, without undue delay, the supervisory authority referred to, as the case may be, in paragraphs 1 and 3, the Commission ***and*** the supervisory authority competent under Article 51 of the opinion and make it public.

7. The European Data Protection Board shall issue an opinion on the matter, if the European Data Protection Board so decides by ***qualified*** majority of its members or any supervisory authority or the Commission so requests within one week after the relevant information has been provided according to paragraph 5. The opinion shall be adopted within one month by ***qualified*** majority of the members of the European Data Protection Board. The chair of the European Data Protection Board shall inform, without undue delay, the supervisory authority referred to, as the case may be, in paragraphs 1 and 3, the Commission, the ***competent*** supervisory ***and the controller or processor*** of the opinion and make it public.

Or. en

Justification

This amendment is consistent with the amendments to Recital 106 and Article 51.2. The controller or processor should be informed about any opinion of the European Data Protection Board as far as they are concerned by the content of such opinion.

Amendment 82

Proposal for a regulation

Article 58 – paragraph 7

Text proposed by the Commission

Amendment

8. The ***supervisory*** authority referred to in paragraph 1 ***and the supervisory authority competent under***

8. The ***competent*** supervisory authority referred to in paragraph 1 shall take account of the opinion of the

Article 51 shall take account of the opinion of the European Data Protection Board and shall within two weeks after the information on the opinion by the chair of the European Data Protection Board, electronically communicate to the chair of the European Data Protection Board and to the Commission whether it maintains or amends its draft measure and, if any, the amended draft measure, using a standardised format.

European Data Protection Board and shall within two weeks after the information on the opinion by the chair of the European Data Protection Board, electronically communicate to the chair of the European Data Protection Board and to the Commission whether it maintains or amends its draft measure and, if any, the amended draft measure, using a standardised format.

Or. en

Justification

This amendment is consistent with the amendments to Article 51.2.

Amendment 83

Proposal for a regulation

Article 59 – paragraph 2

Text proposed by the Commission

Amendment

2. Where the Commission has adopted an opinion in accordance with paragraph 1, the supervisory authority concerned shall take utmost account of the Commission's opinion and inform the Commission and the European Data Protection Board whether it intends to maintain or amend its draft measure.

2. Where the Commission has adopted an opinion in accordance with paragraph 1, the **competent** supervisory authority concerned shall take utmost account of the Commission's opinion and inform the Commission and the European Data Protection Board whether it intends to maintain or amend its draft measure.

Or. en

Justification

This amendment is consistent with the amendments to Article 51.2.

Amendment 84

Proposal for a regulation

Article 59 – paragraph 4

Text proposed by the Commission

Amendment

4. Where the **supervisory** authority concerned intends not to follow the opinion of the Commission, it shall inform the Commission **and** the European Data Protection Board thereof within the period referred to in paragraph 1 and provide a justification. In this case the draft measure shall not be adopted for one further month.

4. Where the **competent** supervisory authority concerned intends not to follow the opinion of the Commission, it shall inform the Commission, the European Data Protection Board **and the controller or processor** thereof within the period referred to in paragraph 1 and provide a justification. In this case the draft measure shall not be adopted for one further month.

Or. en

Justification

The first part of the amendment is consistent with the amendment to Article 51.2. The controller or processor should be informed about any decision of the competent supervisory authority as far as they are directly or

indirectly, effectively or potentially concerned by the content of such decision.

Amendment 85

Proposal for a regulation

Article 61 – paragraph 1

Text proposed by the Commission

1. In exceptional circumstances, where **a** supervisory authority considers that there is an urgent need to act in order to protect the interests of data subjects, in particular when the danger exists that the enforcement of a right of a data subject could be considerably impeded by means of an alteration of the existing state or for averting major disadvantages or for other reasons, by way of derogation from the procedure referred to in Article 58, it may immediately adopt provisional measures with a specified period of validity. The **supervisory** authority shall, without delay, communicate those measures, with full reasons, to the European Data Protection Board **and to the Commission**.

Amendment

1. In exceptional circumstances, where **the competent** supervisory authority considers that there is an urgent need to act in order to protect the interests of data subjects, in particular when the danger exists that the enforcement of a right of a data subject could be considerably impeded by means of an alteration of the existing state or for averting major disadvantages or for other reasons, by way of derogation from the procedure referred to in Article 58, it may immediately adopt provisional measures with a specified period of validity. The **competent** supervisory authority shall, without delay, communicate those measures, with full reasons, to the European Data Protection Board, the Commission **and the controller or processor**.

Or. en

Justification

The first part of the amendment is consistent with the amendment to Article 51.2. The controller or processor should be informed about any decision of the competent supervisory authority as far as they are directly or indirectly, effectively or potentially concerned by the content of such decision or any measure the competent authority intends to take.

Amendment 86

Proposal for a regulation

Article 61 – paragraph 2

Text proposed by the Commission

2. Where **a** supervisory authority has taken a measure pursuant to paragraph 1 and considers that final measures need urgently be adopted, it may request an urgent opinion of the European Data Protection Board, giving reasons for requesting such opinion, including for the urgency of final measures.

Amendment

2. Where **the competent** supervisory authority has taken a measure pursuant to paragraph 1 and considers that final measures need urgently be adopted, it may request an urgent opinion of the European Data Protection Board, giving reasons for requesting such opinion, including for the urgency of final measures.

Or. en

Justification

This amendment is consistent with the amendment to Article 51.2.

Amendment 87

Proposal for a regulation

Article 63 – paragraph 1

Text proposed by the Commission

Amendment

1. For the purposes of this Regulation, an enforceable measure of the supervisory authority of one Member State shall be enforced in all Member States concerned.

1. For the purposes of this Regulation, an enforceable measure of the **competent** supervisory authority of one Member State shall be enforced in all Member States concerned.

Or. en

Justification

This amendment is consistent with the amendment to Article 51.2.

Amendment 88

Proposal for a regulation

Article 63 – paragraph 2

Text proposed by the Commission

Amendment

2. Where **a** supervisory authority does not submit a draft measure to the consistency mechanism in breach of Article 58(1) to (5), the measure of the supervisory authority shall not be legally valid and enforceable.

2. Where **the competent** supervisory authority does not submit a draft measure to the consistency mechanism in breach of Article 58(1) to (5), the measure of the supervisory authority shall not be legally valid and enforceable.

Or. en

Justification

This amendment is consistent with the amendment to Article 51.2.

Amendment 89

Proposal for a regulation

Article 66 – paragraph 1

Text proposed by the Commission

Amendment

1. The European Data Protection Board shall ensure the consistent application of this Regulation. To this effect, the European Data Protection Board shall, on its own initiative **or** at the request of the Commission, in particular:

1. The European Data Protection Board shall ensure the consistent application of this Regulation. To this effect, the European Data Protection Board shall, on its own initiative, at the request of the Commission **or other interested parties**, in particular:

Or. en

Justification

Interested parties should have the possibility to access the European Data Protection Board and submit to it data protection related matters of concern in terms of consistent EU-wide application.

Amendment 90

Proposal for a regulation

Article 66 – paragraph 1 – point b

Text proposed by the Commission

(b) examine, on its own initiative or on request of one of its members or on request of the Commission, any question covering the application of this Regulation and issue guidelines, recommendations and best practices addressed to the supervisory authorities in order to encourage consistent application of this Regulation;

Amendment

(b) examine, on its own initiative or on request of one of its members or on request of the Commission **or other interested parties**, any question covering the application of this Regulation and issue guidelines, recommendations and best practices addressed to the supervisory authorities in order to encourage consistent application of this Regulation;

Or. en

Justification

This amendment is in line with amendment to Article 66.1.

Amendment 91

Proposal for a regulation

Article 66 – paragraph 4 (new)

Text proposed by the Commission

Amendment

4a. Where appropriate, the European Data Protection Board shall, in its execution of the tasks as outlined in this Article, consult interested parties and give them the opportunity to comment within a reasonable period. The European Data Protection Board shall, without prejudice to Article 72, make the results of the consultation procedure publicly available.

Or. en

Justification

This amendment intends to provide interested parties the opportunity to be consulted and provide comments within a reasonable timeframe before the European Data Protection Board adopts opinions or reports. The possibility for industry to be consulted also exists in other regulatory domains (e.g. the European Regulators Group BEREC in the context of the EU's telecoms regulatory framework).

Amendment 92

Proposal for a regulation

Article 77 – paragraph 1

1. Any person who has suffered damage as a result of an unlawful processing operation or of an action incompatible with this Regulation shall have the right to receive compensation from the controller **or the**

Amendment

1. Any person who has suffered damage as a result of an unlawful processing operation or of an action

processor for the damage suffered.

incompatible with this Regulation shall have the right to receive compensation from the controller for the damage suffered.

Or. en

Justification

This amendment is consistent with the amendments to Article 26.

Amendment 93

Proposal for a regulation

Article 77 – paragraph 2

Text proposed by the Commission

Amendment

2. Where more than one controller *or processor* is involved in the processing, each controller *or processor* shall be jointly and severally liable for the entire amount of the damage.

2. Where more than one controller is involved in the processing, each controller shall be jointly and severally liable for the entire amount of the damage, ***to the extent that liability has not already been established in the determination of responsibilities envisaged in Article 24.***

Or. en

Justification

This amendment is consistent with the amendments to Article 26.

Amendment 94

Proposal for a regulation

Article 77 – paragraph 3

Text proposed by the Commission

Amendment

3. The controller *or the processor* may be exempted from ***this*** liability, in whole or in part, if the controller *or the processor* proves that ***they are*** not responsible for the event giving rise to the damage.

3. The controller may be exempted from liability ***under paragraph 2***, in whole or in part, if the ***respective*** controller proves that ***it is*** not responsible for the event giving rise to the damage.

Justification

This amendment is consistent with the amendments to Article 26.

Amendment 95

Proposal for a regulation

Article 77 – paragraph 3a (new)

Text proposed by the Commission

Amendment

3a. If a processor processes personal data other than as instructed by the controller, he may be held liable should any person suffer damage as a result of such

processing.

Justification

This amendment is consistent with the amendments to Article 26.

MEP Christian Engström
Parlement européen
Bât. Altiero Spinelli 08G153
60, rue Wiertz B-1047 Bruxelles/Brussel

November 19th, 2012

Dear Mr. Engström,

Nokia is very interested in the draft Data Protection Regulation. The legislation will heavily impact on our ability to seek for optimal protection of our customer's data, our possibilities to successfully offer location-based services, and it will determine whether a globally competitive digital marketplace can develop in Europe.

As the political work on the proposed Data Protection Regulation advances, we understand that key issues are being singled out by the rapporteur, shadows and other interested Members of Parliament, for being made subject to amendments. On the basis of our solid and long-term data protection experience, we would like to recommend that the 'Accountability' principle receives high attention in the parliamentary work and be implemented in the Regulation.

The Accountability concept lays down essential elements of an effective privacy program that all data controllers need to implement, rather than being confronted with old-fashioned static and detailed compliance requirements. This allows controllers to operate according to the best suited up-to-date tools to deliver optimal data protection. It is through the implementation of the accountability concept that Nokia managed to undergo a real transformation towards embracing a true privacy culture. The company is now pro-actively integrating privacy solutions at early stages and in a horizontal fashion into all products and processes instead of perceiving data protection merely as a compliance-led ex-post audit activity.

The Regulation will have to strike a balance between the effective protection of private data and not over-burdening SMEs with obligations. And also in this respect, it would be better to opt for the flexible and size-adaptable Accountability approach rather than working with multiple exceptions for SMEs which complicate the legislation and ultimately reduce protection of data subjects.

Nokia supports the harmonization approach and a sufficient level of detail where this is appropriate (definitions, privacy principles, conditions for processing). But over-prescriptive and inflexible requirements in other sections (art. 28 'documentation', art. 33 'data protection impact assessment' and 34 (prior authorization and consultation etc.) will lead to burdensome compliance-driven approaches within companies and turn the focus away from implementing optimal protection according to the Accountability principle. Mandating data protection impact assessments for instance for an arbitrarily selected 'rough' category of processing operations and obliging controllers to await reviews by DPAs of the considerable amounts of assessments that will be submitted every week will not be the best way to identify and mitigate risks.

Please find attached to this letter a one pager describing the Accountability concept in further detail and a set of draft amendments which would implement the concept in the draft Regulation. Please do not hesitate to contact us if you have questions or if you would like to discuss this issue in more detail.

Best regards,



Mikko Niva

A new experience for utility customers

The future of customer engagement starts with better information

COMPANY HIGHLIGHTS

- » Working with more than 75 utility clients—including 8 of the 10 largest in the US—to engage more than 15 million customers
- » A multi-channel Software-as-a-Service (SaaS) solution
- » 250+ employees
- » More than \$20 million in R&D investment
- » Founded in 2007, with offices in Arlington, VA, San Francisco, CA and London, UK



About Opower

Opower was founded on a simple premise: it's time to engage the millions of people who are in the dark about their energy use. We're the industry's only customer engagement solutions provider designed to motivate customers across multiple channels and on a large scale. Our Software-as-a-Service platform combines cutting-edge behavioural science techniques and a patent-pending data-analytics engine to provide an unparalleled customer experience—one that enables our utility partners to connect with their customers in a highly targeted fashion.

Since being founded in 2007, we have grown rapidly to more than 250 employees, and now work with more than 75 utility clients—including 8 of the 10 largest utilities in the United States. On behalf of our clients, we currently serve more than 15 million customers; the number of households we reach is growing at an exponential rate, as existing clients expand their current programmes and new clients embrace our platform.

Why Opower?

Utilities partner with us to drive measurable business results across a range of strategic initiatives. Our solutions consistently generate cost-effective, verified, sustainable energy savings, along with increased participation in other utility-marketed programmes. Our programmes also motivate customers to reduce their energy use during peak times and seasons—when it matters the most. For utilities with Smart Grid deployments, we promote customer acceptance of Advanced Metering Infrastructure (AMI) through clearly demonstrating its value. In competitive utility markets, we increase customer lifetime value through enhanced acquisition and retention rates, and cross-sale of other utility services. This is all done with a clear focus on customer experience, leading to increases in overall customer satisfaction.

“Opower is changing the way people interact with their utilities.”

—BLOOMBERG BUSINESSWEEK

SELECTED CLIENTS

- » AEP Ohio (OH)
- » Arizona Public Service (AZ)
- » Burbank Water and Power (CA)
- » Commonwealth Edison (IL)
- » Connexus Energy (MN)
- » Constellation / Baltimore Gas & Electric (MD)
- » EDF (France)
- » First Utility (UK)
- » Southern Company / Gulf Power (FL)
- » National Grid (MA, NY)
- » Pacific Gas & Electric (CA)
- » PPL Electric Utilities (PA)
- » San Diego Gas & Electric (CA)
- » Xcel Energy (MN, CO)

AWARDS

- » Cleantech Group names Opower "2012 Global Cleantech 100 Company of the Year"
- » World Economic Forum names Opower a 2011 "Global Tech Pioneer"
- » *BusinessWeek* names Opower one of "50 Tech Start-Ups to Know About"
- » The *Washington Post* names Opower one of "5 Companies that Will Lead in 2011"

Opower's unique customer engagement solution suite

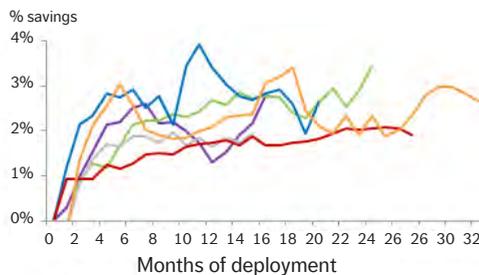
Our approach to customer engagement puts every customer's energy use in personal perspective: through providing them with better information, we empower people to take greater control of the way they use energy, and do so regardless of age, income, education, or access to technology. We merge and analyse utility and third-party data streams to create individual customer profiles, and use those profiles to generate personalised insights delivered through the channels via which customers are most apt to respond. Across our entire platform, we generate targeted messaging that leverages each channel's distinct advantages in order to engage and motivate customers on an ongoing basis.



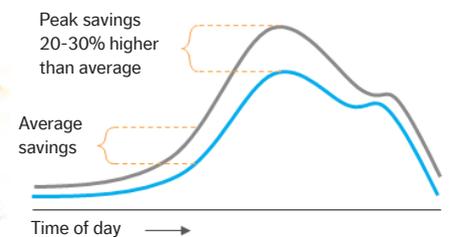
Opower's results

We've measured and verified our results with our utility partners since Day One, and we've built an expanding data array that comes to a simple, compelling conclusion: Opower works.

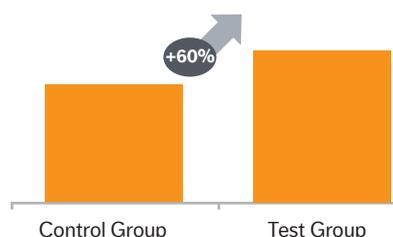
Energy savings



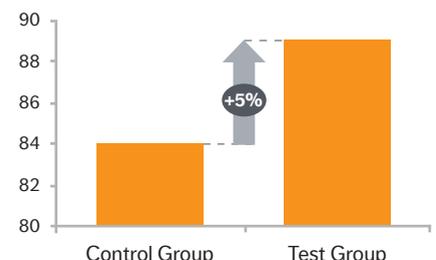
Peak reduction



Programme participation



Customer satisfaction



For more information, please contact us at solutions@opower.com

Opower's position on the European Commission's proposal for a General Data Protection Regulation

About Opower

Opower is the global leader in behavioural energy efficiency and smart grid customer engagement. Opower works with over 75 utilities globally, including 8 of the 10 largest in the United States, with EDF in France and with First Utility in the United Kingdom, to deliver energy savings to nearly 15 million households.

Through September 2012, Opower has saved families over 1.5 Terawatt-hours, which is equivalent to about €140 million in householder bill savings.

Opower combines behavioural science techniques and data-analytics to engage householders and empower them to take greater control of the way they use energy by providing them with better information. We merge and analyse utility and third-party data streams to create individual customer profiles, and use those profiles to generate personalised insights delivered through the channels via which customers are most apt to respond (e.g. paper, web, mobile phones).

Opower's behaviour-based programmes generate sustained, verified, and cost-effective energy savings across all consumer segments, regardless of age, income, education, or relative access to technology. Our programmes also motivate customers to reduce their energy use during peak times and seasons—when it matters the most. For utilities with Smart Grid deployments, we promote customer acceptance of Advanced Metering Infrastructure (AMI) by clearly demonstrating its value to consumers.

Comments on the General Data Protection Regulation proposal

Opower would like to offer comments on two main areas of the proposal:

- 1) The legitimate interest of the controller to process personal data in the energy sector.
- 2) The need to include a definition of anonymous data

1) Legitimate interest of the controller - recitals 30 to 38 and Article 5(b)

This is a widely used and legally defined principle, and Opower strongly believes that the integrity of the current text cannot be undermined.

Opower believes that the meaning of "legitimate interest" of the controller should be clarified with respect to the electricity and gas utilities and distribution network operators.

Energy utilities and distribution network operators have traditionally taken a conservative approach to when and how they would allow processors to analyse customers' personal data. In order for data analytics firms such as Opower to operate in this industry, utilities must be comfortable that the use processors make of their customers' personal data fulfils their legitimate interests as indicated in the proposed Regulation.

To this aim, Opower recommends the inclusion of language providing clarification around the legitimate interest of energy data controllers (e.g. energy retailers, distribution system operators) and processors.

The proposed text is based on principles that have been successfully adopted in California¹ in 2010, which has been a leader in implementing smart grid technology while preserving consumer privacy.

Proposed amendment:

Recital (40) (new)

The processing of data to the extent strictly necessary for the purposes of ensuring that electrical or distribution system operators as defined in Directive 2009/72/EC and Directive 2009/73/EC can meet system, grid, or operational needs, or the implementation of demand response, energy management, or energy efficiency programs, provided that the electrical or gas undertaking or the distribution system operator has required by contract that the processor fulfils the requirements outlined in this Regulation.

2) The need to exclude anonymised data from the scope of the proposed Regulation

Some important services provided by Opower rely on the use of anonymised data. These include, for example, the comparison of energy usage of a data subject who receives information from Opower with usage of similar anonymised data, and the use of anonymised data for evaluating, monitoring and verifying the energy savings achieved through Opower programmes.

Recital 23 of the proposed Regulation excludes data rendered anonymous from the scope of the Regulation.

However, the proposal does not provide a definition of anonymised data, and an exclusion from its scope in the legally binding part of the text.

Proposed amendments

Article 4: Definitions

For the purposes of this Regulation:

(...)

4(3): ‘anonymised data’ shall mean information that has never related to a data subject or has been collected, altered or otherwise processed so that it cannot be attributed to a data subject.

Article 2: Material Scope

2(2): This Regulation does not apply to the processing of personal data:

2(2)(f): that has been anonymised.

¹¹ http://www.leginfo.ca.gov/pub/09-10/bill/sen/sb_1451-1500/sb_1476_bill_20100929_chaptered.html

APPENDIX

Opower's Approach to personal data protection

Opower implements an all-encompassing approach to safeguarding consumer energy data that exceeds legal standards in the US and helps preserve the fundamental right to personal data protection in accord with European Union Directive 95/46/EC.

- **Opower Data Principles:** Opower has proactively embedded Privacy by Design in a set of Data Principles that guide data, privacy and security practices at every stage of our business.²
Our approach already embraces the key principles enshrined in the proposed Regulation, namely:
 - **Right to transparency:** Obligates data controllers to provide consumers with transparent and easily understandable information about how data is collected, stored and processed.
 - **Principle of data minimisation:** Requires controllers incorporate privacy by design and protection by default, limiting activity to what is minimally necessary to achieve a purpose.
 - **Right to data access and data portability:** Gives consumers the right to obtain personal data in a commonly used electronic format and to transfer that data to competing service providers.
 - **Right to be forgotten:** Obligates controllers to destroy and no longer process personal data upon demand from the consumer.
- **Best-in-class security:** All data sent to Opower from its supplier clients is delivered through a secure ftp transfer, encrypted, and stored in compliance with SSAE-16 standards.
- **Safe Harbour certification:** Opower complies with the EU Safe Harbor Framework as set forth by the U.S. Department of Commerce and is a licensee of the TRUSTe Privacy Program.

² <http://opower.com/company/data-principles>



Meeting Europe's new efficiency requirements with large-scale behavioural energy-efficiency programmes

Earlier this year, the European Union approved a new Energy Efficiency Directive (EED) that will require energy retailers and/or distributors to achieve up to 1.5% annual energy savings amongst their final customers beginning in 2014¹. Opower can help European energy retailers and distributors meet these new energy-savings obligations by delivering verified, cost-effective savings at scale.

About Opower

Opower is the global leader in customer engagement software for the energy industry. Opower's home energy management software platform combines behavioural science techniques and a patent-pending data-analytics engine to engage householders and empower them to take greater control of the way they use energy through providing them with better information. The Opower platform has consistently delivered energy savings across all consumer segments, regardless of age, income, education, or relative access to technology.

Opower was founded to help energy suppliers and distributors in the United States meet their energy-savings obligations, and our platform currently drives savings among over 14 million residential households in 27 US

states. Through September 2012, Opower has saved families over 1.5 Terawatt-hours, which is equivalent to about €140 million in householder bill savings. Opower works in partnership with over 75 energy suppliers globally, including 8 of the 10 largest in the United States, Australia, New Zealand, and the United Kingdom.

Energy companies choose to work with Opower to meet efficiency goals because Opower's behaviour-based programmes generate sustained, verified, and cost-effective energy savings, while also improving customer satisfaction with their utility.

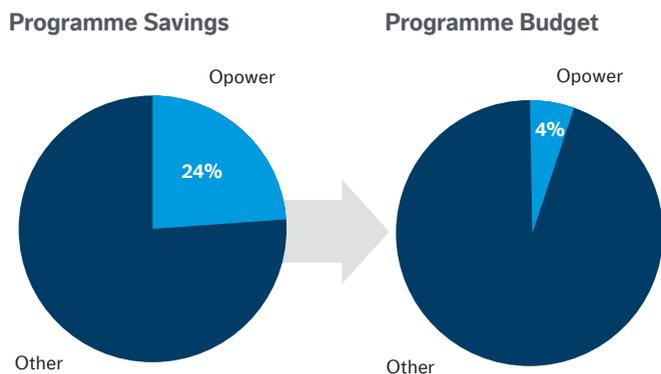
Opower's record of results

Having deployed dozens of behavioural programs and conducted hundreds of large-scale field tests, Opower has amassed the world's largest body of experience and expertise on successfully delivering results from behavioural energy-efficiency programmes. Opower's programmes consistently and predictably deliver verified energy savings of 1.5–3.5%; these savings are sustained over time, allowing utilities with behavioural energy-efficiency programmes to realise significant savings in their portfolios. National Grid, for example, faces some of

1. http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/trans/132717.pdf

the most rigorous energy-efficiency mandates in the US. Its behavioural programmes delivered 24% of its total residential energy-efficiency portfolio from 2010 to 2012, using only 4% of its overall budget.

National Grid (US) three-year efficiency plan



Surveys of tens of thousands of customers in multiple geographies indicate Opower programmes consistently strengthen customer relationships with—and perceptions of—their utility.

Using Opower to meet regulatory requirements

The EU's Energy Efficiency Directive expressly endorses behavioural efficiency as a means of meeting energy-efficiency obligations since these programmes, if implemented correctly, can yield precise, unbiased, and statistically significant results. Opower uses randomised controlled trials to evaluate its programmes. Statistical confidence in these savings is greater than 90% in each case, and has exceeded 95% on many occasions. 17 independent evaluations of these programmes have verified the statistical rigour and accuracy of our approach. As a result, energy suppliers can use Opower's platform with confidence, knowing they will receive credit for their efforts.

For more information about the EED and how Opower can help meet its requirements, please contact:

Michela Beltracchi

Director, EMEA Regulatory Affairs

michela.beltracchi@opower.com

O +44 (0) 203 585 5094

M + 44 (0) 771 023 3474

Nandini Basuthakur

Senior Vice President & Managing Director of Europe, Middle East, and Africa

nandini.basuthakur@opower.com

M + 44 (0) 771 023 3474

Michael Sachse

VP Regulatory Affairs & General Counsel

michael.sachse@opower.com

O +1 571 384 1257

M +1 646 265 0556

eBay Inc. position

Industry, Research and Energy Committee draft opinion on the General Data Protection Regulation

eBay Inc. thanks Sean Kelly MEP for his work for the Industry, Research and Energy Committee on the General Data Protection Regulation proposal. We believe the draft opinion reinforces legal certainty and streamlines the general rules affecting data processing for companies.

As a leading player in connected commerce, eBay Inc. hereby suggests some additional changes, in particular on the main establishment, the extraterritorial scope of the Regulation, the use of consent in situations of ‘significant imbalance between a data controller and data subject’, the right to data portability, the right to rectification, bureaucratic requirements and data breach notification requirements.

Main establishment and one-stop-shop

In order to reinforce legal certainty and avoid disputes over Data Protection Authorities competences, Mr. Kelly rightfully advises for a controller to be responsible to designate its main establishment, based on objective criteria. We believe these criteria should also be explicitly referred to in Recital 27. Secondly, it should be clarified that the designation of an establishment for data protection compliance purposes should be without prejudice to such designation for other purposes of EU law.

Recital 27

Text proposed by the Commission

(27) The main establishment of **a controller** in the Union should be **determined** according to objective criteria and should imply the effective and real exercise of management activities determining the main decisions as to **the purposes, conditions and means of** processing through stable arrangements. This criterion should not depend whether the processing of personal data is actually carried out at that location; the presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute such main establishment and are therefore no determining criteria for a main establishment. **The main establishment of the processor should be the place of its central administration in the Union.**

Amendment

The main establishment of **an enterprise or group of undertakings** in the Union should be **designated** according to objective criteria and should imply the effective and real exercise of management activities determining the main decisions as to **data** processing through stable arrangements. This criterion **shall apply both to data controllers and data processors** and should not depend whether the processing of personal data is actually carried out at that location; the presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute such main establishment and are therefore no determining criteria for a main establishment. **Objective criteria for the designation of main establishment include the global or European headquarters of an enterprise or group of undertakings; the location of the group's European headquarters, or, the location of the company within the group with delegated data protection responsibilities, or, the location of the company which is best placed (in terms of management function, administrative capability etc) to address and enforce the rules as set out in this Regulation, or, the place where the main decisions as to the purposes of processing are taken for the regional group.**

Recital (28 a new)

Text proposed by the Commission

Amendment

(28 a new) The designation of an establishment for data protection compliance purposes should be without prejudice to such designation for other purposes of European Union law such as tax, insolvency and other compliance purposes.

Extraterritorial scope of the Regulation

eBay acknowledges that it is desirable to have companies based outside of the EU respect EU data protection standards when processing personal data of EU citizens. However, in a cross-border context, we believe that the term ‘offering’ of goods and services does not constitute a valid legal basis for determining the applicable law and jurisdiction. In accordance with European Court of Justice jurisprudence, we suggest replacing the word ‘offering’ in Article 3.2(a) with ‘targeting’ or ‘directing’ goods or services and to clarify in corresponding recitals that the mere availability of the controller’s website to a data subject residing in the Union is insufficient to trigger the application of EU data protection laws.

Recital 20

Text proposed by the Commission

Amendment

In order to ensure that individuals are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects residing in the Union by a controller not established in the Union should be subject to this Regulation where the processing activities are related to the offering of goods or services to such data subjects, or to the monitoring of the behaviour of such data subjects.

In order to ensure that individuals are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects residing in the Union by a controller not established in the Union should be subject to this Regulation where the processing activities are related to the offering of goods or services **expressly targeted** to such data subjects, or to the monitoring of the behaviour of such data subjects. **The mere availability of goods and services from third countries to data subjects residing in the Union should not trigger the application of EU data protection legislation.**

Article 3

Text proposed by the Commission

Amendment

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller **or** a processor in the Union.
2. This Regulation applies to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are related to:
(a) the offering of goods or services to such data subjects in the Union; or
(b) the monitoring of their behaviour.
3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where the national law of a Member State applies by virtue of public international law.

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller, a processor **or enterprise** in the Union.
2. This Regulation applies to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are related to:
(a) the offering of goods or services **expressly targeted** to such data subjects in the Union; or
(b) the monitoring of their behaviour.
3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where the national law of a Member State applies by virtue of public international law.

Conditions for consent

We would like to question the notion that an imbalance between a data subject and a data controller (Article 7.4) would invalidate the use of consent as legal ground for processing personal data. eBay considers that the language proposed by the Commission is too broad and could actually miss its target. Let us take the example of a professional seller who works from home and relies on eBay to generate business. eBay would process data that, although business-related, can also be considered personal data as the individual seller would probably use his name and physical address for transactions. The fact that eBay is the main source of revenue of this seller should in no circumstances prevent eBay as a data controller from using consent as a legal ground for processing the seller's personal data. Similarly, data controllers should not be prevented from using consent when their service is very popular thanks to a network effect. eBay believes the objective of this wording is better achieved through court decisions and DPA enforcement on a case-by-case basis taking into account the condition that consent shall only be valid if it is "freely given", as required in the definition of consent (Article 4.8).

Recital 34

Text proposed by the Commission

Amendment

(34) Consent should not provide a valid legal ground for the processing of personal data, where there is a clear imbalance between the data subject and the controller. This is especially the case where the data subject is in a situation of dependence from the controller, among others, where personal data are processed by the employer of employees' personal data in the employment context. Where the controller is a public authority, there would be an imbalance only in the specific data processing operations where the public authority can impose an obligation by virtue of its relevant public powers and the consent cannot be deemed as freely given, taking into account the interest of the data subject.

Deleted

Article 7 – paragraph 4

Text proposed by the Commission

Amendment

4. Consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller.

Deleted

RIGHT TO DATA PORTABILITY

Article 18 is meant to establish data portability rights for user-generated content stored on platform systems to avoid 'lock-in'. However, it has been drafted to apply to any type of personal data in any type of processing, including non-platform systems used in the back office of the data controller. Non-platform systems, such as Human Resources - or Customer Relationship Management-systems, are created serving the purposes of the data controller only. The data in such systems are not meant or suited to be portable. Platform services on the other hand are filled by users and serve the purposes of the users in their use of the platform. Our proposed solution would therefore be to differentiate between user-generated data that are created and uploaded by data subjects

themselves (such as pictures, videos, blogs and so on) and data that are compiled as the result of their interaction with the service providers and other users of the service. The right to data portability should only apply to user-generated data. Secondly, we suggest clarifying that Article 18 does not impact the right for the controller to retain personal data for compliance reasons or other legitimate purposes. We take the view that Article 18 should include a paragraph limiting the applicability of the right to data portability similar to the list of exceptions mentioned for the right to be forgotten.

Recital 55

Text proposed by the Commission

To further strengthen the control over their own data and their right of access, data subjects should have the right, where personal data are processed by electronic means and in a structured and commonly used format, to obtain a copy of the data concerning them **also in commonly used electronic format. The data subject should also be allowed to transmit those data, which they have provided**, from one automated application, such as a social network, into another one. **This should apply where the data subject provided the data to the automated processing system, based on their consent or in the performance of a contract.**

Amendment

To further strengthen the control over their own data and their right of access, data subjects should have the right, where personal data are **published by the data subject and** processed by electronic means and in a structured and commonly used format, to obtain a copy of the data concerning them **which allows the further use of such data by them, such as the transmission of user-generated content** from one automated application, such as a social network, into another one. **This right should be without prejudice to the continued processing of the personal data by the controller for the controller's legitimate interests, as there may be a necessity to process the personal data after the data have been transmitted to the data subject, such as the continuation of services provided to the data subject, compliance with Union or Member State law or for the retention of personal data for purposes of proof.**

Article 18

Text proposed by the Commission

1. The data subject shall have the right, where personal data are processed **by electronic means and in a structured and commonly used format**, to obtain from the controller a copy of **data undergoing processing in an electronic and structured format** which **is commonly used and** allows for further use by the data subject.

2. Where the data subject has provided the personal data and the processing is based on consent or on a contract, the data subject shall have the right to transmit those personal data and any other information provided by the data subject and retained by an automated processing system, into another one, in an electronic format which is commonly used, without hindrance from the controller from whom the personal data are withdrawn.

3. The Commission may specify the electronic format referred to in paragraph 1 and the technical standards, modalities and procedures for the transmission of personal data pursuant to paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Amendment

1. The data subject shall have the right, where personal data **are published by the data subject through an information society service**, to obtain from the **information society service provider** a copy of **such content**, which allows for further use by the data subject.

2. Deleted

3. Paragraph 1 shall be without prejudice to the continued processing of the personal data by the controller for the legitimate purposes for which the data were collected or further processed, in particular the retention of such personal data for purposes of compliance with a legal obligation or proof.

Article 21

Text proposed by the Commission

1. **Union or Member State law may restrict by way of a legislative measure the scope of the** obligations and rights

Amendment

1. **The** obligations and rights provided for in points (a) to (e) of Article 5 and Articles 11 to 20 and Article 32 **may be**

provided for in points (a) to (e) of Article 5 and Articles 11 to 20 and Article 32, when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard:

- (a) public security;
- (b) the prevention, investigation, detection and prosecution of criminal offences;
- (c) other public interests of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters and the protection of market stability and integrity;
- (d) the prevention, investigation, detection and prosecution of breaches of ethics **for regulated professions**;
- (e) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (a), (b), (c) and (d);
- (f) the protection of the data subject or the rights and freedoms of others.

2. **In particular**, any legislative measure referred to in paragraph 1 shall contain specific provisions at least as to the objectives to be pursued by the processing and the determination of the controller.

restricted, when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard:

- (a) public security;
- (b) the prevention, investigation, detection and prosecution of criminal offences;
- (c) other public interests of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters and the protection of market stability and integrity;
- (d) the prevention, investigation, detection and prosecution of breaches of ethics **or confidentiality obligations**;
- (e) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (a), (b), (c) and (d);
- (f) the protection of health, safety and security of individuals;**
- (g) the legitimate interests of the controller and its employees, in particular the protection of intellectual property rights, trade secrets, reputation or the preservation of confidentiality in business transactions;**
- (h) the protection of the data subject or the rights and freedoms of others.

2. Any legislative measure **of the Union or the Member States restricting the rights** referred to in paragraph 1 **for the purposes referred to in paragraph 1 section (a) to (g)** shall contain specific provisions at least as to the objectives to be pursued by the processing and the determination of the controller.

RIGHT TO RECTIFICATION

eBay believe a distinction should be made between user-generated data and data that are the results of an interaction between a user and a service provider. Indeed, Article 16 may prove to be an issue with regard to information of a subjective nature, such as feedback left by buyers and sellers on the eBay marketplace. We therefore suggest excluding user-generated data from the scope of Article 16, with the exception of defamatory remarks.

Article 16

Text proposed by the Commission

The data subject shall have the right to obtain from the controller the rectification of personal data relating to them which are inaccurate. The data subject shall have the right to obtain completion of incomplete personal data, including by way of supplementing a corrective statement.

Amendment

1. The data subject shall have the right to obtain from the controller the rectification of personal data relating to them which are inaccurate. The data subject shall have the right to obtain completion of incomplete personal data, including by way of supplementing a corrective statement.

2. The controller shall restrict processing of personal data where their accuracy is contested by the data subject, for a period enabling the controller to verify the accuracy of the data.

3. Paragraph 1 shall not apply to personal data published via information society services, with the exception of data which are of a defamatory nature.

Administrative requirements

eBay believes instead of encouraging the use of privacy enhancing measures, thereby reducing the administrative obligations on controllers and processors, the Commission proposal introduces new

and onerous requirements that will substantially increase the compliance burden for businesses without mitigating potential privacy risks unless they are appropriately defined. Mr. Kelly amendments are to be welcomed in that regard and we suggest making the following additional changes: impact assessments should be applied on a risk based approach, compliance requirements should be eased for controllers that are part of a group and should in no circumstances be duplicated in sectors that are already regulated.

Recital 70

<i>Text proposed by the Commission</i>	<i>Amendment</i>
<p>Directive 95/46/EC provided for a general obligation to notify processing of personal data to the supervisory authorities. While this obligation produces administrative and financial burdens, it did not in all cases contribute to improving the protection of personal data. Therefore such indiscriminate general notification obligation should be abolished, and replaced by effective procedures and mechanism which focus instead on those processing operations which are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes. In such cases, a data protection impact assessment should be carried out by the controller or processor prior to the processing, which should include in particular the envisaged measures, safeguards and mechanisms for ensuring the protection of personal data and for demonstrating the compliance with this Regulation.</p>	<p>Directive 95/46/EC provided for a general obligation to notify processing of personal data to the supervisory authorities. While this obligation produces administrative and financial burdens, it did not in all cases contribute to improving the protection of personal data. Therefore such indiscriminate general notification obligation should be abolished, and replaced by effective procedures and mechanism which focus instead on those processing operations which are likely to present significant risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes. In such cases, privacy impact assessment should be carried out by the controller prior to the processing, which should include in particular the envisaged measures, safeguards and mechanisms for ensuring the protection of personal data and for demonstrating the compliance with this Regulation.</p>

Article 22

<i>Text proposed by the Commission</i>	<i>Amendment</i>
<p>4. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures referred to in paragraph 1 other than those already referred to in paragraph 2, the conditions for the verification and auditing mechanisms referred to in paragraph 3 and as regards the criteria for proportionality under paragraph 3, and considering specific measures for micro, small and medium-sized-enterprises.</p>	<p>4. Paragraphs 1 and 3 of this article, do not apply to controllers, which are part of a group of undertakings, provided such group of undertakings, through its main establishment or otherwise, has implemented a common framework of policies and measures as referred to in paragraphs 1 and 2, which cover the processing of personal data by such controllers.</p> <p>5. Paragraphs 1 and 3 shall also not apply if and insofar as the controller is subject to a similar obligation by virtue of Union law and under supervision of an independent sectorial supervisory authority.</p> <p>6. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures referred to in paragraph 1 other than those already referred to in paragraph 2, the conditions for the verification and auditing mechanisms referred to in paragraph 3 and as regards the criteria for proportionality under paragraph 3, and considering specific measures for micro, small and medium-sized-enterprises.</p>

Article 33 – title

<i>Text proposed by the Commission</i>	<i>Amendment</i>
Data protection impact assessment	Privacy impact assessment

Article 33 – paragraph 1

Text proposed by the Commission

1. Where processing operations present **specific** risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller **or the processor acting on the controller's behalf** shall carry out an assessment of the impact of the envisaged processing operations on the **protection of personal data**.

Amendment

1. Where processing operations **are likely to** present **significant** risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller shall carry out an assessment of the impact of the envisaged processing operations on **the rights and freedoms of the data subjects, especially their right to privacy**.

Article 33 – Paragraph 4

Text proposed by the Commission

4. The controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations.

Amendment

4. The controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations, **unless this is factually impossible or would require a disproportionate effort on the part of the controller**.

Data breach notifications

While we welcome amendments from Mr. Kelly on data breach notifications, we provide below some additional clarifications, such as the possibility to allow for a full exemption when technical protection measures have been implemented to render the data unintelligible.

Article 31

Text proposed by the Commission

1. **In the case of a personal data breach**, the controller shall **without undue delay and, where feasible, not later than 24 hours after having become aware of it**, notify the personal data breach to the supervisory authority. **The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within 24 hours.**

2. Pursuant to point (f) of Article 26(2), the processor shall alert and inform the controller immediately after the establishment of a personal data breach.

3. The notification referred to in paragraph 1 must at least:

(a) describe the nature of the personal data breach including the categories and number of data subjects concerned and the categories and number of data records concerned;

(b) communicate the **identity and** contact details of the **data protection officer** or other contact point where more information can be obtained;

(c) recommend measures to mitigate the possible adverse effects of the personal data breach;

Amendment

1. **Where a personal data breach is likely to have a significant adverse effect on the rights and freedoms of the data subjects, especially their right to privacy**, the controller, **after having become aware of it**, shall **within reasonable** notify the personal data breach to the supervisory authority.

2. Pursuant to point (f) of Article 26(2), the processor shall alert and inform the controller immediately after the establishment of a personal data breach.

3. The notification of a personal data breach shall not be required if the controller or the processor has implemented appropriate technological protection measures, which were applied to the data concerned by the personal data breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it.

4. In case of joint controllers or where the controller is part of a group of undertakings, the personal data breach may be notified by the controller or undertaking designated by the joint controllers or group of undertakings.

5. Without prejudice to Article 51, paragraph 2, controllers shall notify the supervisory authority of the Member State in which they are established. Controllers which are not

(d) describe the consequences of the personal data breach;

(e) describe the measures proposed or taken by the controller to address the personal data breach.

4. The controller shall document any personal data breaches, comprising the facts surrounding the breach, its effects and the remedial action taken. This documentation must enable the supervisory authority to verify compliance with this Article. The documentation shall only include the information necessary for that purpose.

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for establishing the data breach referred to in paragraphs 1 and 2 and for the particular circumstances in which a controller and a processor is required to notify the personal data breach.

6. The Commission may lay down the standard format of such notification to the supervisory authority, the procedures applicable to the notification requirement and the form and the modalities for the documentation referred to in paragraph 4, including the time limits for erasure of the information contained therein. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

established on the territory of the European Union shall notify the supervisory authority of the Member State in which their representative is established.

6. The notification referred to in paragraphs 1 **and** 2 must at least:

- (a) describe the nature of the personal data breach including the categories and number of data subjects concerned and the categories and number of data records concerned;
- (b) communicate the contact details of the **controller** or other contact point where more information can be obtained;
- (c) recommend measures to mitigate the possible adverse effects of the personal data breach;
- (d) describe the consequences of the personal data breach;
- (e) describe the measures proposed or taken by the controller **or processor** to address the personal data breach.

7. The controller shall document any personal data breaches, comprising the facts surrounding the breach, its effects and the remedial action taken. This documentation must enable the supervisory authority to verify compliance with this Article. The documentation shall only include the information necessary for that purpose. ***This obligation shall also apply to the processor insofar as he is responsible for the personal data breach.***

8. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for establishing the data breach referred to in paragraphs 1 and 2 and for the particular circumstances in which a controller and a processor is required to notify the personal data breach.

9. The Commission may lay down the standard format of such notification to the supervisory authority, the procedures applicable to the notification requirement and the form and the modalities for the documentation referred to in paragraph 4, including the time limits for erasure of the information contained therein. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Article 32

Text proposed by the Commission

1. When the personal data breach is likely to adversely affect the protection of the personal data or privacy of the data subject, the controller shall, after the notification referred to in Article 31, communicate the personal data breach to the data subject without undue delay.

2. The communication to the data subject referred to in paragraph 1 shall describe the nature of the personal data breach and contain at least the information and the recommendations provided for in points (b) and (c) of Article 31(3).

3. The communication of a personal data breach to the data subject shall not be required if the controller demonstrates to the satisfaction of the supervisory authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the personal data breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it.

4. Without prejudice to the controller's obligation to communicate the personal data breach to the data subject, if the controller has not already communicated the personal data breach to the data subject of the personal data breach, the supervisory authority, having considered the likely adverse effects of the breach, may require it to do so.

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements as to the circumstances in which a personal data breach is likely to adversely affect the personal data referred to in paragraph 1.

6. The Commission may lay down the format of the communication to the data subject referred to in paragraph 1 and the procedures applicable to that communication. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Amendment

1. **The controller shall, after the notification referred to in Article 31, communicate the personal data breach to the data subject without undue delay, unless this is factually possible or would require a disproportionate effort on the part of the controller.**

2. In case of joint controllers or where the controller is part of a group of undertakings, the personal data breach may be communicated by the controller or undertaking designated by the joint controllers or group of undertakings.

3. The communication to the data subject referred to in paragraph 1 shall describe the nature of the personal data breach and contain at least the information and the recommendations provided for in points (b) and (c) of Article 31(3).

4. (deleted in favour of Art. 31.3 new)

4. Without prejudice to the controller's obligation to communicate the personal data breach to the data subject, if the controller has not already communicated the personal data breach to the data subject of the personal data breach, the supervisory authority, having considered the likely adverse effects of the breach, may require it to do so.

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements as to the circumstances in which a personal data breach is likely to adversely affect the personal data referred to in paragraph 1.

6. The Commission may lay down the format of the communication to the data subject referred to in paragraph 1 and the procedures applicable to that communication. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

For further information, please contact:

Jan Barnes, Senior Manager Government Relations EU eBay Inc.: jabarnes@ebay.com

About eBay Inc.

Founded in 1995 in San Jose, Calif., eBay Inc. (NASDAQ:EBAY) is about enabling commerce. We do so through eBay, the world's largest online marketplace, which allows users to buy and sell in nearly every country on earth; through PayPal, which enables individuals and businesses to securely, easily and quickly send and receive online payments; and through GSI, which facilitates ecommerce, multichannel retailing and digital marketing for global enterprises. X.commerce brings together the technology assets and developer communities of eBay, PayPal and Magento, an ecommerce platform, to support eBay Inc.'s mission of enabling commerce. We also reach millions through specialized marketplaces such as StubHub, the world's largest ticket marketplace, and eBay classifieds sites, which together have a presence in more than 1,000 cities around the world. For more information about the company and its global portfolio of online brands, visit www.ebayinc.com.

eBay Inc. position

Legal Affairs Committee draft opinion on the General Data Protection Regulation

eBay Inc. thanks Marielle Gallo MEP work for the Legal Affairs Committee on the General Data Protection Regulation proposal. We believe the draft opinion reinforces legal certainty and streamlines the general rules affecting data processing for companies.

In particular, we very much welcome amendments 8 and 36 (data portability); amendments 12 and 48 (data breach notifications) and amendment 71 (technology neutrality).

While a lot of other amendments clearly improve the Regulation requirements, eBay Inc. hereby suggests some additional changes, in particular on the definition of consent, the definition of main establishment, the extraterritorial scope of the Regulation, the compatibility of purposes, the processing of data relating to criminal convictions, the right to be forgotten and on administrative requirements, that we think fulfil the objectives set out by the rapporteur.

Definition and conditions for consent

eBay believes that requiring explicit consent in every situation where consent forms the legal basis for processing personal data is too strict and creates an unnecessary obstacle to online and mobile business models. Often, consent may be inferred from the user's action or request for a service. Therefore, eBay proposes a context-based approach to consent to avoid 'click-fatigue' amongst consumers and to improve their user experience. Furthermore, we propose the deletion of Article 7.4 as it could unjustifiably forbid the use of consent for certain businesses. The objective of this article is better achieved through the condition that consent shall only be valid if it is 'freely given'.

Recital 25

Text proposed by the Commission

(25) Consent should be given **explicitly** by any appropriate method enabling a freely given specific and informed **indication of the data subject's wishes, either by a statement or by a clear affirmative action by the data subject, ensuring that individuals are aware that they give their consent to the processing of personal data, including by ticking a box when visiting an Internet website or by any other statement** or conduct which **clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data. Silence or inactivity** should therefore not constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. **If the data subject's consent is to be given following an electronic request, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.**

Amendment

(25) Consent should be given by any appropriate method enabling a freely given specific and informed **expression of will, either by a statement or an action** or conduct which, **in view of the context and circumstances at the time consent is required, signifies the data subject's agreement to the processing of the personal data. Inactivity** should therefore not constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes.

Recital 34

Text proposed by the Commission

Amendment

(34) Consent should not provide a valid legal ground for the processing of personal data, where there is a clear imbalance between the data subject and the controller. This is especially the case where the data subject is in a situation of dependence from the controller, among others, where personal data are processed by the employer of employees' personal data in the employment context. Where the controller is a public authority, there would be an imbalance only in the specific data processing operations where the public authority can impose an obligation by virtue of its relevant public powers and the consent cannot be deemed as freely given, taking into account the interest of the data subject.

Deleted

Article 4 – paragraph 1 – point 8

Text proposed by the Commission

Amendment

(8) 'the data subject's consent' means any **freely given** specific, informed **and explicit indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed;**

(8) 'the data subject's consent' means any **free**, specific, **and informed expression of will, either by a statement or an action, which, in view of the context and circumstances at the time consent is required, signifies the data subject's agreement to the processing of the personal data;**

Article 7 – paragraph 4

Text proposed by the Commission

Amendment

4. Consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller.

Deleted

Main establishment and one-stop-shop

In order to reinforce legal certainty and avoid disputes over Data Protection Authorities competences, we believe it should be the controller's responsibility to designate its main establishment, and we suggest further clarification of the criteria for that designation. Such criteria should be similar to the checklist used by the European Commission in determining the lead data protection authority for the approval of Binding Corporate Rules¹. Secondly, it should be clarified that the designation of an establishment for data protection compliance purposes should be without prejudice to such designation for other purposes of EU law. Finally, eBay Inc. strongly supports the introduction of a 'one-stop-shop' approach with respect to the competence of the lead data protection authority in the Member States where the company has its main establishment, as it allows companies to operate in multiple Member States, while streamlining companies' relationship with enforcement authorities.

¹ European Commission's DG Justice Guidance on how to designate the lead authority in the framework of Binding Corporate Rules, accessible at: http://ec.europa.eu/justice/policies/privacy/binding_rules/designation_authority_en.htm

Recital 27

Text proposed by the Commission

(27) The main establishment of **a controller** in the Union should be **determined** according to objective criteria and should imply the effective and real exercise of management activities determining the main decisions as to **the purposes, conditions and means of** processing through stable arrangements. This criterion should not depend whether the processing of personal data is actually carried out at that location; the presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute such main establishment and are therefore no determining criteria for a main establishment. **The main establishment of the processor should be the place of its central administration in the Union.**

Amendment

The main establishment of **an enterprise or group of undertakings** in the Union should be **designated** according to objective criteria and should imply the effective and real exercise of management activities determining the main decisions as to **data** processing through stable arrangements. This criterion **shall apply both to data controllers and data processors** and should not depend whether the processing of personal data is actually carried out at that location; the presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute such main establishment and are therefore no determining criteria for a main establishment. **Objective criteria for the designation of main establishment include the global or European headquarters of an enterprise or group of undertakings; the country where a group company of an enterprise or group of undertakings established on the territory of the European Union has delegated data protection responsibilities with respect to data processing subject to this Regulation (delegated data protection responsibilities may be inferred from formal arrangements between group companies as well as management decisions or other measures indicating the intention to centralise data protection responsibilities within the enterprise or group, such as the appointment of a group data protection officer or the designation of group compliance responsibilities); the legal entity which takes the most decisions in terms of purposes and means of data processing in group companies established in multiple Member States; or the group company which is best placed (in terms of management function and administrative requirements) to deal with the application and to enforce the group's compliance framework, such as the group's binding corporate rules.**

Recital (28 a new)

Text proposed by the Commission

Amendment

(28 a new) The designation of an establishment for data protection compliance purposes should be without prejudice to such designation for other purposes of European Union law such as tax, insolvency and other compliance purposes.

Article 4 – paragraph 1 - point 13

Text proposed by the Commission

Amendment

(13) 'main establishment' means **as regards the controller**, the place of **its** establishment in the Union where the main decisions as to **the purposes, conditions and means** of the processing of personal data are taken; **if no decisions as to the purposes, conditions and means of the processing of personal data are taken in the**

(13) 'main establishment' means the place of establishment **of the controller, the processor, the enterprise or group of companies** in the Union where the main decisions as to the processing of personal data are taken; **The controller should designate its main establishment based on objective criteria such as the**

Union, the main establishment is the place where the main processing activities in the context of the activities of an establishment of a controller in the Union take place. As regards the processor, 'main establishment' means the place of its central administration in the Union;

global or European headquarters of an enterprise or group of undertakings; the country where a group company of an enterprise or group of undertakings has delegated data protection responsibilities; the legal entity which takes the most decisions in terms of purposes and means of data processing in group companies established in multiple Member States; or the group company which is best placed to deal with the application and to enforce the group's compliance framework, such as the group's binding corporate rules.

Article 51 – paragraph 2

Text proposed by the Commission

Amendment

2. Where the processing of personal data takes place in the context of the activities of an establishment of **a controller or a processor** in the Union, and the **controller or processor** is established in more than one Member State, the supervisory authority of the main establishment **of the controller or processor** shall **be competent** for the supervision of the processing activities of the **controller or the processor** in all Member States, without prejudice to the provisions of Chapter VII of this Regulation.

2. Where the processing of personal data takes place in the context of the activities of an establishment of **an enterprise or group of undertakings** in the Union, and the **enterprise or group of undertakings** is established in more than one Member State, the supervisory authority of the main establishment shall **have final competence** for the supervision of the processing activities of the **enterprise or group of undertakings** in all Member States, without prejudice to the provisions of Chapter VII of this Regulation.

Extraterritorial scope of the Regulation

eBay acknowledges that it is desirable to have companies based outside of the EU respect EU data protection standards when processing personal data of EU citizens. However, in a cross-border context, we believe that the term 'offering' of goods and services does not constitute a valid legal basis for determining the applicable law and jurisdiction. In accordance with European Court of Justice jurisprudence, we suggest replacing the word 'offering' in Article 3.2(a) with 'targeting' or 'directing' goods or services and to clarify in corresponding recitals that the mere availability of the controller's website to a data subject residing in the Union is insufficient to trigger the application of EU data protection laws.

Recital 20

Text proposed by the Commission

Amendment

In order to ensure that individuals are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects residing in the Union by a controller not established in the Union should be subject to this Regulation where the processing activities are related to the offering of goods or services to such data subjects, or to the monitoring of the behaviour of such data subjects.

In order to ensure that individuals are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects residing in the Union by a controller not established in the Union should be subject to this Regulation where the processing activities are related to the offering of goods or services **expressly targeted** to such data subjects, or to the monitoring of the behaviour of such data subjects. **The mere availability of goods and services from third countries to data subjects residing in the Union should not trigger the application of EU data protection legislation.**

Article 3

Text proposed by the Commission

Amendment

1. This Regulation applies to the processing of personal

1. This Regulation applies to the processing of personal

data in the context of the activities of an establishment of a controller **or** a processor in the Union.

2. This Regulation applies to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are related to:

- (a) the offering of goods or services to such data subjects in the Union; or
- (b) the monitoring of their behaviour.

3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where the national law of a Member State applies by virtue of public international law.

data in the context of the activities of an establishment of a controller, a processor **or enterprise** in the Union.

2. This Regulation applies to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are related to:

- (a) the offering of goods or services **expressly targeted** to such data subjects in the Union; or
- (b) the monitoring of their behaviour.

3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where the national law of a Member State applies by virtue of public international law.

Compatibility of purposes

In order to avoid legal uncertainty when determining ‘compatibility’ of purposes, we suggest inserting in Article 5 criteria similar to Article 9.2 of the current Dutch Data Protection Act: similarity of purpose, nature of the data, consequences for the data subject, and adequate safeguards to protect the interests of the data subject. Furthermore, we would like to point out that Article 5(b) (prohibiting further processing in a way incompatible with initial purposes) and Article 6.4 (detailing the conditions for further processing of personal data which purpose is not compatible with the one for which the personal data have been initially collected) are inconsistent. We advise adding the objective of Article 6.4 to the compatibility criteria as suggested for Article 5.

Recital 40

Text proposed by the Commission

The processing of personal data for other purposes should be only allowed where the processing is compatible with those purposes for which the data have been initially collected, in particular where the processing is necessary for historical, statistical or scientific research purposes.

Where the other purpose is not compatible with the initial one for which the data are collected, the controller should obtain the consent of the data subject for this other purpose or should base the processing on another legitimate ground for lawful processing, in particular where provided by Union law or the law of the Member State to which the controller is subject. In any case, the application of the principles set out by this Regulation and in particular the information of the data subject on those other purposes should be ensured.

Amendment

The processing of personal data for other purposes should be only allowed where the processing is compatible with those purposes for which the data have been initially collected (**‘further processing’**), in particular where the processing is necessary for historical, statistical or scientific research purposes. **The further processing of personal data shall be deemed compatible if the further processing is based on the consent of the data subject, is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract, is necessary for compliance with a legal obligation to which the controller is subject, or is necessary in order to protect the vital interests of the data subject. When determining the compatibility between the purpose for which the data were collected and the purposes of the further processing necessary for the performance of a task carried out in the public interest, in the exercise of official authority vested in the controller or necessary for the purposes of the legitimate interests pursued by a controller, the controller shall take into account: the relationship between the purpose of the intended processing and the purpose for which the data were obtained, the nature of the data concerned, the consequences of the further processing for the data subject, and the extent to which appropriate measures and safeguards have been put in place to protect the interests of the data subject.** In any case, the application of the principles set out by this Regulation and in particular the information of the data subject on those other purposes should be ensured.

Article 5

Text proposed by the Commission

Personal data must be:

- (a) processed lawfully, fairly and in a transparent manner in relation to the data subject;
- (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;
- (c) adequate, relevant, and limited to the minimum necessary in relation to the purposes for which they are processed; they shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data;
- (d) accurate and kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the data will be processed solely for historical, statistical or scientific research purposes in accordance with the rules and conditions of Article 83 and if a periodic review is carried out to assess the necessity to continue the storage;
- (f) processed under the responsibility and liability of the controller, who shall ensure and demonstrate for each processing operation the compliance with the provisions of this Regulation.

Amendment

1. Personal data must be:

- (a) processed lawfully, fairly and in a transparent manner in relation to the data subject;
- (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;
- (c) adequate, relevant, and limited to the minimum necessary in relation to the purposes for which they are processed; they shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data;
- (d) accurate and kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the data will be processed solely for historical, statistical or scientific research purposes in accordance with the rules and conditions of Article 83 and if a periodic review is carried out to assess the necessity to continue the storage;
- (f) processed under the responsibility and liability of the controller, who shall ensure and demonstrate for each processing operation the compliance with the provisions of this Regulation.

2. *The further processing of personal data for other purposes than the purpose or purposes for which the data were collected shall be deemed compatible if the further processing has a legal basis in one of the grounds referred to in points (a) to (d) of paragraph 1 of Article 6.*

3. *Where the further processing of personal data is based on the grounds referred to in points (e) or (f) of paragraph 1 of Article 6, the controller shall take into account:*

- (a) the relationship between the purpose of the intended processing and the purpose for which the data were obtained;***
- (b) the nature of the data concerned;***
- (c) the consequences of the further processing for the data subject; and***
- (d) the extent to which appropriate measures and safeguards have been put in place to protect the interests of the data subject.***

Article 6

Text proposed by the Commission

1. Processing of personal data shall be lawful only if and to the extent that at least one of the following applies:
- (a) the data subject has given consent to the processing of their personal data for one or more specific purposes;

Amendment

1. Processing of personal data shall be lawful only if and to the extent that at least one of the following applies:
- (a) the data subject has given consent to the processing of their personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by **a** controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks.

2. Processing of personal data which is necessary for the purposes of historical, statistical or scientific research shall be lawful subject to the conditions and safeguards referred to in Article 83.

3. The basis of the processing referred to in points (c) and (e) of paragraph 1 must be provided for in:

(a) Union law, or

(b) the law of the Member State to which the controller is subject.

The law of the Member State must meet an objective of public interest or must be necessary to protect the rights and freedoms of others, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued.

4. Where the purpose of further processing is not compatible with the one for which the personal data have been collected, the processing must have a legal basis at least in one of the grounds referred to in points (a) to (e) of paragraph 1. This shall in particular apply to any change of terms and general conditions of a contract.

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the conditions referred to in point (f) of paragraph 1 for various sectors and data processing situations, including as regards the processing of personal data related to a child.

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by **the controller or a third party**, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks.

2. Processing of personal data which is necessary for the purposes of historical, statistical or scientific research shall be lawful subject to the conditions and safeguards referred to in Article 83.

3. The basis of the processing referred to in points (c) and (e) of paragraph 1 must be provided for in:

(a) Union law, or

(b) the law of the Member State to which the controller is subject.

The law of the Member State must meet an objective of public interest or must be necessary to protect the rights and freedoms of others, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued.

4. Deleted (transferred to Art. 5.2)

4. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the conditions referred to in point (f) of paragraph 1 for various sectors and data processing situations, including as regards the processing of personal data related to a child.

Processing of data relating to criminal convictions

While we welcome paragraph 2 of Article 9 which lists exceptions to the prohibition of processing personal data that are related to criminal convictions, the Regulation requires a *law* of the Member State or the Union authorizing the processing of criminal data. However, in most cases, such authorizations currently exist in the national data protection acts, which implement Directive 95/46/EC. In order to overcome this incoherence, we would suggest including in the Regulation itself additional exceptions which are already enshrined in national data protection laws. As an example, Article 22.2 of the current Dutch Data Protection Act allows for the processing of criminal data insofar relevant for the assessment of a request of the data subject, or for the protection of the controller or his employees against crimes. Similarly, Article 22.4 allows group companies to process criminal data in order to protect the interests of another group company.

Article 9 – paragraph 2

Text proposed by the Commission

Amendment

(j) processing of data relating to criminal convictions or related security measures is carried out either under the control of official authority or when the processing is necessary for compliance with a legal or regulatory obligation to which a controller is subject, or for the performance of a task carried out for important public interest reasons, and in so far as authorised by Union law or Member State law providing for adequate safeguards. A complete register of criminal convictions shall be kept only under the control of official authority.

(j) Deleted

3 (new). Paragraph 1 shall not apply where processing of data relating to criminal convictions or related security measures is carried out:

(a) under the control of an official authority;

(b) when the processing is necessary for compliance with a legal or regulatory obligation to which a controller is subject;

(c) when the processing is necessary for the performance of a task carried out for important public interest reasons, and in so far as authorised by Union law or Member State law providing for adequate safeguards;

(d) when the processing is necessary for the assessment of a request of the data subject to provide a service to him or the assessment of an application of the data subject to take a decision against him, and insofar the controller has provided for adequate safeguards to protect the interests of the data subject;

(e) when the processing is necessary for the protection of the legitimate interests of a controller or to prevent harm to his employees, customers or persons under his care, and insofar the controller has provided for adequate safeguards to protect the interests of the data subject.

The processing of other data mentioned in paragraph 1 shall be allowed insofar as such processing is necessary in addition to the processing of offences, criminal convictions or related security measures as specified in this paragraph. A complete register of criminal convictions shall be kept only under the control of official authority.

3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria, conditions and appropriate safeguards for the processing of the special categories of personal data referred to in paragraph 1 and the exemptions laid down in paragraph 2.

4. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria, conditions and appropriate safeguards for the processing of the special categories of personal data referred to in paragraph 1 and the exemptions laid down in paragraph 2 **and 3.**

Right to rectification

eBay believe a distinction should be made between user-generated data and data that are the results of an interaction between a user and a service provider. Indeed, Article 16 may prove to be an issue with regard to information of a subjective nature, such as feedback left by buyers and

sellers on the eBay marketplace. We therefore suggest excluding user-generated data from the scope of Article 16, with the exception of defamatory remarks.

Article 16

Text proposed by the Commission

The data subject shall have the right to obtain from the controller the rectification of personal data relating to them which are inaccurate. The data subject shall have the right to obtain completion of incomplete personal data, including by way of supplementing a corrective statement.

Amendment

1. The data subject shall have the right to obtain from the controller the rectification of personal data relating to them which are inaccurate. The data subject shall have the right to obtain completion of incomplete personal data, including by way of supplementing a corrective statement.

2. *The controller shall restrict processing of personal data where their accuracy is contested by the data subject, for a period enabling the controller to verify the accuracy of the data.*

3. *Paragraph 1 shall not apply to personal data published via information society services, with the exception of data which are of a defamatory nature.*

Right to be forgotten

While eBay understands the objective of the right to be forgotten, we are concerned by the requirement for controllers to “take all reasonable steps to inform third parties of the request to erase any links to, copies or replications of the data”. Article 17.2 does not seem to sufficiently take the nature of the Internet into account. Once information is publicly available, we do not have any control over the way in which these data are treated by third parties – e.g. they may be transferred, duplicated, etc. It would be therefore impossible for a data controller to comply with this obligation, and we suggest the deletion of paragraph 2. In this respect, although we welcome Amendment 11 of the draft report, with regard to Amendment 38, we would rather support Commission’s text.

Recital 54

Text proposed by the Commission

(54) To strengthen the ‘right to be forgotten’ in the online environment, the right to erasure should also be extended in such a way that a controller who has made the personal data public should be obliged to inform third parties which are processing such data that a data subject requests them to erase any links to, or copies or replications of that personal data. To ensure this information, the controller should take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible. In relation to a third party publication of personal data, the controller should be considered responsible for the publication, where the controller has authorised the publication by the third party.

Amendment

deleted

Article 16 – new paragraph 2

Text proposed by the Commission

Amendment

Their accuracy is contested by the data subject, for a

period enabling the controller to verify the accuracy of the data;

Article 17

Text proposed by the Commission

1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child, where one of the following grounds applies:

- (a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data;
- (c) the data subject **objects** to the processing of personal data pursuant to Article 19;
- (d) the processing of the data does not comply with this Regulation for other reasons.

2. Where the controller referred to in paragraph 1 has made the personal data public, it shall take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible, to inform third parties which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data. Where the controller has authorised a third party publication of personal data, the controller shall be considered responsible for that publication.

3. The controller shall carry out the erasure without delay, except to the extent that the retention of the personal data is necessary:

- (a) for exercising the right of freedom of expression in accordance with Article 80;
- (b) for reasons of public interest in the area of public health in accordance with Article 81;
- (c) for historical, statistical and scientific research purposes in accordance with Article 83;
- (d) for compliance with a legal obligation to retain the personal data by Union or Member State law to which the controller is subject; Member State laws shall meet an objective of public interest, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued;
- (e) in the cases referred to in paragraph 4.

4. Instead of erasure, the controller shall restrict processing of personal data where:

- (a) their accuracy is contested by the data subject, for a period enabling the controller to verify the accuracy of the data;**
- (b) the controller no longer needs the personal data for the accomplishment of its task but they have to be maintained for purposes of proof;**

Amendment

1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child, where one of the following grounds applies:

- (a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data;
- (c) the data subject **has successfully objected** to the processing, **collection or retention** of personal data pursuant to Article 19;
- (d) the processing of the data does not comply with this Regulation for other reasons.

2. Deleted

2. The controller shall carry out the erasure within **reasonable** delay.

3. The controller may deny a request for erasure where processing of the personal data is necessary:

- (a) for exercising the right of freedom of expression in accordance with Article 80;
- (b) for reasons of public interest in the area of public health in accordance with Article 81;
- (c) for historical, statistical and scientific research purposes in accordance with Article 83;
- (d) for compliance with a legal obligation to retain the personal data by Union or Member State law to which the controller is subject; Member State laws shall meet an objective of public interest, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued;
- e) in the cases referred to in paragraph 4.

4. Instead of erasure, the controller shall restrict processing of personal data where:

- (a) Deleted (move to 16.2 new)**
- (b) the controller no longer needs the personal data for the accomplishment of its task but they have to be maintained for purposes of proof;**
- (c) Deleted**

(c) the processing is unlawful and the data subject opposes their erasure and requests the restriction of their use instead;

(d) Deleted

(d) the data subject requests to transmit the personal data into another automated processing system in accordance with Article 18(2).

Administrative requirements

eBay believes instead of encouraging the use of privacy enhancing measures, thereby reducing the administrative obligations on controllers and processors, the proposal introduces new and onerous requirements that will substantially increase the compliance burden for businesses without mitigating potential privacy risks unless they are appropriately defined. More specifically, impact assessments should be applied on a risk based approach, compliance requirements should be eased for controllers that are part of a group and should in no circumstances be duplicated in sectors that are already regulated.

Recital 65

Text proposed by the Commission

Amendment

In order to demonstrate compliance with this Regulation, the controller or processor should document **each** processing operation. Each controller and processor should be obliged to co-operate with the supervisory authority and make this documentation, on request, available to it, so that it might serve for monitoring those processing operations.

In order to demonstrate compliance with this Regulation, the controller or processor should document processing operations **which likely pose a significant risk to the fundamental rights of the data subjects, in particular their right to privacy**. Each controller and processor should be obliged to co-operate with the supervisory authority and make this documentation, on request, available to it, so that it might serve for monitoring those processing operations.

Recital 70

Text proposed by the Commission

Amendment

Directive 95/46/EC provided for a general obligation to notify processing of personal data to the supervisory authorities. While this obligation produces administrative and financial burdens, it did not in all cases contribute to improving the protection of personal data. Therefore such indiscriminate general notification obligation should be abolished, and replaced by effective procedures and mechanism which focus instead on those processing operations which are likely to present **specific** risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes. In such cases, a **data protection** impact assessment should be carried out by the controller **or processor** prior to the processing, which should include in particular the envisaged measures, safeguards and mechanisms for ensuring the protection of personal data and for demonstrating the compliance with this Regulation.

Directive 95/46/EC provided for a general obligation to notify processing of personal data to the supervisory authorities. While this obligation produces administrative and financial burdens, it did not in all cases contribute to improving the protection of personal data. Therefore such indiscriminate general notification obligation should be abolished, and replaced by effective procedures and mechanism which focus instead on those processing operations which are likely to present **significant** risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes. In such cases, **privacy** impact assessment should be carried out by the controller prior to the processing, which should include in particular the envisaged measures, safeguards and mechanisms for ensuring the protection of personal data and for demonstrating the compliance with this Regulation.

Article 22

Text proposed by the Commission

Amendment

4. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for

4. Paragraphs 1 and 3 of this article, do not apply to controllers, which are part of a group of undertakings, provided such group of undertakings, through its main

appropriate measures referred to in paragraph 1 other than those already referred to in paragraph 2, the conditions for the verification and auditing mechanisms referred to in paragraph 3 and as regards the criteria for proportionality under paragraph 3, and considering specific measures for micro, small and medium-sized-enterprises.

establishment or otherwise, has implemented a common framework of policies and measures as referred to in paragraphs 1 and 2, which cover the processing of personal data by such controllers.

5. Paragraphs 1 and 3 shall also not apply if and insofar as the controller is subject to a similar obligation by virtue of Union law and under supervision of an independent sectorial supervisory authority.

6. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures referred to in paragraph 1 other than those already referred to in paragraph 2, the conditions for the verification and auditing mechanisms referred to in paragraph 3 and as regards the criteria for proportionality under paragraph 3, and considering specific measures for micro, small and medium-sized-enterprises.

Article 28 – paragraph 1

Text proposed by the Commission

1. Each controller and processor and, if any, the controller's representative, shall maintain documentation of all processing operations under its responsibility.

Amendment

1. Each controller and, if any, the controller's representative, shall maintain documentation of all processing operations under its responsibility, ***which pose a significant risk to the fundamental rights of the data subjects, in particular their right to privacy, pursuant to the outcome of the privacy impact assessment as referred to in Article 33.***

Article 33 – title

Text proposed by the Commission

Data protection impact assessment

Amendment

Privacy impact assessment

Article 33 – paragraph 1

Text proposed by the Commission

1. Where processing operations present ***specific*** risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller ***or the processor acting on the controller's behalf*** shall carry out an assessment of the impact of the envisaged processing operations on the ***protection of personal data***.

Amendment

1. Where processing operations ***are likely to*** present ***significant*** risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller shall carry out an assessment of the impact of the envisaged processing operations on ***the rights and freedoms of the data subjects, especially their right to privacy***.

Article 33 – Paragraph 4

Text proposed by the Commission

4. The controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations.

Amendment

4. The controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations, ***unless this is factually impossible or would require a disproportionate effort on the part of the controller.***



For further information, please contact:

Claire Vasile, Manager Government Relations EU eBay Inc.: cvasile@ebay.com

About eBay Inc.

Founded in 1995 in San Jose, Calif., eBay Inc. (NASDAQ:EBAY) is about enabling commerce. We do so through eBay, the world's largest online marketplace, which allows users to buy and sell in nearly every country on earth; through PayPal, which enables individuals and businesses to securely, easily and quickly send and receive online payments; and through GSI, which facilitates ecommerce, multichannel retailing and digital marketing for global enterprises. X.commerce brings together the technology assets and developer communities of eBay, PayPal and Magento, an ecommerce platform, to support eBay Inc.'s mission of enabling commerce. We also reach millions through specialized marketplaces such as StubHub, the world's largest ticket marketplace, and eBay classifieds sites, which together have a presence in more than 1,000 cities around the world. For more information about the company and its global portfolio of online brands, visit www.ebayinc.com.

Insurance Europe key messages on the European Commission's proposed General Data Protection Regulation

Our reference:	SMC-DAT-12-064	Date:	3 September 2012
Related documents:	Proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)		
Contact person:	William Vidonja, Head of Single Market and Social Affairs, Lamprini Gyftokosta, Policy Advisor	E-mail:	Vidonja@insuranceeurope.eu Gyftokosta@insuranceeurope.eu
Pages:	7	Transparency Register ID	33213703459-54

Introduction

Insurance Europe welcomes the European Commission's (EC) objective to harmonise further the data protection legislation within the EU and strengthen individuals' rights. The EC proposed Regulation on the protection of individuals with regard to the processing of personal data and the free movement of such data may however, have unintended consequences for insurers and consumers.

Insurers are concerned that the EC proposed Regulation will restrict insurers' ability to process and use data to properly assess risk. Collecting and processing personal data are at the core of insurance business. Being able to access and process personal data through automated processing enables insurers to process and pay claims, determine the level of cover needed, assess the risk and hence provide consumers with the appropriate premium that fairly reflects the individuals' needs and risks.

If insurers are not able to properly assess risks, there will be a significant negative impact on consumers. For example, it would prevent or delay the reimbursement of medical treatment or the compensation for car accidents, as without an appropriate assessment of the risks, insurers are unable to determine the right amounts of reimbursement or compensation. Further potential negative consequences include the increase of premiums, decrease in insurance coverage and the fact that some products may be withdrawn entirely from the market.

Furthermore Insurance Europe believes that parts of the proposal have been designed with the intention to address problems stemming from social networking, online tracking and search engine technology. These parts should not apply to other highly regulated fields of activities, to which they are not adapted, such as insurance.

Therefore, any changes to the EU data protection legislation should be relevant and proportionate, balancing the individuals' privacy right with data security, taking into consideration the way insurance works. It explicitly should recognise the need for insurers and reinsurers to process personal data in order to calculate fair premiums, and respect contract law requirements. It should also enable insurers to verify the accuracy of information provided and prevent fraud and other financial crime.

Finally, the Regulation must not overlap or be in conflict with other pieces of national or EU legislation, such as the Solvency II Framework Directive and the Anti-money laundering Directive.

1. Insurance specific concerns with regard to the EC's proposed General Data Protection Regulation

1.1 Consent

1.1.1 Definition of consent – Recital 25, Article 4par.8

Based on insurers' experience across member states, consumers do not encounter problems with the current rules on consent in Directive 95/46/EC. Article 2(h) of Directive 95/46/EC provides a suitable protection for the consumer without being unnecessarily burdensome, either for the consumer or for the insurer or both. The requirements of and for consent as provided by the proposed Regulation must be relevant and suitable to the purposes for which the consent is obtained. It should not prevent the insurer from delivering necessary services to the consumer.

Insurance Europe calls for the Article 2(h) Directive 95/46/EC rules on consent to be maintained.

1.1.2 Right to withdraw consent – Article 7par.3

Insurance Europe is concerned that the data subject's right to withdraw consent, as proposed by the draft Regulation, would:

- (i) hinder the execution of the insurance contract: Should the consumer exercise his/her right to withdraw consent to the processing of personal data, this will give rise to serious legal problems under insurance contract law as the insurer will no longer be able to perform the contractual obligations.
- (ii) lead to a cancellation of the contract because it is not foreseen by the parties: The consumer's right to withdraw consent should not result in a right of the consumer to cancel the policy. Based on insurance contract law, the insurer and the consumer fix the terms of the contract at the beginning of their contractual relationship. Some contracts permit cancellation during a given period under specific conditions. This is different from the consumer's right to withdraw consent deriving from the proposed Regulation: it was not foreseen by the parties when signing the contract and it will be perceived as a breach of the contract.
- (iii) Conflict with other legal instruments: Financial service providers are required to retain data to meet legal and regulatory obligations. For example, Directive 2005/60/EC on anti-money laundering and terrorist financing, requires insurers to store data for at least 5 years after the end of the business relationship with natural or legal persons, because of public authorities' control and internal investigations amongst other reasons. National insurance legislation can also require insurers to store data for longer periods, for example 10 years in Italy and 26 years in Poland.

Insurance Europe suggests that the proposed provision on the right to withdraw consent at any time should be redesigned to take into account situations:

- Where data must be retained for the conclusion and execution of insurance contracts, the settlement of a claim and
- Where data must be processed for regulatory, anti-fraud or legal purposes

1.1.3 Right to be forgotten – Article 17

The EC proposal introduces the concept of the "right to be forgotten" whereby individuals can request the deletion of their personal data. Insurance Europe believes that while the intention of this requirement is to address concerns related to internet services (such as social networking sites), there is a concerning overspill to other areas where it is vital to hold data.

This is the case where there is a contractual relationship between an organisation and an individual, and data are needed for the proper performance of the contract. For example if a health insurance policyholder withdraws consent for their health data to be used or requests that information to be deleted, while this data forms an integral part of the contract, the risk assessment, as well as the assessment and processing of claims

cannot take place. This is also the case where there are regulatory requirements to retain data and where there is a need to retain data for fraud prevention purposes, as explained above.

Insurance Europe recommends that the draft Regulation is amended to clearly state that the right to be forgotten does not apply where:

- There is a contractual relationship between an organisation and an individual, and data are needed for the proper performance of the contract.
- There are regulatory requirements to retain data.
- There is a need to retain data for fraud prevention purposes

1.1.4 Significant imbalance – Recital 34, Article 7par.4

The introduction of the new term “significant imbalance” creates legal uncertainty. It could be interpreted as if there is a “significant imbalance” between insurers and consumers, in which case, the data subject’s consent for processing (non) sensitive data would be invalidated and would prevent insurers from offering their services to new and existing customers.

For instance, insurers have only one legal ground to process sensitive data, that of consent. If the rule of significant imbalance applies to them, insurers will not be able to process health data anymore.

Insurance Europe calls on removing or at least amending the provision in a way that limits the unintended consequences for the insurance industry.

1.2 Health data

1.2.1 Definition of health data – Recital 26, Article 4par.12

Insurers need to process health-related data to provide certain insurance products. By way of example, health-related data for private medical insurance is processed to ensure that the consumer receives appropriate cover at a fair price for the risk that he/she poses, or to reimburse all or part of health care where the individual requires medical treatment covered by the insurance policy.

Insurance Europe believes that the definition of health data is too broad and will increase the consent requirements for certain administrative data. Treating purely administrative data as sensitive is disproportionate and will impose administrative burden on consumers and insurers. For instance, it will create delays in the pay-out of covered medical expenses which is important for insurance products that require medical data processing, for example health, motor or travel insurance.

Moreover, the indication of the patient’s health problem on an accident claim or the hospitalisation admission will be considered sensitive health data and therefore the administrative employees could not process them without the explicit consent of the data subject. This, again, is burdensome for all the parties and does not provide any benefit to the data subject.

Insurance Europe calls for the definition of health data to be clear and restricted to clinical and medical information, and to exclude administrative information. Administrative information should be categorised as non-sensitive data.

1.2.2 Processing of health data – Recital 42, Article 9par.2 (h), Article 81pa.1(c)

Insurance Europe understands that insurers can process health data for the management of health care services and settling claims for the benefits and services in the health insurance system, as stated in rec.42.

However, Insurance Europe finds unclear whether insurance falls under the provisions of either Article 81 or Article 9par.2 (h). Processing sensitive data is imperative for insurers and it is crucial to clarify that the conclusion and execution of insurance contracts, including the management of health care services and settling claims for benefits and services in the health insurance system, should be permissible.

Insurance Europe calls for a confirmation of the application of either Article 9par (h) or Article 81 to the insurance or an extension of the scope for collecting and processing health data for all insurance purposes, for example health, life, accident, third party liabilities insurance and reinsurance.

1.3 Data sharing and fraud prevention - Article 6par4 and Article 9par.2(j)

Insurance Europe is concerned that changes to the EU data protection framework may have an impact on insurers' ability to share information and prevent fraud¹, which benefits honest consumers and is in the interest of the society.

Insurance Europe is concerned that the proposed Regulation will:

- Restrict insurers' ability to collect, process and use information needed for fraud prevention and detection. One of the ways insurers detect suspicious activity is by considering previous claims history (multiple claims of the same nature, multiple claims featuring same parties, etc). If they are prohibited to do so, insurers will not be allowed to protect their customers against insurance fraud whilst the majority of honest consumers will have to pay the price through higher tariffs. For instance, it is estimated that the figure for health care fraud and corruption in the EU is at least €80 million every day².
- Hinder the development and use of systems for the identification of fraudulent policyholders, applicants and claims which already exist in member states.

Insurance Europe suggests taking into consideration the Council of Europe (CoE) Recommendation (2002)⁹ on the treatment of personal data for the purposes of fraud prevention and detection as essential for the insurance activity. According to the recommendation, "actuarial activities" and risk rating are allowed; the same applies to preparing and issuing insurance covers, ie risk-based pricing and premium calculation. For this to happen, collecting and using data is indispensable.

Insurance Europe recommends that the proposed Regulation explicitly recognises the need for organisations, including insurers, to process and share information to prevent and detect fraud. This could be done through an exemption for both sensitive and non-sensitive data where processing is necessary for the purposes of preventing, detecting and addressing fraud.

1.4 Profiling – Article 20par.1

Being able to access, process and store personal data through automated processing is central to insurers' ability to provide consumers with appropriate products and services at fair prices.

There is a direct correlation between the consumers' profiled risk – as derived from multiple data used for risk assessment – and the likely claims history of a policyholder during the policy period, which, combined, determines the fair premium charged to policyholders.

Insurance Europe is concerned the proposed provision on profiling will prohibit insurers from using data effectively. This would be to consumers' detriment in the form of higher prices, lack of product innovation and/or lack of available insurance.

Insurance Europe recommends that the rules on profiling as proposed in the draft Regulation are amended to avoid prohibiting or restricting risk-adequate rating, rate classification and risk assessments necessary for premium calculation.

1.5 Data portability – Article 18

Insurance Europe believes the proposed right on data portability clearly falls outside the scope of the draft Regulation. This right deals with the use of data and not with data protection. It appears to have been created to facilitate transferring data from one social network to another.

¹ Country facts: According to a 2011 survey, 4% of German households admit to have committed an insurance fraud within the last five years. For non-life insurance only, the estimated loss arising from fraud is €4 billion each year. In 2010, the number of fraudulent claims in Italy reached almost 2.5% of total claims against insurers. The actual number is estimated much higher, but is difficult to detect fraud accurately. In 2010, in the UK, insurance fraud is adding on average an extra £50 a year to each UK policyholder's insurance bill. In 2011, in the NL, there were 3.371 proved cases of fraud, amounting to 29 million euros. The estimated loss from undetected fraud could add up to 150€ per family p.a. The actual number of false claims is estimated to be higher, but goes undetected.

² [European Healthcare Fraud and Corruption Network \(EFHCN\)](#)

Insurance Europe also believes the ability to change providers easily is a consumer and/ or competition issue, not a data protection one. From an insurance perspective, Insurance Europe is concerned that the proposed provision would have implications for competition and intellectual property as it may unintentionally force data controllers to disclose confidential or intellectually protected information to underwriters, eg underwriting criteria, risk and pricing tools.

Insurance Europe calls for the removal of Article 18, or at minimum, provisions should be included to adequately protect confidential and intellectually protected information.

2 General concerns with regard to the EC's proposed General Data Protection Regulation

2.1 Delegated and implementing acts

Insurance Europe is concerned that the number of delegated and implementing acts causes legal uncertainty as it is impossible to predict the final content and interpretation of key provisions³. The large number of delegated and implementing acts is even more worrying since the chosen legal instrument, a Regulation, is directly applicable.

Insurance Europe calls for a reduction of the number of delegated and implementing acts.

2.2 Administrative sanctions - Article 79

Insurance Europe believes the proposed sanctions for breaching the regulation are disproportionate. This is because Data Protection Authorities (DPAs) do not have discretion when deciding to impose a fine. For instance, the DPAs are obliged to impose a fine ("*shall impose a fine*") even if the violation has not produced any damage to the data subject or if it is the first violation without considering any other mitigating circumstances.

This would lead to situations where a fine of up to 0.5% of annual worldwide turnover (which would run into millions for some insurers) will apply for responding a few days late to a request for access to personal data. Insurance Europe considers that such a sanction is disproportionate, especially where there is no impact for the individual.

Insurance Europe calls for:

- The sanctions to be defined as a competence ("*may impose*") and not as an obligation ("*shall impose*").
- A revision of the level of fines, and suggests linking their amount with the damages and harms caused by the sanctioned violation to the data subject.
- The inclusion of a provision introducing a right to appeal against the sanctions.

3 Administrative burden - Articles 31 to 34

Insurance Europe welcomes the EC's intention to reduce companies' administrative burden. However, Insurance Europe identified several proposed provisions having the opposite outcome.

3.1 Data breach notification Articles 31 and 32

Insurance Europe is in favour of a notification system with clear purposes: supporting individuals, who may have been affected to take steps to protect themselves, or allowing the appropriate regulatory bodies to perform their functions, provide advice and deal with complaints.

In contrast, Insurance Europe is concerned that excessive notification requirements, as the draft Regulation proposes, could lead to consumer apathy, as has been the case in the US. Excessive notification will also distract data protection authorities from their important role of investigating serious breaches, and where necessary, taking action. This would not be in the public interest.

Insurance Europe suggests that:

- Only breaches posing significant risk of harm to data subjects - and where data subjects should take action (eg to prevent identity theft) or remain vigilant - or a serious violation of their rights should be notified

³ Such as articles 9(3), 20(5), 6(5), 6(5), 9(3), 15(3), 17(9), 28, 31, 32, 33, 34, 81(3).

- The Regulation should not impose concrete deadlines for the notification of the data breach to the supervisory authority, but should encourage the data controller to provide a response as soon as feasible and without excessive delay.

3.2 Impact assessment and prior authorisation and consultation - Articles 33 and 34

Insurance Europe believes that the duties of assessing the impact of the envisaged processing operation imposed by Article 33 and of prior notification and authorisation of the processing of data by Article 34 are disproportionate to the objective pursued as it would lead to an extensive administrative burden.

For instance article 33par.4 and the obligation to seek the data subject's view on the intended data processing, interferes with the entrepreneurial freedom to determine its own business policy and way of processing the data. The same applies to Article 34par.2 regarding prior authorisation and consultation between the data controller and the supervisory authority before the processing of data. Moreover, Insurance Europe believes that the distinction between prior consultation and prior authorisation in Article 34 is not clear and creates legal uncertainty.

Finally, according to article 33par.7, the Commission may adopt implementing and delegating acts that will specify the criteria and conditions for the processing operations that should be included in the impact assessment. This creates further uncertainty for the insurance companies as they are not aware of the when and in what manner the impact assessment is to be made; while at the same time they are facing sanctions based on Article 79par.6(i) in case the data controller (insurance company) does not carry and impact assessment.

The impact assessment duty is also raising competition concerns:

- Article 33par.2 (e) allows each supervisory authority to list processing operations subject to an impact assessment. This means that each supervisory authority could list different operations that are subject to the impact assessment, weakening thus the impact of maximum harmonisation and creating an uneven playing field between competitors.
- The obligation to publish the assessments endangers insurers' trade secrets, and may force them to make unlawful disclosures of confidential insurance information.

Insurance Europe calls for:

- The removal of Article 33, or at least,
- Clarification of which type of data is subject to impact assessment.
- Clarifications on whether there is a difference between a prior authorisation and a prior consultation.

3.3 Information to the data subject – Article 14

The proposed provision would oblige data controllers, (eg European insurers or reinsurers) intending to transfer sensitive or non-sensitive data either to a third-country data processor (like a computing centre or other service provider) or a third-country data controller to inform every data subject (insured) of such data transfer. According to the present [Standard Contractual Clauses \(Processors\) 2010/87/EU](#), such an obligation applies currently only when sensitive (e.g. health-related) data are involved.

Insurance Europe is concerned that reinsurers will not be able to meet this requirement to inform every insured of a data transfer, as reinsurers have no direct relationship with the insured persons.

Insurance Europe calls on removing or at least amending the provision in a way that excludes the unintended consequences for the insurance industry.



Insurance Europe is the European insurance and reinsurance federation. Through its 34 member bodies — the national insurance associations — Insurance Europe represents all types of insurance and reinsurance undertakings, eg pan-European companies, monoliners, mutuals and SMEs. Insurance Europe, which is based in Brussels, represents undertakings that account for around 95% of total European premium income. Insurance makes a major contribution to Europe's economic growth and development. European insurers generate premium income of over €1 100bn, employ nearly one million people and invest almost €7 500bn in the economy.

www.insuranceeurope.eu

Insurance Europe key messages on the European Commission's proposed General Data Protection Regulation

Our reference:	SMC-DAT-12-064	Date:	3 September 2012
Related documents:	Proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)		
Contact person:	William Vidonja, Head of Single Market and Social Affairs, Lamprini Gyftokosta, Policy Advisor	E-mail:	Vidonja@insuranceeurope.eu Gyftokosta@insuranceeurope.eu
Pages:	7	Transparency Register ID	33213703459-54

Introduction

Insurance Europe welcomes the European Commission's (EC) objective to harmonise further the data protection legislation within the EU and strengthen individuals' rights. The EC proposed Regulation on the protection of individuals with regard to the processing of personal data and the free movement of such data may however, have unintended consequences for insurers and consumers.

Insurers are concerned that the EC proposed Regulation will restrict insurers' ability to process and use data to properly assess risk. Collecting and processing personal data are at the core of insurance business. Being able to access and process personal data through automated processing enables insurers to process and pay claims, determine the level of cover needed, assess the risk and hence provide consumers with the appropriate premium that fairly reflects the individuals' needs and risks.

If insurers are not able to properly assess risks, there will be a significant negative impact on consumers. For example, it would prevent or delay the reimbursement of medical treatment or the compensation for car accidents, as without an appropriate assessment of the risks, insurers are unable to determine the right amounts of reimbursement or compensation. Further potential negative consequences include the increase of premiums, decrease in insurance coverage and the fact that some products may be withdrawn entirely from the market.

Furthermore Insurance Europe believes that parts of the proposal have been designed with the intention to address problems stemming from social networking, online tracking and search engine technology. These parts should not apply to other highly regulated fields of activities, to which they are not adapted, such as insurance.

Therefore, any changes to the EU data protection legislation should be relevant and proportionate, balancing the individuals' privacy right with data security, taking into consideration the way insurance works. It explicitly should recognise the need for insurers and reinsurers to process personal data in order to calculate fair premiums, and respect contract law requirements. It should also enable insurers to verify the accuracy of information provided and prevent fraud and other financial crime.

Finally, the Regulation must not overlap or be in conflict with other pieces of national or EU legislation, such as the Solvency II Framework Directive and the Anti-money laundering Directive.

1. Insurance specific concerns with regard to the EC's proposed General Data Protection Regulation

1.1 Consent

1.1.1 Definition of consent – Recital 25, Article 4par.8

Based on insurers' experience across member states, consumers do not encounter problems with the current rules on consent in Directive 95/46/EC. Article 2(h) of Directive 95/46/EC provides a suitable protection for the consumer without being unnecessarily burdensome, either for the consumer or for the insurer or both. The requirements of and for consent as provided by the proposed Regulation must be relevant and suitable to the purposes for which the consent is obtained. It should not prevent the insurer from delivering necessary services to the consumer.

Insurance Europe calls for the Article 2(h) Directive 95/46/EC rules on consent to be maintained.

1.1.2 Right to withdraw consent – Article 7par.3

Insurance Europe is concerned that the data subject's right to withdraw consent, as proposed by the draft Regulation, would:

- (i) hinder the execution of the insurance contract: Should the consumer exercise his/her right to withdraw consent to the processing of personal data, this will give rise to serious legal problems under insurance contract law as the insurer will no longer be able to perform the contractual obligations.
- (ii) lead to a cancellation of the contract because it is not foreseen by the parties: The consumer's right to withdraw consent should not result in a right of the consumer to cancel the policy. Based on insurance contract law, the insurer and the consumer fix the terms of the contract at the beginning of their contractual relationship. Some contracts permit cancellation during a given period under specific conditions. This is different from the consumer's right to withdraw consent deriving from the proposed Regulation: it was not foreseen by the parties when signing the contract and it will be perceived as a breach of the contract.
- (iii) Conflict with other legal instruments: Financial service providers are required to retain data to meet legal and regulatory obligations. For example, Directive 2005/60/EC on anti-money laundering and terrorist financing, requires insurers to store data for at least 5 years after the end of the business relationship with natural or legal persons, because of public authorities' control and internal investigations amongst other reasons. National insurance legislation can also require insurers to store data for longer periods, for example 10 years in Italy and 26 years in Poland.

Insurance Europe suggests that the proposed provision on the right to withdraw consent at any time should be redesigned to take into account situations:

- Where data must be retained for the conclusion and execution of insurance contracts, the settlement of a claim and
- Where data must be processed for regulatory, anti-fraud or legal purposes

1.1.3 Right to be forgotten – Article 17

The EC proposal introduces the concept of the "right to be forgotten" whereby individuals can request the deletion of their personal data. Insurance Europe believes that while the intention of this requirement is to address concerns related to internet services (such as social networking sites), there is a concerning overspill to other areas where it is vital to hold data.

This is the case where there is a contractual relationship between an organisation and an individual, and data are needed for the proper performance of the contract. For example if a health insurance policyholder withdraws consent for their health data to be used or requests that information to be deleted, while this data forms an integral part of the contract, the risk assessment, as well as the assessment and processing of claims

cannot take place. This is also the case where there are regulatory requirements to retain data and where there is a need to retain data for fraud prevention purposes, as explained above.

Insurance Europe recommends that the draft Regulation is amended to clearly state that the right to be forgotten does not apply where:

- There is a contractual relationship between an organisation and an individual, and data are needed for the proper performance of the contract.
- There are regulatory requirements to retain data.
- There is a need to retain data for fraud prevention purposes

1.1.4 Significant imbalance – Recital 34, Article 7par.4

The introduction of the new term “significant imbalance” creates legal uncertainty. It could be interpreted as if there is a “significant imbalance” between insurers and consumers, in which case, the data subject’s consent for processing (non) sensitive data would be invalidated and would prevent insurers from offering their services to new and existing customers.

For instance, insurers have only one legal ground to process sensitive data, that of consent. If the rule of significant imbalance applies to them, insurers will not be able to process health data anymore.

Insurance Europe calls on removing or at least amending the provision in a way that limits the unintended consequences for the insurance industry.

1.2 Health data

1.2.1 Definition of health data – Recital 26, Article 4par.12

Insurers need to process health-related data to provide certain insurance products. By way of example, health-related data for private medical insurance is processed to ensure that the consumer receives appropriate cover at a fair price for the risk that he/she poses, or to reimburse all or part of health care where the individual requires medical treatment covered by the insurance policy.

Insurance Europe believes that the definition of health data is too broad and will increase the consent requirements for certain administrative data. Treating purely administrative data as sensitive is disproportionate and will impose administrative burden on consumers and insurers. For instance, it will create delays in the pay-out of covered medical expenses which is important for insurance products that require medical data processing, for example health, motor or travel insurance.

Moreover, the indication of the patient’s health problem on an accident claim or the hospitalisation admission will be considered sensitive health data and therefore the administrative employees could not process them without the explicit consent of the data subject. This, again, is burdensome for all the parties and does not provide any benefit to the data subject.

Insurance Europe calls for the definition of health data to be clear and restricted to clinical and medical information, and to exclude administrative information. Administrative information should be categorised as non-sensitive data.

1.2.2 Processing of health data – Recital 42, Article 9par.2 (h), Article 81pa.1(c)

Insurance Europe understands that insurers can process health data for the management of health care services and settling claims for the benefits and services in the health insurance system, as stated in rec.42.

However, Insurance Europe finds unclear whether insurance falls under the provisions of either Article 81 or Article 9par.2 (h). Processing sensitive data is imperative for insurers and it is crucial to clarify that the conclusion and execution of insurance contracts, including the management of health care services and settling claims for benefits and services in the health insurance system, should be permissible.

Insurance Europe calls for a confirmation of the application of either Article 9par (h) or Article 81 to the insurance or an extension of the scope for collecting and processing health data for all insurance purposes, for example health, life, accident, third party liabilities insurance and reinsurance.

1.3 Data sharing and fraud prevention - Article 6par4 and Article 9par.2(j)

Insurance Europe is concerned that changes to the EU data protection framework may have an impact on insurers' ability to share information and prevent fraud¹, which benefits honest consumers and is in the interest of the society.

Insurance Europe is concerned that the proposed Regulation will:

- Restrict insurers' ability to collect, process and use information needed for fraud prevention and detection. One of the ways insurers detect suspicious activity is by considering previous claims history (multiple claims of the same nature, multiple claims featuring same parties, etc). If they are prohibited to do so, insurers will not be allowed to protect their customers against insurance fraud whilst the majority of honest consumers will have to pay the price through higher tariffs. For instance, it is estimated that the figure for health care fraud and corruption in the EU is at least €80 million every day².
- Hinder the development and use of systems for the identification of fraudulent policyholders, applicants and claims which already exist in member states.

Insurance Europe suggests taking into consideration the Council of Europe (CoE) Recommendation (2002)⁹ on the treatment of personal data for the purposes of fraud prevention and detection as essential for the insurance activity. According to the recommendation, "actuarial activities" and risk rating are allowed; the same applies to preparing and issuing insurance covers, ie risk-based pricing and premium calculation. For this to happen, collecting and using data is indispensable.

Insurance Europe recommends that the proposed Regulation explicitly recognises the need for organisations, including insurers, to process and share information to prevent and detect fraud. This could be done through an exemption for both sensitive and non-sensitive data where processing is necessary for the purposes of preventing, detecting and addressing fraud.

1.4 Profiling – Article 20par.1

Being able to access, process and store personal data through automated processing is central to insurers' ability to provide consumers with appropriate products and services at fair prices.

There is a direct correlation between the consumers' profiled risk – as derived from multiple data used for risk assessment – and the likely claims history of a policyholder during the policy period, which, combined, determines the fair premium charged to policyholders.

Insurance Europe is concerned the proposed provision on profiling will prohibit insurers from using data effectively. This would be to consumers' detriment in the form of higher prices, lack of product innovation and/or lack of available insurance.

Insurance Europe recommends that the rules on profiling as proposed in the draft Regulation are amended to avoid prohibiting or restricting risk-adequate rating, rate classification and risk assessments necessary for premium calculation.

1.5 Data portability – Article 18

Insurance Europe believes the proposed right on data portability clearly falls outside the scope of the draft Regulation. This right deals with the use of data and not with data protection. It appears to have been created to facilitate transferring data from one social network to another.

¹ Country facts: According to a 2011 survey, 4% of German households admit to have committed an insurance fraud within the last five years. For non-life insurance only, the estimated loss arising from fraud is €4 billion each year. In 2010, the number of fraudulent claims in Italy reached almost 2.5% of total claims against insurers. The actual number is estimated much higher, but is difficult to detect fraud accurately. In 2010, in the UK, insurance fraud is adding on average an extra £50 a year to each UK policyholder's insurance bill. In 2011, in the NL, there were 3.371 proved cases of fraud, amounting to 29 million euros. The estimated loss from undetected fraud could add up to 150€ per family p.a. The actual number of false claims is estimated to be higher, but goes undetected.

² [European Healthcare Fraud and Corruption Network \(EFHCN\)](#)

Insurance Europe also believes the ability to change providers easily is a consumer and/ or competition issue, not a data protection one. From an insurance perspective, Insurance Europe is concerned that the proposed provision would have implications for competition and intellectual property as it may unintentionally force data controllers to disclose confidential or intellectually protected information to underwriters, eg underwriting criteria, risk and pricing tools.

Insurance Europe calls for the removal of Article 18, or at minimum, provisions should be included to adequately protect confidential and intellectually protected information.

2 General concerns with regard to the EC's proposed General Data Protection Regulation

2.1 Delegated and implementing acts

Insurance Europe is concerned that the number of delegated and implementing acts causes legal uncertainty as it is impossible to predict the final content and interpretation of key provisions³. The large number of delegated and implementing acts is even more worrying since the chosen legal instrument, a Regulation, is directly applicable.

Insurance Europe calls for a reduction of the number of delegated and implementing acts.

2.2 Administrative sanctions - Article 79

Insurance Europe believes the proposed sanctions for breaching the regulation are disproportionate. This is because Data Protection Authorities (DPAs) do not have discretion when deciding to impose a fine. For instance, the DPAs are obliged to impose a fine ("*shall impose a fine*") even if the violation has not produced any damage to the data subject or if it is the first violation without considering any other mitigating circumstances.

This would lead to situations where a fine of up to 0.5% of annual worldwide turnover (which would run into millions for some insurers) will apply for responding a few days late to a request for access to personal data. Insurance Europe considers that such a sanction is disproportionate, especially where there is no impact for the individual.

Insurance Europe calls for:

- The sanctions to be defined as a competence ("*may impose*") and not as an obligation ("*shall impose*").
- A revision of the level of fines, and suggests linking their amount with the damages and harms caused by the sanctioned violation to the data subject.
- The inclusion of a provision introducing a right to appeal against the sanctions.

3 Administrative burden - Articles 31 to 34

Insurance Europe welcomes the EC's intention to reduce companies' administrative burden. However, Insurance Europe identified several proposed provisions having the opposite outcome.

3.1 Data breach notification Articles 31 and 32

Insurance Europe is in favour of a notification system with clear purposes: supporting individuals, who may have been affected to take steps to protect themselves, or allowing the appropriate regulatory bodies to perform their functions, provide advice and deal with complaints.

In contrast, Insurance Europe is concerned that excessive notification requirements, as the draft Regulation proposes, could lead to consumer apathy, as has been the case in the US. Excessive notification will also distract data protection authorities from their important role of investigating serious breaches, and where necessary, taking action. This would not be in the public interest.

Insurance Europe suggests that:

- Only breaches posing significant risk of harm to data subjects - and where data subjects should take action (eg to prevent identity theft) or remain vigilant - or a serious violation of their rights should be notified

³ Such as articles 9(3), 20(5), 6(5), 6(5), 9(3), 15(3), 17(9), 28, 31, 32, 33, 34, 81(3).

- The Regulation should not impose concrete deadlines for the notification of the data breach to the supervisory authority, but should encourage the data controller to provide a response as soon as feasible and without excessive delay.

3.2 Impact assessment and prior authorisation and consultation - Articles 33 and 34

Insurance Europe believes that the duties of assessing the impact of the envisaged processing operation imposed by Article 33 and of prior notification and authorisation of the processing of data by Article 34 are disproportionate to the objective pursued as it would lead to an extensive administrative burden.

For instance article 33par.4 and the obligation to seek the data subject's view on the intended data processing, interferes with the entrepreneurial freedom to determine its own business policy and way of processing the data. The same applies to Article 34par.2 regarding prior authorisation and consultation between the data controller and the supervisory authority before the processing of data. Moreover, Insurance Europe believes that the distinction between prior consultation and prior authorisation in Article 34 is not clear and creates legal uncertainty.

Finally, according to article 33par.7, the Commission may adopt implementing and delegating acts that will specify the criteria and conditions for the processing operations that should be included in the impact assessment. This creates further uncertainty for the insurance companies as they are not aware of the when and in what manner the impact assessment is to be made; while at the same time they are facing sanctions based on Article 79par.6(i) in case the data controller (insurance company) does not carry and impact assessment.

The impact assessment duty is also raising competition concerns:

- Article 33par.2 (e) allows each supervisory authority to list processing operations subject to an impact assessment. This means that each supervisory authority could list different operations that are subject to the impact assessment, weakening thus the impact of maximum harmonisation and creating an uneven playing field between competitors.
- The obligation to publish the assessments endangers insurers' trade secrets, and may force them to make unlawful disclosures of confidential insurance information.

Insurance Europe calls for:

- The removal of Article 33, or at least,
- Clarification of which type of data is subject to impact assessment.
- Clarifications on whether there is a difference between a prior authorisation and a prior consultation.

3.3 Information to the data subject – Article 14

The proposed provision would oblige data controllers, (eg European insurers or reinsurers) intending to transfer sensitive or non-sensitive data either to a third-country data processor (like a computing centre or other service provider) or a third-country data controller to inform every data subject (insured) of such data transfer. According to the present [Standard Contractual Clauses \(Processors\) 2010/87/EU](#), such an obligation applies currently only when sensitive (e.g. health-related) data are involved.

Insurance Europe is concerned that reinsurers will not be able to meet this requirement to inform every insured of a data transfer, as reinsurers have no direct relationship with the insured persons.

Insurance Europe calls on removing or at least amending the provision in a way that excludes the unintended consequences for the insurance industry.



Insurance Europe is the European insurance and reinsurance federation. Through its 34 member bodies — the national insurance associations — Insurance Europe represents all types of insurance and reinsurance undertakings, eg pan-European companies, monoliners, mutuals and SMEs. Insurance Europe, which is based in Brussels, represents undertakings that account for around 95% of total European premium income. Insurance makes a major contribution to Europe's economic growth and development. European insurers generate premium income of over €1 100bn, employ nearly one million people and invest almost €7 500bn in the economy.

www.insuranceeurope.eu

Telefonica

**Telefónica's proposed amendments to the Proposal for a
REGULATION OF THE EUROPEAN PARLIAMENT AND
OF THE COUNCIL on the protection of individuals with regard to the
processing of personal data and on the free movement of such data
(General Data Protection Directive)**

Proposed Amendment 1

Article 4 Definitions	
Commission Proposal	Telefónica Amendment (proposed new text in blue)
<p>For the purposes of this Regulation:</p> <p>(1) 'data subject' means an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;</p> <p>(2) 'personal data' means any information relating to a data subject;</p>	<p>For the purposes of this Regulation:</p> <p>(1) 'personal data' means any data specifically relating to an identified living natural person or a natural person whose specific identity can be identified, directly or indirectly, by means likely reasonably to be used by the Controller; whilst identification number, location data, online identifiers, unique identifiers, or other specific factors as such can constitute personal data, they need not necessarily be considered as personal data in all circumstances, this will depend on the context.</p> <p>2) 'data subject' means an identified living natural person or a living natural person whose specific identity can be identified, directly or indirectly, by means likely reasonably to be used by the Controller, in particular by reference to an identification number or other identifier(s) or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.</p>

Justification:

The notion of what is and what is not personal data defines the scope of the regulation. Therefore, a clear definition is of outmost importance in order to ensure legal certainty.

Telefónica believes that the proposed definition of personal data is too broad: Personal data cannot simply be “any information relating to a data subject” (art.4.2). This would lead to too much information being deemed personal. Telefónica proposes a simpler definition.

The reference to a third party being able to identify an individual and this meaning that a controller possesses “personal data” means that under the proposed Regulation, a controller would have to live with a considerable amount of uncertainty. Data that is not considered “personal data” may transform itself into “personal data” if it is combined or cross-referenced with other data from a different source, or by some future technological innovation. The original data controller does not know what third parties or future technologies can do to make the data become “personal data”. This is a source of legal uncertainty.

Telefónica therefore believes that the definition should be reconsidered:

Firstly, Telefónica would like to emphasise that information should be “specifically” relating to the individual. This would seek to establish that even though information may relate to an individual e.g. be linked to an individual, it must be specifically about that individual. Hence “personal”. Hence aggregated data is not specifically about an individual.

Secondly, Telefónica seeks to make clear that you must be able to specifically identify the individual. In this way, anonymised data which does not reveal the identity of the individual to the recipient but which nonetheless uses a unique reference number would still be considered as providing “privacy” protection and hence not be considered personal data. For example, we want to ensure that where we release anonymous data to third parties, even though we (as a controller) may have the key to unlock the anonymisation, provided that the key is not provided to third parties, the data can still be considered anonymous.

Professional contact data and data related to deceased individuals should be excluded from the definition of personal data, as it already

occurs in the legislation of some Member States.

Telefónica welcomes the new wording "... by means likely reasonably to be used by the controller". Indeed, in some cases the means necessary to identify a natural person are not reasonable. In these cases, data should not be considered as personal. Furthermore, the means reasonably to be used should be in direct relation to the data controller. Therefore, Telefónica proposes that the reference to "or by any other natural or legal person" be deleted.

Finally, Recital 24 states: "identification numbers, location data, online identifiers or other specific factors as such need not necessarily be considered as personal data in all circumstances". Telefónica agrees with this, and for legal certainty and clarity, would suggest that this wording be introduced within the article itself and to also include "unique identifiers" to make clear that may not be personal data, provided that the key to unlock the anonymization is not provided to third parties.

Proposed Amendment 2

Article 4 Definitions	
Commission Proposal	Telefónica Proposal (proposed new text in blue)
<p>(5) 'controller' means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes, conditions and means of the processing of personal data; where the purposes, conditions and means of processing are determined by Union law or Member State law, the controller or the specific criteria for his nomination may be designated by Union law or by Member State law;</p>	<p>(5) 'controller' means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes; conditions and means of the processing of personal data; where the purposes, conditions and means of processing are determined by Union law or Member State law, the controller or the specific criteria for his nomination may be designated by Union law or by Member State law;</p>

Justification:

The definition of controller should be based on the decision of the purposes for which personal data are processed (i.e. “why” the data are processed) rather than the conditions or means by which this is achieved (i.e. “how” the data are processed).

The control over the reason/purpose for processing is the logical basis for allocating different responsibilities between controllers who are responsible for what and why data is processed and processing parties who deal with how data is processed”.

A clear divide between controller and processor and their roles and responsibilities is key in a Cloud environment. More and more data processing is outsourced by the controller to a service provider (processor). Controllers often rely on their service providers to determine the most effective technological solutions to deliver outsourced processing. In fact, service providers sell themselves to their customers on the basis of their technical expertise, and necessarily exercise a certain, but limited, autonomy over the means and conditions by which they process data **on their customers’ behalf**. However, by doing so, service providers risk exposure under the current Proposal to the full compliance requirements of the Directive, a disproportionate burden when considering that the purposes for which they process data are entirely mandated by their customer as stated in the service agreement. It is also not in alignment with the typical practice of sharing responsibilities of the service providers and their customers in commercial agreements regarding such data processing services.

Proposed Amendment 3

Article 4 and Recital 25 Definitions	
Commission Proposal	Telefónica Proposal (proposed new text in blue)
<p>(8) 'the data subject's consent' means any freely given specific, informed and explicit indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed;</p> <p>Recital 25</p> <p>“Consent should be given by any appropriate method enabling a freely given and informed indication of the data subject's wishes, either by a statement or by a clear action by the data subject, [...] Silence should therefore normally not constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. If the data subject's consent is to be given following an electronic request, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided”.</p>	<p>(8) 'the data subject's consent' means any freely given specific, informed and explicit unambiguous indication of his or her wishes by which the data subject, either for example by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed;</p> <p>Recital 25</p> <p>“Consent should be given by any appropriate method enabling a freely given and informed indication of the data subject's wishes, either by a statement or by a clear action by the data subject, [...] Silence should therefore normally not constitute consent, unless certain conditions providing information and control to the data subject are met. Consent should cover all processing activities carried out for the same purpose or purposes. If the data subject's consent is to be given following an electronic request, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided”</p>

Justification:

In light of the existing case law and decision making practice, the term “explicit” is likely to be misunderstood to mean that data subjects are always required to tick a box, to state “yes, I accept my data to be processed”. This would lead to a very rigid regime incompatible with future services.

We propose that the word “explicit” be deleted and replaced with the term “informed, unambiguous consent”.

Indeed, requiring explicit consent combined with the requirement that the controller bears “the burden of proof for the data subject's consent to the processing of their personal data for specified purposes”, as provided for by Art. 7.1, is not workable especially in the digital environment and will hinder the development of innovative online services and products. Systematically requiring explicit consent may lead to practices which are both user unfriendly (“click fatigue”) while not leading to a higher level of privacy protection for data subjects.

User’s actions can provide a clear indication where there is a shared understanding of what is happening. For example, downloading a data based application on a mobile phone can constitute consent for the processing of personal data or other actions such as clicking an icon, sending an email or subscribing to a service.

In summary, the precise mechanisms by which valid informed consent is obtained may vary. The crucial consideration is that individuals must fully appreciate that they are consenting and what they are consenting to.

In addition, Article 6.1.b should be understood in a way that also covers those cases where a customer requires information based on his/her geographic location and is thus, by requiring the service, directly providing his/her authorization for personal location data to be processed.

Proposed Amendment 4

Article 4 Definitions of child	
Commission Proposal	Telefónica Proposal (proposed new text in blue)
(18) 'child' means any person below the age of 18 years;	(18)) 'child' means any person below the age of 18 13 years;

Justification:

We consider that the objective of this Regulation is to create consistent restrictions for the processing of personal data, wherever and however that processing occurs, and to provide clear protection for that data especially as it relates to children.

However, the definition of “child” in Art 4 point 18, creates two distinct age definitions in a single regulatory instrument, especially without clear definition or explanation regarding the requirements and circumstances applied to each age-group.

In the scope of a Regulation aimed exclusively at the processing of personal data, the creation of a distinction in online and offline data processing in the definition of a child seems an unnecessary, confusing, and potentially dangerous line to draw, only exacerbated by the definition-by-omission currently used to draw this distinction.

It is fundamental for an effective application of the new Regulation that definition of “child” in Article 4 be modified to set a single and clear restriction that does not allow the processing of personal data for anyone below the age of 13 years of age without parental authorization, regardless of the sector in which that processing occurs. In this sense, we suggest that a simple term in the customer contract whereby a parent “authorises” use of data relating to the device/account will be sufficient. Hence if they give the phone to a child, then they have authorised such use.

Finally, we would like to make a distinction between children and minors. A minor is any person below the age of 18. Pretending that minors in the upper range do not use online services means the regulation inapplicable. Therefore, we propose to consider a child that person below 13.

Proposed Amendment 5

Article 4 (New) Definition of “anonymous data”.	
Commission Proposal	Telefónica Proposal (proposed new text in blue)
	<p>(20) Anonymous data are those data altered in such a way that the specific identity of the data subject is no longer identifiable. To determine whether a person is specifically individually identifiable, account should be taken of all the means likely reasonably to be used by the controller (or by the recipient of the data in case of disclosures) to identify the specific individual.</p>
<u>Justification:</u>	
<p>Telefónica fully supports the exclusion of “anonymous data” from the scope of this Directive.</p> <p>However, the current Proposal is unclear and does not go far enough to give companies the guaranteed space to innovate and exploit new opportunities. Anonymization can allow organisations to publish or share useful information derived from personal data, whilst protecting the privacy rights of individuals.</p> <p>Since “anonymous data” are the key to many future services, Telefónica firmly believes that a clear definition of anonymous data should be included in Article 4.</p> <p>In this sense we propose a definition in which as long as the recipient is not reasonably likely to be able to identify the individual, then it is anonymous. In this way the controller can hold the key, and anonymous data can still be released provided that key is not provided to third parties. It is only if the controller releases the key -or the key is available- that the information should cease to be anonymous in the hands of the recipient.</p>	

Proposed Amendment 6

Article 6 Lawfulness of Processing	
Commission Proposal	Telefónica Proposal (proposed new text in blue)
<p>4. Where the purpose of further processing is not compatible with the one for which the personal data have been collected, the processing must have a legal basis in one of the grounds referred to in points (a) to (e) of paragraph 1. This shall in particular apply to any change of terms and general conditions of contract.</p>	<p>4. Where the purpose of further processing is not compatible with the one for which the personal data have been collected, the processing must have a legal basis in one of the grounds referred to in points (a) to (e^f) of paragraph 1. This shall in particular apply to any change of terms and general conditions of contract.</p>

Proposed Amendment 7

Article 7 Conditions for consent	
Commission Proposal	Telefónica Proposal (proposed new text in blue)
(4) Consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller.	(4) Consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller.
<p style="text-align: center;"><u>Justification:</u></p> <p>Art. 7.4. is very broad and therefore does not provide the necessary legal certainty which is needed for a provision such decisive. Telefónica proposes its deletion.</p> <p>Although, Recital 34 refers to the employment context, the current wording of Art.7.4. is too broad and could make this article applicable in all situations, even when a "good quality consent" had provided the legal basis for processing. Such wording leads to legal uncertainty.</p> <p>An alternative to the above mentioned deletion it could be: "Consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller, provided that the processing affects adversely to the data subject"</p>	

Proposed Amendment 8

Article 8 Processing of personal data of a child	
Commission Proposal	Telefónica Proposal (proposed new text in blue)
<p>For the purposes of this Regulation, in relation to the offering of information society services directly to a child, the processing of personal data of a child below the age of 13 years shall only be lawful if and to the extent that consent is given or authorised by the child's parent or custodian. The controller shall make reasonable efforts to obtain verifiable consent, taking into consideration available technology.</p>	<p>For the purposes of this Regulation, in relation to the offering of information society services directly to a child, the processing of personal data of a child below the age of 13 years shall only be lawful if and to the extent that consent is given or authorised by the child's parent or custodian. The controller shall make reasonable efforts to obtain verifiable consent, taking into consideration available technology.</p>

Justification:

As the Regulation proposal currently stands, a “child” is defined as anyone under 18 years of age. However, the only mention of requirements that apply to a specific age-group is found in the new Article 8, entitled “Processing the personal data of a child”; the text of the Article refers only to requirements related to “a child below the age of 13 years” and to “information society services directly to a child”. This definition-by-omission leads to the conclusion that any service not considered part of the “information society” will be subject to different requirements for processing the data of a child (under 18 years of age); those services and/or their requirements, however, are not contemplated further in this Article or anywhere else in the current Regulation proposal.

Following this reasoning, Telefónica cannot find answers in the Regulation to some important questions related to processing the personal data of a child as What is the minimum age at which a data controller can process a data subject’s data offline (not included in “information society services”) or What differences exist in legal requirements or protection for children between the ages of 13 and 18, and to what specific activities or services are those differences applied?

We consider that the objective of this Regulation is to create consistent restrictions for the processing of personal data, wherever and however that processing occurs, and to provide clear protection for that data especially as it relates to children. In the scope of a Regulation aimed exclusively at the processing of personal data, the creation of a distinction in online and offline data processing in the definition of a child seems an unnecessary, confusing, and potentially dangerous line to draw, only exacerbated by the definition-by-omission currently used to draw this distinction.

Therefore it is fundamental for an effective application of the new Regulation that Article 8 on “Processing the personal data of a child” be modified to set a single and clear restriction that does not allow the processing of personal data for anyone below the age of 13 years of age without parental authorization, regardless of the sector in which that processing occurs.

Finally, we would like to make a distinction between children and minors. A minor is any person below the age of 18. Pretending that minors in the upper range do not use online services means the regulation inapplicable. Therefore, we propose to consider a child that person below 13.

Proposed Amendment 9

Article 10 Processing not allowing identification	
Commission Proposal	Telefónica Proposal (proposed new text in blue)
If the data processed by a controller do not permit the controller to identify a natural person, the controller shall not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation.	Data Protection Regulation should not apply to data rendered anonymous. If the data processed by a controller do not permit the controller to identify a natural person, the controller shall not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation.
<p style="text-align: center;"><u>Justification:</u></p> <p>Art. 10 provides that since some processing of data does not allow the controller to trace the data subject's identity, the controller itself will not be obliged to collect any further information in order to identify the data subject, even if so required by some provisions of the Regulation itself.</p> <p>But Article 10 should be clarified and improved as proposed above following the spirit of Recital 23.</p>	

Proposed Amendment 10

Article 16 Right of access	
Commission Proposal	Telefónica Proposal (proposed new text in blue)
<p>1. The data subject shall have the right to obtain from the controller at any time, on request, confirmation as to whether or not personal data relating to the data subject are being processed.</p>	<p>1. The data subject shall have the right to obtain from the controller at any time, on request and under reasonable terms, confirmation as to whether or not personal data relating to the data subject are being processed.</p>
<p style="text-align: center;">Justification:</p> <p>Under some European Member States regulation, the right of access is a right that can be exercised only every twelve months, unless a legitimate interest is accredited. The reason why this right is temporarily limited is grounded in the fact that its exercise shall be free of charge.</p> <p>Therefore, we propose to limit this right of access when there are reasonable grounds to do it, i.e, when a legitimate interest is accredited.</p>	

Proposed Amendment 11

Article 17 Right to be Forgotten	
Commission Proposal	Telefónica Proposal (proposed new text in blue)
<p>(1) The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child, where one of the following grounds applies:</p> <p>(a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;</p> <p>(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data;</p> <p>(c) the data subject objects to the processing of personal data pursuant to Article 19;</p> <p>(d) the processing of the data does not comply with this Regulation for other reasons.</p>	<p>(1) The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child, where one of the following grounds applies:</p> <p>(a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;</p> <p>(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data;</p> <p>(c) the data subject objects to the processing of personal data pursuant to Article 19;</p> <p>(d) the processing of the data does not comply with this Regulation for other reasons.</p> <p>new par. (2) The controller shall take all reasonable steps to communicate any erasure to each legal entity to whom the data have been disclosed, unless this involves</p>

(2) Where the controller referred to in paragraph 1 has made the personal data public, it shall take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible, to inform third parties which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data. Where the controller has authorised a third party publication of personal data, the controller shall be considered responsible for that publication.

(9) The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying:

- (a) the criteria and requirements for the application of paragraph 1 for specific sectors and in specific data processing situations;
- (b) the conditions for deleting links, copies or replications of personal data from publicly available communication services as referred to in paragraph 2;
- (c) the criteria and conditions for restricting the processing of personal data referred to in paragraph 4.

a disproportionate effort.

~~(2)~~ (3) Where the controller referred to in paragraph 1 has made the personal data public, it shall take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible, to inform ~~third parties~~ legal entities to whom the original controller had authorised to further process personal data ~~upon request of the data subject~~ and which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data. In any case the controller will not be responsible for the personal data that the data subject by a voluntary act has made public.

~~(9) The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying:~~

- ~~(a) the criteria and requirements for the application of paragraph 1 for specific sectors and in specific data processing situations;~~
- ~~(b) the conditions for deleting links, copies or replications of personal data from publicly available communication services as referred to in paragraph 2;~~
- ~~(c) the criteria and conditions for restricting the processing of personal data referred to in paragraph 4.~~



Justification:

The Right to be Forgotten is, in our view, not something new as data controllers already have to delete personal data whenever the data subject ask for erasure or cancellation. The basic principles on Data Quality (art. 6), Right of access and Right of rectification (Art. 12) and Consent (Art. 7) of Directive 95/46/EC are the basis of this “new right to be forgotten”.

However, although we probably have a common understanding of what we want to achieve, the wording of the current proposal, especially of Art 17.2, extends the concept well beyond “personal data” and may oblige companies to delete data that is not personal in nature, such as information that someone has voluntarily published on the internet. Data controllers must inform any third party to “erase any links to, or copy or replication of that personal data”. This information obligation is triggered by a request by the data subject to the original controller to erase data. This is technically far more challenging, if not impossible. This extended interpretation cannot and should not be the objective of this article.

With this extended scope of “personal data”, this provision is difficult to apply in practice for social networking, blogs and Internet search businesses: the original controller of that data might not be aware of any third party processing. The controller would therefore have to track content across their service or worse across the entire Internet. In other words, by requiring that controllers inform any third parties, this provision seems to envisage that companies can oversee the entirety of the World Wide Web and control the information on it – an obligation that is directly at odds with the open architecture of the Internet. The e-Commerce Directive already recognises that it would be unreasonable to ask companies to monitor the Internet. It makes it clear that companies that act as intermediaries in the provision of services of the Information Society should not be required to do so.

In order to render this provision workable, we propose the following modifications:

This obligation should only be applied to personal data that the data subject has made available to the Data Controller specifically. Other data, for example, a journalist writing an article, tweets or someone commenting on a blog post, should be excluded from the scope of this obligation. Companies are only asked to “forget” personal data, not somebody’s complete history. The data controller should not be responsible for the personal data that the data subject himself has made public.

The right to be forgotten should be limited to the original Data Controller who received the personal data directly from the user who contracted the service, and any third party who processes data on behalf of the Data Controller.

It should be clarified that no tracking of data published on own services is required from the controller and that the information obligation is only triggered by explicit request by the data subject and only to those third legal entities the controller directly authorised to further process personal data.

Telefónica welcomes the inclusion of Art. 13 on rights in relation to recipients, by which the obligation to inform is limited if it proves impossible or involves a disproportionate effort. Therefore, for the sake of legal certainty, Art. 13 should be moved in order to complete Art. 17.2. This would reinforce the wording related to “reasonable steps”: “...the original controller shall take all reasonable steps, including technical measures, unless this proves impossible or involves a disproportionate effort”.

Proposed Amendment 12

Article 18 Right to data portability	
Commission Proposal	Telefónica Proposal (proposed new text in blue)
<ol style="list-style-type: none"> 1. The data subject shall have the right, where personal data are processed by electronic means and in a structured and [...]. 2. Where the data subject has provided the personal data and the processing is based on consent or on a contract, [...]. 3. The Commission may specify the electronic format referred to in paragraph 1 and the technical standards, [...]. 	<ol style="list-style-type: none"> 1. The data subject shall have the right, where personal data are processed by electronic means and in a structured and [...]. 2. Where the data subject has provided the personal data and the processing is based on consent or on a contract, [...]. 3. The Commission may specify the electronic format referred to in paragraph 1 and the technical standards, [...].

Justification:

Data portability is fraught with technical and competition issues and therefore easier said than done. But apart from this enforcement difficulties, Telefónica would like to make a more important point: in essence, it is a competition or market organisation measure, but not related to data protection or privacy.

Transparency as a whole will be of further more importance to obtain confidence from our customers, therefore the market will provide for the most suitable forms of Data Subjects Access Rights. Some of our Operating Businesses are already today providing answers to customer requests for data in an electronic form and the customers are free to use it however they want. This will evolve in the future due to increasing amounts of data and the necessary process development going along with it.

We would, therefore, suggest striking it from this Regulation and strengthening and make easier the right to access to data. In other words to reinforce the data Subject Access Rights.

Proposed Amendment 13

Article 20	
Measures based on profiling Automated Decision Making	
Commission Proposal	Telefónica Proposal (proposed new text in blue)
<p>(1) Every natural person shall have the right not to be subject to a measure which produces legal effects concerning this natural person or significantly affects this natural person, and which is based solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour.</p> <p>2. Subject to the other provisions of this Regulation, a person may be subjected to a measure of the kind referred to in paragraph 1 only if the processing:</p> <p>(a) is carried out in the course of the entering into, or performance of, a contract, where the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or where suitable measures to safeguard the data subject's legitimate interests have been</p>	<p>(1) Every natural person shall have the right not to be subject to a measure decision which produces legal effects concerning this natural person or significantly affects this natural person, and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to this natural person, or to analyse or predict in particular the natural person's such as his/her performance at work, economic situation, location, health, personal preferences creditworthiness, reliability or behaviour.</p> <p>(2) Subject to other provisions of this Regulation, a person may be subjected to a measure decision of the kind referred to in paragraph 1 only if that decision:</p> <p>(a) is carried out is taken in the course of the entering into, or performance of, a contract, where provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or where that there are suitable measures to safeguard his legitimate</p>

<p>adduced, such as the right to obtain human intervention; or</p> <p>(b) is expressly authorized by a Union or Member State law which also lays down suitable measures to safeguard the data subject's legitimate interests; or</p> <p>(c) is based on the data subject's consent, subject to the conditions laid down in Article 7 and to suitable safeguards.</p> <p>3. Automated processing of personal data intended to evaluate certain personal aspects relating to a natural person shall not be based solely on the special categories of personal data referred to in Article 9.</p> <p>4. In the cases referred to in paragraph 2, the information to be provided by the controller under Article 14 shall include information as to the existence of processing for a measure of the kind referred to in paragraph 1 and the envisaged effects of such processing on the data subject.</p> <p>5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for suitable measures to safeguard the data subject's legitimate interests referred to in paragraph 2.</p>	<p>interests, such as arrangements allowing him to put his point of view; or</p> <p>(b) is expressly authorised by a Union or Member State law which also lays down measures to safeguard the data subject's legitimate interest; or</p> <p>(c) is based on the data subject's consent, subject to the conditions laid down in Article 7 and to suitable safeguards.</p> <p>3. Automated processing of personal data intended to evaluate certain personal aspects relating to a natural person shall not be based solely on the special categories of personal data referred to in Article 9.</p> <p>4. In the cases referred to in paragraph 2, the information to be provided by the controller under Article 14 shall include information as to the existence of processing for a measured decision of the kind referred to in paragraph 1 and the envisaged effects of such processing on the data subject.</p> <p>5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for suitable measures to safeguard the data subject's legitimate interests referred to in paragraph 2.</p>
---	---

Justification:

The provisions on profiling are excessive and unclear, whilst we cannot see how they will enhance the user's privacy. There is a perception that profiling per se is bad. We would highlight that profiling can have very positive applications (eg.: traffic management).

Evenmore, Telefónica believes that "profiling" is not the main issue, but rather the consent is with automated decisions. The off and online world (both Private and Public Sectors) makes use of profiling day in day out in order to make decisions about what products, services, prices, levels of service, etc. are to be offered to customers. We understand that online behavioural advertising is singled out as a specific cause for concern which this Article seeks to regulate. In this sense we proposed to replace references to "profiling" and "measures" with "automated decision taking" in the recital and the article itself.

Article 20.4 obliges data controllers to ensure that data subjects are given sufficient information about the 'envisaged effects' of such processing on them. In addition, Article 33.2.a. obliges organisations to conduct Privacy Impact Assessments for such processing and to seek the views of the data subject or their representatives on it (Art. 33.4).

We call for the removal of this obligation to inform individuals about "envisaged effects" as it is an ambiguous and extremely subjective term and will be practically unworkable. The effects of a specific processing may be dependent on information and circumstances beyond the control of the data controller.

We are also calling for the removal of the obligations to conduct a Privacy Impact Assessment and to seek the views of data subjects or their representatives (Art. 33.2.a.). These requirements are excessive and costly and will not necessarily enhance the privacy of individuals.

Proposed Amendment 14

Article 25 Representatives of controllers not established in the Union	
Commission Proposal	Telefónica Proposal (proposed new text in blue)
<p>1. In the situation referred to in Article 3(2), the controller shall designate a representative in the Union.</p> <p>2. This obligation shall not apply to: (a) a controller established in a third country where the Commission has decided that the third country ensures an adequate level of protection in accordance with Article 41; or (b) an enterprise employing fewer than 250 persons; or (c) a public authority or body; or (d) a controller offering only occasionally goods or services to data subjects residing in the Union.</p> <p>3. The representative shall be established in one of those Member States where the data subjects whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, reside.</p> <p>4. The designation of a</p>	<p>1. In the situation referred to in Article 3(2), the controller shall designate a representative in the Union.</p> <p>2. This obligation shall not apply to: (a) a controller established in a third country where the Commission has decided that the third country ensures an adequate level of protection in accordance with Article 41; or (b) an enterprise employing fewer than 250 persons; or (c) a public authority or body; or (d) a controller offering only occasionally goods or services to data subjects residing in the Union.</p> <p>3. The representative shall be established in one of those Member States where the data subjects whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, reside.</p> <p>4. The designation of a</p>

representative by the controller shall be without prejudice to Legal actions which could be initiated against the controller itself.	representative by the controller shall be without prejudice to Legal actions which could be initiated against the controller itself.
---	---

Justification:

Article 25 (2) provides significant exceptions to this obligation in particular for enterprises employing less than 250 persons, public authorities or in the case of occasional offers of goods and services.

Telefónica does not understand why there should be an exemption from the obligation for enterprises employing less than 250 persons or in the case of occasional offers of goods and services. The simple fact that they are dealing with personal data of European citizens must be enough to be submitted to EU data protection rules. All European citizens deserve the same level of protection regardless of company size or assiduity in business relationship with customers resident in Europe.

We propose to delete point (b) and (d) from article 25 paragraph 2.

Proposed Amendment 15

Article 26 Processor	
Commission Proposal	Proposal (proposed new text in blue)
<p>1. Where a processing operation is to be carried out on behalf of a controller, the controller shall choose a processor providing sufficient guarantees to implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject, in particular in respect of the technical security measures and organizational measures governing the processing to be carried out and shall ensure compliance with those measures.</p> <p>2. The carrying out of processing by a processor shall be governed by a contract or other legal act binding the processor to the controller and stipulating in particular that the processor shall:</p> <p>(a) act only on instructions from the controller, in particular, where the transfer of the personal data used is prohibited;</p>	<p>1. Where a processing operation is to be carried out on behalf of a controller, the controller shall choose a processor providing sufficient guarantees to implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject, in particular in respect of the technical security measures and organizational measures governing the processing to be carried out and shall ensure compliance with those measures.</p> <p>2. The carrying out of processing by a processor shall be governed by a contract or other legal act binding the processor to the controller and stipulating in particular that the processor shall:</p> <p>(a) act only on instructions from the controller, in particular, where the transfer of the personal data used is prohibited;</p>

(b) employ only staff who have committed themselves to confidentiality or are under a statutory obligation of confidentiality;

(c) take all required measures pursuant to Article 30;

(d) only enlist another further processors only with the prior permission of the controller that enable the requirements of this Regulation to be met;

(e) insofar as this is possible given the nature of the processing, create in agreement with the controller the necessary technical and organisational requirements for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;

(f) assist the controller in ensuring compliance with the obligations pursuant to Articles 30 to 34;

(g) hand over all results to the controller after the end of the processing and not process the personal data further after the end of the agreed processing otherwise;

(h) upon request make available to the controller and the supervisory authority all relevant and permissible information necessary to control compliance with the

(b) employ only staff who have committed themselves to confidentiality or are under a statutory obligation of confidentiality;

(c) take all required measures pursuant to Article 30;

~~(d) only enlist another further processors only with the prior permission of the controller that enable the requirements of this Regulation to be met;~~

(e) insofar as this is possible given the nature of the processing, create in agreement with the controller the necessary technical and organisational requirements for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;

(f) assist the controller in ensuring compliance with the obligations pursuant to Articles 30 to 34;

(g) hand over all results to the controller after the end of the processing and not process the personal data further after the end of the agreed processing otherwise;

(h) upon request make available to the controller ~~and the supervisory authority~~ all relevant and permissible information necessary to control compliance with the obligations laid

obligations laid down in this Article.

3. The controller and the processor shall document in writing the controller's instructions and the processor's obligations referred to in paragraph 2.

4. If a processor processes personal data other than as instructed by the controller, the processor shall be considered to be a controller in respect of that processing and shall be subject to the rules on joint controllers laid down in Article 24.

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the responsibilities, duties and tasks in relation to a processor in line with paragraph 1, and conditions which allow facilitating the processing of personal data within a group of undertakings, in particular for the purposes of control and reporting.

down in this Article.

3. The controller and the processor shall document in writing the controller's instructions and the processor's obligations referred to in paragraph 2.

~~4. If a processor processes personal data other than as instructed by the controller, the processor shall be considered to be a controller in respect of that processing and shall be subject to the rules on joint controllers laid down in Article 24.~~

~~5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the responsibilities, duties and tasks in relation to a processor in line with paragraph 1, and conditions which allow facilitating the processing of personal data within a group of undertakings, in particular for the purposes of control and reporting.~~

Justification:

This article introduces many new obligations on processors that should preferably be set in the contractual agreements between controllers and processors.

Furthermore, we suggest to delete the possibility for the Commission to adopt delegated.

Insofar we share the same thoughts than the Art. 29 Working Party reflected in its Opinion 8/2012 (October 5th, 2012, p. 26). We do not consider the relationship between a Controller and a Processor as “standardizeable” as various agreements are possible depending - for example - on the kind of data involved or the purposes of the processing. As far as the Controller according to Art. 26(1) has to take account of the general processing of personal data, we favour to leave space for individual agreements to generate an adequate protection level.

Proposed Amendment 16

Article 28 Documentation	
Commission Proposal	Telefónica Proposal (proposed new text in blue)
(1) Each controller and processor	(1) Each controller and processor

and, if any, the controller's representative, shall maintain documentation of all processing operations under its responsibility.

2. The documentation shall contain at least the following information:

- (a) the name and contact details of the controller, or any joint controller or processor, and of the representative, if any;
- (b) the name and contact details of the data protection officer, if any;
- (c) the purposes of the processing, including the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);
- (d) a description of categories of data subjects and of the categories of personal data relating to them;
- (e) the recipients or categories of recipients of the personal data, including the controllers to whom personal data are disclosed for the legitimate interest pursued by them;
- (f) where applicable, transfers of data to a third country or an international organisation, including the identification of that third country or international organisation and, in case of transfers referred to in point (h) of Article 44(1), the documentation of appropriate safeguards;
- (g) a general indication of the time limits for erasure of the different categories of data;
- (h) the description of the

and, if any, the controller's representative, shall maintain documentation in respect of processing operations under its responsibility.

2. The documentation shall contain at least the following information:

- (a) the name and contact details of the controller, or any joint controller or processor, and of the representative, if any;
- (b) the name and contact details of the data protection officer, if any;
- c) a general description of its uses of personal data

~~(c) the purposes of the processing, including the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);~~

~~(d) a description of categories of data subjects and of the categories of personal data relating to them;~~

~~(e) the recipients or categories of recipients of the personal data, including the controllers to whom personal data are disclosed for the legitimate interest pursued by them;~~

~~(f) where applicable, transfers of data to a third country or an international organisation, including the identification of that third country or international organisation and, in case of transfers referred to in point (h) of Article 44(1), the documentation of appropriate safeguards;~~

~~(g) a general indication of the time limits for erasure of the different~~

<p>mechanisms referred to in Article 22(3).</p> <p>5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the documentation referred to in paragraph 1, to take account of in particular the responsibilities of the controller and the processor and, if any, the controller's representative.</p> <p>6. The Commission may lay down standard forms for the documentation referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>	<p>categories of data; (h) the description of the mechanisms referred to in Article 22(3).</p> <p>5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the documentation referred to in paragraph 1, to take account of in particular the responsibilities of the controller and the processor and, if any, the controller's representative.</p> <p>6. The Commission may lay down standard forms for the documentation referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>
--	--

Justification:

With the aim to reduce administrative burden on controllers, Art. 28 replaces the general obligation to notify individual processing operations to the supervisory authority under Articles 18(1) and 19 of Directive 95/46/EC. However, we believe this new obligation to maintain documentation of all processing operations will involve heavy bureaucratic requirements and therefore seriously risk increasing rather than reducing the administrative burden, compared to the current rules.

We are also concerned that identical obligations apply to data controllers and data processors (which currently are not subject to any notification obligation). This poses a particular problem in the area of cloud computing. Indeed, imposing disproportionate documentation obligations on data processors -identical to the controllers' obligations- risks severely slowing the development and roll out of new cloud computing offerings and services in Europe.

Finally, we firmly believe Article 28 conflicts with the principles of accountability and efficiency that are set out in Article 22 of the GDPR, therefore it should be simplified in order to become effective and proportionate. Only Article 28.2.a. and 28.2.b. should be maintained, combined with a general duty to keep an inventory and description of the way the controller ensures that processing operations comply with data protection rules.

Finally, we suggest to delete the possibility for the Commission to adopt delegated and implementing acts in line with Art.29 Working Party's Opinion 8/2012 (October 5th, 2012, p. 27).

Proposed Amendment 17

Article 30 Security of processing	
Commission Proposal	Telefónica Proposal (proposed new text in blue)
<p>(3) The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the technical and organisational measures referred to in paragraphs 1 and 2, including the determinations of what constitutes the state of the art, for specific sectors and in specific data processing situations, in particular taking account of developments in technology and solutions for privacy by design and data protection by default, unless paragraph 4 applies.</p> <p>(4) The Commission may adopt, where necessary, implementing acts for specifying the requirements laid down in paragraphs 1 and 2 to various situations, in particular to:</p> <ul style="list-style-type: none"> (a) prevent any unauthorised access to personal data; (b) prevent any unauthorised disclosure, reading, copying, modification, erasure or removal of personal data; (c) ensure the verification of the lawfulness of processing operations. <p>Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>	<p>(3) The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the technical and organisational measures referred to in paragraphs 1 and 2, including the determinations of what constitutes the state of the art, for specific sectors and in specific data processing situations, in particular taking account of developments in technology and solutions for privacy by design and data protection by default, unless paragraph 4 applies.</p> <p>(4) The Commission may adopt, where necessary, implementing acts for specifying the requirements laid down in paragraphs 1 and 2 to various situations, in particular to:</p> <ul style="list-style-type: none"> (a) prevent any unauthorised access to personal data; (b) prevent any unauthorised disclosure, reading, copying, modification, erasure or removal of personal data; (c) ensure the verification of the lawfulness of processing operations. <p>Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>

Justification:

We suggest to delete the possibility for the Commission to adopt delegated and implementing acts as the Commission does not know the technology and the architecture of companies. To meet the state of the art protection measures and to ensure the adequate and proportionate protection of personal data it is more appropriate to let companies build up the protection mechanism while implementing new products and services during the product development process itself.

Proposed Amendment 18

Article 31 Notification of a personal data breach to the supervisory authority	
Commission Proposal	Telefónica Proposal (proposed new text in blue)
<p>(1) In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 24 hours after having become aware of it, notify the personal data breach to the supervisory authority. The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within 24 hours.</p> <p>(2) Pursuant to point (f) of Article 26(2), the processor shall alert and inform the controller immediately after the establishment of a personal data breach.</p> <p>(3) The notification referred to in paragraph 1 must at least:</p> <p>(a) describe the nature of the personal data breach including the categories and number of data subjects concerned and the categories and number of data records concerned;</p> <p>(b) communicate the identity and contact details of the data protection officer or other contact point where more information can be obtained;</p> <p>(c) recommend measures to mitigate the possible adverse effects of the personal</p>	<p>(1) In the case of a significant and material personal data breach, the controller shall without undue delay and, where feasible, not later than 24 hours after having become aware of it, notify the personal data breach to the supervisory authority. The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within 24 hours.</p> <p>(2) Pursuant to point (f) of Article 26(2), the processor shall alert and inform the controller immediately without undue delay after the identification establishment of a significant and material personal data breach.</p> <p>(3) The notification referred to in paragraph 1 must, where available, at least:</p> <p>(a) describe the nature of the personal data breach including the categories and number of data subjects concerned and the categories and number of data records concerned;</p> <p>(b) communicate the identity and contact details of the data protection officer or other contact point where more information can be obtained;</p> <p>(c) recommend measures to mitigate the possible adverse effects of the</p>

<p>data breach; (d) describe the consequences of the personal data breach; (e) describe the measures proposed or taken by the controller to address the personal data breach.</p>	<p>personal data breach; (d) describe, <i>if possible</i>, the consequences of the personal data breach; (e) describe, <i>if possible</i>, the measures proposed or taken by the controller to address the personal data breach <i>and/or mitigate its adverse effects</i>.</p>
---	--

Justification:

Notifying data breaches is already an obligation imposed by the ePrivacy Directive. Therefore, we welcome the extension of the data breach notification obligation to all data controllers, which will ensure both a level playing field between providers and a consistent protection framework for European data subjects. However, the requirements imposed by both the ePrivacy Directive and the draft Regulation should be aligned to avoid a dual notification obligation for e-communications providers and a different level of protection for data subjects.

Telefónica would suggest some modifications in the current wording in order for these provisions to be not only feasible, but effective.

The current definition of “personal data breach” requires further clarification, especially regarding the source of the “accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data...”, currently defined in Art. 4.9.

We understand that the responsibilities placed on the controller in relation to a personal data breach should apply only in situations in which there is a breach of security in the controller’s systems or networks, or due to some action, decision, technical or security error, or other cause associated with the systems and/or activities of the controller.

It should not apply in cases such as phishing, when a data subject voluntarily grants access to their personal information to a third party based on deceptive activity by that third party.

A “24 hours requirement” to notify to the Supervisory Authority is arbitrary and unjustified. Notification is only useful after a first technical verification of the cause. This is often not possible in 24 hours and it is distracting from the real and critical objective of fixing the data breach as soon as possible.

Moreover, the DPAs will not have the resources to deal with it and the general public will get “notification fatigue” undermining the core policy objective of notifications. This very significant burden introduced on EU businesses would then simply result in the paralysis of the competent authorities. A more pragmatic approach is that a company must log all data breaches and that this log can be inspected by the DPA at any time, but that only more serious breaches have to be actively reported within a reasonable time frame.

To sum up, given the limited time frame for notifications and the potential

Proposed Amendment 19

Article 33 Data Protection Impact Assessment	
Commission Proposal	Telefónica Proposal (proposed new text in blue)
<p>(1) Where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller or the processor acting on the controller's behalf shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.</p> <p>(2) The following processing operations in particular present specific risks referred to in paragraph 1:</p> <p>(a) a systematic and extensive evaluation of personal aspects relating to a natural person or for analysing or predicting in particular the natural person's economic situation, location, health, personal preferences, reliability or behaviour, which is based on automated processing and on which measures are based that produce legal effects concerning the individual or significantly affect the individual; [...]</p> <p>(c) monitoring publicly accessible areas, especially when using optic-electronic devices (video surveillance) on a large scale;</p> <p>(4) The controller shall seek the views of data subjects or their representatives on the intended</p>	<p>(1) Where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller or the processor acting on the controller's behalf shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.</p> <p>(2) The following processing operations in particular present specific risks referred to in paragraph 1:</p> <p>(a) a systematic and extensive evaluation of personal aspects relating to a natural person or for analysing or predicting in particular the natural person's economic situation, location, health, personal preferences, reliability or behaviour, which is based on automated processing and on which measures are based that produce legal effects concerning the individual or significantly affect the individual; [...]</p> <p>(c) monitoring publicly accessible areas, especially when using optic-electronic devices (video surveillance) on a large scale;</p> <p>(4) The controller shall seek the views of data subjects or their</p>

processing, without prejudice to the protection of commercial or public interests or the security of the processing operations.

~~representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations.~~

Justification:

Data controllers should have flexibility in determining risks under the principle of accountability. Data controllers know the particularities of their products, services or sectors and can better adapt DPIAs to their needs.

A PIA is naturally a duty of the controllers, therefore, imposing this obligation also on processors should be questioned as it could be even more counterproductive, diluting the liabilities between the data controller and the data processor. This poses a particular problem in the area of cloud, where more than ever the responsibilities and roles of the data controller and the data processor shall be clearly differentiated.

We call for the removal of the obligation to conduct a PIA of a processing based on profiling, as we do not agree with the fact that profiling per se presents “specific risks”.

Article 33 (4) obliges data controllers to seek the views of data subjects or their representatives (e.g., consumer organisations) on the intended processing of their personal data. This obligation is disproportionate and would create commercial concern for companies developing new products and services in highly competitive markets. Therefore, we suggest its deletion.

Proposed Amendment 20

Article 43 Transfers by way of binding corporate rules	
Commission Proposal	Telefónica Proposal (proposed new text in blue)
<p>1. A supervisory authority shall in accordance with the consistency mechanism set out in Article 58 approve binding corporate rules, provided that they:</p> <p>(a) are legally binding and apply to and are enforced by every member within the controller’s or processor's group of undertakings, and include their employees;</p> <p>(b) expressly confer enforceable rights on data subjects;</p> <p>(c) fulfil the requirements laid down in paragraph 2.</p>	<p>1. (New)One supervisory authority shall in accordance with the consistency mechanism set out in Article 58 and through a single act of approval authorize binding corporate rules for a group of undertakings.</p> <p>2. (New)Those rules will allow multiple intercompany international transfers in and out of Europe, provided that they:</p> <p>(a) are legally binding and apply to and are enforced by every member within the controller’s or processor's group of undertakings, and include their employees;</p> <p>(b) expressly confer enforceable rights on data subjects;</p> <p>(c) fulfil the requirements laid down in paragraph 2.</p>

Justification:

Telefónica welcomes the recognition of the concept of “group of undertakings” as well as the Binding Corporate Rules (BCRs) for data transfer within a Group of undertakings.

BCRs already exist under the current regulatory framework; however they do not work in practice. They have proven to be too onerous and inflexible to be a workable solution, because companies were requested to receive the green light from all national DPAs of those Member States where they were active. That implied an extraordinary administrative burden for companies.

The BCRs under the new Regulation must be designed to become the useful solution the Commission intends it to be. Therefore, to be a workable solution, Telefónica ask for a streamline approval process of the BCR’s through which they allow one data protection Agency approval which in turn allow multiple intercompany international transfers in and out of Europe. In other words, just only one company of the Group of Companies is requested to receive green light from one DPA of one of the Member States.

Proposed Amendment 21

Article 44 Derogations	
Commission Proposal	Telefónica Proposal (proposed new text in blue)
1 (h) the transfer is necessary for the purposes of the legitimate interests of the controller or processor, which cannot be qualified as frequent or massive, and where the	1 (h) the transfer is necessary for the purposes of the legitimate interests of the controller or processor, which cannot be qualified as frequent or massive, and where the

Proposed Amendment 22

Article 51 Competence	
Commission Proposal	Telefónica Proposal (proposed new text in blue)
<p>2. Where the processing of personal data takes place in the context of the activities of an establishment [...], the supervisory authority of the main establishment of the controller or processor shall be competent for the supervision of the processing activities of the controller or the processor in all Member States, without prejudice to the provisions of Chapter VII of this Regulation.</p>	<p>2. Where the processing of personal data takes place in the context of the activities of an establishment [...], the supervisory authority of the main establishment of the controller or processor shall be competent for the supervision of the processing activities of the controller or the processor respectively in all Member States, without prejudice to the provisions of Chapter VII of this Regulation.</p>

Justification:

According to our understanding the one-stop shop criteria depend on where the company providing the service is established.

There is, however, one situation that is not quite clear under the proposed Art. 51. The specific example Telefónica is thinking about is the following:

- Telefónica's cloud services are provided by its UK based subsidiary Telefónica Digital, so the ICO is the relevant authority;
- However, this service is marketed by Telefónica's Operating Businesses across the EU. Telefónica Digital acts as a processor.
- In this case, the supervisory authority would also be the ICO for all matters related to the obligations of the processor and not the supervisory authority of the main establishment of the data controller.

Telefónica therefore would like to suggest an amendment to Art 51 by adding the word "respectively" with the aim of making clear that in these cases the supervisory authority for the processing activities of the processor should be the authority where the main establishment of the processor is located.

Proposed Amendment 23

Article 77	
Right to compensation and liability	
Commission Proposal	Proposal (proposed new text in blue)
<p>1. Any person who has suffered damage as a result of an unlawful processing operation or of an action incompatible with this Regulation shall have the right to receive compensation from the controller or the processor for the damage suffered.</p> <p>2. Where more than one controller or processor is involved in the processing, each controller or processor shall be jointly and severally liable for the entire amount of the damage, to the extent that liability has not already been established in the determination of responsibilities envisaged in Article 24.</p> <p>3. The controller or the processor may be exempted from this liability, in whole or in part, if the controller or the processor proves that they are not responsible for the event giving rise to the damage.</p>	<p>1. Any person who has suffered damage as a result of an unlawful processing operation or of an action incompatible with this Regulation shall have the right to receive compensation from the controller or the processor for the damage suffered.</p> <p>2. Where more than one controller or processor is involved in the processing, each controller or processor shall be jointly and severally liable for the entire amount of the damage, to the extent that liability has not already been established in the determination of responsibilities envisaged in Article 24.</p> <p>3. The controller or the processor may be exempted from this liability, in whole or in part, if the controller or the processor proves that they are it is not responsible for the event giving rise to the damage.</p>

Justification:

Liability should be maintained on the data controller as it is currently the case further to the Directive 1995/46/EC. The controller is the one who has the direct link with the data subject and is the one responsible vis-à-vis the data subject. If the controller considers any eventual damage was due to the processor's incorrect processing, the data controller will ask compensation from the processor. Furthermore, the controller and the processor normally establish the liability relationship in the contractual arrangements, for cases where the processor does not act as requested by the data controller.

This article instead of helping data subjects creates confusion for controllers, processors and even more importantly for data subjects.

Proposed Amendment 22

Article 79 Sanctions	
Commission Proposal	Telefónica Proposal (proposed new text in blue)
<p>(3) In case of a first and non-intentional non-compliance with this Regulation, a warning in writing may be given and no sanction imposed, where:</p> <p>(a) a natural person is processing personal data without a commercial interest; or</p> <p>(b) an enterprise or an organisation employing fewer than 250 persons is processing personal data only as an activity ancillary to its main activities.</p> <p>(4) The supervisory authority shall impose a fine up to 250.000 EUR, or in case of an enterprise up to 0,5 % of its annual worldwide turnover, to anyone who, intentionally or negligently:</p> <p>(a) does not provide the mechanisms for requests by data subjects or does not respond promptly or not in the required format to data subjects pursuant to Articles 12(1) and (2);</p> <p>(b) charges a fee for the information or for responses to the requests of data subjects in violation of Article 12(4).</p> <p>(5) The supervisory authority shall impose a fine up to 500.000 EUR, or in case of an enterprise up to 1 % of its annual worldwide turnover, to anyone who, intentionally or</p>	<p>(3) In case of a first and non-intentional non-compliance with this Regulation, a warning in writing may be given and no sanction imposed, where:</p> <p>(a) a natural person is processing personal data without a commercial interest; or</p> <p>(b) an enterprise or an organisation employing fewer than 250 persons is processing personal data only as an activity ancillary to its main activities.</p> <p>(4) The supervisory authority shall shall may impose a fine up to 250.000 EUR, or in case of an enterprise up to 0,5 % of its annual worldwide turnover, to anyone who, intentionally or negligently:</p> <p>(a) does not provide the mechanisms for requests by data subjects or does not respond promptly or not in the required format to data subjects pursuant to Articles 12(1) and (2);</p> <p>(b) charges a fee for the information or for responses to the requests of data subjects in violation of Article 12(4).</p> <p>(5) The supervisory authority shall shall may impose a fine up to 500.000 EUR, or in case of an enterprise up to 1 % of its annual worldwide turnover, to anyone who, intentionally or</p>

<p>negligently: [...] (f) does not or not sufficiently maintain the documentation pursuant to Article 28, Article 31(4), and Article 44(3);</p> <p>(6) The supervisory authority shall impose a fine up to 1.000.000 EUR or, in case of an enterprise up to 2 % of its annual worldwide turnover, to anyone who, intentionally or negligently: [...] (h) does not alert on or notify a personal data breach or does not timely or completely notify the data breach to the supervisory authority or to the data subject pursuant to Articles 31 and 32;</p>	<p>negligently: [...] (f) does not or not sufficiently maintain the documentation pursuant to Article 28, Article 31(4), and Article 44(3);</p> <p>(6) The supervisory authority shall may impose a fine up to 1.000.000 EUR or, in case of an enterprise up to 2 % of its annual worldwide turnover, to anyone who, intentionally or negligently: [...] (h) does not alert on or notify a personal data breach or does not timely or completely notify the data breach to the supervisory authority or to the data subject pursuant to Articles 31 and 32;</p>
---	--

Justification:

Sanctions should not be automatically imposed. A margin of evaluation and assessment should be left for national DPAs to take into account the specific situations and the circumstances of a given infringement (eg. willingness to cooperate to solve the data breach, adoption of voluntary remedies, quality of the dialogue between the company and the DPA).

The word “shall” should be replaced by “may” in Articles 79.4, 79.5 and 79.6.

Sanctions must be proportionate to the risks and any privacy harms associated with the specific context of processing and only after consideration of all facts. This requires the development of objective criteria to guide DPAs. It also requires reconsideration of fines related to a company’s worldwide annual turnover, which is not directly related to the severity of the infringement and is therefore disproportionate.

Any reference to a percentage of “annual worldwide turnover” should be deleted. Such a criteria is unpredictable and would lead to uncertainty for companies. To ensure legal certainty, a maximum amount of fine should be established.

In terms of proportionality and considering the very high sanctions foreseen, some of the sanctions foreseen are seemingly not related to the severity of the infringement, therefore are not proportionate.

The Regulation should address non compliance that has harmful consequences for individuals. Sanctions should envisage enhancing the protection of privacy, rather than punishing failure of administrative requirements without impact for data subjects. The individual should be the protected interest, not the data itself.

Concrete examples of this lack of proportionality are Art. 79.5.f, Art. 79.6.h.

PROTECTING PRIVACY WHILE MAINTAINING GLOBAL TRADE AND SECURITY REQUIRES FLEXIBLE SOLUTIONS

The United States and the European Union (EU) are both committed to protecting privacy and our respective legal regimes are founded on the same core principles. We have a long-standing relationship of cooperation on data privacy and a deep understanding of the robust privacy protections both of our frameworks provide.

However, the European Commission has proposed a draft data protection framework that will generally require third countries to either be deemed "adequate" or adhere to "appropriate safeguards," a standard that essentially necessitates countries to mirror the EU system for enforcing privacy protections, as a prerequisite for maintaining the free flow of personal data in the commercial, regulatory and law enforcement contexts.

Instead of approaching international privacy protection as a legal harmonization exercise, we should work towards the interoperability of our privacy frameworks based on common principles and accountability mechanisms, as we have always done.

In their current form, the Regulation and Directive can have far-reaching negative effects. Economically, they could stifle innovation and inhibit growth. The legislation could also jeopardize the ability of regulators to maintain global financial market stability, and protect consumers, health and safety. On the law enforcement front, it could endanger the flow of information that is critical to our joint efforts to fight international terrorism and transnational crime, including human trafficking, child pornography and cybercrime.

Above all, given the complex and unpredictable effects the EU legislation may have and the enormous implications for global trade and security, a careful, thorough examination of all of the potential consequences should be carried out and the legislation revised to ensure that security and commerce are not adversely affected.

THE REGULATION: IMPACT ON TRADE, COMMERCE AND INTEROPERABILITY

Like the EU, the United States recognizes the need to apply our privacy principles to new, rapidly evolving technologies. To achieve this goal, we are strengthening our already robust system by initiating multi-stakeholder processes to develop codes of conduct based on the Consumer Privacy Bill of Rights introduced by the Obama Administration. (<http://www.whitehouse.gov/sites/default/files/privacy-final.pdf>) Nonetheless, our framework will contain variations from EU law and it is critical that these differences not impede transatlantic commerce. Interoperability of our respective privacy regimes is critical to maintaining our extraordinary economic relationship, fostering trade and preventing non-tariff barriers, and unlocking the full potential for our economic innovation and growth. Both the U.S. and the EU seek to achieve the same outcomes, including empowering and protecting consumers, despite our different privacy frameworks. We urge the EU to look more toward outcomes that provide

meaningful protection for privacy and focus less on formalistic requirements.

The U.S.-EU Safe Harbor Framework is a concrete example of a flexible mechanism that enables interoperability of our respective regimes. We are pleased that the proposed EU Data Protection Regulation ensures the Safe Harbor Framework will continue to enable trade and privacy protection by keeping its existing adequacy determination in place, and also endorses the use of Binding Corporate Rules. The EU could do more in the new legislation, however, to facilitate cross-border data flows. The United States recommends that the EU encourage the development and adoption of cross-border codes of conduct and other accountability mechanisms as an independent basis for data transfers to third countries. These mechanisms would strengthen privacy protections while promoting innovation and enhanced trade.

THE REGULATION: APPLYING PRIVACY PROTECTIONS TO NEW TECHNOLOGIES AND THE CIRCUMSTANCES OF OUR TIMES

The Internet operates on standards that are developed in voluntary consensus-based multi-stakeholder processes, allowing all stakeholders to voice their concerns and opinions. As a result, these standards are adaptable to a quickly changing technological environment. The OECD recently affirmed the importance of these multi-stakeholder bodies in the Council Recommendation on Principles for Internet Policy-Making. We urge the EU to encourage the development of standards in multi-stakeholder processes, rather than regulatory processes that may lack the flexibility to adapt to rapid technological advancements. We recommend a more flexible approach to consent than currently appears in the draft legislation. The United States believes that consent should be meaningful and that the methods of expressing such consent take into account the context in which it is being given as well as the relevant privacy risks in that context. For example, consent need not always be express, affirmative consent, and the means for individuals to communicate their choices should match the scale, scope, and sensitivity of the personal data that organizations collect, use, or disclose.

The United States also recommends that the EU carefully examine the proposed "right to be forgotten" and "right to erasure" and make appropriate modifications to avoid hampering the ability to innovate, compete, and participate in the global economy. For example, we suggest that the EU reconsider the feasibility of placing obligations on a data controller for publications made by others after consent is withdrawn.

Modifications to these rights are necessary to ensure consistency with the right to freedom of expression enshrined in the Universal Declaration of Human Rights and the International Covenant of Civil and Political Rights.

Based on our extensive experiences with data breach laws in the United States, we believe the proposed notification period for informing supervisory authorities and individuals of data breaches is too short. In our experience, the process of detecting breaches and assessing their scope may require more than 24 hours. Furthermore,

requiring businesses to provide notice if possible within 24 hours could lead to over-notification to consumers as businesses will include and notify consumers before the scope of the breach is fully assessed. Such a practice could lead consumers to ignore notifications or act on information later determined to be erroneous.

THE REGULATION: IMPACT ON INFORMATION EXCHANGES AND TRANSFERS TO REGULATORS, LITIGANTS IN CIVIL CASES, AND LAW ENFORCEMENT AUTHORITIES

The Regulation's provisions regarding the transfer of data to third countries or international organizations have potentially disastrous ramifications for regulatory enforcement and private litigation, which depend on transfer of information and personal data among regulators or other government authorities, or between private entities and third country government entities, or litigants in civil and administrative cases.

By the terms of Chapter V, the continued robust sharing of information between our regulatory agencies may be jeopardized unless the scope of the Regulation is clarified to exclude it, or the EC bestows a finding of adequacy or "appropriate safeguards" that applies to sharing among such regulators. We also note with concern that Chapter VI appears to provide data protection authorities with unlimited ability to suspend the transfer of information to third countries, apparently at their sole discretion. We are equally concerned that the sanctions imposed under Chapter VIII will discourage processors and controllers from making transfers in cases where the precise application of the Regulation is unclear.

This Regulation will seriously weaken international regulatory cooperation. U.S. and EU regulators are parties to various bilateral and multilateral informal arrangements and they follow principles of international organizations pursuant to which they collect and share certain information. To the extent that the Regulation restricts how EU and Member State regulators collect, process and transfer data on behalf of U.S. or other non-EU regulators, it may run contrary to their longstanding arrangements.

Similarly, information needed in civil and administrative litigation in third countries often contains personal data, which may include personal data of EU residents. Were the Regulation to encumber the national rules, international agreements and practice that have developed in this area, it would weaken the ability of litigants, including EU persons and businesses, to enforce their claims.

In addition, under the draft Regulation, data controllers may process and transfer personal data if it is done pursuant to a legal obligation or in the public interest, but only if the obligation or public interest is set forth in Union or Member State law. There are several problems with this approach.

First, the proposed Regulation does not fully delineate which matters fall within the public interest, providing instead for the European Commission to further specify this important concept in a delegated act. The Regulation should clarify under what circumstances government authorities (e.g., EU financial regulators, consumer protection regulators, or even data protection authorities) or private entities may share data with regulators in third countries without an adequacy determination. These activities are generally in the public interest and should not be subject to the level of uncertainty found in the proposed Regulation.

Second, even if the scope of the public interest exception were clarified, the requirement that the obligation or public interest be set forth in Union or Member State law ignores the practical reality that data transfers will continue to be necessary for enforcement and compliance with non-EU laws and other public interests not currently contemplated. For example, many multinational entities are subject to existing legal obligations to process and transfer data under both EU and non-EU laws, which arise from regulation, civil and criminal law enforcement requests and compliance monitoring, and discovery requests or court orders associated with civil litigation. These obligations are often crucial for regulators worldwide to safeguard financial markets from abusive practices and systemic risk for market stability purposes, to protect the public through export/import regulations and to enforce competition, consumer protection, privacy, and other laws.

The same serious legal obligations and concerns related to restrictions on the transfer of data to third countries will apply to private parties, including EU persons and entities, in the adjudication of their cases before U.S. civil or administrative courts. These provisions of the draft Regulation would also restrict voluntary reporting of criminal conduct to third country authorities, thereby endangering third country public interests and inhibiting EU persons and entities' ability to obtain leniency from third country authorities.

Third, while we believe it inadvertent, Article 3(2) on scope can be read as implicating the activities of third country regulatory agencies where an EU resident engages in certain activities they regulate. It should be modified to remove this ambiguity.

There is also great uncertainty about the extent to which regulatory functions fall into the scope of the proposed Regulation or the proposed Directive. While the Regulation appears to apply to data processing in civil contexts, Recital 16 of the Regulation states that "data processed by public authorities under this Regulation when used for the purposes of prevention, investigation, detection and prosecution of criminal offences or the execution of criminal penalties, should be governed by [the Directive]." U.S. regulators who solely exercise civil enforcement powers often cooperate with criminal authorities, such that the line between "civil" and "criminal" is not clearly defined. Moreover, U.S. and European legal systems sometimes differ as to which offenses are considered criminal and which are civil regulatory matters. It appears that the Directive could be read to impose restrictions on those regulators without consideration for any of the exceptions, derogations or other protections that the Regulation may offer.

The proposed Regulation affects law enforcement activities of third countries. U.S. law enforcement agencies - including the Departments of Justice, Treasury and Homeland Security - also exercise regulatory functions (e.g., with respect to immigration, financial transactions, importation of drugs or weapons). The administrative investigations they and other U.S. regulators carry out can be referred for prosecution and the data they gather are often crucial evidence in civil and criminal cases. The Regulation's detrimental impact on third country regulatory activities is therefore also of concern to law enforcement authorities of non-EU countries. It is also unclear how the Regulation will apply when conduct is treated as a civil violation in some jurisdictions and a criminal violation in others. For instance, price fixing by international cartels is treated as a criminal violation under U.S. law and under the law of some EU Member States but as a civil violation under EU law.

THE DIRECTIVE: IMPACT ON LAW ENFORCEMENT RELATED ACTIVITIES

Similarly, we are concerned that the Directive will have a detrimental impact on global law enforcement cooperation. A number of these concerns are similar to those discussed above regarding the Regulation's impact on regulatory cooperation.

Specifically, (1) Chapter V of the Directive appears to require third countries to adopt an EU-style data protection system in order to ensure continued robust information sharing; (2) Chapter VI gives data protection officials - who by and large will have no law enforcement experience - the final say on whether cooperation should be provided; and (3) Chapter VIII provides for joint and several liability for failure by law enforcement officials to meet the Directive's requirements, even where these requirements are not particularly clear and where the purported violation was not intentional; a penalty that will undoubtedly have a chilling effect on transfers.

In addition, Article 60 would require Member States to renegotiate international agreements to conform with the detailed provisions of the Directive. This would entail the re-opening of hundreds of bilateral and multilateral agreements in force in the criminal justice area, which would be onerous in terms of its resource implications. We also note that renegotiation and modification of international agreements, by definition, require the consent of the other party. Such agreements should instead be "grandfathered", along with the numerous other international cooperation systems in which EU Member States currently participate, including the Interpol system, the Egmont Group of financial intelligence units, the Financial Action Task Force recommendations, and the 24/7 High Tech Crime Network.

The current negotiations of an umbrella agreement on exchanges related to criminal law enforcement between the U.S. and EU that you have undoubtedly heard about will not alone solve the problems with the proposed Directive described above. The implications of the Directive go well beyond the relationship between the U.S. and the EU; the adverse impact on other non-EU countries will weaken our collective efforts to protect the public.



The Consumer Voice in Europe

Data Protection

Proposal for a Regulation

BEUC Position Paper

Contact: **Kostas Rossoglou and Nuria Rodríguez –
digital@beuc.eu**

Ref.: X/2012/039 - 27/07/2012

Summary

The European Consumer Organisation (BEUC) welcomes the European Commission's proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). We agree with the general direction taken by the European Commission, acknowledging that while the objectives of Directive 95/46 remain relevant, a thorough review has become indispensable owing to the technological and social changes which have occurred in the digital environment.

Overall, the draft Regulation addresses the main challenges and the shortcomings of the current framework with the aim of enhancing the rights of data subjects and restoring control over the processing of their own personal data, especially in light of constantly evolving ICT developments.

Although the proposal in general constitutes a major improvement for individuals, a number of provisions still need to be clarified or modified to ensure the new EU framework is effective and becomes the global standard of personal data protection and privacy.

Our key concerns and our suggestions to further improve the Commission's proposal are summarised below:

<p>General provisions</p>	<p>Material scope (art. 2) We welcome the general scope of application. Yet, the exceptions to the scope should be clearly defined to ensure legal certainty and uniform application of the Regulation:</p> <ul style="list-style-type: none"> - the exception on activities related to "national security" should be further defined; - The exception on household activities should <u>not</u> apply when data is made available to an indefinite number of people. <p>Territorial scope (art. 3) We welcome that the Regulation applies to controllers established in and outside of the European Union (when processing personal data in the EU).</p> <ul style="list-style-type: none"> - For controllers established in the EU, the Regulation should address the issue of national applicable law. - For controllers <u>not</u> established in the EU, the application of the regulation to the "monitoring of behaviour" of data subjects must be clarified, to ensure that it includes tracking and profiling of data subjects as well as services which are based on monetizing the secondary use of consumers' personal data. <p>Definitions (art. 4) <u>"Personal data"</u>:</p>
----------------------------------	---

	<p>BEUC welcomes the broad definition of personal data as reflected in the proposal as it will provide the necessary flexibility in the light of rapid ICT developments. In order to ensure legal certainty, it should be clarified that when there is a close relation between the data and an individual that singles out the individual, this will trigger the application of data protection rules.</p> <p><u>“Consent”</u>: BEUC welcomes recital 25 stating that consent can be given by any appropriate method and that electronic consent should not hinder the data subject’s on line experience. There is no 'one size fits all' solution to the issue of consent but consent must always be meaningful. In addition, compliance with the principles for data processing including data minimization and purpose limitation needs to be ensured.</p> <p><u>“Main establishment”</u>: We welcome the definition of “main establishment” of the controller. However, the regulation should address the case of undertakings with decentralized decision making structure: in these cases the main establishment of the group may be used as the determining factor, or alternatively the dominant influence of one establishment over the others.</p> <p><u>“Transfer” of personal data (new)</u> A definition of what is to be considered as “transfer” of personal data needs to be introduced in relation to the exchange of data between companies in the same country and other types of exchanges on networks, such as servers of companies.</p>
Principles	<p>(Arts. 5, 6 and 7) BEUC welcomes the introduction of the principle of <u>transparency</u> and the strengthening of the data minimization principle;</p> <p>As regards the principle of <u>purpose limitation</u>, a clear definition of what is to be considered as “compatible” use with the initial purpose of processing needs to be introduced;</p> <p>The concept of <u>legitimate interests</u> of the data controller must be clearly defined; it should not be left to a delegated act, as there is a risk of surpassing the legal grounds;</p>
Special categories of data	<p>Personal data of a child and sensitive data (arts. 8 and 9)</p> <p>BEUC welcomes the requirement of parental consent for the processing of personal data of a child. However, verification procedures of parental consent should <u>not</u> lead to further processing of data which otherwise would not be necessary</p>

	<p>to process.</p> <p>BEUC welcomes the prohibition of collection/processing of <u>sensitive</u> data as the general rule (article 9). The list of sensitive personal data must remain exhaustive and also include financial data revealing personal solvency.</p>
<p>Rights of the data subject</p>	<p>Transparency (art. 11) BEUC welcomes the new requirement that information has to be provided in an <u>intelligible form</u> and using <u>clear and plain language</u>.</p> <p>Modalities for exercising of rights (art. 12) BEUC welcomes the requirements in article 12 of the proposal: - Data controllers are required to respond to requests by data subjects without undue delay and no later than one month; - Data controllers will not be able to charge for the data subject's exercise of his rights, as long as this right is not abused.</p> <p>Rights in relation to recipients (art. 13) BEUC welcomes the introduction of an obligation for the data controller to notify each recipient (third parties) to whom data has been disclosed, in case of request of rectification or erasure by the data subject.</p> <p>Information to the data subject (art. 14) The list of information obligations of the controller is rather comprehensive. BEUC suggests adding the following items to the list: - the type of personal data collected and processed; - the procedures to lodge complaints; - whether processing is done for tracking and profiling purposes and its consequences on individuals; - which personal data is obligatory to provide and which is voluntary; - Where applicable, the information that personal data is collected in exchange for so-called "free services".</p> <p>Right to be forgotten (art. 17) BEUC supports the intention of the "Right to be forgotten" which aims to strengthen the right to erase personal data. It should be made clear that the obligation to delete the consumer's data lies upon the controller of the information and not upon the downstream parties (host providers, search engines etc), in order to ensure the compatibility with the provisions on the liability of Internet Service Providers under the Directive on e-commerce.</p> <p>Right to data portability (art. 18) BEUC welcomes the introduction of the new right to data portability. The right to data portability allows the consumer</p>

	<p>to be in control of his data and retain the ownership, by being able to shift the data to other services. Yet, for this right to be effectively implemented the development of interoperable or compatible standards is necessary.</p> <p>Right to object (art. 19) It should be clarified that the right to object, if upheld by the controller should result in the deletion of the data by the controller.</p> <p>Profiling (art. 20) BEUC welcomes the specific inclusion of profiling practices in the proposed regulation. In addition to the right not to be subject to profiling, consumers should be informed of the techniques and procedures used for profiling and the possible consequences of profiling techniques applied to them. Profiling of vulnerable consumers such as children should be prohibited.</p> <p>Restrictions (art. 21) BEUC considers that the conditions and guarantees under which the rights of the data subject may be restricted must be explicitly and further defined.</p>
<p>Controller and processor</p>	<p>Responsibility of the controller (art. 22) BEUC welcomes the provisions on controller's responsibility and accountability. However, the principle of accountability should not be perceived as an alternative to compliance with legal obligations or as an excuse to avoid administrative sanctions.</p> <p>Data protection by design and by default (art. 23) BEUC very much welcomes the introduction of the principles of data protection by design and by default; the following requirements should be added:</p> <ul style="list-style-type: none"> - Reference to the use of Privacy Enhancing Technologies (PETs) should be introduced, as a tool to implement technical solutions to comply with the principle of data protection by design. - The principle of Data Protection by default should be revised to make it explicit that the privacy settings on services and products should by default comply with the general principles of data protection, such as data minimization and purpose limitation; - The data processor should also be obliged to implement privacy by design and privacy by default when processing personal data on behalf of the controller. <p>Joint controllers (art. 24) BEUC welcomes the obligation of joint controllers to define their respective responsibilities for compliance with their obligations, by means of an arrangement between them. We would also suggest introducing the principle of joint responsibility between the controller and the processor.</p>

	<p>Representatives of controllers not established in the Union (art. 25) BEUC welcomes the requirement for controllers not established in the EU to designate a representative in the Union. The representative is expected to be the contact point for both data protection authorities and the data subject. Any exceptions to this requirement must be fully justified or otherwise deleted.</p> <p>Documentation (art. 28) The obligation to maintain documentation as defined in this provision is welcome and should <u>not</u> be weakened: it includes the most relevant information which should ensure that controllers are able to demonstrate compliance upon request by the DPAs.</p> <p>Data breach notification (art. 31) BEUC welcomes the introduction of a horizontal data breach notification obligation.</p> <ul style="list-style-type: none"> - Only those breaches that <u>adversely affect</u> the individual should be notified to data subjects. - BEUC supports a risk-based definition of the adverse effect of data breaches. - The notification to data protection authorities must take place as soon as possible without undue delay, and not beyond 72 hours after the controller becomes aware of the data breach. - A specific deadline must be introduced for the DPA to act on a breach notification, as well as a deadline within which the data controller should notify the breach to the data subject. <p>Data Protection Impact Assessment (DPIA) (art. 32) BEUC welcomes the introduction of the obligation to carry out an assessment of the impact on the protection of personal data of the processing operations that present specific risks.</p> <ul style="list-style-type: none"> - A DPIA should also be carried out when processing operations <u>"are likely"</u> to present specific risks to the rights and freedoms of data subjects; - The DPIA should be made publicly available, or at least a summary of it; DPIAs must be audited by Data Protection Authorities. <p>Data Protection Officer (arts 35-37) BEUC welcomes the introduction of the obligation to appoint a Data Protection Officer (DPO). Only those entities that are processing personal data as an accessory activity could be excepted from this obligation. The independence of DPOs needs to be strengthened.</p>
--	--

	<p>Exception for SMEs BEUC is opposed to the exceptions from specific obligations for enterprises with less than 250 employees. The determining factor for introducing an exception should not be the number of employees but the nature of the processing activities, the number of personal data involved and the number of data subjects the enterprise processes data about.</p> <p>Codes of conduct (art. 38) Self regulatory codes can only be endorsed if they entail an added value for consumers' rights (by offering a higher level of protection), are backed up by suitably robust auditing or testing procedures and provide for independent and effective complaint handling and sanctions.</p> <p>Certification (art. 39) BEUC supports the establishment of EU certification schemes, including European Privacy Seals, as long as clear certification criteria are developed and the administration is entrusted to independent third party organisations. It is also important to clarify that the granting of a seal would not simply certify compliance with the law but also offer an added layer of protection.</p>
<p>Transfer to third countries</p>	<p>(Arts 40-45) BEUC welcomes the provisions on transfer of data to third countries. However, transfers should not be possible for those countries for which the European Commission has already adopted a decision not recognizing the <u>adequate</u> status.</p> <p><u>Derogations</u> from "adequate decisions" or "appropriate safeguards" must only apply for a restricted number of cases of occasional transfer that cannot be qualified as frequent, massive or structural.</p> <p><u>Disclosure of personal data to law enforcement authorities</u> of third countries must only be possible upon prior authorization by the supervisory authority.</p>
<p>Supervisory Authorities</p>	<p>(Arts 46-54) BEUC welcomes the provisions that require explicitly the independent status of supervisory authorities</p> <p>The establishment of a "<u>one stop shop</u>" for data controllers or processors might result in forum shopping; effective coordination between all relevant DPA should be ensured.</p> <p>Specific rules on the assignment of a lead authority when the <u>controller is not established in the EU</u> should also be defined.</p> <p>Specific rules of allocation of financial resources to DPAs must be introduced.</p>

<p>Cooperation and consistency</p>	<p>(Arts 55-63) BEUC welcomes the focus of the draft Regulation on enhancing cooperation between data protection authorities; strengthening cooperation and coordination is crucial as a data breach may well affect data subjects in many countries across the EU and beyond.</p> <p>However, the possibilities to trigger the <u>consistency</u> mechanism go too far. There needs to be a threshold in the draft Regulation to ensure that the consistency mechanism only applies to processing that raises serious risks to data subjects across Europe.</p> <p>The <u>powers of the European Commission</u> within the consistency mechanism must be carefully drafted in order not to undermine the independence of DPAs.</p>
<p>Remedies, liabilities and sanctions</p>	<p>(Arts 73-79) <u>Judicial collective actions for compensation</u> by representative bodies should be introduced.</p> <p>Consumer organizations must be entitled to bring actions for breaches of data protection law.</p> <p>Part of the fines imposed on companies should also be used to finance the actions of organizations defending the rights of data subjects.</p>
<p>Specific situations</p>	<p>Processing of personal data and freedom of expression (art. 80) BEUC welcomes the exemption from the application of the regulation when personal data is processed for journalistic purposes or for the purpose of artistic and literary expression. The notion of journalistic purposes should be clarified to include not only the traditional media, but also new activities whose object is the disclosure to the public of information, opinions or ideas.</p> <p>Processing of personal data concerning health (art. 81) The use of sensitive health data for marketing purposes should remain prohibited. Tracking and profiling technologies in health related web sites should not be allowed. Only authorised and specifically trained health care professionals should be allowed to have access to patients' health records.</p>
<p>Delegated and implementing acts</p>	<p>BEUC regrets that too many issues in the draft Regulation are left to be dealt with by delegated and implementing acts. The number of delegated and implementing acts should be cut down and limited to those provisions addressing non-essential issues, such as design requirements or criteria for technical measures.</p>

Introduction

The European Consumer Organisation (BEUC) welcomes the European Commission's proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). We agree with the general direction taken by the European Commission, acknowledging that while the objectives of Directive 95/46 remain relevant, a thorough review has become indispensable owing to the technological and social changes which have occurred in the digital environment.

Overall, the draft Regulation addresses the main challenges and the shortcomings of the current framework with the aim of enhancing the rights of data subjects and restoring control over the processing of their own personal data, especially in light of constantly evolving ICT developments. The European Union needs a consolidated, general framework which applies across the board and which can then be complemented by more specific rules as necessary.

The revision of the current framework also acknowledges the changes brought about by the Lisbon Treaty. In fact, both the European Charter of Fundamental Rights and the European Convention on Human Rights which recognise the fundamental rights to protection of personal data and privacy, will now need to be fully complied with by the EU institutions and Member States, acting within the scope of the EU law.

Although the proposal in general constitutes a major improvement for individuals, a number of provisions still need to be clarified or modified to ensure the new EU framework is effective and becomes the global standard of personal data protection and privacy.

The on-going revision should not result in the reduction of protection. BEUC wishes to highlight that the adoption of a user-centred approach and the placement of data subjects at the forefront of considerations constitutes a *sine qua non* requirement to achieve the objectives of the EU Digital Agenda, which aims to build consumer trust in the online environment. The revision should not be used as an opportunity to weaken fundamental principles of data protection.

Consequently, the forthcoming revision must not result in a lower level of protection which would jeopardise the fundamental rights of individuals, citizens and consumers. On the contrary, the review is an opportunity to provide effective protection of consumers' fundamental rights to the protection of their personal data and privacy as well as ensuring proper enforcement of the rules.

It must also be borne in mind that the European framework for data protection has been used as a global standard and has provided a basis for the development of legislation in other countries. The EU should therefore respond to the expectations of citizens and consumers in Europe and beyond.

CHAPTER I – GENERAL PROVISIONS

Article 2 – Material scope

Article 2 of the proposal defines the material scope of the regulation in the same terms as Directive 95/46: it applies to *“the processing of personal data wholly or partly by automated means or to the processing of non-automatic means of personal data which forms part or is tended to form part of a filing system.”*

However, the exceptions to the general scope are broader in the proposal than in the current Directive. While we do not oppose the exceptions, we assert that they must be better defined to avoid different interpretations and undue use of personal data in borderline cases.

With regard to the exception of **national security**, we would like to highlight that the scope of this notion often differs from one Member State to another, which will undermine the uniform application. Thus, we think that the Regulation should introduce certain criteria which better define the extent of this exception.

With regard to the exception of **personal and household activities**, we welcome the reference to the gainful interest as the main criterion for the application of the exception. The question of whether individuals processing data for personal and household activities is particularly important within a technological context, with individuals posting content online via social networking sites, blogging sites etc. We would however recommend including in Article 2 the elements of the definition of “gainful interest” provided in Recital 15, namely that the notion is linked to professional or commercial activity.

Furthermore, the draft Regulation does not clarify the application of the exception when data is made available to an indefinite number of individuals. According to the case law of the European Court of Justice¹, the exception should only apply when the data is made available to a limited number of individuals. We would therefore suggest that the exception of Article 2.2.d be complemented with the criterion of indefinite number of people, thus clarifying that an indefinite number of individuals shall in principle mean that the household exception no longer applies

Article 3 – Territorial scope

Article 3 deals with the territorial scope of the proposal, addressing when the data controller is established within or outside the European Union.

Article 3.1 introduces the criterion of **establishment in the EU** to determine whether EU law would apply. However, the definition of the establishment, as the place where the main decisions as to the purposes, conditions and means of processing are taken (Article 4.13) is not appropriate for undertakings with a decentralised decision making structure, such as where the locations of where central administration and management decisions on data processing differ.

¹ See ECJ 6 November 2003, Lindquist and Satamedia, C-101/0.

Furthermore, Article 3.1 only provides for the application of EU law without any criteria to determine which national law shall apply. In principle this is logical as the Regulation is supposed to be a self-standing instrument. However, the Regulation leaves some scope for the application of national law in some of its provisions and Member States maintain the freedom to adopt specific legislation in a limited number of areas. The draft Regulation only provides for criteria to define the leading Data Protection Authority (Article 51) where several Member States are concerned, but does not address the issue of applicable national law.

Article 3.2 refers to instances where the data controller is **not established in the EU**, but the processing activities are related to the offering of goods and services to data subjects residing in the EU or monitoring their behaviour. Compared to Article 3 of the current directive, this new provision takes away the criterion of “use of equipment”.

BEUC welcomes the new criteria that will ensure that consumers will be protected against the collection and processing of their personal data by companies not established in the EU; the current criterion of “equipment” has often turned out to be an obstacle to the enforcement of European law against such companies. In order to ensure more legal certainty, we believe that further clarification is needed to ensure that the offering of goods and services also includes so-called ‘free services’, which are based on monetising the secondary use of consumers’ data².

We would also suggest that the meaning of “monitoring of behaviour” is clarified to include tracking and profiling done by controllers outside the EU. For these provisions to deliver benefits to European consumers, effective enforcement mechanisms and procedures need to be in place.

Article 4 – Definitions

❖ Article 4.1- Definition of “data subject” (personal data)

Compared to the present Directive, the criteria in the new proposal for the definition of “personal data” are transferred to the definition of “data subject”. The main elements of the definitions remain in place, which BEUC welcomes. We believe the broad definition in the proposal provides the necessary flexibility to be applied to different situations and developments affecting the fundamental right of privacy and data protection in the light of rapid ICT developments³. It is equally important that the definition provides legal certainty as to when data is personal and the processing of which would be within the scope of the Regulation.

In particular, BEUC welcomes the fact that the new proposal widens the definition by including the concepts of online identifiers and location data. However, the proposed new definition contrasts with the wording of recital 24, according to which *“...identification numbers, location data, on line identifiers...need not necessarily be considered as personal data in all circumstances”*. This sentence undermines the

² Opinion 01/2012 on the data protection reform proposals by Article 29 Data Protection Working Party.

³ The proposal follows the recommendations of the opinion of the 29 Data Protection Working Party: Opinion 7/2007 of 20 June 2007.

aim of the new definition, which is to cover any information or means allowing the identification of a data subject. As soon as the information allows the data controller to identify an individual, the information should be deemed personal data.

BEUC thus proposes the last sentence of **recital 24** to be redrafted clarifying that **when there is a close relation between the information and an individual that singles out the individual**; this will trigger the application of data protection rules.

BEUC would caution against overstretching the application of data protection rules to every single situation where information is processed, but rather its application should depend on the **specific context** and on whether the information processed can be linked to a specific person.

❖ Article 4.8- Data subject's consent

The draft Regulation establishes the consent of data subjects as one of the possible grounds for legitimising data processing. Article 4.8 requires consent to be freely given, specific, informed and explicit, while Article 7 establishes a number of conditions for consent, including placing the burden of proof on the controller that the consent requirements have been met.

BEUC welcomes the provision in recital 25 that consent can be given by "any appropriate method", which allows for a certain degree of flexibility, provided it is transparent and meaningful. We also endorse the requirement that the request to give consent in the online environment should not disrupt use of the service and should not hinder the data subject's online experience.

BEUC recognises that there is no 'one size fits all' solution to the issue of consent, while the means of implementation of consent of consumers should be flexible and user-friendly. We believe that practices could be assessed against the following two criteria:

- An analysis of the potential consumer detriment linked to a specific practice/ technique.
- An evaluation of whether a practice/technique meets the 'reasonable expectations' of use of information by a typical consumer or by the average member of a group when directed to several consumers.

Such an assessment will have to be done on a case by case basis. The definition of consumer expectations raises a number of challenges both in terms of the process to be followed but also in terms of constantly emerging new services, especially in the digital environment. We believe consumer associations have significant experience of deploying surveys, analysing consumer behaviour, using appropriate tools to determine consumer expectations of products and services and so can be instrumental in any regulatory work in this field.

BEUC would suggest focusing on the requirement for **consent** to be **meaningful**, while it needs to be clearly stated that consent is only one of the legal grounds for processing and not necessarily the most appropriate one in all circumstances. For example, consent cannot be valid when the requirements of transparency and information have not been met, or when collection of personal data is unnecessary for consumers to access a specific service. Consent must not lead to further

processing of data which is otherwise unnecessary. Most importantly, compliance with the principles of data protection processing, including data minimisation and purpose limitation, needs to be ensured.

❖ Article 4.13- Main establishment

The main establishment is defined as the place where the main decisions as to the purposes, conditions and means of processing are taken. However, this definition is inappropriate for undertakings by a decentralised decision making structure, where the locations of central administration and management decisions about data processing may differ. For those cases, the main establishment of the group may be used as the determining factor, or alternatively the dominant influence of one establishment over the others.

❖ Article 4.20 (new)- Transfer of personal data

BEUC regrets that the draft proposal does not provide a definition of what is to be considered the transfer of personal data. The main questions arise in relation to the passing of data between companies in the same country and other types of exchanges on networks, such as servers of companies. In a number of Member States, such transfers are prohibited and therefore the omission of this rule from the draft Regulation would result in a significant decrease of consumer protection.

CHAPTER II – Principles

Chapter II of the proposal deals with the principles of data processing and adds specific requirements for the collection and processing of data related to minors and of sensitive data. BEUC welcomes that the general principles of data processing are maintained in the proposal while significant improvements are put forward, in particular as regards the principle of transparency.

Article 5 – Principles relating to personal data processing

BEUC welcomes the introduction of the **principle of transparency** in relation to the collection and processing of data. This reflects the stronger obligations put on the controller to inform data subjects (article 14 of the proposal) about the most relevant information regarding the processing, including the identify and the contact details of the controller, the purposes of the processing, the retention period, the existence of rights and the modalities to exercise them etc., as defined in Article 14.

Lacks of transparency and information are major deterrents to users asserting their rights. If they do not know how their data is being used, for what purpose and by whom, they will not be in a position to exercise and enforce their rights.

The proposal enhances the principle of **data minimisation** by giving it more visibility in a new paragraph(e). The strengthening of this principle is necessary in order to address the current trends of data harvesting and data mining used for profiling consumers and which involve large amounts of personal data being collected.

Many data controllers who are not in a contractual relationship with consumers retain data beyond the necessary time to perform the service. In the specific case of search engines, the Article 29 Working Party required search engine providers “to delete or irreversibly anonymise personal data once they no longer serve the specified and legitimate purpose they were collected for and be capable of justifying retention and the longevity of cookies deployed at all times”.

The principle of data minimisation also mirrors the new principles of privacy by design and privacy by default. According to these, data protection principles need to be embedded in privacy-sensitive technologies and services from the beginning of their development.

The principle of **purpose limitation** of data processing is of utmost importance in relation to the proliferation of business models which are construed on the basis of data sharing with third parties. The business models of many internet companies (e.g. some search engines, social networking sites...) are often incompatible with the principle of purpose limitation and the specification of use of personal data. Many companies collecting personal data transmit the data to third parties who process this data for purposes different to those initially pursued by the data controller and often without informing the data subject.

BEUC **regrets** that the concept of “compatibility” (with the original purpose of processing) is undefined in the proposal. The criterion of “compatibility” has brought about divergences at national level due to its vagueness (without specification of what is compatible or incompatible). In a few countries the principle is defined in excessively broad terms undermining the very principle. In this regard, we think that the new regulation should include some criteria as to what is considered “compatible”, drawing on best practices of the way “compatibility” has been interpreted at national level.

Article 6 – Lawfulness of processing

Article 6 of the proposal reproduces the grounds for processing present in the current Directive. The processing of personal data is lawful when at least one of the following applies:

- a) The data subject has given its consent to the processing,
- b) Processing is necessary for the performance of a contract,
- c) Processing is necessary for compliance with a legal obligation,
- d) Processing is necessary to protect the vital interests of the data subject,
- e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of a public authority vested on the controller,
- f) Processing is necessary for the purposes of the legitimate interest of the data controller unless such interest contrasts with the fundamental rights and freedoms of the data subject.

Compared to the existing directive, the proposal contains a few, but very important, novelties. The most welcome changes relate to the definition and the conditions for “consent” (Article 7) as well as the provision on the processing of personal data of a child (Article 8).

When processing is based either on controller's compliance with a legal obligation or on the public interest, the basis for the processing will have to be provided either in EU law or the national law of a Member State (Article 6.3). This provision is very important as it excludes the law of a non-EU country as the legal basis, as would be the case where processing of personal data of EU residents may be required for law enforcement purposes by third countries.

BEUC is concerned that unless properly defined, the general notion of "**legitimate interests** of the controller" might open the door to abusive processing. The concept of legitimate purposes is vague and subjective. This concept should be defined clearly in the proposal and should not be left to a delegated act, as there is a risk of surpassing the legal grounds.

Article 7 – Conditions for consent

The draft Regulation establishes data subject's consent as one of the possible grounds for legitimising data processing. Article 7 establishes a number of conditions for consent, including the burden of proof on the controller to demonstrate that the consent requirements have been met.

BEUC welcomes the provision in recital 25 that consent can be given by any appropriate method, which allows for a certain degree of flexibility, as well as the provision that the request to give consent in the online environment should not be disruptive to the use of the service and should not hinder the data subject's online experience of the service. As stated above, there is no 'one size fits all' solution to the issue of consent, while the means of implementation of consent should be flexible, user-friendly and ensure it is meaningful when it is given.

We are satisfied that Article 7 puts the burden of proof of the consent on the controller. Thus the controller should pay special attention to the reliability of the means used to obtain consent of the data subject in accordance with recital 25. We also welcome the inclusion of the right to withdraw consent at any time.

However, for consent to be valid, the conditions of informed, specific and free will have to be met. The draft regulation provides examples of cases where consent cannot be valid due to a lack of balance between the parties, for instance in the employment sector. We highlight however that the lack of balance is present also in other sectors such as the insurance sector – where often the benefit of special conditions is tied to the consent of the consumer to the processing of his/her data; recital 34 should thus add the insurance sector as an example of possible lack of balance. As regards the "informed" consent, the data subject should receive clear and understandable information (in a concise manner) on key elements which are defined in Article 14.

We are also concerned that under the proposal, the consumer may be requested to provide consent once that would cover multiple data processing operations. It is questionable whether the consumer is able to deduce the consequences and understand the implications.

Article 8 - Processing of the personal data of a child

BEUC welcomes the new provision in Article 8 requiring parental consent for the processing of personal data of a child.

In particular in the online environment minors do not always have the knowledge to realise the consequences of the collection or processing of their personal data. The internet and new technologies offer ever wider possibilities for children to share data (photos, videos, messages, localisation information through blogs, videos, social networks...) which, combined with the lack of awareness of the risks and dangers of data collecting, make children and teenagers the most vulnerable group in the digital world.

However, we see a number of problems regarding the implementation of the obligation of parental consent. First, the threshold of 13 years old might conflict with national laws relating to the legal capacity to conclude a contract, the processing of data occurring very often in the context of a contractual relationship. Second, the obligation to develop means to verify the legitimacy of parental consent, should not lead to further processing of data which otherwise would not be necessary to process. We also think that the criteria and modalities for the parental consent should not be totally left to delegated acts of the Commission; some criteria should be included in the regulation itself.

In addition this provision seems to apply only in the context of the “offering of information society services”. The meaning of offering information society services seems to be too restrictive and it should be clarified; the provision should apply to any processing of personal data of a child both on and off-line.

Article 9 - Processing of special categories of personal data

We welcome the prohibition of the collection or processing of sensitive data as referred to in Article 9.1 of the proposal. BEUC believes that the list of sensitive personal data must be exhaustive to ensure legal certainty and avoid divergent implementation at national level. However, we put forward that financial data which reveals personal solvency should also be added to the list of Article 9.2 Other forms of financial data such as unpaid debts of clients to the company with which it is or has been in a contractual relationship would not make part of this category.

Finally, we believe that the specificities, conditions and safeguards for the processing of sensitive data should not be left to delegated acts of the Commission; sensitive data requires an additional layer of protection and thus the conditions for their processing need to be clarified in the regulation. Alternatively, this could be the object of opinions or reports of the European Data Protection Board.

CHAPTER III – Rights of the data subject

Article 11 – Transparent information and communication

Lack of transparency and lack of clear information is a major deterrent to users in the assertion of their rights. Consumers rarely understand privacy notices which are generally too lengthy. The privacy policies of many online service providers include complex and legal terms which fail to comply with the principles of transparency and fairness, aiming exclusively at complying with legal requirements rather than informing consumers. They are often obscure on issues where clear explanations matter the most, for instance on the question of whether data is shared with or sold to third parties, who these third parties are and what they intend to do with the data, the use of cookies and other data collecting technologies and data retention limits. Privacy policies are not always easy to spot on websites, while they may not be updated once they are published, even when the content and the nature of the service have evolved.

According to different surveys, although consumers are concerned about their privacy, they do not view privacy policies as a suitable way to understand and answer their privacy concerns. These findings are confirmed by behavioural economics considerations, which show that consumers do not read privacy notices and are prone to accept default settings.

According to the figures provided by the Eurobarometer⁴ 64% of users feel that information on the processing of their data is unsatisfactory. According to a study by the Norwegian Consumer Council⁵, 73% of users aged 15-30 years seldom read Terms of privacy notices while the research carried out by Which? in March 2010 found that only 6% adults aged 16+ with internet access questioned have read the privacy policies of websites

The proposal significantly strengthens the information obligations of the controller to the data subject (Articles 11, 12 and 13). We in particular welcome the new requirement that information has to be provided in an intelligible form while using clear and plain language. We also support the regulation of procedures for providing the information to the data subjects as this will strengthen accountability of the controller *vis-à-vis* the data subject.

⁴ Eurobarometer survey on data protection in the EU - citizens' perceptions, February 2008.

⁵ <http://www.sintef.no/upload/Konsern/Media/Person%20og%20forbrukervern.pdf> .

Article 12 – Procedures and mechanisms for exercising the rights of the data subject

BEUC welcomes the introduction of specific modalities for the exercise of the rights of the data subject. Data controllers should respond to requests by data subjects without undue delay and no later than one month. Furthermore, data controllers should not be able to charge a data subject for access to his own personal data, as long as this right is not abused. As regards the right to correct, erase and delete data, it should always remain free of charge, as it is also to the benefit of the data controller to have correct and updated data.

Article 13 – Rights in relation to recipients

BEUC welcomes the introduction of an obligation for the data controller to notify each recipient to whom data has been disclosed in case of rectification or erasure, as long as it is possible without a disproportionate effort. This provision is particularly important in the online environment, where data can be easily shared with third parties and therefore inaccuracies need to be corrected. However, we are concerned as regards the exception in cases where such communication would involve a disproportionate effort (Article 13.5.c). Such a broad and subjective condition cannot be justified, as it will always be the case that providing information might require an effort by the data controller.

Article 14 - Information to the data subject

Article 14 sets up a list of all the information the data controller is obliged to give to the data subject when his personal data has been collected. Overall this provision is comprehensive and encompasses the relevant information the data subject needs to have. However, information about the type of personal data collected and processed is currently missing from the list and should be added.

We particularly welcome the new obligation of the data controller to inform the data subject of his right to lodge a complaint to the supervisory authority and the contact details, reflecting the new right of the data subject to directly lodge complaints (Article 15.1 [f]). However, data subjects also need to know about the procedures to lodge such complaints; this should be added to the text - often consumers are not aware of the procedural steps to lodge complaints.

In addition, this provision should echo the inclusion of a specific article dealing with profiling (Article 20) by requiring information about tracking and profiling purposes and its consequences on individuals to be added under Article 14.1 b.

Regarding the exceptions to the information obligations listed in Article 14.5, we think that the exception in Article 14.5b (when the information to the data subject proves impossible or carries a disproportionate effort) should be better defined in the regulation, instead of letting the Commission adopt delegated acts to specify such exception. The provision of information will always require an effort from the data controller, which he may claim is disproportionate.

It is equally important to inform the data subject which personal data is obligatory to provide and which is voluntary. As regards services whose business model is based on monetising the use of consumers' personal data in exchange for so-called 'free services', it should be made crystal clear to the consumer that this exchange is taking place, while the processing of data should comply with the general principles of data minimisation, purpose limitation etc.

We support the reference to standard forms to lay out the information provided to the data subject, but we think this should be a requisite rather than optional. Standard forms generally offer better and more structured information to consumers. We also think that the new European Data Protection Board (EDPB) should take the lead in developing such standard privacy notices alongside consumer representatives and businesses.

Finally, the possibility for data controllers to present the information by using multi-layered notices should be expressly allowed.

Article 15 - Right of access for the data subject

Article 15 includes a list of information obligations in relation to the right of the data subject to access at any time the processed data. Compared to the current Directive, the addition of the obligation to inform about the right to lodge a complaint with the supervisory authority and its contact details (15.1 (f)) is very welcome. Yet, as said above, data subjects should also be informed about the procedures to lodge complaints. Consumers cannot fully benefit from their rights if they are not informed about the ways to complain and to obtain redress where there have been infringements.

Article 17 - Right to be forgotten and to erasure

The digital print left by individuals when personal data is processed online is problematic for consumers; consumers may well wish to erase the traces they leave behind on the Web at one point in time. The consumer should be able to delete the information provided to a company when the data is no longer necessary or when he withdraws consent.

BEUC supports the intention of the 'right to be forgotten' which aims to strengthen the right to erase personal data. Even though the right of erasure is included in the current directive, its application in the online environment is very often ignored.

The new Article 17 should allow better enforcement of the existing right of erasure in the digital environment. Indeed, according to the new proposal the controller will be held liable in case he has made the personal data public or has authorised the processing of the data by third parties.

Users have the right to expect online companies to delete their personal information upon request. For example, users of social network services, email services, and other similar services should not worry that companies will retain their information after they are no longer users of the service. With respect to search companies, users might also reasonably expect that personal information, acquired by the company for commercial gain, should not be republished where the user has made an explicit request.

However, we consider the naming (“forgotten”) to be misleading as the limitations of a “right to be forgotten” are manifold and have to be acknowledged. It should be made clear that the obligation to delete the consumer’s data lies upon the controller of the information and not the downstream parties (host providers, search engines etc.), in order to ensure compatibility with the provisions on the liability of Internet Service Providers under the Directive on e-Commerce. The implementation and enforcement of the right to be forgotten must not result in the application of technical measures resulting in the filtering of online communications. The relationship with the provisions of the e-Commerce Directive on the liability of information service providers needs to be carefully assessed.

Moreover, in many cases it would be impossible to inform all parties to whom data has been disclosed and track down all possible links and copies of data. In this regard, Article 17.2 should be understood in the sense that only an obligation of effort is imposed on the controller and not an obligation of result. To this end, different metadata techniques which could convey the information regarding the appropriate use of the data could be used.

Finally, the requirements, conditions and criteria for the implementation of the right to be forgotten should not be left to delegated acts of the Commission but should be defined in the regulation.

Article 18 - Right to data portability

BEUC very much welcomes the introduction of the new right to data portability in the proposal (Article 18). In the online environment, consumers store huge amounts of information (e.g. social networks, e-mail services...). At present, consumers are too often ‘locked-in’ to online services and platforms with no possibility of transferring this data onto other (competing) platforms. Existing terms and services appear to be mostly unfair in this regard: often service providers claim ownership of the data stored in their services.

This situation is incompatible with the right of consumers to be in control of their data and to object to the processing of their data. It also hinders competition among service providers and prevents switching. The right to data portability allows the consumer to be in control of his data and retain the ownership, by being able to shift the data to other services.

The relationship between the right to data portability and the right of erasure should be better clarified in the proposal. It should be clearly established that the right to data portability implies erasure of the data by the original service provider (the use of the word “copy” in Article 18.1 seems to imply that the original service provider can retain the data and only give away a copy). In any case the data controller is always obliged to delete the data when they are no longer necessary for the purpose for which they were processed (Article 5 [e]).

However, effective implementation of the right to data portability necessitates the development of interoperable or compatible standards.

Article 19 – Right to object

Article 19 of the proposal establishes the data subject’s right to object to the processing of their data, unless the controller demonstrates compelling legitimate grounds for the processing. This is a significant improvement from the current situation, where the data subject only has a right to prevent processing where they can demonstrate damage is caused. According to Article 19, the data subject will have a default right to object to processing and it will be for the data controller to demonstrate why the objection is invalid and to justify the processing.

This provision however, does not make clear the consequences of the right to object in the relation to the data at stake. It should be clarified that the right to object, if upheld by the controller should result in the deletion of the data by the controller.

Moreover, the notion of “compelling legitimate grounds” which (despite the objection) could legitimise the process, should be clearly defined in the Regulation.

Article 20 - Measures based on profiling

Article 20 addresses the processing of personal data for the purposes of profiling individuals according to their personal aspects, preferences and behaviour. Advertising business models which use the profiles of individuals are proliferating and consumers are often unaware of these practices or the consequences in the economic decisions they take. Consumers have almost no control over the current complex “media and marketing ecosystem”.

Therefore, BEUC welcomes the specific inclusion of profiling practices in the proposed regulation. BEUC is not opposed to the online profiling of consumers in principle. According to this logic, the draft Regulation does not prohibit profiling, but rather gives the consumer the right to object to profiling.

However, in order to ensure legal certainty it must be clarified what is meant by “legal effects” and “significantly affects”. Moreover, the right to object should be accompanied by the right to be informed about the techniques and procedures used for profiling in the advertising ecosystem; this obligation already exists in the current Directive and it should be reintroduced in the proposal. Equally, consumers should be informed of the possible consequences of profiling techniques applied to them.

The draft proposal should also prohibit profiling of vulnerable consumers such as children as those consumers often lack critical judgment and understanding of marketing techniques; those techniques could have a negative impact on children and young people's development.

Regarding paragraph 5, we do not support the reliance on delegated acts to specify the safeguards to protect consumers' legitimate interests in case of profiling. On the contrary, the safeguarding measures should be defined in the Regulation.

Article 21 - Restrictions

Article 21 of the proposal introduces a number of possible restrictions to the rights of data subjects. We note that this Article is much wider than the corresponding Article in the current Directive (Article 13). Contrary to the current Directive, the new Article 21 can be used to limit almost all the rights of the data subject (including the principles of processing, the right to object, measures based on profiling and the right to be notified of a data breach).

We believe that Article 21 should include certain guarantees in relation to the purposes, proportionality, necessity, categories of data processed and the persons authorised to do so. There is a need for more clarity on the specific guarantees that the law allowing such restrictions should establish in order to safeguard the legitimate interests of the data subject.

Under the current wording, Article 21 contains vague, undefined terms, such as "economic and financial interest", "monetary, budgetary and taxation matters" and even "market stability and integrity", the latter phrase having been added to Directive 95/46 without any further precision.

CHAPTER IV – Controller and processor

Article 22- Responsibility of the controller

The draft Regulation introduces the principle of accountability, according to which the data controller must put in place measures and control systems which ensure compliance and provide evidence to demonstrate compliance to external stakeholders, including supervisory authorities.

Article 22 introduces a general obligation for the controller to implement appropriate measures and demonstrate compliance, while the following Articles of Chapter IV introduce further elements of accountability, including the carrying out of Data Protection Impact Assessments, the appointment of Data Protection Officers, the implementation of Data Protection by Design and by Default and the obligation to notify data breaches.

BEUC welcomes the new provisions enhancing controller's responsibilities which will help create a privacy and data protection culture within companies. They will also allow controllers to adopt the measures most appropriate for the nature of their processing operations, thus providing a high degree of flexibility as required by fast-evolving technology.

In addition to the requirement to demonstrate compliance to the DPA, it is equally important the controller demonstrates compliance to the public in general by means of an annual report describing the measures adopted.

The principle of accountability should not be perceived as an alternative to compliance with legal obligations or as an excuse to avoid administrative sanctions. The right to the protection of personal data is a fundamental right in Europe and its effective protection should not depend solely on the willingness of a company.

Strong enforcement and dissuasive sanctions are required when companies fail to comply with the law. It is however important to ensure that monetary fines do not become an objective per se in order to ensure the funding of DPAs, but should be proportionate to the infringement. When considering fines, the infringer should be given the opportunity to correct its behaviour.

Article 23 – Data protection by design and by default

BEUC welcomes the introduction of the principles of data protection by design and by default in the draft Regulation, making it compulsory for data controllers to implement appropriate measures to comply with them. These two principles will help empower data subjects' control and enhance enforcement of data protection legislation.

Article 23.1 establishes the principle of **data protection by design**, which would require privacy and data protection to be embedded within the entire life cycle of the technology, from the very early design stage, right through to their ultimate deployment, use and ultimate disposal. BEUC welcomes flexibility provided to data controllers to comply with the general principles. BEUC would also welcome the inclusion of a reference to the use of Privacy Enhancing Technologies (PETs) as a tool to implement technical solutions to comply with the principle of data protection by design.

As regards the principle of **data protection by default**, BEUC believes that Article 23.2 should be revised to make it explicit that the privacy settings on services and products should by default comply with the general principles of data protection, such as data minimisation and purpose limitation. The data subject should have the choice to change the privacy settings and decide whether he wants to share his personal data and with whom. Privacy settings are an important aspect of online privacy. Consumers expect companies to create privacy settings that provide transparency and control over the ways in which organisations collect, use, and store personal information.

BEUC is also concerned that Article 23 only addresses the data controller. However, the processor should also be obliged to implement privacy by design and privacy by default while processing personal data on behalf of the controller. Such a requirement should be added in Article 26 which defines the obligations for data processors.

Article 24-Joint controllers

BEUC welcomes the provision on joint controllers (Article 24) and the introduction of an obligation to define their respective responsibilities for compliance with the obligations by means of an arrangement between them, while failure to comply with this obligation will entail administrative sanctions according to Article 79.5.e.

In practice, the chain of responsibility and liability is getting difficult to follow for data subjects not only as regards data controllers, but also controllers and processors (e.g. cloud computing), let alone that the distinction between data controller(s), data processor(s) and third parties is not obvious to the consumer. Although Article 26 requires the controller to define the respective responsibilities with data processor processing data on their behalf, BEUC recommends including a specific provision on joint responsibility between the controller and the processor, allowing the data subject to seek redress from each of them.

Article 25- representatives of controllers not established in the Union

BEUC welcomes the requirement for controllers not established within the EU to designate a representative to the Union. The representative is expected to be the contact point for both data protection authorities and the data subject. However, the broad exceptions to this obligation, including when the controller employs less than 250 employees cannot be justified. The exceptions must be fully justified or otherwise deleted.

Article 28- Documentation

Article 28 introduces the obligation for controllers and processors to maintain documentation of the processing operations instead of the cumbersome requirement for notification of the data controllers' personal data handling practices. Under the new Framework, data controllers should document any processing operation and be able to demonstrate compliance upon request to the Data Protection Authorities.

The documentation obligation, as defined in Article 28.2, includes the most relevant information and should not be simplified. The contact details of the controller and of the data protection officers, the types of personal data, the recipients of personal data, the purposes for processing, possible transfers to third countries and retention periods are the minimum information that any responsible and accountable organisation needs to keep records of. It will also make the checking by Data Protection Authorities easier and help improve monitoring of compliance and enforcement.

However, in order to comply with their obligations under Article 22, data controllers will in any case be able to demonstrate compliance with the legislation and the effectiveness of the undertaken measures. We would therefore support the proposal put forward by the European Data Protection Supervisor⁶, to introduce an obligation to keep an inventory of all processing operations that would encompass general information, namely the contact details of the controllers (and joint controllers and processors if applicable), the contact details of the data protection officer and the description of the mechanisms implemented to ensure the verification of the measures undertaken in order to ensure compliance. More specific information should be part of an additional obligation to inform data protection authorities upon request.

As regards the exception from the documentation obligation for organisations with less than 250 employees, BEUC would suggest its deletion or its replacement with a criterion based on the nature of the processing activities, the number of personal data involved and the number of data subjects the enterprise processes data on. The exception should only apply to those entities that are processing data as an accessory activity.

Article 31-32- Notification of a personal data breach authority

BEUC welcomes the introduction of a horizontal data breach notification obligation for the controller, beyond the telecommunications sector. Consumers may suffer at least the same harm from the undue disclosure of their bank account details as from the disclosure of their telephone bills.

Individuals have the right to be informed about the use of their personal data, including when their data has been compromised. According to the research carried out by our UK member organisation Which?, the vast majority of UK consumers (74%) would always wish to be notified of a data breach.

The draft Regulation introduces a dual system of notification, according to which all breaches must be notified to the Data Protection Authorities (Article 31), while only those breaches that adversely affect the protection of personal data and privacy should be notified to the individuals (Article 32).

BEUC agrees that only those breaches that adversely affect the individual should be notified to data subjects. A general obligation to notify individuals whenever personal data has been compromised might be counter-productive and lead to “notification fatigue” and de-sensitisation.

⁶ Opinion of the European Data Protection Supervisor on the data protection reform package, 7 March 2012.

However, the definition of what constitutes a breach of adverse effect is only partly provided in Recital 67. In order to ensure legal certainty and a consistent approach across Europe, BEUC would suggest including the definition in Article 32. Such a definition should be broad and encompass not only those breaches which result in economic loss, but also breaches which may cause immaterial damages, such as any moral and reputational damages. Additional criteria, such as time spent in attempts to rectify the breach and distress should also be considered when assessing the adverse effect.

BEUC supports a risk-based definition of the adverse effect of data breaches. In order to determine the level of risk, both quantitative and qualitative indicators need to be considered. For example, the type of data, the number of individuals affected and the amount of data breached would have to be considered.

As regards the content of the notification, the requirements set in Article 32.2 should also comprise a description of the consequences of the personal data breach (Article 31.3[d]); in addition, the individual should be informed about their rights and be provided with the contact details of the Data Protection Authority and consumer associations who can help them seek redress.

BEUC also suggests including a specific requirement for the notification to be clear and comprehensive, i.e. without technical jargon. It should be sufficient for the individual to read the notice in order to understand the risks and recommended actions.

BEUC regrets the fact that only the data controller is required to notify breaches. This obligation should also cover breaches occurring while personal data is being processed by the data processor. In this case, the data controller should bear the responsibility to notify.

As regards the notification to the data protection authorities, BEUC believes that the notification must take place as soon as possible, without undue delay and not beyond 72 hours after the controller becomes aware of the data breach.

We would also suggest that a specific deadline is introduced for the DPA to act on a breach notification, as well as a deadline within which the data controller should notify the breach to the data subject.

Articles 33-34 – Data Protection Impact Assessment and prior authorisation

BEUC welcomes the introduction in the EU Data Protection framework of an obligation for the controller and the processor to carry out an assessment of the impact on the protection of personal data of the processing operations that present specific risks. The implementation of meaningful PIAs complying with high privacy standards also figures in the Madrid Privacy Declaration adopted by the International Conference of Privacy and Data Protection Commissioners in November 2009.

A robust framework of Data Protection Impact Assessments can be an effective tool to address the challenges of a fast evolving ICT sector and help identify the risks to consumers' fundamental rights to privacy and to protection of personal data at an early stage. As such, a DPIA is an integral part of the privacy by design principle. It also enables data controllers and processors to demonstrate compliance with the requirements of the Regulation.

A DPIA should also be carried out when processing operations "are likely" to present specific risks to the rights and freedoms of data subjects⁷

We are also concerned with the limitation of processing operations to processing on a large scale when information about the sex life, health, race and ethnic origin or for the provision of healthcare etc. (Article 33.2.[b]). This type of information is sensitive personal data and therefore a PIA should be mandatory irrespective of the scale of processing.

BEUC also suggests introducing in Article 30 a specific requirement for the DPIA to be made publicly available, or at least a summary of it. It should be for the national Data Protection Authorities to maintain a registry of PIAs, similar to the system in the District of Columbia in Canada⁸. This would allow individuals to consult the PIAs and increase their confidence in handling of their personal data. It goes without saying that the PIAs or their summaries should be published in a reader-friendly format.

BEUC would support the audit of DPIAs by the Data Protection Authorities to ensure it fulfils the conditions set out in the Regulation. This would increase the reliability of DPIAs and would also facilitate the establishment of a central registry open to consultation by all stakeholders.

Articles 35-37- Data Protection Officer

BEUC welcomes the introduction of the obligation for both controller and processor to appoint a Data Protection Officer (DPO) within the framework of the accountability principle. DPOs are familiar with the problems and the processing activities of the entity they work for and can therefore provide valuable advice as to implementation of the Regulation and monitor compliance. It is also expected that the appointment of a DPO will help increase awareness of data protection rules within the entity; according to a Eurobarometer (2008) survey, only 13% of people responsible for data protection within companies said that they were very familiar with the provisions of data protection law⁹.

⁷ This will also align the wording of Article 33.1 with the wording in Articles 34.2(a) and 33.6.

⁸ PIAF, Privacy Impact Assessment Framework for data protection and privacy rights, Deliverable 1 http://www.piafproject.eu/ref/PIAF_D1_21_Sept2011Revlogo.pdf

⁹ Eurobarometer survey on data protection in the EU, February 2008.

The appointment of a DPO should be mandatory, except for those entities processing personal data as an accessory activity. The proposed threshold of 250 employees for requiring the designation is unjustified, given that all Small and Medium Enterprises would escape this obligation. BEUC counters that the determining factor should not be the number of employees, but the nature of the processing activities, the volume and the type of personal data involved and the number of data subjects the enterprise processes the data of.

DPOs must have expert knowledge of data protection law and sufficient experience to carry out the assigned tasks. Given their special role, there must be mechanisms in place to check and verify the qualification of DPAs. This will also be to the benefit of data controllers, who risk administrative sanctions for failing to appoint a DPO or for not respecting the conditions for its appointment, according to Article 79.6.[j]. DPAs could also organise regular training seminars for appointed DPOs.

The draft Regulation requires DPOs to be independent from the data controller or processor. However, in practice there will most often be an employment relationship between the two parties. Therefore, BEUC would suggest further strengthening the independence of DPOs by requiring the controller or processor to submit a fully justified report to a DPA in instances of the dismissal of a DPO (Article 35.7). In addition, in instances of disagreement between the DPO and the controller or processor, or doubt as to compliance with rules, it should be for the supervisory DPA to provide guidance.

Articles 38-39– Codes of conduct and certification

BEUC is concerned by the encouragement of codes of conduct to be developed by controllers and processors. Self-regulatory codes can only be endorsed if they entail an added value for consumers' rights by offering a higher level of protection, are backed up by suitably robust auditing or testing procedures and provide for independent complaint handling and enforcement mechanisms.

However, Article 38 does not address these concerns. On the contrary, it only provides for the possibility for industry associations to submit the draft codes to supervisory authorities, which can only issue a non-binding opinion. Furthermore, the draft Regulation is rather weak when it comes to complaint handling mechanisms, the development of which is left exclusively to data controllers and processors. Similar inter-company complaint handling schemes should by no means be recognised as out of court dispute resolution procedures as they lack independence.

The development of EU certification schemes and privacy seals could become an effective means of ensuring 'privacy compliant' or even 'privacy enhancing' IT products, websites, companies and services. It will also provide an incentive for developers and providers of such products and services to invest in better privacy protection, while allowing users to make an informed and quicker choice. However, it is important to clarify that the granting of a seal would not simply certify compliance with the law, but provide an added layer of protection.

BEUC supports the establishment of EU certification schemes, including European Privacy Seals, as long as clear certification criteria are developed and the administration is entrusted to independent third party organisations. The establishment of a Certification Authority for the issuing of the seals and the accreditation of specially trained and tested independent experts, who carry out the primary evaluation of the products provide for additional safeguards.

It is therefore regrettable that the Commission has reserved the right to specify by way of delegated acts the criteria and requirements, including the conditions for granting and withdrawal. It would be preferable if more substantive rules are included in Article 39 to ensure legal certainty.

CHAPTER V – Transfer of personal data to third countries or international organisations (Articles 40-45)

As more and more processing operations take place in a global context, it is important to adapt the EU framework with the aim of ensuring the free flow of data, while guaranteeing the level of protection for data subjects' rights. The draft Regulation recognises the new reality and abandons the presumption that personal data may not be transferred without an adequacy level of protection, setting instead a number of principles which must be fulfilled when personal data is transferred outside the EU.

BEUC welcomes the inclusion among the factors to be considered when assessing the **adequacy** of , elements related to the rule of law, the existence of effective and enforceable rights as well as means of redress for data subjects (Article 41.2.[a]). It is also positive that the adequacy recognition will also depend on the international commitments of the third country, which would also include ratification of the Council of Europe Convention.

In the absence of an adequacy decision, the draft Regulation allows for the transfer of data provided that the controller and/or the processor have adduced appropriate safeguards in a legally binding instrument. Such safeguards will be provided by Binding Corporate Rules (BCRs), standard data protection clauses approved by the Commission or adopted by a DPA.

BEUC regrets that the proposal opens the possibility for transfer when safeguards are not provided in a legally binding instrument (Article 42.5), which might urge controllers to adopt codes of conduct. A similar derogation cannot be justified and therefore it should either be deleted or limited to a few specific cases.

Transfers should not be possible for those countries for which the European Commission has already adopted a decision not recognising the adequacy of their status.

Binding Corporate Rules have already been endorsed by the Article 29 Data Protection Working Party and therefore their explicit recognition as an adequate mechanism for transfer of data to third countries in Article 43 is welcome. It is important that BCRs are binding and enforceable upon all members of the controller and processor's undertakings and that implementation will require approval by the supervisory authority.

BEUC is concerned with the broad scope of Article 44 on **derogations**. It should be made explicit that derogations can only apply to a restricted number of cases of occasional transfer that cannot be qualified as frequent, massive or structural, as pointed out by Article 29 Data Protection Working Party¹⁰ and the European Data Protection Supervisor.

Furthermore, the consent of the data subject can be used as derogation to the rules on international transfers. As already outlined, it is questionable whether the data subject has the sufficient knowledge to fully assess the implications of any transfer of their personal data to a third country without an adequate level of protection and with no safeguards from the controller. Article 44.1 should therefore be deleted.

We are also concerned with the broad definition of the "public interest" which would also cover the transfer of personal data to third countries for the prevention, investigation, detection and prosecution of criminal offences (Recital 87). A similar provision would increase the risk of abusive transfers to law enforcement authorities without any safeguard for the protection of data subjects' fundamental rights.

As regards **international cooperation** on the protection of personal data, Article 45 aims for enhanced cooperation between data protection authorities in **enforcing the law**. Although such cooperation is crucial, we are concerned by the role envisaged for stakeholders in enforcing the law. Such a provision relates to the recently announced Consumer Privacy Bill of Rights in the USA which foresees the development of codes of conduct as a tool to enforce the law. BEUC is concerned that such schemes of self and/or co-regulation fail to provide a robust enforcement system.

Lastly, BEUC regrets the deletion during the inter-service consultation of a provision that would have prohibited the transfer of personal data based on **orders or requests from non-EU courts, tribunals, administrative authorities and other governmental entities**. It stated that in cases where a third country requests the disclosure of personal data, the controller or processor had to obtain prior authorisation for the transfer from its local supervisory authority. This provision is particularly relevant with regards to requirements under US law for the disclosure of data, in particular based on law enforcement requirements or e-discovery requests. The US uses instruments such as the Foreign Intelligence Surveillance Act (FISA) and the Patriot Act to retrieve data on the political activities of foreign individuals who may have no links whatsoever to the USA, via companies with US offices. We would suggest that this provision is added in a separate, new Article.

¹⁰ Working document of the Article 29 Working Party of 26 November 2005 on a common interpretation of Article 26.1 of Directive 95/46 of 24 October 1995 (WP114).

CHAPTER VI – Independent Supervisory Authorities (Articles 46-54)

BEUC welcomes the provisions of the draft Regulation which establish explicitly the **independent** status of Data Protection Authorities in order to ensure the effectiveness and reliability of the supervision of compliance with the legal framework.

However, we regret the absence of specific standards for the **funding** of the operations of Data Protection Authorities. Article 47.5 only calls upon Member States to ensure that DPAs are provided with adequate human, technical and financial resources¹¹. Adequate funding is a key element to ensure the independence of DPAs. Such funding should be proportionate to the number of data controllers DPAs regulate and the individuals whose personal data is processed.

We therefore suggest that specific provisions are added in Article 47 which would outline complementary sources of funding for DPAs. In its document 'The future of privacy', the Article 29 Data Protection Working Party suggested alternative sources of **funding**, which may range from a fully fee-based model (based e.g. on notification fees and the levying of fines for breaches of the law) to a fully state-funded model¹². We would also like to underline that, in many cases, DPAs may be reluctant to impose sanctions against companies due to the increased costs of counter-litigation if companies challenge the sanctions imposed. This may undermine the capacity of DPAs to undertake action.

As regards the provisions on the competence of DPAs and the introduction of a "**one stop shop**" for data controllers or processors, BEUC is concerned that **Article 51** might result in **forum shopping**. It should be made explicit that the powers of the lead authority are not exclusive and that coordination between all relevant DPAs is ensured. Otherwise, there is a significant risk that the data controller will decide to establish itself in those Member States with less stringent rules, as a degree of flexibility on the applicable law would still be left to Member States.

There should also be a clear definition of the main establishment. As previously stressed, the definition provided in Article 4 is inappropriate for undertakings with a decentralised decision making structure, where the central administration and location of management decisions about data processing differ. It would be more appropriate to introduce a number of specific factors/criteria needed to be considered to assess the lead authority, such as the number of data subjects whose personal data is affected.

¹¹ See also Article 29 Data Protection Working Party letter to Vice-President Reding.

http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2012/20120404_letter_to_vp_reding_resources_en.pdf

¹²http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/others/2011_01_14_letter_artwp_vp_reding_commission_communication_approach_dp_en.pdf.

Furthermore, the rules on the lead authority will only apply where the controller has an establishment in the European Union. **Article 51 does not cover those cases where there is no establishment in the EU**, in cases where the processing activities are related to the offering of goods and services to data subjects residing in the Union or the monitoring of their behaviour. Given that similar processing activities may easily affect data subjects in multiple EU Member States, specific rules on the assignment of a lead authority should also be defined. BEUC believes the lead authority should be that of the Member State where most data subjects have been affected, or the Member State where a specific complaint has been lodged.

A key issue which is left unaddressed in the draft proposal is who should be responsible for the appointment of the lead authority (the authority or the controller) and how disputes regarding appointment of the lead authority are to be solved.

Article 52 provides for the duties of supervisory authorities, including the power to hear **complaints lodged by data subjects** (52.1.[b]). Given that the lead authority might be different from the one of the residence of the data subject, a number of practical problems need to be solved, including who bears the costs for translation and/or interpretation. These should not be borne by the data subject, as it would be a major obstacle to the exercise of his fundamental right to redress.

CHAPTER VII – Cooperation and consistency (Articles 55-72)

BEUC welcomes the focus of the draft Regulation on enhancing **cooperation and coordination** between Data Protection Authorities. Article 56 empowers DPAs to undertake joint operations, including joint investigations and joint enforcement measures. Article 55.2 introduces the duty to take action upon request of another DPA within one month. Failing to comply with this duty, the DPAs may take provisional enforcement or compliance actions in another Member State. Nevertheless, we are concerned about the nature and the scope of similar measures since it might raise problems of interference with national procedural and constitutional law.

Strengthening the cooperation between DPAs is crucial, given that a data breach may well affect data subjects across Europe and beyond. However, this should not be the only mechanism for ensuring cross-border enforcement of data protection laws. To this end, the experience with the Consumer Protection Cooperation Regulation needs to be assessed. A number of interesting conclusions can be derived from the most recent report on the implementation of the CPC Regulation published in March 2012. Despite the fact that the CPC network has already been established for several years (since 2006), there is still no uniform understanding among the national authorities about how to use the cooperation tools. Furthermore, the average time for the handling of mutual assistance requests is 92 days. Article 55.2 of the draft Regulation requests DPAs to act within 30 days¹³.

¹³ http://ec.europa.eu/consumers/enforcement/docs/comm_biennial_report_2011_en.pdf

With regards the “**consistency**” mechanism, BEUC sees the merits of the need for a more coherent approach of DPAs to issues of common interest. However, we are concerned that in almost every case when a DPA considers the adoption of measures against a company operating internationally, it will trigger the consistency mechanism. There needs to be a threshold in the draft Regulation to ensure consistency only applies to processing that raises serious risks to data subjects across Europe.

Furthermore, the draft Regulation allows the European Commission to intervene extensively in the context of the consistency mechanism. In particular, the Commission can ask for the consistency mechanisms to be applied, but can also suspend a measure adopted by a DPA if there are serious doubts as to its effectiveness (Article 60). BEUC agrees with the European Data Protection Supervisor to limit the suspension to cases where there is, *prima facie*, a clear breach of EU law subject to scrutiny of the Court of Justice¹⁴. The same concerns are raised by the power of the European Commission to overrule a decision of a national DPA via an implementing act (Article 50.1 and 62.1.[a]).

The provisions of the draft Regulation may undermine the independence of DPAs and subject their decisions to the external influence of the European Commission. The Commission could adopt its own Opinion but without any effect on the decision of the European Data Protection Board, while in cases of serious conflict it should be for the European Court of Justice to decide.

Lastly, BEUC welcomes the provisions on the establishment of the **European Data Protection Board** to replace the Article 29 Data Protection Working Group, particularly with regards to its independence. The status and the legal nature of the Opinions of the Board are necessary to ensure they become binding particularly when they concern the interpretation of provisions of the Regulation.

CHAPTER VIII – Remedies, liabilities and sanctions (Articles 73-79)

Efficient redress is a key component of a data subject’s empowerment. Although the current Directive already foresees the possibility for individuals to seek redress and compensation for damages suffered as a result of a data breach, in practice this provision has not been implemented effectively. The high costs related to individual litigation, as well as the legal uncertainty of the competent forum and applicable law, act as a deterrent in the enforcement of data subjects’ rights and an impediment to the fundamental right of access to justice.

BEUC welcomes the introduction of provisions which provide for **several redress mechanisms** with the view to facilitate enforcement by the data subject (Article 73). It is important that individuals can choose to lodge a **complaint with any DPA**, mainly that of their country of residence. However, it must be clarified that any costs related to the translation or transfer of the complaint to the competent

¹⁴ Opinion of the European Data Protection Supervisor on the data protection package reform, 7 March 2012.

DPA of another Member State should not be borne by the data subject.

As regards the right to a **judicial remedy** against the controller and the processor, BEUC welcomes the provision enabling the individual to lodge the complaint either before the court of the country of establishment of the controller or the court of the residence of the data subject. In cases where individuals from different countries have lodged complaints in different jurisdictions, the complexity can be solved through the establishment of clear rules regarding the competence of courts. For instance, it can be clarified that the court of the place of the most affected data subjects is the competent one and the others should suspend proceedings until the ruling is issued. However it should be ensured that the ruling can be recognised and executed in all other Member States.

Despite our support for the proposed redress mechanisms, we believe that in addition, more cost and time efficient methods for consumers to enforce their rights should be considered.

BEUC welcomes the right of organisations **or associations defending data subjects' rights** to lodge a complaint before a supervisory authority (Article 73) or bring an action to court (Article 76) on behalf of data subjects. However, we regret that the proposal has stopped short of introducing fully fledged **collective judicial actions** whereby representative bodies can claim compensation for the damages suffered by data subjects.

BEUC supports a system of collective judicial actions on the basis of Europe's legal tradition and the experiences of EU Member States. A number of safeguards need to be included to ensure such a system is not abused. BEUC has developed ten golden rules for a European, judicial, collective action¹⁵ which addresses the risk of abuse and provides a cost-effective and fair mechanism.

BEUC calls for a specific provision to be included in Article 77 which allows a representative organisation to bring judicial actions for compensation. There should be a clarification as regards the **quantification of damages and the calculation of compensation**. To this end, the possibility for **flat rate compensation** to be provided in circumstances of data breaches should be considered. When it comes to data breaches, the damages suffered are typically too small on an individual scale and would entail significant and disproportionate costs; however, the collective damage is significantly more substantial and consequently so is the illegal benefit of the non-compliant company.

An illegal behaviour of abuse of personal data can easily affect a high number of people, especially in the online environment, where internet services are cross-border and often provided from outside the EU. Furthermore, damages suffered are often intangible and it is difficult to assign a value and determine the responsibility of the involved parties, while in some cases, there might be no immediate damages, such as when confidential data (credit card numbers) are leaked.

¹⁵ European Group Action, BEUC's ten golden rules
<http://docshare.beuc.org/docs/2/MMOLGAFDFOMBPINPIJPOEMDPDBW9DB67K9DW3571KM/BEUC/docs/LS/2008-00394-01-E.pdf>

It should also be clarified that consumer organisations are entitled to bring actions for breaches of data protection law. In some EU Member States, consumer organisations can only act for breaches of consumer protection legislation, and data protection falls outside their remit. Nevertheless, consumer associations are credible entities with long experience in defending consumers and should therefore be entitled to act in the field of data protection. It should also be clarified that **damages** should include not only material and quantifiable damages, but also immaterial damages and distress. It is also important that consumer associations have standing to represent also consumers from other Member States that have suffered damage from the same illegal behaviour.

BEUC also welcomes the **joint liability** of the data controller and data processor, particularly as it may be difficult for the data subject to determine which entity is the data controller and who bears the liability in cases of damages suffered.

Article 79 aims to strengthen the mechanisms for **sanctions** in case of data protection infringements. The sanctions foreseen resemble the ones established under competition law and aim to act as a major deterrent for companies involved in the processing of personal data. However, BEUC proposes that the fines imposed on companies could be used, at least in part, to finance the actions of organisations defending the rights of data subjects. Furthermore, safeguards need to be included if fines are to be used mainly for the funding of DPAs to ensure that the system is not abused.

As regards the **exceptions** foreseen for processing by natural persons without commercial benefit and for entities below 250 employees for which personal data processing is an activity ancillary to its main activities, BEUC believes the important factor should not be the number of employees, but rather on the nature of the activities. For example, consumer organisations may well carry out surveys with the aim of advising consumers that might involve the processing of personal data. Such an activity is ancillary to the normal activities of consumer organisations and should therefore be exempted from the scope of Article 79.

CHAPTER IX – Provisions relating to specific data processing situations (Articles 80-85)

Chapter IX leaves room for national rules for specific processing situations related to freedom of expression, health, employment, professional secrecy, churches and religious associations.

Article 80: Processing of personal data and freedom of expression

BEUC welcomes the exemption from the regulation when personal data is carried out for journalistic purposes or for the purpose of artistic and literary expression. The freedom of expression must be balanced with the right to protection of personal data to ensure the effective exercise of both. To this end, an assessment on a case by case basis may be required to ensure that the right to data protection is not misused to hinder freedom of expression and freedom of information.

We would also suggest that the notion of journalistic purposes is clarified to include not only the traditional media, but also all new activities whose object is the public disclosure of information, opinions or ideas, irrespective of who is carrying on such activities (not necessarily a media undertaking), of the medium which is used to transmit the processed data (a traditional medium such as paper, radio waves or an electronic medium such as the internet) and of the nature (profit-making or not) of those activities, in line with the rulings of the European Court of Justice¹⁶.

Article 81- Processing of personal data concerning health

Article 81 foresees a number of exceptions to the general prohibition of processing sensitive health data: we support those exceptions as they ensure a good balance between the right to privacy, consumer safety and public health interests, but we think that certain aspects should be further clarified to prevent abuses. Moreover the use of sensitive health data for marketing purposes should remain prohibited. Tracking and profiling technologies in health related websites should not be allowed.

Article 81 allows the use of compiled health data for research purposes, for better managing healthcare expenditures, for monitoring and improving the quality, safety and the effectiveness of medicines and medical devices. Whilst we do not question the benefit of this for the safety of the individuals and for public health, we question the actual possibility of ensuring the anonymity of data. Technological advances in data analysis and combination with other data sets could endanger anonymity and lead to the identification of individuals. Unanswered questions remain also as to who exactly would have access to such data. For example, would the research sector include pharmaceutical companies? Would public accessibility mean that insurers can access the data? The legislation also lacks an indication as to how the amount of information seen will differ according to the role of the person accessing it. For example, how will the data which patients see differ from the data available to healthcare staff, policy makers and third party researchers?

It is crucial that only authorised and specifically trained healthcare professionals have access to patients' health records. Article 81 mentions the processing of data could be done by a person other than the healthcare professional provided that they are subject to an equivalent obligation of confidentiality. The definition of another person should be further specified to prevent abuses and inconsistency with the other provisions of the legislation.

¹⁶ C-73/07- *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy*.

Article 83- processing for historical, statistical and scientific research purposes

BEUC welcomes the exemption when personal data is processed for historical, statistical and scientific purposes. It should however, be stressed that the preferred option should be the processing of anonymised data and that only when it is impossible for the specific research, personal data should be processed when the conditions of Article 83 are met.

CHAPTER X – Delegated acts and implementing acts (Articles 86-87)

The draft Regulation often empowers the European Commission to adopt delegated and implementing acts. Although such acts can in certain cases ensure a uniform implementation of the Regulation, BEUC is concerned that the extensive use of this mechanism, as foreseen by the proposal, will undermine the objective of establishing a clear and comprehensive set of rules to the detriment of both data subjects and businesses. We are also concerned about the time required for all delegated acts to be issued: according to the estimated financial impact statement accompanying the Regulation proposal, only two delegated acts will be administered per year, and therefore a period of ten years will be required to adopt all acts and achieve legal certainty.

Furthermore, we are concerned with the lack of democratic oversight in the adoption of delegated and implementing acts; all EU institutions should have been involved.

BEUC suggests that the number of provisions subject to the adoption of delegated and implementing acts should be significantly reduced and limited to those provisions addressing non-essential issues, such as design requirements, criteria for technical measures etc. Furthermore, the mechanism of Article 86 could be used as the basis to adopt sector-specific rules clarifying the application of the general framework to specific areas of law. We would therefore suggest the possibility for the adoption of delegated acts and implemented acts is **maintained** only for the following provisions:

- Article 8.3 referring to the definition of criteria and requirements to verify parental consent in case of processing of personal data of a child below the age of 13 years old;
- Article 14.7 with regards to the modalities for the provision of information to the data subject;
- Article 15.3 on the content of the communication to the data subject of the personal data undergoing processing following a request to access data;
- Article 22.4 on the appropriate measures to be adopted by the data controller to ensure compliance in accordance with the principle of accountability which requires a certain degree of flexibility;
- Article 23.3 on the design requirements for the application principle of data protection by design on specific products and sectors;

- Article 26.5 regarding the measures to be adopted by the data processor in order to comply with the obligations established in the Regulation;
- Article 28.5 on definition of criteria and requirements for the documentation obligation;
- Article 30.3 which deals with technical aspects of security;
- Article 35.11 on the qualification of the data protection officer;
- Article 37.2 regarding the tasks, certification, status, powers and resources of the data protection officer;
- Article 43.3 on further specifying the criteria and requirements of binding corporate rules;
- Article 79.6 on the update of the amounts of the administrative fines.

As regards the remainder of the cases, it is crucial that further clarification is included in the current Regulation, as they refer to substantive and essential elements and therefore call for legal certainty. This is the case with the following provisions:

- Article 6.5 which foresees the adoption of sector-specific rules clarifying the application of the legitimate interests of the data controller as grounds for lawful processing; there is the risk that unless clearly specified, the legitimate interests of the controller may be invoked by controller to legitimise processing even when there is no appropriate legal grounds;
- Article 9.3 referring to sensitive data; the processing of sensitive data requires an additional layer of protection due to the nature of the information they can reveal about an individual and therefore the conditions and the safeguards for their processing must be clearly defined in the draft Regulation. Alternatively, this could be the object of opinions or reports of the European Data Protection Board;
- Article 12.4 regarding the definition of threshold above which requests to access and correct one's own data will be considered excessive. Otherwise, there is a risk that Member States use different thresholds and thus hinder the effective exercise of the individual rights;
- Article 17.9 on the implementation of the right to be forgotten. Given the interaction with fundamental freedoms, the conditions for deleting links, copies from publicly available communication services should be defined upfront;
- Article 18 regarding the right to data portability, the effective implementation of which requires the development of interoperable or compatible standards;
- Article 20.5 reserving the right for the Commission to define the safeguards for the data subject when profiling is allowed. This provision touches upon essential and substantive elements of data subjects' protection;
- Article 31.5 which refers to the threshold for data breach notification; unless a threshold is clearly defined in the Regulation, all breaches might have to be notified to the data protection authority;

- Article 32.5 on the communication of a data breach to the data subject. It is crucial to define when a breach will seriously affect the rights of the individual and will therefore require notification;
- Article 33.6 regarding the definition of operations presenting specific risks and therefore subject to a data protection impact assessment;
- Article 34.8 on the definition of the high degree of specific risk demonstrated by an impact assessment;
- Article 39.2 on certification mechanisms and privacy seals. For certification and seals to be endorsed by data subjects, full compliance with the legal framework and high standards of protection need to be ensured. It is therefore important that the conditions for the granting and the recognition within the EU are clearly defined;
- Article 44.7 on the notion of the public interest that might justify a derogation from the rules on transfer to third countries;
- Article 81.3 on the notion of public interest in relation with the processing of personal data concerning health;
- Article 83.3 regarding the criteria for limiting data subjects' rights for the processing of historical, statistical and scientific research purposes.

END



AmCham EU Proposed Amendments on the General Data Protection Regulation

CONTENTS

1. CONSENT AND PROFILING	3
2. DEFINITION OF PERSONAL DATA / PROCESSING FOR SECURITY AND ANTI-ABUSE PURPOSES	11
3. THE RIGHT TO ERASURE / PORTABILITY OF DATA	19
4. ADMINISTRATIVE BURDEN AND DATA CONTROLLER/ DATA PROCESSOR ISSUES	25
5. FINES / REMEDIES	47
6. APPLICABLE LAW (ONE-STOP-SHOP / “MAIN ESTABLISHMENT/LEAD DPA/CONSISTENCY) / GOVERNANCE PRINCIPLES AND TRANSPARENCY	50
7. CERTIFICATION / CODES OF CONDUCT	72
8. INTERNATIONAL DATA TRANSFERS / BCRS / SAFE HARBOR	76
9. DEFINITION OF A CHILD	84
10. DATA BREACH	86

1. Consent and profiling

Proposal for a regulation

Recital 25

Text proposed by the Commission

(25) Consent should be given **explicitly** by any appropriate method enabling a freely given specific and informed indication of the data subject's wishes, either by a statement or by a clear affirmative action by the data subject, ensuring that individuals are aware that they give their consent to the processing of personal data, including by ticking a box when visiting an Internet website or by any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data. **Silence or inactivity should therefore not constitute consent.** Consent should cover all processing activities carried out for the same purpose or purposes. If the data subject's consent is to be given following an electronic request, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.

AmCham EU Amendment

(25) Consent should be given by any appropriate method enabling a freely given specific and informed indication of the data subject's wishes, either by a statement or by a clear affirmative action by the data subject, ensuring that individuals are aware that they give their consent to the processing of personal data, including by ticking a box when visiting an Internet website or by any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data. Consent should cover all processing activities carried out for the same purpose or purposes. If the data subject's consent is to be given following an electronic request, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.

Justification

The imposition of "explicit" consent in every circumstance is not compatible with the notion that a request "must not be unnecessarily disruptive to the use of the service for which it is provided". The economic consequences of such a paradigm shift – which would fundamentally change the nature of internet users' relationship with the internet - need much greater investigation. Ruling out implied or tacit consent will encourage data controllers to authenticate users, increasing the amount of personal data held rather than reducing it. Explicit consent should be reserved for sensitive categories of data.

Proposal for a regulation

Recital 33

Text proposed by the Commission

(33) In order to ensure free consent, it should be clarified that consent does not provide a valid legal ground where the individual has no genuine and free choice and is subsequently not able to refuse or withdraw consent **without detriment.**

AmCham EU Amendment

(33) In order to ensure free consent, it should be clarified that consent does not provide a valid legal ground where the individual has no genuine and free choice and is subsequently not able to refuse or withdraw consent.

Justification

The concept of "without detriment" places an excessive burden on the organization from whom consent is withdrawn. Organisations should not be in a situation where they are unable to terminate a service once consent is withdrawn for fear of causing an undefined "detriment" to the data subject. This provision effectively regulates the terms and conditions which organisations of services

Proposal for a regulation

Recital 34

Text proposed by the Commission

AmCham EU Amendment

(34) Consent should not provide a valid legal ground for the processing of personal data, where there is a clear imbalance between the data subject and the controller. This is especially the case where the data subject is in a situation of dependence from the controller, among others, where personal data are processed by the employer of employees' personal data in the employment context. Where the controller is a public authority, there would be an imbalance only in the specific data processing operations where the public authority can impose an obligation by virtue of its relevant public powers and the consent cannot be deemed as freely given, taking into account the interest of the data subject.

(34) deleted

Justification

“Significant imbalance” is too vague a standard to provide any legal certainty to data subjects or to businesses (since it could be argued that any online relationship between a service provider and a user implies a significant imbalance) and is in any case already implied in the concept of consent being freely given. Including both concepts is confusing and unnecessary.

This amendment should be combined with the deletion paragraph 4 article 7

Proposal for a regulation

Article 4, Paragraph 8 - The data subject’s consent

Text proposed by the Commission

AmCham EU Amendment

(8) 'the data subject's consent' means any freely given specific, informed **and explicit** indication of his or her wishes by which the data subject, **either by a statement or by a clear affirmative action**, signifies agreement to personal data relating to them being processed;

(8) 'the data subject's consent' means any freely given specific **and**, informed indication of his or her wishes by which the data subject signifies agreement to personal data relating to them being processed;

Justification

The requirement of “explicit” consent is likely to unnecessarily disrupt the provision of services, particularly in the online environment, and is contrary to the intention specified in Recital 25 that the request must not be unnecessarily disruptive to the use of the service for which it is provided.

Proposal for a regulation

Article 7 - Conditions for consent

Text proposed by the Commission

1. The controller shall bear the burden of proof for the data subject's consent to the processing of their personal data for specified purposes.
2. If the data subject's consent is to be given in the context of a written declaration which also concerns another matter, the requirement to give consent must be presented distinguishable in its appearance from this other matter.
3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.
- 4. Consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller.**

AmCham EU Amendment

1. The controller shall bear the burden of proof for the data subject's consent to the processing of their personal data for specified purposes.
2. If the data subject's consent is to be given in the context of a written declaration which also concerns another matter, the requirement to give consent must be presented distinguishable in its appearance from this other matter.
3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.
- 4. For the processing of special categories of personal data in accordance with Article 9, consent shall be explicit.**

Justification

Explicit consent is not appropriate in all circumstances, and should be reserved for situations where sensitive categories of data are concerned. Reversing the burden of proof to oblige the data controller to demonstrate consent in every context, and making the failure to do so potentially punishable by sanctions, incentivizes data controllers to authenticate users and disincentivises the provision of anonymous services or website browsing. This will increase the amount of explicitly personal data held by data controllers, the opposite of what a well-calibrated privacy regulation should achieve.

Proposal for a regulation

Article 9, Paragraph 2 - Processing of special categories of personal data

Text proposed by the Commission

2. Paragraph 1 shall not apply where:
 (a) the data subject has given consent to the processing of those personal data, subject to the conditions laid down in Articles 7 and 8, **except where Union law or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject; or**

AmCham EU Amendment

2. Paragraph 1 shall not apply where :
 (a) the data subject has given consent to the processing of those personal data, subject to the **following** conditions
i. The controller shall bear the burden of proof for the data subject's consent to the processing of their personal data for specified purposes.
ii. the data subject has given his explicit consent to the processing of those data

Justification

To be viewed in conjunction with amendments to Article 7.

It is important to reserve specific and explicit consent for the processing of sensitive data. Currently the draft Regulation makes very little distinction between sensitive data and all other data. Requiring explicit consent for the processing of every category of data makes sensitive data indistinguishable in treatment from other data, and makes it difficult for users to make choices about when it is appropriate to give or withhold their consent.

Profiling

Proposal for a regulation

Article 3, Paragraph 2 - Territorial scope

Text proposed by the Commission

2. This Regulation applies to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are related to:
(a) the offering of goods or services to such data subjects in the Union; or
(b) the monitoring of their behaviour.

AmCham EU Amendment

2. This Regulation applies to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are related to the offering of goods or services to such data subjects in the Union.

Justification

Read in conjunction with Recital 21, it can only be understood that this provision aims at extending the scope of the Regulation to controllers established outside the Union when their processing activities are related to the profiling of individuals. It is not justified in the text or logically why the use of a particular technique enabled by various technologies, i.e. profiling, should be used as a criterion to define the extraterritorial scope of this Regulation. Not least, since this provision does not specify uses or applications or sectors targeted but rather takes a one-size-fits-all approach towards profiling. Such a provision would clearly go against the principle of technology neutrality included in Recital 13. It is also not clear how this would be enforceable in law.

Proposal for a regulation

Article 20 - Measures based on profiling

Text proposed by the Commission

1. **Every natural person** shall **have the right** not to be subject to a **measure** which **produces legal effects concerning this natural person or significantly affects this natural person**, and which is based solely on automated processing intended to evaluate certain personal aspects relating to this **natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour**.

2. **Subject to the other provisions of this Regulation, a person may be subjected to a measure of the kind referred to in paragraph 1 only if the processing:**

(a) is carried out in the course of the entering into, or performance of, a contract, where the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or where suitable measures to safeguard the data subject's legitimate interests have been adduced, such as the right to obtain human intervention; or

(b) is expressly authorized by a Union or Member State law which also lays down suitable measures to safeguard the data subject's legitimate interests; or

(c) is based on the data subject's consent, subject to the conditions laid down in Article 7 and to suitable safeguards.

3. **Automated processing of personal data intended to evaluate certain personal aspects relating to a natural person shall not be based solely on the special categories of personal data referred to in Article 9.**

4. **In the cases referred to in paragraph 2, the information to be provided by the controller under Article 14 shall include information as to the**

AmCham EU Amendment

1. **A data subject** shall not be subject to a **decision** which **is unfair or discriminatory**, and which is based solely on automated processing intended to evaluate certain personal aspects relating to this **data subject**.

2. **deleted**

3. **deleted**

4. **deleted**

5. **deleted**

existence of processing for a measure of the kind referred to in paragraph 1 and the envisaged effects of such processing on the data subject.

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for suitable measures to safeguard the data subject's legitimate interests referred to in paragraph 2.

Justification

Para 1:

- *Article 20 essentially prohibits profiling techniques and enabling technologies across sectors and irrespective of the objectives pursued showing no recognition of the many positive uses of profiling. It demonises the technology rather than aiming to limit the existing or potential negative uses of this technology whilst protecting beneficial uses. In addition, it does not take into account the fact that there are different levels of risk associated with profiling and disparate types of impact on the privacy of individuals also related to the sensitivity of the data processed with profiling. Therefore a one-size-fits-all approach is not appropriate. Furthermore, the chosen terms “produces legal effects” and “significantly affects” are very broad, unclear and not defined in the Regulation or other EU law. Therefore the proposed amendment aims to focus the prohibition on the negative uses of profiling techniques which are either “unfair” or “discriminatory” rather than the technology itself and therefore is also in line with the technology neutrality principle of Recital 13. As defined in Directive 2005/29/EC on Unfair Commercial Practices (Article 5§2), a decision is “unfair” if: (a) it is contrary to the requirements of professional diligence, and (b) it materially distorts or is likely to materially distort the economic behaviour with regard to the product (or service) of the average consumer whom it reaches or to whom it is addressed, or of the average member of the group when a commercial practice is directed to a particular group of consumers. The Guidance on the Unfair Commercial Practices Directive issued by the European Commission and the national enforcers, offers further clarification on terms such as “professional diligence, “to materially distort” and “average consumer”.*
- *The term “measure” targets the use of profiling technologies and techniques, rather than how those may be applied to a single individual which is actually the concern here. It is suggested to revert to the language of the existing Directive and therefore replace this word with “decision”.*
- *Following the suggested amendment to this, the list of examples included at the end no longer applies.*

Para 2, 3, 4, 5: Following the proposed amendments to paragraph 1 introducing a blank prohibition of unfair or discriminatory profiling without exceptions paragraphs 2, 3, 4 and 5 should be deleted.

Proposal for a regulation
Recital 58

Text proposed by the Commission

AmCham EU Amendment

(58) Every natural person should have the right not to be subject to a measure which is based on profiling by means of automated processing. However, such measure should be allowed when expressly authorised by law, carried out in the course of entering or performance of a contract, or when the data subject has given his consent. In any case, such processing should be subject to suitable safeguards, including specific information of the data subject and the right to obtain human intervention and that such measure should not concern a child.

(58) Unfair or discriminatory profiling shall be prohibited. As defined in Article 5§2 in Directive 2005/29/EC on Unfair Commercial Practices, the decision referred to in Article 20 of this Regulation is “unfair”

if:
(a) it is contrary to the requirements of professional diligence,
and
(b) it materially distorts or is likely to materially distort the economic behaviour with regard to the product (or service) of the average consumer whom it reaches or to whom it is addressed, or of the average member of the group when a commercial practice is directed to a particular group of consumers.

The Guidance on the Unfair Commercial Practices Directive issued by the European Commission and the national enforcers, offers further clarifications to this definition.

Justification

In line with proposed amendment on Article 20.

Proposal for a regulation

Text proposed by the Commission

AmCham EU Amendment

References to profiling or Article 20 in Recitals 51, 59, 129 and Articles 15 paragraph 1(h), 43 paragraph 2(e), 79 paragraph 6(d).

Deletion of references to profiling or Article 20 in Recitals 51, 59, 129 and Articles 15 paragraph 1(h), 43 paragraph 2(e), 79 paragraph 6(d).

Justification

For consistency with proposed amendment on deletion of Article 20.

Proposal for a regulation
Recital 74

Text proposed by the Commission

AmCham EU Amendment

Where a data protection impact assessment indicates that processing operations involve a high degree of specific risks to the rights and freedoms of data subjects, such as excluding individuals from their right, or by the use of specific new technologies, the supervisory authority should be consulted, prior to the start of operations, on a risky processing which might not be in compliance with this Regulation, and to make proposals to remedy such situation. Such consultation should equally take place in the course of the preparation either of a measure by the national parliament or of a measure based on such legislative measure which defines the nature of the processing and lays down appropriate safeguards-
[...]

deleted
[...]

Justification

In line with changes to Article 34.

2. Definition of personal data / Processing for security and anti-abuse purposes

Proposal for a regulation

Article 4, Paragraphs 1, 2 and 2a, 2b (new)

Text proposed by the Commission

(1) 'data subject' means an identified natural person or a natural person who can be identified, directly or indirectly, by means ***reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;***

(2) 'personal data' means any information relating to a data subject;

AmCham EU Amendment

(1) 'data subject' means an identified natural person or a natural person who can be identified, directly or indirectly, by means ***available in the effective control of the data controller and as part of a specific processing operation in its regular course of business in a way that permits the controller to confirm the identity of the data subject with any appropriate means;***

(2) 'personal data' means information relating to a data subject ***that makes identification by the controller reasonably possible;***

(2a) 'pseudonymous data' means any personal data that has been collected, altered or otherwise processed so that it of itself cannot be attributed to a data subject without the use of additional data which is subject to separate and distinct technical and organisational controls to ensure such non attribution;

(2b) 'anonymous data' means information that does not relate to a data subject or has been collected, altered or otherwise processed so that it cannot be attributed to a data subject;

Justification

Recitals 23 and 24 recognize that context can be a factor in determining whether data identifies a data subject, and that data which does not identify a data subject is not personal data. These important insights should be reflected in the definitions.

Proposal for a regulation

Recital 39

Text proposed by the Commission

(39) **The processing of** personal data to the extent strictly necessary for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data, and the security of the related services offered by, or accessible via, these networks and systems, by public authorities, Computer Emergency Response Teams – CERTs, Computer Security Incident Response Teams – CSIRTs, providers of electronic communications networks and services and by providers of security technologies and **services, constitutes a legitimate interest of the concerned data controller.** This could, for example, include preventing unauthorized access to electronic communications networks and malicious code distribution and stopping ‘denial of service’ attacks and damage to computer and electronic communication systems.

AmCham EU Amendment

(39) **It is lawful to process** personal data to the extent strictly necessary for the purposes of **(i) preserving network resilience and service quality; (ii)** ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data, and the security of the related services offered by, or accessible via, these networks and systems, by public authorities, Computer Emergency Response Teams – CERTs, Computer Security Incident Response Teams – CSIRTs, providers of electronic communications networks and services and by providers of security technologies and **services; (iii) of preventing and monitoring fraud.** This could, for example, include preventing unauthorized access to electronic communications networks and malicious code distribution and stopping ‘denial of service’ attacks and damage to computer and electronic communication systems.

Justification

Self explanatory.

Proposal for a regulation

Article 6 - Amendments on the lawfulness of processing

Text proposed by the Commission

1. Processing of personal data shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of their personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

AmCham EU Amendment

1. Processing of personal data shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of their personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by a controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their **tasks**.

2. Processing of personal data which is necessary for the purposes of historical, statistical or scientific research shall be lawful subject to the conditions and safeguards referred to in Article 83.

3. The basis of the processing referred to in points (c) and (e) of paragraph 1 must be provided for in:

(a) Union law, or

(b) the law of the Member State to which the controller is subject.

The law of the Member State must meet an objective of public interest or must be necessary to protect the rights and freedoms of others, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued.

4. Where the purpose of further processing is not

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by a controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their **tasks**;

(fa) processing is necessary by the controller or a third party for the purposes of preserving network resilience and service quality, of ensuring the ability of a network or an information system to resist at a given level of confidence accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity or confidentiality of stored or transmitted data and the security of the related services offered by or accessible via these networks and systems, or of preventing and monitoring fraud.

2. Processing of personal data which is necessary for the purposes of historical, statistical or scientific research shall be lawful subject to the conditions and safeguards referred to in Article 83.

3. The basis of the processing referred to in points (c) and (e) of paragraph 1 must be provided for in:

(a) Union law, or

(b) the law of the Member State to which the controller is subject.

The law of the Member State must meet an objective of public interest or must be necessary to protect the rights and freedoms of others, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued.

4. Where the purpose of further processing is not

compatible with the one for which the personal data have been collected, the processing must have a legal basis at least in one of the grounds referred to in points (a) to (e) of paragraph 1. This shall in particular apply to any change of terms and general conditions of a contract.

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the conditions referred to in point (f) of paragraph 1 for various sectors and data processing situations, including as regards the processing of personal data related to a child.

compatible with the one for which the personal data have been collected, the processing must have a legal basis at least in one of the grounds referred to in points (a) to (e) of paragraph 1. This shall in particular apply to any change of terms and general conditions of a contract.

5. deleted

Justification

The computer security industry needs to process data such as IP addresses to stop online attacks and protect EU citizens and organisations like banks, hospitals and schools from cyber threats such as denials of services, botnets, hacking, spam and phishing. Security processors' inability to process data classed as personal, even in contexts where they cannot attribute it to any specific individual, may result in the online security, safety and privacy of EU citizens being compromised.

**Proposal for a regulation
 Article 10**

Text proposed by the Commission

If the data processed by a controller **do not permit the controller to identify a natural person**, the controller shall **not** be obliged to acquire additional **information** in order to identify the data subject for the sole purpose of complying with any provision of this Regulation.

AmCham EU Amendment

1. If the data processed by a controller or a processor acting on its behalf is only pseudonymous, neither the controller nor any processor acting on its behalf shall be obliged to acquire additional information, nor to develop the means to engage in any additional processing of personal data for the sole purpose of complying with any provision of this Regulation.

2. (new) In such cases, the processing shall not be subject to Articles 15 to 19, and to Article 32.

3. (new) The processing of personal data for the purpose of rendering the data anonymous or to remove the controller's ability to infer the identity of a natural person from the data processed shall not be subject to Articles 15 to 19, and to Article 32.

Justification

Ensuring the data is secure during the process of anonymisation (since at this stage it remains personal data) is necessary. But since this type of processing will aim to ensure the data can no longer be related to any identified or identifiable person, any further requirements under this Regulation would only pose unnecessary burdens to competent authorities and businesses without effectively advancing the protection of privacy.

Likewise, a data controller may also process data that does not allow identification, and it should be made clear that if a data controller is not able to identify a natural person from the information processed, then processing can be done lawfully, without either having to gain more information in order to identify an individual, or being subject to further unnecessary obligations such as seeking consent.

Proposal for a regulation
Article 14, Paragraph 1(a) new

Text proposed by the Commission

AmCham EU Amendment

1(a). Where the processing of personal data is subject to Article 10, the controller may provide the information referred to in Article 14(1) via an online or offline contact point only.

Justification

Consistency with the amendment proposed to article 10.

Proposal for a regulation
Article 14, Paragraph 5 (ca) new

Text proposed by the Commission

AmCham EU Amendment

(ca) (new) the data are not collected from the data subject and processing takes place on the basis of Article 6(1)(fa); or

Justification

Consistency with the proposed addition of article 6(1)(fa) In situations in networking and information security processing where it is possible to identify the data subject (for example, an ISP which has a direct relationship with their subscribers and can map IP addresses to individuals), it is preferable to undertake certain processing without informing the data subject at the time, such as when there is a compromised machine sending spam and other circumstances where one is using the data to track the control traffic and identify the real malicious actors further up the chain.

Proposal for a regulation
Recital 50

Text proposed by the Commission

AmCham EU Amendment

However, it is not necessary to impose this obligation where the data subject already disposes of this information, or where the recording or disclosure of the data is expressly laid down by law, or where the

However, it is not necessary to impose this obligation where the data subject already disposes of this information, or where the recording or disclosure of the data is expressly laid down by law, **where it would**

provision of information to the data subject proves impossible or would involve disproportionate efforts. The latter could be particularly the case where processing is for historical, statistical or scientific research purposes; in this regard, the number of data subjects, the age of the data, and any compensatory measures adopted may be taken into consideration.

prejudice network and information security or where the provision of information to the data subject proves impossible or would involve disproportionate efforts. The latter could be particularly the case where processing is for historical, statistical or scientific research purposes; in this regard, the number of data subjects, the age of the data, and any compensatory measures adopted may be taken into consideration.

Justification

Consistency with the proposed addition of article 14(5)(ca).

**Proposal for a regulation
 Article 15 paragraph 2(a) new**

Text proposed by the Commission

AmCham EU Amendment

2a. Paragraphs 1 and 2 shall not apply where processing takes place for the purpose defined in Article 6(1)(fa) and the application of paragraphs 1 and 2 would be incompatible with that purpose.

Justification

Consistency with the proposed addition of article 6(1)(fa). The above clarifications would allow for the data subjects to exercise their legitimate rights of access but also recognizes that in some cases, such requirements need to be qualified. Malicious actors should not be given the ability to block the work of CERTs, CSIRTs, providers of electronic communications networks and services and providers of security technologies and services.

**Proposal for a regulation
 Recital 51**

Text proposed by the Commission

AmCham EU Amendment

Any person should have the right of access to data which has been collected concerning them, and to exercise this right easily, in order to be aware and verify the lawfulness of the processing. Every data subject should therefore have the right to know and obtain communication in particular for what purposes the data are processed, for what period, which

Any person should have the right of access to data which has been collected concerning them, and to exercise this right easily, in order to be aware and verify the lawfulness of the processing. Every data subject should therefore have the right to know and obtain communication in particular for what purposes the data are processed, for what period, which

recipients receive the data, what is the logic of the data that are undergoing the processing and what might be, at least when based on profiling, the consequences of such processing. This right should not adversely affect the rights and freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. **However, the result of these considerations should not be that all information is refused to the data subject.**

recipients receive the data, what is the logic of the data that are undergoing the processing and what might be, at least when based on profiling, the consequences of such processing. This right should not adversely affect **network and information security or** the rights and freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software.

Justification

Consistency with the proposed addition of article 15 (2a).

**Proposal for a regulation
 Article 17, Paragraph 3 (da) new**

Commission proposal

Proposed amendment

(da) for the purpose of processing as defined in article 6(1)(fa);

Justification

Consistency with the proposed addition of article 6(1)(fa).

**Proposal for a regulation
 Article 30, Paragraph 3 (new)**

Text proposed by the Commission

AmCham EU Amendment

3. The legal obligations, as referred to in paragraphs 1 and 2, which would require processing of personal data to the extent strictly necessary for the purposes of ensuring network and information security, constitute lawful processing pursuant to Article 6 paragraph 1 (fa).

Justification

Data controllers and processors should ensure that they have the right organizational measures in place to ensure security of processing and hence, enhancing overall network and information security. Where the implementation of such measures would require the processing of data to ensure network and information security by the data controller or the processor, such processing should be deemed to be lawful processing in line with the proposed Article 6(1) (fa) *new*. A practical example of such measures is the blocking of certain IP



numbers by the EU Commission for security purposes, as illustrated in its response to question E-007574/2012 by MEP Marc Tarabella.

3. The Right to Erasure / Portability of Data

Proposal for a regulation

Recital new

Text proposed by the Commission

AmCham EU Amendment

(new) Individuals that determine the purposes and the means of the processing of personal data falling outside the private household exception are also data controllers of such data; this is without prejudice to the fact that in some instances online platforms can act on behalf of the individuals and in others, these online platforms can be considered controllers, when they determine the purposes of the processing and do not act under the instructions of the individual.

Justification

In the current networked society it is important to acknowledge that data subjects too can be controllers of personal data they post and share through online platforms. These platforms are intermediaries when they act on behalf of the data subject, but can also be controllers of the personal data only if they too determine the purposes of the processing that are not determined by the data subject.

Proposal for a regulation

Recital 53

Text proposed by the Commission

AmCham EU Amendment

(53) Any person should have the right to have personal data concerning them rectified and a **'right to be forgotten'** where the retention of such data is not in compliance with this Regulation. In particular, data subjects should have the right that their personal data are erased and no longer processed, where the data are no longer necessary in relation to the purposes for which the data are collected or otherwise processed, where data subjects have withdrawn their consent for processing or where they object to the processing of personal data concerning them or where the processing of their personal data otherwise does not comply with this Regulation. ***This right is particularly relevant, when the data subject has given their consent as a child, when not being fully aware of the risks involved by the processing, and later wants to remove such personal data especially on the Internet.*** However, the further retention of the data should be allowed where it is necessary for historical, statistical and scientific research purposes, for reasons of public interest in

(53) Any person should have the right to have personal data concerning them rectified and ***the*** right to ***have such personal data erased*** where the retention of such data is not in compliance with this Regulation. In particular, data subjects should have the right that their personal data are erased and no longer processed, where the data are no longer necessary in relation to the purposes for which the data are collected or otherwise processed, where data subjects have withdrawn their consent for processing or where they object to the processing of personal data concerning them or where the processing of their personal data otherwise does not comply with this Regulation. However, ***certain exemptions should apply, particularly when identifying all relevant personal data in question proves impossible or involves a disproportionate effort and when in relation to personal data made publicly available by the data subject himself or herself, such right is overridden by the interests or fundamental rights and freedoms of others. An exemption should also apply to enable the data controller to process data for their***

the area of public health, for exercising the right of freedom of expression, when required by law or where there is a reason to restrict the processing of the data instead of erasing them.

legitimate interest, as for instance for the purpose of providing system, network or information security. The further retention of the data should be allowed where it is necessary for historical, statistical and scientific research purposes, for reasons of public interest in the area of public health, for exercising the right of freedom of expression, when required by law or where there is a reason to restrict the processing of the data instead of erasing them.

Justification

The right to erasure is a key data protection principle which already exists under the current data protection directive and should naturally be reaffirmed in the draft Regulation. However certain exemptions should apply to recognise that:

It is not always possible for a controller to identify all of the related personal data (for instance, where a third party makes information about another individual available online).

The right of erasure may be overridden by the interests or fundamental rights and freedoms of others.

An exemption should apply when a controller wishes to process the information for certain legitimate purposes such as for the purpose of providing system, network or information security.

Proposal for a regulation

Recital 54

Text proposed by the Commission

AmCham EU Amendment

(54) To strengthen the 'right to be forgotten' in the online environment, the right to erasure should also be extended in such a way that a controller who has made the personal data public should be obliged to inform third parties which are processing such data that a data subject requests them to erase any links to, or copies or replications of that personal data. To ensure this information, the controller should take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible. In relation to a third party publication of personal data, the controller should be considered responsible for the publication, where the controller has authorised the publication by the third party.

(54) deleted

Justification

It is technically impossible or involves a disproportionate effort for a data controller in the context of the online environment, to identify the data that have been copied or replicated on other platforms.

Furthermore, these provisions might generate negative unintended consequences in the online environment

whereby, in order to meet such obligations, service providers would in practice be obliged to ‘monitor’ peoples’ activities across the internet. It could also lead to the interpretation that intermediary services could be considered responsible for erasing any content related to the data subject that requests it. The erasure of data hosted by other services is not within the technical power of the intermediary and directly conflicts with the way the Internet works and how the current liability status of intermediaries is designed.

Proposal for a regulation

Recital 121

Text proposed by the Commission

(121) The processing of personal data solely for journalistic purposes, or for the purposes of artistic or literary expression should qualify for exemption from the requirements of certain provisions of this Regulation in order to reconcile the right to the protection of personal data with the right to freedom of expression, and notably the right to receive and impart information, as guaranteed in particular by Article 11 of the Charter of Fundamental Rights of the European Union. This should apply in particular to processing of personal data in the audiovisual field and in news archives and press libraries. Therefore, Member States should adopt legislative measures, which should lay down exemptions and derogations which are necessary for the purpose of balancing these fundamental rights. Such exemptions and derogations should be adopted by the Member States on general principles, on the rights of the data subject, on controller and processor, on the transfer of data to third countries or international organisations, on the independent supervisory authorities and on co-operation and consistency. This should not, however, lead Member States to lay down exemptions from the other provisions of this Regulation. In order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary to interpret notions relating to that freedom, such as journalism, broadly. Therefore, Member States should classify activities as "journalistic" for the purpose of the exemptions and derogations to be laid down under this Regulation if the object of these activities is the disclosure to the public of information, opinions or ideas, irrespective of the medium which is used to transmit them. They should not be limited to media undertakings and may be undertaken for profit-making or for non-profit making purposes.

AmCham EU Amendment

(121) The processing of personal data solely **for the purpose of exercising the right to freedom of expression, including for the purposes of journalistic, artistic or literary expression** for journalistic purposes, or for the purposes of artistic or literary expression should qualify for exemption from the requirements of certain provisions of this Regulation in order to reconcile the right to the protection of personal data with the right to freedom of expression, and notably the right to receive and impart information, as guaranteed in particular by Article 11 of the Charter of Fundamental Rights of the European Union. This should apply in particular to processing of personal data in the audiovisual field, ~~and~~ in news archives, ~~and in~~ press libraries, **and in the use of other means of communication, including the internet and social media**. Therefore, Member States should adopt legislative measures, which should lay down exemptions and derogations which are necessary for the purpose of balancing these fundamental rights. Such exemptions and derogations should be adopted by the Member States on general principles, on the rights of the data subject, on controller and processor, on the transfer of data to third countries or international organisations, on the independent supervisory authorities and on co-operation and consistency. This should not, however, lead Member States to lay down exemptions from the other provisions of this Regulation. In order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary to interpret notions relating to that freedom, such as journalism, broadly. Therefore, Member States should classify activities as "journalistic" for the purpose of the exemptions and derogations to be laid down under this Regulation if the object of these activities is the disclosure to the public of information, opinions or ideas, irrespective of the medium which is used to transmit them. They should not be limited to media undertakings and may be undertaken for profit-making or for non-profit making purposes.

Justification

The proposed amendment is aimed at clarifying the notion of freedom of expression. It is important to recognize in the Regulation the right of others to know and to publicise certain facts concerning a data subject, as this is closely linked to the right to freedom of expression and other democratic values.

Proposal for a regulation
Article 4 - Definitions

Text proposed by the Commission

AmCham EU Amendment

(20) (new) ‘Applicable national law’: *is the law of the place where the controller has its main establishment in accordance with this Regulation.*

Proposal for a regulation
Article 3, Paragraph 4 (new)

Text proposed by the Commission

AmCham EU Amendment

3 (4) (new) *For the purposes of compliance with the obligations of this Regulation, the applicable law is to be determined in accordance with Article 4 and 51 of the Regulation.*

Justification

The Regulation does not clarify what national law is applicable in cases where this Regulation builds on national legislation. The internal market cannot be fragmented in cases of personal data processing.

Proposal for a regulation
Article 17, Paragraph 1

Text proposed by the Commission

AmCham EU Amendment

1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, ***especially in relation to personal data which are made available by the data subject while he or she was a child***, where one of the following grounds applies:

(a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

(b) the data subject withdraws consent on which

1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data where one of the following grounds applies:

(a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the

the processing is based according to point (a) of Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data;

(c) the data subject objects to the processing of personal data pursuant to Article 19;

(d) the processing of the data does not comply with this Regulation for other reasons.

processing of the data;

(c) the data subject objects to the processing of personal data pursuant to Article 19;

(d) the processing of the data does not comply with this Regulation for other reasons.

Except where:

(e) identifying all relevant personal data in question proves impossible or involves a disproportionate effort;

(f) such right is overridden by the interests or fundamental rights and freedoms of others.

Justification

The right to erasure in Article 17(1) is a key data protection principle which already exists under the current data protection directive and should naturally be reaffirmed in the draft Regulation. The right to erasure should be reviewed to recognize that the right balance is struck between the rights of a data subject to get their data deleted, the rights of individuals to remember and the right to freedom of expression. The practical difficulties associated with identifying the necessary information to ensure compliance with this provision must also be taken into account. Certain exemptions should apply to recognise that:

- *It is not always possible for a controller to identify all of the related personal data (for instance, where a third party makes information about another individual available online);*
- *The right of erasure may be overridden by the interests or fundamental rights and freedoms of others;*
- *A controller should be able to process the information for a certain legitimate purpose such as for the purpose of providing system, network or information security*

Moreover, the right to be forgotten in Article 17(2) needs very careful consideration It is technically impossible or involves a disproportionate effort for a data controller in the context of the online environment, to identify the data that have been copied or replicated on other platforms.

Furthermore, this provision might generate negative unintended consequences in the online environment whereby, in order to meet such obligations, service providers would in practice be obliged to ‘monitor’ peoples’ activities across the internet. It could also lead to the interpretation that intermediary services could be considered responsible for erasing any content related to the data subject that requests it. The erasure of data hosted by other services is not within the technical power of the intermediary and directly conflicts with the way the Internet works and how the current liability status of intermediaries is designed.

Proposal for a regulation
Article 17

Text proposed by the Commission

2. Where the controller referred to in paragraph 1 has made the personal data public, it shall take all reasonable steps, including technical measures, in relation to data **for the publication** of which the controller is responsible, to inform third parties **which are processing** such data, that a data subject requests them to erase any links to, or copy or replication of that personal data. **Where the controller has authorised a third party publication of personal data, the controller shall be considered responsible for that publication.**

AmCham EU Amendment

2. In cases where the Controller, other than the data subject to whom the information pertains has transferred the personal data to third parties, it shall take all reasonable steps, including technical measures, in relation to data **processing for which the controller is responsible, to inform third parties to whom such data has been transferred** that a data subject requests them to erase any links to, or copy or replication of that personal data.

Justification

In the online networked world, natural persons can determine the means and the purposes for which information related to them can be processed; for instance, a social platform can be chosen by the data subject, as well as the purposes for which the information should be processed on his behalf. However, in these situations, it cannot be excluded completely that more than one controller processes the information. Against this background, the additional duty to inform third parties needs to be framed in the context of the distinct responsibilities of each of the actors, in line with ECJ Jurisprudence.

Proposal for a regulation
Article 17, Paragraph 8

Text proposed by the Commission

8. Where the erasure is carried out, the controller shall not otherwise process such personal data.

AmCham EU Amendment

8. deleted

Justification

Complete erasure as opposed to restriction of personal data processing can have a detrimental effect on the ability of data subjects to exercise other rights, such as access and rectification requests, and the possibility of the controller to verify and proof compliance with such requests.

4. Administrative burden and data controller/ data processor issues

Proposal for a regulation Article 4, Paragraph 5

Text proposed by the Commission

(5) 'controller' means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes, **conditions and means** of the processing of personal data; where the purposes, **conditions and means** of processing are determined by Union law or Member State law, the controller or the specific criteria for his nomination may be designated by Union law or by Member State law;

AmCham EU Amendment

(5) 'controller' means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes, of the processing of personal data; where the purposes, of processing are determined by Union law or Member State law, the controller or the specific criteria for his nomination may be designated by Union law or by Member State law;

Proposal for a regulation Article 24 - Joint controllers

Text proposed by the Commission

24. Where a controller determines the purposes, **conditions and means** of the processing of personal data jointly with others, the joint controllers shall determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the procedures and mechanisms for exercising the rights of the data subject, by means of an arrangement between them.

AmCham EU Amendment

24. Where a controller determines the purposes, of the processing of personal data jointly with others, the joint controllers shall determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the procedures and mechanisms for exercising the rights of the data subject, by means of an arrangement between them. ***The arrangement shall duly reflect the joint controllers' respective effective roles and direct or indirect relationship with data subjects.***

Proposal for a regulation Recital 62

Text proposed by the Commission

(62) The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processor, also in relation to the monitoring by and measures of supervisory authorities, requires a clear attribution of the responsibilities under this Regulation, including where a controller determines the purposes, **conditions and means** of the processing jointly with other controllers or where a processing operation is carried out on

AmCham EU Amendment

(62) The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processor, also in relation to the monitoring by and measures of supervisory authorities, requires a clear attribution of the responsibilities under this Regulation, including where a controller determines the purposes, of the processing jointly with other controllers or where a processing operation is carried out on behalf of a

behalf of a controller.

controller, **due account being taken of their respective roles and direct or indirect relationship with data subjects.**

Justification

Under the proposed Regulation, data “controllers” and data “processors” are subject to different obligations. In light of this framework, it is important that the Regulation include a clear test that organisations can apply to determine when they are operating as controllers and when they are operating as processors. The amendment above would introduce such a clear test.

*As a general rule, controllers typically determine **why** data is processed (i.e. for what purposes) while processors typically determine **how** it is processed (i.e. under what conditions). In a scenario where a cloud service provider offers enterprise customers a hosted email service, for example, the provider is likely to be a data processor. That’s because the cloud service provider only determines “how” the data is processed -- i.e. it stores and delivers email for the purposes and at the direction of its enterprise customers. However, if the cloud service provider also uses the email addresses it collects from the service to profile end users and send them spam, then the cloud service provider has a say in the “why” the data is processed and becomes a data controller. In this scenario, the cloud service provider will be a controller for the same data for which it is a data processor.*

Unhelpfully, however, the test proposed under the Regulation confuses the simple “how” and “why” distinction -- making it harder for organisations to determine whether they are a controller or a processor or both. Under the Regulation, controllers are defined as those that determine not only the “purposes” of processing data (i.e. the “why”), but also the “conditions and means” of processing (i.e. the “how”). As the European Parliament’s study has concluded, this approach isn’t clear.

The above amendment would address this confusion by deleting the reference to “conditions and means,” and making clear that the data controller is the entity that determines the “purposes” of the processing only -- i.e. the entity that determines the “why” data is processed. This change will help to clarify the divide between the important roles of controller and processor and create greater legal certainty.

In addition, for joint controllers, the arrangement should be expressly required to duly reflect the joint controllers' respective roles and relationship with the data subjects, to ensure that joint controllers are on a level playing field. Joint controllers are indeed not necessarily in an equal negotiation position. Moreover, joint controllers have not all equal access to data subjects nor do they control the same kind and amount of personal data.

Proposal for a regulation

Article 14, Paragraphs 1 and 5 - Information to the data subject

Text proposed by the Commission

AmCham EU Amendment

1. Where personal data relating to a data subject are collected, the controller shall provide the data subject with at least the following information:

(a) the identity and the contact details of the controller and, if any, of the controller's representative and of the data protection officer;

(b) the purposes of the processing for which the personal data are intended, **including the contract terms and general conditions where the processing is based on point (b) of Article 6(1) and the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);**

(c) the period for which the personal data will be stored;

(d) the existence of the right to request from the controller access to and rectification or erasure of the personal data concerning the data subject or to object to the processing of such personal data;

(e) the right to lodge a complaint to the supervisory authority **and the contact details of the supervisory authority;**

(f) the recipients or categories of recipients of the personal data;

(g) where **applicable**, that the controller intends to transfer to a third country or international organisation **and on the level of protection afforded by that third country or international organisation by reference to an adequacy decision by the Commission;**

(h) any further information necessary to guarantee fair processing in respect of the data subject, having regard to the specific circumstances in which the personal data are collected.

[.....]

5. Paragraphs 1 to 4 shall not apply, where:

(a) the data subject **has** already the information referred to in paragraphs 1, 2 and 3; or

1. Where personal data relating to a data subject are collected, the controller shall provide the data subject with at least the following information:

(a) the identity and the contact details of the controller and, if any, of the controller's representative and of the data protection officer **or, if appropriate, the identity and contact details of the group of undertakings and its data protection officer;**

(b) the purposes of the processing for which the personal data are intended;

(c) deleted

(d) the existence of the right to request from the controller access to and rectification or erasure of the personal data concerning the data subject or to object to the processing of such personal data;

(e) the right to lodge a complaint to the **lead** supervisory authority;

(f) **where material**, the recipients or categories of recipients **outside the controller or the group of undertakings of which the controller is a member** of the personal data;

(g) where **material**, that the controller intends to transfer to a third country or international organisation **that does not provide an adequate** level of protection;

(h) any further information necessary to guarantee fair processing in respect of the data subject, having regard to the specific circumstances in which the personal data are collected.

[.....]

5. Paragraphs 1 to 4 shall not apply, where:

(a) the data subject already **has or can reasonably be expected to know** the information referred to in

paragraphs 1, 2 and
3; or

Proposal for a regulation
Recital 48

Text proposed by the Commission

(48) The principles of fair and transparent processing require that the data subject should be informed in particular of the existence of the processing operation and its purposes, **how long the data will be stored**, on the existence of the right of access, rectification or erasure and on the right to lodge a complaint. Where the data are collected from the data subject, the data subject should also be informed whether they are obliged to provide the data and of the consequences, in cases they do not provide such data.

AmCham EU Amendment

(48) The principles of fair and transparent processing require that the data subject should be informed in particular of the existence of the processing operation and its purposes on the existence of the right of access, rectification or erasure and on the right to lodge a complaint. Where the data are collected from the data subject, the data subject should also be informed whether they are obliged to provide the data and of the consequences, in cases they do not provide such data.

Justification

There should be greater flexibility and less prescription regarding the information to be provided to the individual, as a part of fair processing notice. The current draft is too prescriptive and would create huge administrative and cost burdens for organizations, without delivering a real benefit for individuals. In global organizations, with global processes and global systems, it is impossible to customise notices for each data controller in the group of undertakings, especially where the information in the notices is same, save for the name of data controller and/ or DP Officer. Furthermore, long and complex notices are never read by individuals, they are cumbersome to draft and deliver effectively and just create work for lawyers – detracting from their main purpose, which is to provide information to individuals that they care about, did not know or can do something about. The long prescriptive list should be made more flexible by including the words “where material” – allowing for flexibility to provide certain information only where that is of essence or important for individual.

It is often difficult, if not impossible, to state accurately how long personal data will be stored as it can depend on unknown factors such as legal proceedings arising. As a result, a requirement to state how long personal data are stored will in many cases lead to generic statements such as “for as long as necessary for the purposes for which the personal data are processed” which does not provide a data subject with any greater transparency or clarity. The requirement to specify the third country destination of a data transfer in the information to the data subject would be unnecessarily burdensome, and should be limited to instances where the third country/organization do not offer an adequate level of protection.

Proposal for a regulation

Article 15, Paragraph 2(a) new - Right of access for the data subject

Text proposed by the Commission

AmCham EU Amendment

2(a) (new) Paragraphs 1 and 2 shall not apply where processing takes place for the purpose defined in Article 6(1)(fa) and the application of paragraphs 1 and 2 would be incompatible with that purpose.

Justification

Consistency with the proposed addition of article 6(1)(fa). The above clarifications would allow for the data subjects to exercise their legitimate rights of access but also recognizes that in some cases, such requirements need to be qualified. Malicious actors should not be given the ability to block the work of CERTs, CSIRTs, providers of electronic communications networks and services and providers of security technologies and services.

Proposal for a regulation

Article 22 - Responsibility of the controller

Text proposed by the Commission

AmCham EU Amendment

1. The controller shall **adopt policies and** implement appropriate measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation.

2. The measures provided for in paragraph 1 shall in particular include:

keeping the documentation pursuant to Article 28;

(a) implementing the data security requirements laid down in Article 30;

(b) performing a data protection impact assessment pursuant to Article 33;

(c) complying with the requirements for prior authorisation or prior consultation of the supervisory authority pursuant to Article 34(1) and (2);

(d) designating a data protection officer pursuant to Article 35(1).

3. The controller shall implement mechanisms to ensure the verification of the effectiveness of the measures referred to in paragraphs 1 and 2. If proportionate, this verification shall be carried out by

1. The controller, **or the group of undertakings of which the controller is a member**, shall implement appropriate measures to ensure and be able to demonstrate **upon request** that the processing of personal data is performed in compliance with this Regulation.

2. The measures provided for in paragraph 1 shall in particular include:

a) management commitment and oversight to ensure processing of personal data is carried out in compliance with this Regulation, including, if appropriate, the appointment of the Data Protection Officer pursuant to Article 35.1;

b) policies and procedures that document the requirements of this Regulation including the security requirements laid down in Article 30;

c) an assessment of risks associated with the processing of personal data such as, but not limited to, data protection impact assessments as required under Article 33;

independent internal or external auditors.

4. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying **any further criteria and requirements for appropriate measures referred to in paragraph 1 other than those already referred to in paragraph 2, the conditions for the verification and auditing mechanisms referred to in paragraph 3 and as regards** the criteria for proportionality under paragraph 3, and considering specific measures for micro, small and medium-sized-enterprises.

d) appropriate documentation of processing activities as laid out in Article 28

3. The controller shall implement mechanisms to ensure the verification of the effectiveness of the measures referred to in paragraphs 1 and 2. If proportionate, this verification shall be carried out by independent internal or external auditors.

4. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying the criteria for proportionality under paragraph 3, and considering specific measures for micro, small and medium-sized-enterprises.

Justification

Most global companies have global data privacy compliance programmes and these are set at global and group company level rather than for each controller. Moreover, the list of measures should be more flexible, listing what constitutes effective compliance without going into prescriptive detail on each of them. The measures should be aligned to the globally emerging accountability model, the Binding Corporate Rules requirements and especially the Corporate Data Management Framework, published by the Canadian Privacy Commissioners. Finally, the measures which the controller must undertake are clearly outlined in paragraph 2. As such, there is no need for the Commission to give itself powers to determine further requirements or criteria, or indeed to define the structure for audits.

**Proposal for a regulation
 Article 26 - Processor**

Text proposed by the Commission

1. Where **a** processing **operation** is to be carried out on behalf of a controller, the controller shall choose a processor providing sufficient guarantees to implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject, in particular in respect of the technical security measures and organizational measures governing the processing to be carried out and shall ensure compliance with those measures.

2. The carrying out of processing by a processor shall be governed by a contract or other legal act binding the processor to the controller and stipulating in particular that the processor shall:

(a) act only on instructions from the controller, in particular, where the transfer of the personal data used is prohibited;

AmCham EU Amendment

1. Where processing is to be carried out on behalf of a controller, the controller shall choose a processor providing sufficient guarantees to implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject, in particular in respect of the technical security measures and organizational measures governing the processing to be carried out and shall ensure compliance with those measures.

2. The carrying out of processing by a processor shall be governed by a contract or other legal act binding the processor to the controller and stipulating in particular that the processor shall:

(a) act only on instructions from the controller **as to the purposes of the processing**, in particular, where the transfer of the personal data used is prohibited;

(b) employ only staff who have committed themselves to confidentiality or are under a statutory obligation of confidentiality;

(c) take all required measures pursuant to Article 30;

(d) enlist another processor only with the prior permission of the controller;

(e) insofar as this is possible given the nature of the processing, create in agreement with the controller the necessary technical and organisational requirements for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;

(f) assist the controller in ensuring compliance with the obligations pursuant to Articles 30 to 34;

(g) **hand over all results to the controller after the end of the processing and** not process the personal data **otherwise**;

(h) make available to the controller **and the supervisory authority** all information necessary to control compliance with the obligations laid down in this Article.

3. The controller and the processor shall document in writing the controller's instructions and the processor's obligations referred to in paragraph 2.

4. If a processor processes personal data other than as instructed by the controller, the processor shall be considered to be a controller in respect of that processing and shall **be subject to the rules on joint controllers laid down in Article 24**.

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the responsibilities, duties and tasks in relation to a processor in line with paragraph 1, and conditions which allow facilitating the processing of personal data within a group of undertakings, in particular for the purposes of control and reporting.

(b) employ only staff who have committed themselves to confidentiality or are under a statutory obligation of confidentiality;

(c) take all required measures pursuant to Article 30;

(d) **where the processor** enlists another processor **solely to perform specific processing operations for the controller, enlist such other processor** only with the prior permission of the controller;

(e) insofar as this is possible given the nature of the processing, create in agreement with the controller the necessary technical and organisational requirements for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;

(f) assist the controller in ensuring compliance with the obligations pursuant to Articles 30 to 34;

(g) not process the personal data further **after the end of the agreed processing except where the personal data are anonymised, retained for compliance purposes or for the purposes referred to in point (g) of paragraph 1 of Article 6**;

(h) **upon request** make available to the controller all **relevant and permissible** information necessary to control compliance with the obligations laid down in this Article.

3. The controller and the processor shall document in writing the controller's instructions and the processor's obligations referred to in paragraph 2.

4. If a processor processes personal data other than as instructed by the controller, the processor shall be considered to be a controller in respect of that processing and shall **comply with all applicable provisions of this Regulation**.

5. deleted

Justification

The proposed text introduces a host of new requirements for data processors and states how these should be included in the contractual arrangements. Some of these additions are unworkable in practice. There are situations where processor uses another processor to perform certain processing operations or provide services to the processor organization, that are not related and specific to any particular controller. For example,

processor should be able to decide on business continuity and recovery services, hosting services, cloud services, or any other IT services which many third party processors provide to a processor organization, without having to ask permission of controller whose data are in the mix and may be included in these services. Controller should have a right to approve sub-processors only where they may be directly performing sub-processing services related to the contract between the controller and processor. In relation to handing over results at the end of processing, there may be no results as such to hand over if the data minimisation principle has been effectively applied, e.g. where the data is anonymised, or where such data should be retained for compliance purposes. There are also instances where a processor is required to process controller's personal data for their own purposes, for example in order to ensure information security in respect of controller's data, or to ensure business continuity. Such processing should be allowed and not subject to any contractual restrictions. Making data available to the supervisory authority should be handled by the controller. Certain information may be subject to a confidentiality obligation under law or contract and hence a processor may not be at liberty to disclose such information to a supervisory authority. Moreover, such data should not be required to be transmitted on a regular basis as this would overburden authorities and further increase the administrative burden. Equally, in the instances where processor uses controller's personal data for their own purposes, the processor becomes a controller, rather than joint controller. Joint controllership would put much onus on both parties and would imply they share the same purposes and means of processing, which may not be true at all in the circumstances. Finally, the word "operation" should be deleted in paragraph 1 after the word "processing" in order to avoid confusion as the word "operation" is used in the definition of "processing" in Article 4(1).

In relation to the delegated act clause, the Lisbon Treaty makes clear that such acts are meant to be used to "supplement or amend certain non-essential elements" of a law. In the context of the proposed Regulation, however, the Commission often appears to be using delegated acts to determine the scope and applicability of core aspects of the law -- including with regard to fundamental issues such as the obligations of processors (Article 26(5)). The obligations of processors should be clearly defined in the Regulation itself. Europe's processors -- and the controllers and data subjects they serve -- should not be required to wait for secondary legislation to be adopted in order to understand the responsibilities, duties and tasks that apply to processors. For this reason, Article 26(5) should be deleted.

Proposal for a regulation
Article 28 - Documentation

Text proposed by the Commission

AmCham EU Amendment

1. Each controller **and processor** and, if any, the controller's representative, shall maintain documentation of **all processing operations** under its responsibility.
2. **The documentation shall contain at least the following information:**
 - (a) **the name and contact details of the controller, or any joint controller or processor, and of the representative, if any;**
 - (b) **the name and contact details of the data protection officer, if any;**
 - (c) **the purposes of the processing, including the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);**
 - (d) **a description of categories of data subjects and of**

1. Each controller and, if any, the controller's representative, shall maintain documentation of **the different categories of** processing under its responsibility.
2. **Such documentation shall include a general description of the categories of data subjects, personal data processed and purposes for which the personal data are generally processed.**
3. The controller and the processor and, if any, the controller's representative, shall make the documentation available, on request, to the **lead** supervisory authority.
4. **Where a controller engages a processor, the controller shall be responsible for maintaining the**

the categories of personal data relating to them;

(e) the recipients or categories of recipients of the personal data, including the controllers to whom personal data are disclosed for the legitimate interest pursued by them;

(f) where applicable, transfers of data to a third country or an international organisation, including the identification of that third country or international organisation and, in case of transfers referred to in point (h) of Article 44(1), the documentation of appropriate safeguards;

(g) a general indication of the time limits for erasure of the different categories of data;

(h) the description of the mechanisms referred to in Article 22(3).

3. The controller **and the processor** and, if any, the controller's representative, shall make the documentation available, on request, to the supervisory authority.

4. The obligations referred to in paragraphs 1 and 2 shall not apply to the following controllers **and processors**:

(a) a natural person processing personal data without a commercial interest; or

(b) an enterprise or an organisation employing fewer than 250 persons that is processing personal data only as an activity ancillary to its main activities.

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the documentation referred to in paragraph 1, to take account of in particular the responsibilities of the controller and the processor and, if any, the controller's representative.

6. The Commission may lay down standard forms for the documentation referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

documentation referred to in Article 28.1 and can request the processor to provide assistance in compiling the information.

5. The controller and, if any, the controller's representative, shall make the documentation available, on request, to the **lead** supervisory authority.

6. The obligations referred to in paragraphs 1 and 2 shall not apply to the following controllers:

(a) a natural person processing personal data without a commercial interest; or

(b) an enterprise or an organisation employing fewer than 250 persons that is processing personal data only as an activity ancillary to its main activities.

5. Deleted

7. The Commission may lay down standard forms for the documentation referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Proposal for a regulation
Recital 65

Text proposed by the Commission

(65) In order to demonstrate compliance with this Regulation, the controller **or processor** should document **each** processing **operation**. Each controller **and processor** should be obliged to co-operate with the supervisory authority and make this documentation, on request, available to it, so that it might serve for monitoring those processing operations.

AmCham EU Amendment

(65) In order to demonstrate compliance with this Regulation, the controller should document **the different categories of** processing. Each controller should be obliged to co-operate with the supervisory authority and make this documentation, on request, available to it, so that it might serve for monitoring those processing operations.

Justification

Requiring both controllers and processors to maintain the same documentation for the same categories of processing is an unnecessary burden that does not enhance the protection of data subjects or facilitate enforcement by the authorities. The controller should be primarily responsible for maintaining the documentation in order to avoid duplication with the processor. If the processor is given an independent duty to maintain documentation, it should be different from the controller. The level of information that controllers should be required to record should be set at much more general level. To prescribe very granular and specific items to record for each processing activity, tool, system or process would create an excessive administrative burden, something which the removal of notification duties in all Member States was designed to avoid. Transparency for individuals will be provided through timely fair processing notices, so there is no obvious benefit for the individual of the sort of detailed internal register proposed here. In groups of undertakings each member of the group is often a controller in respect of at least some personal data, e.g. HR data, but in order to use the data efficiently they will all use the same tools and processes. To require each controller to maintain documentation in relation to the same processing activity would represent a duplication and a disproportionate administrative burden. Finally, whilst the controller should carry the primary responsibility for the documentation, it is recognised that processors can provide useful information to the controller to assist them in this task.

Proposal for a regulation
Article 30 - Security of processing

Text proposed by the Commission

1. The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected, having regard to the state of the art and the costs of their implementation.
2. The controller and the processor shall, following an evaluation of the risks, take the measures referred to in paragraph 1 to protect personal data against accidental or unlawful destruction or accidental loss and to prevent any unlawful forms of processing, in

AmCham EU Amendment

1. The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected, having regard to the state of the art and the costs of their implementation.
2. The controller and the processor shall, following an evaluation of the risks, take the measures referred to in paragraph 1 to protect personal data against accidental or unlawful destruction or accidental loss

particular any unauthorised disclosure, dissemination or access, or alteration of personal data.

3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the technical and organisational measures referred to in paragraphs 1 and 2, including the determinations of what constitutes the state of the art, for specific sectors and in specific data processing situations, in particular taking account of developments in technology and solutions for privacy by design and data protection by default, unless paragraph 4 applies.

4. The Commission may adopt, where necessary, implementing acts for specifying the requirements laid down in paragraphs 1 and 2 to various situations, in particular to:

(a) prevent any unauthorised access to personal data;

(b) prevent any unauthorised disclosure, reading, copying, modification, erasure or removal of personal data;

(c) ensure the verification of the lawfulness of processing operations.

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

and to prevent any unlawful forms of processing, in particular any unauthorised disclosure, dissemination or access, or alteration of personal data.

3. deleted

4. deleted

Proposal for a regulation

Recital 66

Text proposed by the Commission

AmCham EU Amendment

(66) In order to maintain security and to prevent processing in breach of this Regulation, the controller or processor should evaluate the risks inherent to the processing and implement measures to mitigate those risks. These measures should ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks and the nature of the personal data to be protected. ***When establishing technical standards and organisational measures to ensure security of processing, the Commission should promote technological neutrality, interoperability and innovation, and, where appropriate, cooperate with third countries.***

(66) In order to maintain security and to prevent processing in breach of this Regulation, the controller or processor should evaluate the risks inherent to the processing and implement measures to mitigate those risks. These measures should ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks and the nature of the personal data to be protected.

Justification

The security requirements under the current Directive are being effectively applied and while the new proposals make a more direct appeal to the responsibilities of processors, there is no need for the Commission to adopt additional powers in this area. This is particularly true because such security requirements should be technology neutral so as to avoid market distortion and the detailing of blueprints for malicious actors to follow. This is not compatible with the wording in the Commission's additional powers, which talks about specific technologies and solutions.

Proposal for a regulation

Article 33

Text proposed by the Commission

AmCham EU Amendment

1. Where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller or the processor acting on the controller's behalf shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

1. Where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller or the processor acting on the controller's behalf shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

2. The following processing operations ***in particular*** present specific risks referred to in paragraph 1:

2. The following processing operations present specific risks referred to in paragraph 1:

(a) a systematic and extensive evaluation of personal aspects relating to a natural person or for

(a) deleted

analysing or predicting in particular the natural person's economic situation, location, health, personal preferences, reliability or behaviour, which is based on automated processing and on which measures are based that produce legal effects concerning the individual or significantly affect the individual; [...] (e) deleted [...]

[...] 4. deleted

(e) other processing operations for which the consultation of the supervisory authority is required pursuant to point (b) of Article 34(2). [...] 6. deleted [...]

[...]

4. The controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations.

[...]

6. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the processing operations likely to present specific risks referred to in paragraphs 1 and 2 and the requirements for the assessment referred to in paragraph 3, including conditions for scalability, verification and auditability. In doing so, the Commission shall consider specific measures for micro, small and medium-sized enterprises.

[...]

Justification

With the view to ensure legal certainty and enable better enforcement by supervisory authorities and in accordance with Recital 62 which requires “a clear attribution of the responsibilities under this Regulation”, privacy impact assessments should be carried out by the controller. Notably, the controller is in the best position to assess the impact of any processing. The controller, and not the processor, has ready access to all relevant information, including risks and benefits of processing the personal data. The PIA process should only be imposed where the “specific risks” referred to in the proposed Article (a far too imprecise and over-inclusive category) may lead to legal effects that gravely and adversely affect the individual’s fundamental rights. Furthermore, the requirement to seek the views of data subjects is impractical.

Proposal for a regulation
Article 34 - Prior authorisation

Text proposed by the Commission

AmCham EU Amendment

1. The controller or the processor as the case may be shall obtain an authorisation from the supervisory authority prior to the processing of personal data, in order to ensure the compliance of the intended processing with this Regulation and ***in particular*** to mitigate the risks involved for the data subjects where a controller or processor adopts contractual clauses as provided for in point (d) of Article 42(2) or does not provide for the appropriate safeguards in a legally binding instrument as referred to in Article 42(5) for the transfer of personal data to a third country or an international organisation.

2. The controller or processor acting on the controller's behalf shall consult the supervisory authority prior to the processing of personal data in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where:

(a) a data protection impact assessment as provided for in Article 33 indicates that processing operations are by virtue of their nature, their scope or their purposes, likely to present a high degree of specific risks; or

(b) the supervisory authority deems it necessary to carry out a prior consultation on processing operations that are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope and/or their purposes, and specified according to paragraph 4.

3. Where the supervisory authority is of the opinion that the intended processing does not comply with this Regulation, in particular where risks are insufficiently identified or mitigated, it shall prohibit the intended processing and make appropriate proposals to remedy such incompliance.

4. The supervisory authority shall establish and make public a list of the processing operations which are subject to prior consultation pursuant to point (b) of

1. The controller or the processor as the case may be shall obtain an authorisation from the supervisory authority prior to the processing of personal data, in order to ensure the compliance of the intended processing with this Regulation and to mitigate the risks involved for the data subjects where a controller or processor adopts contractual clauses as provided for in point (d) of Article 42(2) or does not provide for the appropriate safeguards in a legally binding instrument as referred to in Article 42(5) for the transfer of personal data to a third country or an international organisation. ***If the supervisory authority has not made a decision to grant or refuse the authorisation within three months from the date on which the request for authorisation was submitted to the supervisory authority, and one month in case a controller uses contractual clauses as provided for in point (d) of Article 42(2), the authorisation shall be deemed to be granted.***

2. deleted

(a) deleted

(b) deleted

3. Where the supervisory authority is of the opinion that the intended processing does not comply with this Regulation, in particular where risks are insufficiently identified or mitigated, it shall prohibit the intended processing and make appropriate proposals to remedy such incompliance.

4. deleted

5. deleted

6. deleted

7. Member States shall consult the supervisory authority in the preparation of a legislative measure to be adopted by the national parliament or of a measure based on such a legislative measure, which defines the nature of the processing, in order to

paragraph 2. The supervisory authority shall communicate those lists to the European Data Protection Board.

5. Where the list provided for in paragraph 4 involves processing activities which are related to the offering of goods or services to data subjects in several Member States, or to the monitoring of their behaviour, or may substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57 prior to the adoption of the list.

6. The controller or processor shall provide the supervisory authority with the data protection impact assessment provided for in Article 33 and, on request, with any other information to allow the supervisory authority to make an assessment of the compliance of the processing and in particular of the risks for the protection of personal data of the data subject and of the related safeguards.

7. Member States shall consult the supervisory authority in the preparation of a legislative measure to be adopted by the national parliament or of a measure based on such a legislative measure, which defines the nature of the processing, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects.

8. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for determining the high degree of specific risk referred to in point (a) of paragraph 2.

9. The Commission may set out standard forms and procedures for prior authorisations **and consultations** referred to in paragraphs 1 **and 2, and standard forms and procedures for informing the supervisory authorities pursuant to paragraph 6.** Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects.

8. deleted

9. The Commission may set out standard forms and procedures for prior authorisations referred to in paragraphs 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Justification

Requiring prior consultation in the case of the wide range of processing operations likely to be captured within the definition of a 'high degree of specific risks' is likely to be a serious impediment to innovation in Europe, and to overwhelm the supervisory authorities. Given the prohibition that already exists in Article 20 of profiling that

causes a significant adverse effect on a data subject, prior authorisations should be reserved for processing involving sensitive categories of data. Allowing supervisory authorities to establish an ex ante list of generic categories of data processing which it considers risky would create exactly the same risk of over-broad use of the authorisation mechanism. There must also be a time limit for the supervisory authority to deliberate and communicate a decision to authorise or not. Otherwise, controllers are subject to undue delay and inefficiencies due to inability to implement systems and tools globally or across Europe at the same time.

Our understanding is that this provision focuses on transfers and have consequently deleted the words ‘in particular’. We have maintained the references to processors in an attempt to allow them use contractual clauses for data transfers they handle on behalf of the controller.

Proposal for a regulation

Recital 74

Text proposed by the Commission

AmCham EU Amendment

(74) Where a data protection impact assessment indicates that processing operations involve a high degree of specific risks to the rights and freedoms of data subjects, such as excluding individuals from their right, or by the use of specific new technologies, the supervisory authority should be consulted, prior to the start of operations, on a risky processing which might not be in compliance with this Regulation, and to make proposals to remedy such situation. Such consultation should equally take place in the course of the preparation either of a measure by the national parliament or of a measure based on such legislative measure which defines the nature of the processing and lays down appropriate safeguards. ***(74) deleted***

Justification

Requiring prior consultation in the case of the wide range of processing operations that may qualify for a ‘high degree of specific risks’, in accordance with the long list in Article 33, is likely to be a serious impediment to innovation in Europe. DPAs could face a deluge of cases that quickly back-up and may in numerous instances have to refer those cases to the European Data Protection Board in accordance with proposed Article 58.2 (a), without there being any imposed reasonable time-limit (i.e. no longer than three months) on the supervisory authorities/European Data Protection Board to adopt any measure further to such consultation, thereby potentially bringing to a halt and crippling innovation and activities. Even if the DPAs and the European Data Protection Board had the resources to handle the case-load (quod certe non), conducting a thorough investigation is likely to be a case of months, not days. An ex-post system is far more fitting to a regime of effective and accountable data protection which does not impede growth and innovation.

Proposal for a regulation

Article 35 - Designation of the data protection officer

Text proposed by the Commission

1. The controller and the processor **shall** designate a data protection officer in any case where:

(a) the processing is carried out by a public authority or body; or

(b) the processing is carried out by an enterprise employing 250 persons or more; or

(c) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects.

2. ***In the case referred to in point (b) of paragraph 1,*** a group of undertakings may appoint a single data protection officer.

3. Where the controller or the processor is a public authority or body, the data protection officer may be designated for several of its entities, taking account of the organisational structure of the public authority or body.

4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may designate a data protection officer.

5. The controller or processor **shall** designate **the** data protection officer on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and ability to fulfil the tasks referred to in Article 37. The necessary level of expert knowledge shall be determined in particular according to the data processing carried out and the protection required for the personal data processed by the controller or the processor.

6. The controller or the processor shall ensure that any other professional duties of the data protection officer are compatible with the person's tasks and duties as data protection officer and do not result in a conflict of interests.

7. The controller or the processor shall designate a data protection officer for a period of at least two years. The data protection officer may be

AmCham EU Amendment

1. The controller and the processor **may** designate a data protection officer

(a) deleted

(b) deleted

(c) deleted

2. ***(new) Where the controller or processor designates a data protection officer in accordance with Article 35, 36 and 37, they will be exempt from Articles 28, 33 and 34. It will also be considered as a mitigating factor in assessing the application of administrative sanctions, in accordance with Article 79(2).***

2. ***Where the (joint) controller(s) or processor(s) are part of an enterprise,*** a group of undertakings may appoint a single data protection officer.

3. Where the controller or the processor is a public authority or body, the data protection officer may be designated for several of its entities, taking account of the organisational structure of the public authority or body.

4. deleted

5. ***Where the controller or processor ~~shall~~ designates ~~the a~~ data protection officer, they shall do so*** on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and ability to fulfil the tasks referred to in Article 37. The necessary level of expert knowledge shall be determined in particular according to the data processing carried out and the protection required for the personal data processed by the controller or the processor.

6. The controller or the processor shall ensure that any other professional duties of the data protection officer are compatible with the person's tasks and duties as data protection officer and do not result in

reappointed for further terms. During their term of office, the data protection officer may only be dismissed, if the data protection officer no longer fulfils the conditions required for the performance of their duties.

8. The data protection officer may be employed by the controller or processor, or fulfil his or her tasks on the basis of a service contract.

9. The controller or the processor shall communicate the name and contact details of the data protection officer to the supervisory authority and to the public.

10. Data subjects shall have the right to contact the data protection officer on all issues related to the processing of the data subject's data and to request exercising the rights under this Regulation.

11. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the core activities of the controller or the processor referred to in point (c) of paragraph 1 and the criteria for the professional qualities of the data protection officer referred to in paragraph 5.

a conflict of interests.

7. deleted

8. The data protection officer may be employed by the controller or processor, or fulfil his or her tasks on the basis of a service contract.

9. The controller or the processor shall communicate the name and contact details of the data protection officer, **if any**, to the supervisory authority and to the public.

10. Data subjects shall have the right to contact the data protection officer, **if any**, on all issues related to the processing of the data subject's data and to request exercising the rights under this Regulation.

11. deleted

Proposal for a regulation

Article 36 - Position of the data protection officer

Text proposed by the Commission

1. **The** controller or the processor shall ensure that the data protection officer is properly and in a timely manner involved in all issues which relate to the protection of personal data.

2. **The** controller or processor **shall ensure that the data protection officer performs the duties and tasks independently and does not receive any instructions as regards the exercise of the function. The data protection officer** shall directly report to the management of the controller or the processor.

3. The controller or the processor shall support the data protection officer in performing the tasks and shall provide staff, premises, equipment and any other resources necessary to carry out the duties and tasks referred to in Article 37.

AmCham EU Amendment

1. **Where the** controller or the processor **designates a data protection officer they** shall ensure that the data protection officer is properly and in a timely manner involved in all issues which relate to the protection of personal data.

2. **Where the** controller or processor **designates a data protection officer they** shall directly report to the management of the controller or the processor.

3. The controller or the processor shall support the data protection officer, **if any**, in performing the tasks and shall provide staff, premises, equipment and any other resources necessary to carry out the duties and tasks referred to in Article 37.

Proposal for a regulation

Article 37 - Tasks of the data protection officer

Text proposed by the Commission

AmCham EU Amendment

1. **The** controller or the processor shall **entrust** the data protection officer **at least with the following tasks**:

(a) to inform and advise the controller or the processor of their obligations pursuant to this Regulation and to document this activity and the responses received;

(b) to monitor the implementation and application of the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, the training of staff involved in the processing operations, and the related audits;

(c) to monitor the implementation and application of this Regulation, in particular as to the requirements related to data protection by design, data protection by default and data security and to the information of data subjects and their requests in exercising their rights under this Regulation;

(d) to ensure that the documentation referred to in Article 28 is maintained;

(e) to monitor the documentation, notification and communication of personal data breaches pursuant to Articles 31 and 32;

(f) to monitor the performance of the data protection impact assessment by the controller or processor and the application for prior authorisation or prior consultation, if required pursuant Articles 33 and 34;

(g) to monitor the response to requests from the supervisory authority, and, within the sphere of the data protection officer's competence, co-operating with the supervisory authority at the latter's request or on the data protection officer's own initiative;

(h) to act as the contact point for the supervisory authority on issues related to the processing and consult with the supervisory authority, if appropriate, on his/her own initiative.

2. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the

1. **Where the** controller or the processor **designates a data protection officer they shall determine the tasks to be performed by** the data protection officer **in order to ensure compliance with this Regulation.**

purpose of further specifying the criteria and requirements for tasks, certification, status, powers and resources of the data protection officer referred to in paragraph 1.

Proposal for a regulation

Recital 75

Text proposed by the Commission

AmCham EU Amendment

(75) Where the processing is carried out in the public sector or where, in the private sector, processing is carried out by a large enterprise, or where its core activities, regardless of the size of the enterprise, involve processing operations which require regular and systematic monitoring, a person should assist the controller or processor to monitor internal compliance with this Regulation. Such data protection officers, whether or not an employee of the controller, should be in a position to perform their duties and tasks **independently**.

(75) The controller or processor **may appoint a person to assist them in** monitoring internal compliance with this Regulation. Such data protection officers, whether or not an employee of the controller, should be in a position to perform their duties and tasks **effectively. Controllers and processors should be given an incentive to appoint such data protection officers through simplification of certain compliance obligations under this Regulation.**

Justification

Under the current Directive, the text provides for incentives for data controllers to act responsibly by providing for an exemption from the general notification regime where the controller appoints a data protection official. The Regulation should reflect this ethos by reducing the administrative burden on controllers and processors who choose to adopt a responsible approach. The controller or processor in question would still have clear obligations to establish effective policies and implement appropriate measures to demonstrate compliance with the Regulation, implement privacy by design and default, undertake effectual data security, provide transparent information to the data subjects and ensure they can apply their right. However, they would have a greater degree of flexibility and ex-ante box-ticking exercises which create a significant administrative burden without significantly increasing data protection would be reduced.

Just like with any other internal compliance roles, most organizations appoint a person in charge of data privacy compliance as a permanent role, and not subject to change or re-appointment every 2 years. It is difficult to imagine that the organization would not have a right to dismiss a data protection official for poor performance, or any other misconduct during the performance of their job. Any role, including the most senior and executive roles are subject to performance review and normal business review processes – there should be no difference for the data protection official. Regarding the independence requirement, the Data Privacy Officer is able to perform their role more effectively if they are an integral part of the business. We are concerned that the proposal to ensure complete separation of the role from the business would have the adverse effect of distancing the DPO from the business and lead to less rather than greater oversight. From a practical perspective, this may preclude many current DPOs from either company share ownership or performing this role. Finally, the tasks of the DPO should not be specified to the degree envisaged in the Commission’s proposal, but should rather be set by the organization in a such way to ensure compliance and oversight over compliance with the Regulation. It is a matter of each organization to determine what these tasks should be and what that means for their own operations, given particular business circumstances. It is expected that they would be in line with Art. 22 – the accountability model.

Proposal for a regulation

Article 77 - Right to compensation and liability

Text proposed by the Commission

1. Any person who has suffered damage as a result of **an** unlawful processing **operation** or of an action incompatible with this Regulation shall have the right to receive compensation from the controller **or the processor** for the damage suffered.
2. Where more than one controller **or processor** is involved in the processing, each controller **or processor** shall be jointly and severally liable for the entire amount of the damage.
3. The controller or the processor may be exempted from this liability, in whole or in part, if the controller or the processor proves that they are not responsible for the event giving rise to the damage.

AmCham EU Amendment

1. Any person who has suffered damage as a result of unlawful processing or of an action incompatible with this Regulation shall have the right to receive compensation from the controller for the damage suffered.
2. Where more than one controller is involved in the processing, each controller shall be jointly and severally liable for the entire amount of the damage, **to the extent that the joint controllers' respective liability has not already been established in the determination of responsibilities envisaged in Article 24.**
- 3. If a processor processes personal data for purposes other than as instructed by the controller, both parties may be held liable should any person suffer damage as a result of such processing.**
3. The controller or the processor may be exempted from this liability, in whole or in part, if the controller or the processor proves that they are not responsible for the event giving rise to the damage.

Justification

Under the current Directive, liability is correctly attributed to the data controller. Essentially, they direct the data processor and if the processor does not act on those orders then contractual arrangements apply to address the circumstances. Introducing a vague liability clause does not clarify the current situation but creates confusion for controllers, processors and data subjects alike. The joint and several liability referred to in paragraph 2 should only apply to joint controllers where they have not determined their respective responsibilities and liabilities in a legal arrangement, as required in article 24.

Proposal for a regulation

Article 91 - Application of the Regulation

Text proposed by the Commission

1. This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.
2. It shall apply from [two years from the date referred to in paragraph 1].

AmCham EU Amendment

1. This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.
2. It shall apply from [two years from the date referred to in paragraph 1] ***to new processing of personal data created on or after the date referred to in paragraph 1. Articles [24, 26, 28, 33, 34(1), 34(2)...] shall apply three years thereafter to processing of personal data existing prior to the date referred to in paragraph 1.***

Justification

The bringing into compliance of processing of personal data existing prior to the Regulation will be extremely resource- and time-consuming, especially for industries where existing processing involve literally tens of thousands of partners, thereby requiring tens of thousands of agreements to be revisited. The exact list of Articles to which the five year derogation applies depends on the final form of the adopted provisions.

5. Fines / Remedies

Proposal for a regulation

Article 79 - Administrative Sanctions

Text proposed by the Commission

1. Each supervisory authority shall be empowered to impose administrative sanctions in accordance with this Article.

2. The administrative sanction shall be in each individual case effective, proportionate and dissuasive. The amount of the administrative fine shall be fixed with due regard to the nature, gravity and duration of the breach, the intentional or negligent character of the infringement, the degree of responsibility of the natural or legal person and of previous breaches by this person, the technical and organisational measures and procedures implemented pursuant to Article 23 and the degree of cooperation with the supervisory authority in order to remedy the breach and the degree of co-operation with the supervisory authority in order to remedy the breach.

4. The supervisory authority **shall** impose a fine up to 250 000 EUR, or in case of an enterprise up to 0,5 % of its annual worldwide turnover, to anyone who, intentionally or negligently:

[...]

5. The supervisory authority **shall** impose a fine up to 500 000 EUR, or in case of an enterprise up to 1 % of its annual worldwide turnover, to anyone who, intentionally or negligently:

[...]

6. The supervisory authority **shall** impose a fine up to 1 000 000 EUR or, in case of an enterprise up to 2 % of its annual worldwide turnover, to anyone who, **intentionally or negligently**:

[...]

j) does not designate a data protection officer or does not ensure the conditions for fulfilling the

AmCham EU Amendment

1. Without prejudice to other sanctions and remedies, the lead supervisory authority shall **have the authority to** sanction the administrative offences listed in paragraphs 2 to 6.

2. The administrative sanction shall be in each individual case effective, proportionate and dissuasive. The amount of the administrative fine shall be fixed with due regard to the nature, gravity and duration of the breach, **the sensitivity of data in question**, the intentional or negligent character of the infringement, **the degree of harm or risk of significant harm created by the violation**, the degree of responsibility of the natural or legal person and of previous breaches by this person, the technical and organisational measures and procedures implemented pursuant to Article 23, **whether the natural or legal person has appointed a data protection officer in accordance with Article 35** and the degree of co-operation with the supervisory authority in order to remedy the breach. **In setting an administrative fine, supervisory authorities shall also take into account fines, damages or other penalties previously imposed by a court or other body on the natural or legal person regarding the same violation.**

2(a) Aggravating factors that support administrative fines at the upper limits established in paragraphs 2-6 shall include in particular:

(i) repeated violations committed in reckless disregard of applicable law,

(ii) refusal to co-operate with or obstruction of an enforcement process, and

(iii) violations that are deliberate, serious and likely to cause substantial damage.

tasks pursuant to Articles 35, 36 and 37;

2(b) Mitigating factors which support lower or no administrative fines at all shall include

(i) measures taken by the natural or legal person to ensure compliance with relevant obligations,

(ii) genuine uncertainty as to whether the activity constituted a violation of the relevant obligations,

(iii) immediate termination of the violation upon knowledge, and

(iv) Co-operation with any enforcement processes.

4. The **lead** supervisory authority **may** impose a fine up to 250 000 EUR, or in case of an enterprise up to 0,5 % of its annual worldwide turnover **up to a maximum of 500 000 EUR**, to anyone who, **in deliberate violation of the law or with reckless disregard for applicable obligations:**

5. The **lead** supervisory authority **may** impose a fine up to 500 000 EUR, or in case of an enterprise up to 1 % of its annual worldwide turnover **up to a maximum of 1 000 000 EUR**, to anyone who, **in deliberate violation of the law or with reckless disregard for applicable obligations:**

[...]

6. The **lead** supervisory authority **may, at its discretion**, impose a fine up to 1 000 000 EUR, or in case of an enterprise up to 2 % of its annual worldwide turnover **up to a maximum of 2 000 000 EUR**, to anyone who, **in deliberate violation of law or with reckless disregard for applicable obligations:**

[...]

[Deletion]

Justification

These amendments modify the proposal in four areas:

- *First, the amendments specify the mitigating and aggravating factors that supervisory authorities should consider when imposing fines. In doing so, the amendments ensure that higher fines are imposed on more serious misconduct, and also encourage compliance and cooperation once a violation is discovered. Specifying these factors will also promote greater consistency across the Member States in terms of the fines imposed.*

- *Second, the amendments proposes to replace the term "shall" by "may" as it relates to Supervisory Authorities. This is to avoid burdensome and bureaucratic procedures for minor infringements and to emphasize that there are circumstances under which such administrative fines would be disproportionate. It is up to the independence and discretion of the Supervisory Authority to decide how to use this sanction.*
- *Third, the amendments make it clear that where an individual or an entity has already been subject to a sanction in another proceeding for the same violation (such as a civil judgment), that fact should be considered in assessing a fine. This avoids penalizing a party twice for the same conduct.*
- *Finally, the amendments reflect the fact that while deliberate or reckless violations of the proposed Regulation should merit substantial penalties, imposing the same penalties on merely negligent violations would be disproportionate. The proposed amendments allow supervisory authorities to impose administrative fines that constitute meaningful deterrents; at the same time, these provisions ensure that the most punitive sanctions are reserved for truly bad actors.*

If the Commission nonetheless concludes that negligent conduct should also be covered in the Regulation, it's crucial to specify the language on how negligence should be assessed:

1. The supervisory authority may also impose administrative sanctions in the case of negligent violations of the provisions identified in paragraphs 4, 5 and 6. In cases of negligent violation, the administrative fine shall be set at the lower limit of the ranges established in paragraphs 4, 5 and 6, and shall take into account the criteria referred to in paragraphs 2, 2(a) and 2(b).

2. Negligent violations are those where the natural or legal person:

(i) fails to take appropriate measures to ensure that the processing of personal data is performed in compliance with its obligations;

(ii) does not commit the violation deliberately or with reckless disregard of the relevant obligations; and

(iii) in committing the violation, exposes the data subject(s) to substantial risk of harm.

The deletion in paragraph 6 relating to the data protection officer is in line with our proposed changes to Article 35, which create incentives for organisations to appoint data protection officers through a reduction in the administrative burden, as opposed to a mandatory approach. This would free resources to improve data protection throughout the organisation as opposed to focusing on mere compliance.

6. Applicable Law (One-Stop-Shop / “Main Establishment/Lead DPA/Consistency) / Governance Principles and Transparency

Proposal for a regulation
Recital 135

Text proposed by the Commission

AmCham EU Amendment

(135) This Regulation **should** apply to all matters concerning the protection of fundamental rights and freedom vis-à-vis the processing of personal data, which are not subject to specific obligations with the same objective set out in Directive 2002/58/EC, including the obligations on the controller and the rights of individuals. In order to clarify the relationship between this Regulation and Directive 2002/58/EC, the latter Directive **should** be amended accordingly.

(135) This Regulation **shall** apply to all matters concerning the protection of fundamental rights and freedom vis-à-vis the processing of personal data, which are not subject to specific obligations with the same objective set out in Directive 2002/58/EC, including the obligations on the controller and the rights of individuals. In order to clarify the relationship between this Regulation and Directive 2002/58/EC, the latter Directive **shall** be amended **by this Regulation** accordingly.

Justification

The word ‘shall’ clarifies that necessary amendments to Directive 2002/58/EC to avoid inconsistencies in the law are to be undertaken by this Regulation and not at a later stage.

Proposal for a regulation
Article 3, Paragraph 2

Text proposed by the Commission

AmCham EU Amendment

2. This Regulation applies to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are related to:

2. This Regulation applies to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are **specifically targeted at such data subjects in order** to:

(a) the offering of goods or services to such data subjects in the Union; or

(a) **offer** goods or services to **them**; or

(b) the monitoring of their behaviour.

(b) **monitor** their behaviour.

Justification

The simple availability of a foreign e-commerce website to be accessed and viewed by individuals in the EU should not in itself fall under the “offering of goods and services to EU residents”. Likewise, general web

analytics, used by the operators of websites around the globe that may be visited by individuals from the EU, should not by themselves fall under the monitoring of EU residents' behaviour. For this provision to be more relevant to the effective protection of EU data subjects' rights, it should cover those controllers whose offers or monitoring activities specifically target data subjects residing in the EU, e.g. a Korean company offering websites in multiple European languages.

One-Stop-Shop / "Main Establishment"/Lead DPA/Consistency

Proposal for a regulation

Recital 27

Text proposed by the Commission

(27) The main establishment **of a controller in the Union** should be determined according to objective **criteria and should imply the effective and real exercise of** management activities determining the main decisions as to the purposes, conditions and means of processing through stable arrangements. This criterion should not depend whether the processing of personal data is actually carried out at that location; the presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute such main establishment and are therefore no determining criteria for a main establishment. **The main establishment of the processor should be the place of its central administration in the Union.**

AmCham EU Amendment

(27) The main establishment **in the Union of an undertaking or of a group of undertakings, whether a controller, a processor or both**, should be determined according to objective **criteria, i.e. the location of the undertaking's or group's European headquarters, or the location where** management activities **are effectively exercised**, determining the main decisions as to the purposes, conditions and means of processing through stable arrangements. This criterion should not depend whether the processing of personal data is actually carried out at that location; the presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute such main establishment and are therefore no determining criteria for a main establishment.

Justification

Today, enterprises operating across the Union find themselves required to comply with multiple and often diverging national data protection regimes. This situation creates legal uncertainty and impedes the free flow of data in the Union.

The proposed Regulation seeks to improve this situation by subjecting enterprises that are processing data in the Union to a single law and a single supervisory authority in the country of "main establishment" (the so-called "one-stop-shop"). This is a significant step forward. Greater harmonisation will dramatically reduce the compliance burdens on European organisations while at the same time ensuring a high level of protection for data subjects.

Less helpful, however, in determining the location of an organisation's "main establishment," the Regulation applies a different test for controllers and processors. This approach ignores the fact that some controllers are

also processors. In these cases, it makes little sense to apply different tests. Doing so will result in these controllers once again faced with the need to comply with multiple regimes.

The amendment above takes a more sensible approach, and applies the same test to controllers and processors in those cases where the controller is also acting as a processor. This approach ensures that such controllers are fully able to benefit from the one-stop-shop that is the centrepiece of the proposed Regulation.

Proposal for a regulation

Recital 28

Text proposed by the Commission

(28) A group of undertakings should cover a controlling undertaking and its controlled undertakings, whereby the controlling undertaking should be the undertaking which can exercise a dominant influence over the other undertakings by virtue, for example, of ownership, financial participation or the rules which govern it or the power to have personal data protection rules implemented.

AmCham EU Amendment

(28) A group of undertakings should cover a controlling undertaking and its controlled undertakings, whereby the controlling undertaking should be the undertaking which can exercise a dominant influence over the other undertakings by virtue, for example, of ownership, financial participation or the rules which govern it or the power to have personal data protection rules implemented. **A group of undertakings may nominate a single main establishment in the Union.**

Justification

The amendment clarifies that a group of undertakings can be viewed as a single entity responsible to a single supervisory authority. The simplification achieved by nominating a single point of contact should not be undermined by various supervisory authorities viewing individual controlled undertakings as separate data controllers or processors.

Proposal for a regulation

Recital 63

Text proposed by the Commission

(63) Where a controller not established in the Union is processing personal data of data subjects residing in the Union whose processing activities are related to the offering of goods or services to such data subjects, or to the monitoring their behaviour, the controller should designate a

AmCham EU Amendment

(63) Where a controller not established in the Union is processing personal data of data subjects residing in the Union whose processing activities are related to the **provision** of goods or services to such data subjects, the controller should designate a representative, unless the controller

representative, unless the controller is established in a third country ensuring an adequate level of protection, or the controller is a small or medium sized enterprise or a public authority or body or where the controller is only occasionally offering goods or services to such data subjects. The representative should act on behalf of the controller and may be addressed by any supervisory authority.

is established in a third country ensuring an adequate level of protection, or the controller is a small or medium sized enterprise or a public authority or body or where the controller is only occasionally providing goods or services to such data subjects. The representative should act on behalf of the controller and may be addressed by any supervisory **authority in accordance with Article 51 of this Regulation.**

Justification

There is no justification to deny the application of the internal market approach to companies that are not established in the EU, but that name a representative in the territory of the Union. As the Regulation provisions apply, article 51 should also apply. Related to "provision" is clearer than "offering".

Proposal for a regulation

Recital 65

Text proposed by the Commission

(65) In order to demonstrate compliance with this Regulation, the controller or **processor** should document **each** processing **operation**. Each controller **and processor** should be obliged to cooperate with the supervisory authority and make this documentation, on request, available to it, so that it might serve for monitoring those processing operations.

AmCham EU Amendment

(65) In order to demonstrate compliance with this Regulation, the controller or **its representative in the Union, where applicable**, should document **the different categories of processing of personal data**. Each controller should be obliged to cooperate with the supervisory authority and make this documentation, on request, available to it, so that it might serve for monitoring those processing operations

Justification

Requiring both controllers and processors to maintain the same documentation for the same categories of processing is an unnecessary burden that does not enhance the protection of data subjects or facilitate enforcement by the authorities. The controller should be primarily responsible for maintaining the documentation in order to avoid duplication with the processor. If the processor is given an independent duty to maintain documentation, it should be different from the controller. The level of information that controllers should be required to record should be set at much more general level. To prescribe very granular and specific items to record for each processing activity, tool, system or process would create an excessive administrative burden, something which the removal of notification duties in all Member States was designed to avoid. Transparency for individuals will be provided through timely fair processing notices, so there is no obvious benefit for the individual of the sort of detailed internal register proposed here. In groups of undertakings each member of the group is often a controller in respect of at least some personal data, e.g. HR data, but in order to use the data efficiently they will all use the same tools and processes. To require each controller to maintain

documentation in relation to the same processing activity would represent a duplication and a disproportionate administrative burden. Moreover, whilst the controller should carry the primary responsibility for the documentation, it is recognised that processors can provide useful information to the controller to assist them in this task. Finally, it is important that the Regulation recognises the different responsibilities and tasks of controllers and the representative, in case of non EU based companies to whom the Regulation applies.

Proposal for a regulation
Recital 97

Text proposed by the Commission

AmCham EU Amendment

(97) Where the processing of personal data **in the context of the activities of an establishment of a controller or a processor in the Union** takes place in more than one Member State, one single supervisory authority should be competent for monitoring the activities of the controller or processor throughout the Union and taking the related decisions, in order to increase the consistent application, provide legal certainty and reduce administrative burden for such controllers and processors.

(97) Where the processing of personal data takes place in more than one Member State, one single supervisory authority should be competent for monitoring the activities of the controller or processor throughout the Union and taking the related decisions, in order to increase the consistent application, provide legal certainty and reduce administrative burden for such controllers and processors.

Justification

The draft Regulation should be clear that the one-stop shop principle applies consistently for both EU and non-EU based controllers subject to the law.

Proposal for a regulation
Recital 105

Text proposed by the Commission

AmCham EU Amendment

(105) In order to ensure the consistent application of this Regulation throughout the Union, a consistency mechanism for co-operation between the supervisory authorities themselves and the Commission should be established. This mechanism should in particular apply where a supervisory authority intends to take a measure as regards processing operations that are related to the offering of goods or services to data subjects in several Member States, **or to the** monitoring such data subjects, or that might substantially affect the free flow of personal data. It should also

(105) In order to ensure the consistent application of this Regulation throughout the Union, a consistency mechanism for co-operation between the supervisory authorities themselves and the Commission should be established. This mechanism should in particular apply where a supervisory authority intends to take a measure as regards processing operations that are related to the offering of goods or services to data subjects in several Member States, **including** monitoring such data subjects, **where the non-EU controller or processor has not appointed a representative in**

apply where any supervisory authority or the Commission requests that the matter should be dealt with in the consistency mechanism. This mechanism should be without prejudice to any measures that the Commission may take in the exercise of its powers under the Treaties.

the EU, or that might substantially affect the free flow of personal data. This mechanism should be without prejudice to any measures that the Commission may take in the exercise of its powers under the Treaties.

Justification

There is no justification to exclude the representative from the internal market rules applicable to other legal or natural persons established in the EU for the purposes of the application of this Regulation.

**Proposal for a regulation
 Article 4, Paragraph 13**

Text proposed by the Commission

AmCham EU Amendment

(13) ‘main establishment’ means as regards **the controller, the place of its establishment in the Union where** the main decisions as to the purposes, conditions and means of the processing of personal data are taken; if no decisions as to the purposes, conditions and means of the processing of personal data **are taken in the Union, the main establishment is the place where the main processing activities in the context of the activities of an establishment of a controller in the Union take place. As regards the processor, ‘main establishment’ means the place of its central administration in the Union;**

(13) ‘main establishment’ **in the Union** means as regards **an undertaking or a group of undertakings, whether controller, processor or both, the European headquarters of the undertaking or group of undertakings, or the location where effective and real management activities are exercised and/or** main decisions **are taken** as to the purposes, conditions and means of the processing of personal data.

**Proposal for a regulation
 Article 4, Paragraph 14**

Text proposed by the Commission

AmCham EU Amendment

(14) ‘representative’ means any natural or legal person established in the Union who, explicitly designated by the controller, acts and may be addressed by any supervisory authority and other bodies in the Union instead of the controller, with regard to the obligations of the controller under this Regulation;

(14) ‘representative’ means any natural or legal person established in the Union who, explicitly designated by the controller **or the processor**, acts instead of the **controller or the processor**, with regard to the obligations of the controller **or the processor** under this Regulation;

Justification

There is no justification to exclude the representative from the internal market rules applicable to other legal or natural persons established in the EU for the purposes of the application of this Regulation.

Proposal for a regulation
Article 4 paragraph 19 (a) (new)

Text proposed by the Commission

AmCham EU Amendment

19(a) (new) ‘lead supervisory authority’ means the supervisory authority of the main establishment of the controller or processor in accordance with article 51 paragraph 2.

Justification

This new definition is meant to bring clarity as to the effective implementation of the “one-stop shop” concept referred to in recital 98.

Proposal for a regulation
Article 12, Paragraph 3

Text proposed by the Commission

AmCham EU Amendment

3. If the controller refuses to take action on the request of the data subject, the controller shall inform the data subject of the reasons for the refusal and on the possibilities of lodging a complaint to the supervisory authority and seeking a judicial remedy.

3. If the controller refuses to take action on the request of the data subject, the controller shall inform the data subject of the reasons for the refusal and on the possibilities of lodging a complaint to the **lead** supervisory authority and seeking a judicial remedy.

Justification

This amendment is meant to effectively implement the “one-stop shop” concept referred to in recital 98.

Proposal for a regulation
Article 15, Paragraph 1 (f)

(f) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority;

(f) the right to lodge a complaint to the **lead** supervisory authority and the contact details of the **lead** supervisory authority;

Justification

This amendment is meant to clarify the implementation of the “one-stop shop” concept referred to in recital 98.

Proposal for a regulation
Article 29

Text proposed by the Commission

AmCham EU Amendment

1. The controller and the processor and, if any, the

1. The controller and the processor and, if any, the

representative of the controller, shall co-operate, on request, with the supervisory authority in the performance of its duties, in particular by providing the information referred to in point (a) of Article 53(2) and by granting access as provided in point (b) of that paragraph.

2. In response to the supervisory authority's exercise of its powers under Article 53(2), the controller and the processor shall reply to the supervisory authority within a reasonable period to be specified by the supervisory authority. The reply shall include a description of the measures taken and the results achieved, in response to the remarks of the supervisory authority.

representative of the controller, shall co-operate, on request, with the **lead** supervisory authority in the performance of its duties, in particular by providing the information referred to in point (a) of Article 53(2) and by granting access as provided in point (b) of that paragraph.

2. In response to the **lead** supervisory authority's exercise of its powers under Article 53(2), the controller and the processor shall reply to the supervisory authority within a reasonable period to be specified by the supervisory authority. The reply shall include a description of the measures taken and the results achieved, in response to the remarks of the supervisory authority.

Justification

This provision is meant to clarify the implementation of the "one-stop shop" concept referred to in recital 98.

**Proposal for a regulation
 Article 31, Paragraph 1**

Text proposed by the Commission

1. In the case of a personal data breach, the controller shall without undue delay **and, where feasible, not later than 24 hours** after having **become aware of it**, notify the personal data breach to **the** supervisory authority. **The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within 24 hours.**

Justification

This provision is meant to clarify the implementation of the "one-stop shop" concept referred to in recital 98.

**Proposal for a regulation
 Article 32, Paragraphs 3 and 4**

Text proposed by the Commission

3. The communication of a personal data breach to the data subject shall not be required if the controller demonstrates to the satisfaction of the supervisory authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the personal data breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it.

AmCham EU Amendment

1. In the case of a personal data breach **that is likely to lead to significant risk of substantial harm to a data subject**, the controller shall without undue delay after having **confirmed that a personal breach has occurred**, notify the personal data breach to **its lead** supervisory authority.

AmCham EU Amendment

3. The communication of a personal data breach to the data subject shall not be required if the controller demonstrates to the satisfaction of the **lead** supervisory authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the personal data breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it.

4. Without prejudice to the controller's obligation to communicate the personal data breach to the data subject, if the controller has not already communicated the personal data breach to the data subject of the personal data breach, the supervisory authority, having considered the likely adverse effects of the breach, may require it to do so.

4. Without prejudice to the controller's obligation to communicate the personal data breach to the data subject, if the controller has not already communicated the personal data breach to the data subject of the personal data breach, the **lead** supervisory authority, having considered the likely adverse effects of the breach, may require it to do so.

Justification

This provision is meant to clarify the implementation of the “one-stop shop” concept referred to in recital 98.

Proposal for a regulation

Article 39, Paragraph 9

Text proposed by the Commission

AmCham EU Amendment

9. The controller or the processor shall communicate the name and contact details of the data protection officer to the supervisory authority and to the public.

9. The controller or the processor shall communicate the name and contact details of the data protection officer to the **lead** supervisory authority and to the public.

Justification

This provision is meant to clarify the implementation of the “one-stop shop” concept referred to in recital 98.

Proposal for a regulation

Article 43, Paragraphs 2 (j) and (k)

Text proposed by the Commission

AmCham EU Amendment

(j) the mechanisms for reporting and recording changes to the policies and reporting these changes to the supervisory authority;

(j) the mechanisms for reporting and recording changes to the policies and reporting these changes to the **lead** supervisory authority;

(k) the co-operation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings, in particular by making available to the supervisory authority the results of the verifications of the measures referred to in point (i) of this paragraph.

(k) the co-operation mechanism with the **lead** supervisory authority to ensure compliance by any member of the group of undertakings, in particular by making available to the **lead** supervisory authority the results of the verifications of the measures referred to in point (i) of this paragraph.

Justification

This provision is meant to clarify the implementation of the “one-stop shop” concept referred to in recital 98.

Proposal for a regulation

Article 43, Paragraphs 3

Text proposed by the Commission

AmCham EU Amendment

3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for binding corporate rules within the meaning of this Article, in particular as regards the criteria for their approval, the application of points (b), (d), (e) and (f) of paragraph 2 to binding corporate rules adhered to by processors and on further necessary requirements to ensure the protection of personal data of the data subjects concerned.

3. Where a processor wishes to provide appropriate safeguards by binding corporate rules as referred to in point (a) of paragraph 2 of Article 42, the matters referred to in points (a) to (k) of paragraph 2:

(a) shall only apply to the extent they are applicable to the processor and are material to the data subject and

(b) can be specified in relation to each controller.

Justification

This provision is meant to clarify the implementation of the “one-stop shop” concept referred to in recital 98.

**Proposal for a regulation
 Article 44, Paragraph 6**

Text proposed by the Commission

6. The controller or processor shall document the assessment as well as the appropriate safeguards adduced referred to in point (h) of paragraph 1 of this Article in the documentation referred to in Article 28 and shall inform the supervisory authority of the transfer.

AmCham EU Amendment

6. The controller or processor shall document the assessment as well as the appropriate safeguards adduced referred to in point (h) of paragraph 1 of this Article in the documentation referred to in Article 28 and shall inform the **lead** supervisory authority of the transfer.

Justification

This provision is meant to clarify the implementation of the “one-stop shop” concept referred to in recital 98.

**Proposal for a regulation
 Article 52, Paragraph 1 (b)**

Text proposed by the Commission

(b) hear complaints lodged by any data subject, or by an association representing that data subject in accordance with Article **73**, **investigate**, to the extent **appropriate**, the **matter** and inform the data subject or the association of the progress and the outcome of the complaint within a reasonable period, in particular if further **investigation or** coordination with another supervisory authority is necessary;

AmCham EU Amendment

(b) hear complaints lodged by any data subject, or by an association representing that data subject in accordance with Article **73**;, to the extent **that it has competence in accordance with article 51 paragraph 2, investigate** the **matter**; **or, if it does not have competence, refer the matter in accordance with the provisions of Section 1 of Chapter VII to the lead supervisory authority**; and inform the data subject or the association of the progress and the outcome of the complaint within a reasonable period, in particular if further **investigation**, coordination with **or referral to** another supervisory authority is necessary;

Justification

This provision is essential to conciliate the right of data subjects or of their representatives and associations to lodge complaints with the authority of their choice on the one hand, and the concept of one lead authority for each controller or processor on the other hand.

Proposal for a regulation

Article 53

Text proposed by the Commission

AmCham EU Amendment

(paragraph 1)

(paragraph 1 unchanged)

1(a) (new) Powers referred to in points (a) to (h) of paragraph 1 are conferred upon the lead supervisory authority in accordance with article 51 paragraph 2. A supervisory authority that is not the lead supervisory authority in the meaning of article 51 paragraph 2 may in accordance with Section 1 of Chapter VII request the lead supervisory authority to exercise such powers in relation to a controller or processor under that supervisory authority's competence:

2. Each supervisory authority shall have the investigative power to obtain from the controller or the processor:

2. Each supervisory authority shall have the investigative power to obtain from the controller or the processor ***under its competence in accordance with article 51 paragraph 2:***

Justification

This provision is essential to clarify the implementation of the “one-stop shop” concept referred to in recital 98.

Proposal for a regulation
Article 58, Paragraphs 2, 3 and 4

Text proposed by the Commission

2. The obligation set out in paragraph 1 shall apply to a measure intended to produce legal effects and which:

(a) relates to processing activities which are related to the offering of goods or services to data subjects in several Member **States, or to the monitoring of their behaviour;** or

(b) may substantially affect the free movement of personal data within the **Union; or**

(c) aims at adopting a list of the processing operations subject to prior consultation pursuant to Article 34(5); or

(d) aims to determine standard data protection clauses referred to in point (c) of Article 42(2); or

(e) aims to authorise contractual clauses referred to in point (d) of Article 42(2); or

(f) aims to approve binding corporate rules within the meaning of Article 43.

3. Any supervisory authority or the European Data Protection Board may request that any matter shall be dealt with in the consistency mechanism, **in particular** where a supervisory authority does not submit a draft measure referred to in paragraph 2 or does not comply with the obligations for mutual assistance in accordance with Article 55 or for joint operations in accordance with Article 56.

4. In order to ensure correct and consistent application of this Regulation, the Commission may request that any matter shall be dealt with in the consistency mechanism.

AmCham EU Amendment

2. The obligation set out in paragraph 1 shall apply to a measure intended to produce legal effects and which:

(a) relates to processing activities **of personal data including the monitoring of behaviour** which are related to the offering of goods or services to data subjects in several Member **States when the non-EU controller or processor does not name a representative in the territory of the European Union;** or

(b) may substantially affect the free movement of personal data within the **Union.**

(c) deleted

(d) aims to determine standard data protection clauses referred to in point (c) of Article 42(2); or

(e) aims to authorise contractual clauses referred to in point (d) of Article 42(2); or

(f) Deleted

3. Any supervisory authority or the European Data Protection Board may request that any matter shall be dealt with in the consistency mechanism where a supervisory authority does not submit a draft measure referred to in paragraph 2 or does not comply with the obligations for mutual assistance in accordance with Article 55 or for joint operations in accordance with Article 56.

4. deleted

Justification

There is no justification to discriminate against non- EU companies that are covered by the Regulation, by automatically applying the consistency mechanism to these companies. Where the non EU company names a representative in the EU, there is no need to submit these companies to the data protection board in all circumstances. The competence of the data protection board to non- EU companies that are entirely covered by

the Regulation should be equivalent to EU companies. If the non EU company does not name a representative, it is justified. Please see also comments on point 3. The list of processing operations subject to prior consultation should be determined in the regulation and not left to DPAs, because that in itself leads to inconsistency (each DPA naming different lists). The consistency mechanism needs to be an exceptional mechanism and not a body of appeal of legitimate decisions of the lead DPA. Otherwise the consistency mechanism becomes an appeal mechanism that slows decision taking and becomes a bureaucratic step in detriment of all actors.

Proposal for a regulation
Article 86, Paragraph 2

Text proposed by the Commission

AmCham EU Amendment

2. The delegation of power referred to in **Article 8(3), Article 9(3), Article 12(5), Article 14(7), Article 15(3), Article 17(9), Article 20(5), Article 22(4), Article 23(3), Article 26(5), Article 28(5), Article 30(3), Article 31(5), Article 32(5), Article 33(6), Article 34(8), Article 35(11), Article 37(2), Article 39(2), Article 43(3), Article 44(7), Article 79(7),¹** Article 81(3), Article 82(3) and Article 83(3) shall be conferred on the Commission for an indeterminate period of time from the date of entry into force of this Regulation.

2. The delegation of power referred to in Article 12(5), Article 14(7), Article 15(3), Article 23(3), Article 81(3), Article 82(3) and Article 83(3) shall be conferred on the Commission for an indeterminate period of time from the date of entry into force of this Regulation.

Proposal for a regulation
Article 86, Paragraph 3

Text proposed by the Commission

AmCham EU Amendment

3. The delegation of power referred to in **Article 8(3), Article 9(3), Article 12(5), Article 14(7), Article 15(3), Article 17(9), Article 20(6), Article 22(4), Article 23(3), Article 26(5), Article 28(5), Article 30(3), Article 31(5), Article 32(5), Article 33(6), Article 34(8), Article 35(11), Article 37(2), Article 39(2), Article 43(3), Article 44(7), Article 79(7),** Article 81(3), Article 82(3) and Article 83(3) may be revoked at any time by the European Parliament or by the Council. A decision of revocation shall put an end to the delegation of power specified in that decision. It shall take effect the day following the publication of the decision in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

3. The delegation of power referred to in Article 12(5), Article 14(7), Article 15(3), Article 23(3), Article 81(3), Article 82(3) and Article 83(3) may be revoked at any time by the European Parliament or by the Council. A decision of revocation shall put an end to the delegation of power specified in that decision. It shall take effect the day following the publication of the decision in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

¹ Note that this Article is mis-cited in the proposed Regulation as Article 79(6). The correct reference is to Article 79(7).

Proposal for a regulation
Article 86, Paragraph 4

Text proposed by the Commission

4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

AmCham EU Amendment

4. **The Commission shall present proposals for delegated acts to be adopted pursuant to Article 12(5), Article 14(7), Article 15(3), Article 23(3), Article 81(3), Article 82(3) and Article 83(3) within two years of the date of publication of this Regulation in the Official Journal of the European Union.** As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

Proposal for a regulation
Article 86, Paragraph 5

Text proposed by the Commission

5. A delegated act adopted pursuant to **Article 8(3), Article 9(3), Article 12(5), Article 14(7), Article 15(3), Article 17(9), Article 20(6), Article 22(4), Article 23(3), Article 26(5), Article 28(5), Article 30(3), Article 31(5), Article 32(5), Article 33(6), Article 34(8), Article 35(11), Article 37(2), Article 39(2), Article 43(3), Article 44(7), Article 79(7)**, Article 81(3), Article 82(3) and Article 83(3) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or the Council.

AmCham EU Amendment

5. A delegated act adopted pursuant to Article 12(5), Article 14(7), Article 15(3), Article 23(3), Article 81(3), Article 82(3) and Article 83(3) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or the Council.

Justification

Of the 91 articles in the Regulation, 26 include provisions that would allow the Commission to adopt “delegated acts.” Each delegated act provision empowers the Commission to create new, secondary legal regimes, binding across the EU.

The many delegated act provisions mean that organisations could face new rules for many years after the Regulation is adopted. This creates confusion about data subjects’ rights. It also makes it difficult for organisations processing data to understand their obligations. Because the Regulation includes substantial sanctions for non-compliance (up to 2% of annual worldwide turnover for certain violations), it is critical that organisations understand clearly what their obligations are.

To address these issues, the number of delegated acts should be significantly reduced. Delegated acts should be used only where needed and appropriate. Specifically:

- 1. Consistent with the Lisbon Treaty, any delegated act provisions that deal with essential elements of the law should be deleted.** Many of the delegated act provisions -- including Article 9(3), Article 22(4), Article 26(5), Article 31(5), Article 32(5), Article 33(6), Article 34(8), Article 43(3), Article 44(7) and Article 79(7) -- address essential elements of the data protection framework. However, under the Lisbon Treaty, delegated acts are intended to supplement “non-essential elements” of the Law. Essential issues should be addressed in the Regulation, not deferred until a later date. Allowing the Commission to defer legislating on essential elements of the law undermines legal certainty and makes it difficult for companies to plan for compliance. These Articles should be deleted.
- 2. Consistent with EU policy, those delegated acts that allow the Commission to dictate how technologies should be developed should also be deleted.** Certain delegated acts provisions -- including Article 8(3), Article 17(9) and Article 30(3) -- threaten to undermine the principle of technology neutrality by allowing the Commission to adopt prescriptive rules, standards and formats. Technology neutrality is well established in European law and policy. Technology neutral policies allow for competition among different solutions, which in turn drives innovation. At the same time, technology neutrality ensures that legislation is not “frozen in time,” as technology evolves. But by allowing the Commission to dictate how obligations should be implemented at a technical level, these provisions give the Commission the power to substitute regulatory intervention for industry innovation. Again, these Articles should be deleted.
- 3. Delegated acts that remain in the Regulation should be subject to a clear timetable for adoption.** Without a clear timeline for the adoption of delegated acts, controllers, processors and data subjects could face a lengthy period of uncertainty about their obligations and their rights. The Article 29 Working Party has acknowledged this concern, stating in its Opinion on the proposal that “At the very least the Working Party calls on the Commission to set out which delegated acts it intends to adopt in the short, medium and long term.”

[Corresponding amendments will need to be made to Recital 129 and Recital 131 and Article 6(5), Article 8(3), Article 9(3), Article 17(9), Article 20(5), Article 22(4), Article 26(5), Article 28(5), Article 30(3), Article 31(5), Article 32(5), Article 33(6), Article 34(8), Article 35(11), Article 37(2), Article 39(2), Article 43(3), Article 44(7), and Article 79(7).]

Governance Principles and Transparency

Proposal for a regulation

Recital 61

Text proposed by the Commission

(61) **The** protection of the rights and freedoms of data subjects with regard to the processing of personal data require that appropriate technical and organisational measures **are** taken, both at the time of the design of the processing and at the time of the processing itself, to ensure that the requirements of this Regulation are met. **In order to ensure and demonstrate compliance with this Regulation, the controller should adopt internal policies and implement appropriate measures, which meet in particular the principles of data protection by design and data protection by default.**

Proposal for a regulation

Recital 110 (a) (new)

Text proposed by the Commission

Justification
Consistency with the new Article 70(a) proposed below.

AmCham EU Amendment

(61) **To meet consumer and business expectations around the** protection of the rights and freedoms of data subjects with regard to the processing of personal data, appropriate organisational measures **may be** taken, both at the time of the design of the processing and at the time of the processing itself, to ensure that the requirements of this Regulation are met. **Measures having as an objective to increase consumer information and ease of choice shall be encouraged, based on industry cooperation and favouring innovative solutions, products and services.**

(110) (a) The European Data Protection Board should have a Permanent Stakeholders' Group as an advisory body, to ensure regular dialogue with the private sector, data subjects' associations, consumer organisations and other relevant stakeholders. The Permanent Stakeholders' Group, set up by the Board on a proposal by the Chair, should focus on issues relevant to all stakeholders and bring them to the attention of the Board. The Chair may, where appropriate and according to the agenda of the meetings, invite representatives of the European Parliament and other relevant bodies to take part in meetings of the Group.

Proposal for a regulation

Recital 129

Text proposed by the Commission

(129) In order to fulfil the objectives of this Regulation, namely to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal ***data and to ensure the free movement of personal data within the Union, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the Commission. In particular, delegated acts should be adopted in respect of [...] criteria and requirements in relation to the responsibility of the controller and to data protection by design and by default;***

AmCham EU Amendment

(129) In order to fulfil the objectives of this Regulation, namely to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data, ***appropriate industry lead measures and policies shall take due account of the principles of technology, service and business model neutrality so as to favour the free movement of personal data within the Union.***

Proposal for a regulation

Recital 130

Text proposed by the Commission

(130) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission for: specifying standard forms in relation to the processing of personal data of a child; standard procedures and forms for exercising the rights of data subjects; standard forms for the information to the data subject; standard forms and procedures in relation to the right of access; the right to data portability; standard forms in relation to the responsibility of the controller to data protection by design and by default and to the documentation; specific requirements for the security of processing; the standard format and the procedures for the notification of a personal data breach to the supervisory authority and the communication of a personal data breach to the data subject; standards and procedures for a data protection impact assessment; forms and procedures for prior authorisation and prior consultation; technical standards and mechanisms for certification; the adequate level of protection afforded by a third country or a territory or a processing sector within that third country or an international organisation; disclosures not authorized by Union law; mutual assistance; joint operations; decisions under the consistency mechanism. Those powers should be exercised in accordance with Regulation (EU) No

AmCham EU Amendment

(130) In implementing the provisions of this Regulation, it shall be ensured that no mandatory requirements for specific technical features are imposed on products and services, including terminal or other electronic communications equipment, which could impede the placing of equipment on the market and the free circulation of such equipment in and between Member States.

182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers. In this context, the Commission should consider specific measures for micro, small and medium-sized enterprises.

**Proposal for a regulation
 Article 23**

Text proposed by the Commission

1. Having regard to the state of the art and the cost of implementation, ***the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures and procedures in such a way that the processing will meet*** the requirements of this Regulation and ensure the protection of the rights of the data subject.

2. The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals.

3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures and mechanisms referred to in paragraph 1 and 2, in particular for data protection by design requirements applicable across sectors, products and services.

4. The Commission may lay down technical standards for the requirements laid down in paragraph 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

AmCham EU Amendment

1. Having regard to the state of the art, the cost of implementation ***and international best practices, appropriate measures and procedures may be put in place to ensure the processing operation meets*** the requirements of this Regulation and ensures the protection of the rights of the data subject.

2. Such measures and procedures shall:

- ***take due account of existing technical standards and regulations in the area of public safety and security***
- ***follow the principle of technology, service and business model neutrality***
- ***be based on global industry-led efforts and standards***
- ***take due account of international developments***

3. In implementing the provisions of this Regulation, it shall be ensured that no mandatory requirements for specific technical features are imposed on products and services, including terminal or other electronic communications equipment, which could impede the placing of equipment on the market and the free circulation of such equipment in and between Member States.

4. Where required, measures may be adopted to ensure that terminal equipment is constructed in a way that is compatible with Council Decision 87/95/EEC of 22 December 1986 on standardisation in the field of information technology and

communications, and consistent with international industry-led standardisation efforts.

Justification

Privacy by Design/Default (PbD) is a concept currently being discussed internationally, relating to internal privacy and data protection processes for organizations based on a number of factors including their business models, size and interaction with personal data. Although every organisation should strive to integrate privacy and data protection into its internal processes, the actual way it does so should remain flexible and leave room for adaptation based on their business models, size and interaction with personal data. This is to say that there is no one right way which is especially true in the case of SMEs, given their specific circumstances and for entities that are far removed from processing identifiable personal data. It is essential that any PbD concept be technology-neutral and not introduce specific technology or operational mandates, or contribute to a differentiation between ICT and other economic sectors. The concept should therefore focus on designing privacy into processes and people and should maintain as a key objective providing consumers with appropriate tools to make an informed choice. Industry-led innovation in this area will create trust and allow for innovative solutions, services and technologies to flourish in the spirit of the European Digital Agenda. There is also a clear need to look into the issue with a global perspective to avoid further fragmentation, taking stock of industry's own efforts and taking technology developments into account.

Proposal for a regulation

Article 70 paragraph 1 point (aa) (new) - Permanent Stakeholders' group

Text proposed by the Commission

AmCham EU Amendment

(aa) convene the meetings of the Permanent Stakeholders' Group and prepare its agenda;

Justification

Consistency with the new Article 70a proposed below.

Proposal for a regulation
Article 70(a) (new) - Permanent Stakeholders' Group

Text proposed by the Commission

AmCham EU Amendment

1. The European Data Protection Board shall set up a Permanent Stakeholders' Group on a proposal by the Chair, composed of experts representing the relevant stakeholders, such as but not limited to relevant private sector players, data subjects' associations, consumer groups and academic experts in privacy and data protection.

2. Procedures for, in particular, the number, composition, and appointment of the members by the Board, proposal by the Chair and the operation of the Group shall be specified in the Board's internal rules of operation and shall be made public.

3. The Group shall be chaired by the Chair of the Board.

4. The term of office of the Group's members shall be two-and-a-half years. Members of the Board may not be members of the Group. Commission staff shall be entitled to be present at the meetings and participate in the work of the Group.

5. The Group shall advise the Board in the performance of its activities and tasks.

Justification

Like data controllers and processors, the EDPB should also be accountable and transparent in guiding the interpretation and enforcement of the regulatory framework. The consultation and decision making mechanism proposed here is meant to ensure that the Board and supervisory authorities pursue an ongoing transparent dialogue with all interested stakeholders, including the private sector, data subjects, and academia, for the shared benefit of all involved parties.

Proposal for a regulation
Article 71, Paragraph 3

Text proposed by the Commission

AmCham EU Amendment

3. The secretariat shall be responsible in particular for:

(a) the day-to-day business of the European Data Protection Board;

3. The secretariat shall be responsible in particular for:

(a) the day-to-day business of the European Data Protection Board;

(b) the communication between the members of the European Data Protection Board, *its chair* and the Commission and for communication with other institutions and the public;

(c) the use of electronic means for the internal and external communication;

(d) the translation of relevant information;

(e) the preparation and follow-up of the meetings of the European Data Protection **Board**;

(f) the preparation, drafting and publication of opinions and other texts adopted by the European Data Protection **Board**.

(b) the communication between the members of the European Data Protection Board, **the members of the Permanent Stakeholder Group, the Chair** and the Commission and for communication with other institutions and the public;

(c) the use of electronic means for the internal and external communication;

(d) the translation of relevant information;

(e) the preparation and follow-up of the meetings of the European Data Protection **Board and of the Permanent Stakeholders' Group**;

(f) the preparation, drafting and publication of opinions and other texts adopted by the European Data Protection **Board, as well as of documents of the Permanent Stakeholders' Group**.

Justification

Consistency with the new Article 70(a) proposed above.

Proposal for a regulation Article 72 - Confidentiality and publicity

Text proposed by the Commission

1. The discussions of the European Data Protection Board shall be **confidential**.

2. Documents submitted to members of the European Data Protection Board, experts and representatives of third parties shall be confidential, unless access is granted to those documents in accordance with Regulation (EC) No 1049/2001 or the European Data Protection Board otherwise makes them public.

3. The members of the European Data Protection Board, as well as experts and representatives of third parties, shall be required to respect the

AmCham EU Amendment

1. The discussions of the European Data Protection Board shall **only be confidential in so far as and to the extent that they relate to specific cases. Discussions pursuant to the carrying out of the tasks of general interest laid down in points (a), (b), (c), (e),(f) and (g) of paragraph 1 of Article 66, as well as, to the extent that they do not relate to specific cases, the discussions pursuant to the adoption of opinions under the consistency mechanism in accordance with Article 58 shall be public.**

2. Documents **relating to specific cases** submitted to members of the European Data Protection Board, experts and representatives of third parties shall be confidential, unless access is granted to those documents in accordance with Regulation (EC) No 1049/2001 or the European Data Protection Board otherwise makes them public.

3. The members of the European Data Protection Board, as well as experts and representatives of third parties, shall be required to respect the

confidentiality obligations set out in this Article. The chair shall ensure that experts and representatives of third parties are made aware of the confidentiality requirements imposed upon **them**.

confidentiality obligations set out in this Article. The chair shall ensure that experts and representatives of third parties are made aware of the confidentiality requirements imposed upon **them where applicable**. **The chair shall also ensure the appropriate publicity of discussions not falling under a confidentiality requirement.**

Justification

The EDPB has a major advisory and interpretation role with respect to the general privacy regime and its implementation. Data subjects, data controllers, data processors, representatives of the European and national legislators, as well as supervisory authorities themselves and all other relevant stakeholders should have the opportunity to be informed of the discussions of general interest and general relevance that will be pursued in the EDPB.

7. Certification / Codes of Conduct

Proposal for a regulation

Article 38

Text proposed by the Commission

1. The Member States, the supervisory authorities and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the **proper application of this Regulation, taking account of the specific features of the various data processing sectors, in particular in relation to:**

(a) fair and transparent data processing;

(b) the collection of data;

(c) the information of the public and of data subjects;

(d) requests of data subjects in exercise of their rights;

(e) information and protection of children;

(f) transfer of data to third countries or international organisations;

(g) mechanisms for monitoring and ensuring compliance with the code by the controllers adherent to it;

(h) out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with respect to the processing of personal data, without prejudice to the rights of the data subjects pursuant to Articles 73 and 75.

2. Associations and other bodies representing categories of controllers or processors in one Member State **which intend to draw up** codes of conduct or **to amend or extend** existing codes of conduct **may submit them** to an opinion of the supervisory authority in that Member State. The supervisory authority may give **an** opinion whether the draft code of conduct or the amendment is **in compliance** with this Regulation. The supervisory authority shall seek the views of **data subjects or their representatives** on these **drafts**.

3. Associations and other bodies representing categories of controllers in several Member States may submit **draft** codes of conduct and amendments or extensions to existing codes of conduct to the

AmCham EU Amendment

1. The Member States, the supervisory authorities and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the **protection of personal data or to compliance with this Regulation. Particular encouragement shall be given to European-level codes of conduct.**

2. Associations and other bodies representing categories of controllers or processors in one Member State **may submit new** codes of conduct or **amendments** or **extensions to** existing codes of conduct to an opinion of the supervisory authority in that Member State **on a voluntary basis**. The supervisory authority may give **a non-binding** opinion **on** whether the draft code of conduct or the amendment **or the extension contributes to the protection of personal data or to compliance** with this Regulation. The supervisory authority may seek the views of **all stakeholders** on these **codes, in which case it shall deliver its opinion within 90 days**.

3. Associations and other bodies representing categories of controllers in several Member States may submit **new** codes of conduct and amendments or extensions to existing codes of conduct to the

Commission.

4. The Commission may adopt implementing acts for deciding that the codes of conduct and amendments or extensions to existing codes of conduct submitted to it pursuant to paragraph 3 have general validity within the Union. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).

5. The Commission shall ensure appropriate publicity for the codes which have been decided as having general validity in accordance with paragraph 4.

Proposal for a regulation
Article 39 - Certification

1. The Member States and the Commission shall encourage, in particular at European level, the establishment of data protection certification mechanisms and of data protection seals and marks, allowing data subjects to quickly assess the level of data protection provided by controllers and processors. The data protection certifications mechanisms shall contribute to the proper application of this Regulation, taking account of the specific features of the various sectors and different processing operations.

2. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the data protection certification mechanisms referred to in paragraph 1, including conditions for granting and withdrawal, and requirements for recognition within the Union and in third countries.

3. The Commission may lay down technical standards

Commission. *These initiatives should be fully in line with existing legal obligations and not aim at preventing the free circulation of goods and services in the internal market.*

4. The Commission may adopt **non-binding opinions on whether** the codes of conduct and amendments or extensions to existing codes of conduct submitted to it pursuant to paragraph 3 **contribute to the protection of personal data, or are compatible with this Regulation, or contribute to compliance with it. In addition, the Commission's opinions shall consider whether the codes of conduct contribute to the functioning of the Internal Market. The Commission shall seek the views of all stakeholders on these codes, and shall deliver its opinion within 90 days.**

4(a) (new) The opinions of the supervisory authorities and of the Commission pursuant to paragraphs 2 and 4 shall be a separate matter from formal determinations of individual operators' compliance with the law.

5. The Commission shall ensure appropriate publicity for the codes which have been **the subject of positive opinions in accordance with paragraph 4(a) (new).**

1. The Member States and the Commission shall **work with controllers, processors and other stakeholders to** encourage **voluntary** data protection certification mechanisms and data protection seals and marks, allowing data subjects to quickly assess the level of data protection provided by controllers and processors. **Such** mechanisms shall, in cases where clear legal obligations do not exist:

- **be voluntary, affordable, and available via a process that is transparent and not unduly burdensome**
- **take due account of existing security measures and regulations in the area of public safety and security**
- **follow the principle of technology, service and business model neutrality**
- **be elaborated in consultation with the Member States Data Protection Authorities**
- **be based on industry lead efforts and standards**
- **take due account of international developments**

for certification mechanisms and data protection seals and marks and mechanisms to promote and recognize certification mechanisms and data protection seals and marks. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).

2. (Based on Article 14 of the ePrivacy Directive) - In implementing the provisions of this Regulation, Member States shall ensure, that no mandatory requirements for specific technical features are imposed on products and services, including terminal or other electronic communication equipment which could impede the placing of equipment on the market and the free circulation of such equipment in and between Member States.

3. Where required, measures may be adopted to ensure that terminal equipment is constructed in a way that is compatible with the right of users to protect and control the use of their personal data, in accordance with Directive 1999/5/EC and Council Decision 87/95/EEC of 22 December 1986 on standardisation in the field of information technology and communications and consistent with international industry lead standardisation efforts.

4. National data protection authorities [N.B. or the EU board, if it is going to be created] shall be the repositories of such data protection certification mechanisms and data protection seals and marks, thus providing for easy access for citizen.

Justification

Industry- developed and managed certification should be favoured, provided they remain voluntary and affordable. Such certifications should be open to companies both inside and outside the EEA in order to facilitate international data flows and be elaborated in consultation with the relevant stakeholders. They should enable competition and be industry driven and favor innovative solutions for the consumers. Indeed, industry is able to adapt to new market realities at a faster pace than government, and government does not have the same competitive incentive to enforce proper use of certifications (e.g. icons or seals on web pages) as industry does. In the long term, an industry-developed and managed certification that is endorsed by both EU and non-EU regulators would help reduce compliance burdens on operators and foster competitiveness. Certification mechanisms shall however not be used to create discrimination between sectors or value chains. Specifically, certification schemes would need to:

- **Be based on industry lead standards and practices.**
- **Be developed with stakeholder input at EU level.** To help create effective schemes and encourage widespread adoption, Member States and the Commission should work with stakeholders to establish the process of developing EU level certifications, seals and marks.
- **Be voluntary.** Mandatory certification schemes can chill innovation and deter competition in the development of enhanced privacy protections.
- **Be affordable.** Some privacy certification regimes involve costs of upwards of €150,000 simply to certify one feature of a product or service. These costs create barriers to entry for all but the largest service providers, and discourage wide-scale use of the regime.
- **Be available via a process that is transparent and not unduly burdensome.** To ensure organisations apply for and adopt certifications, seals and marks that give individuals confidence about how their data is being processed, the process to apply for and be awarded a mark should not be unduly bureaucratic or burdensome.

- Be capable of being **rolled-out and recognised globally**. To help reduce the compliance burden on providers, any certification scheme should be capable of being endorsed by regulators in third countries as well as by those in the Union.
- Be **neutral** as to system, service, platform or technology. Similarly situated services and products should be subject to the same assessment criteria. Favouring some solutions over others creates market distortions and hinders innovation.

8. International Data Transfers / BCRs / Safe Harbor

Proposal for a regulation

Article 42, Paragraph 1

Text proposed by the Commission

1. Where the Commission has taken no decision pursuant to Article 41, a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has adduced appropriate safeguards with respect to the protection of personal data in a legally binding instrument.

AmCham EU Amendment

1. Where the Commission has taken no decision pursuant to Article 41, **or has not taken a positive decision pursuant to Article 41(3)** a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has adduced appropriate safeguards with respect to the protection of personal data in a legally binding instrument.

Proposal for a regulation

Article 42, Paragraph 2 (b) and (c)

Text proposed by the Commission

2. The appropriate safeguards referred to in paragraph 1 shall be provided for, in particular, by: ...

(b) standard data protection clauses adopted by the Commission. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2); or

(c) standard data protection clauses adopted by a supervisory authority in accordance with the consistency mechanism referred to in Article 57 when declared generally valid by the Commission pursuant to point (b) of Article 62(1); or ...

AmCham EU Amendment

2. The appropriate safeguards referred to in paragraph 1 shall be provided for, in particular, by: ...

(b) standard data protection clauses **between the controller or processor and the recipient of the data outside the EEA, which may include standard terms for onward transfers outside the EEA**, adopted by the Commission. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2); or

(c) standard data protection clauses **between the controller or processor and the recipient of the data outside the EEA, which may include standard terms for onward transfers outside the EEA**, adopted by a supervisory authority in accordance with the consistency mechanism referred to in Article 57 when declared generally valid by the Commission pursuant to point (b) of Article 62(1); or ...

Justification

In its Study on “Reforming the Data Protection Package”, the Parliament’s Policy Department points out that under the proposed Regulation, standard clauses do not extend to agreements between processors and sub-processors. As the Study points out, this gap could significantly disadvantage European firms, including new technology start-ups. The Article 29 Working Party has also recognised the need for sub-processors to be subject to the same obligations as apply to processors with regard to transferred data.

The amendment above is designed to close this gap. Data processors often subcontract processing activities to other companies, and such arrangements are now routine in the context of cloud computing. But without standard clauses -- a key tool enabling international data transfers -- European enterprises will be placed at a competitive disadvantage as they will be restricted from choosing sub-processors outside of Europe.

For example, a European cloud start-up (the data processor) may build the service it offers to customers on technology offered by a third party (the sub-processor). Without standard clauses to protect the flow of data to sub-processors outside of the Union, the cloud start-up will be restricted in its choosing platforms on which to build its service -- and may, as a result, ultimately be forced to offer a cloud service that is less competitive.

In line with the Study’s recommendation, the amendment above explicitly allows the Commission and Member States to extend standard clauses to sub-processors. This will give EU-based cloud providers and others greater flexibility and freedom in choosing adequate sub-processors.

Proposal for a regulation
Article 42 – paragraph 2 (e) (new)

Text proposed by the Commission

AmCham EU Amendment

2. The appropriate safeguards referred to in paragraph 1 shall be provided for, in particular, by: ...

2. The appropriate safeguards referred to in paragraph 1 shall be provided for, in particular, by: ...

(e) contractual clauses between the controller or processor and the recipient of the data that supplement standard data protection clauses as referred to in points (b) and (c) of paragraph 2 of this Article, and are authorised by the lead supervisory authority in accordance with paragraph 4.

Proposal for a regulation
Article 42, Paragraph 3

Text proposed by the Commission

AmCham EU Amendment

3. A transfer based on standard data protection clauses or binding corporate rules as referred to in points (a), (b) or (c) of paragraph 2 shall not require any further authorisation.

3. The appropriate safeguards referred to in paragraph 1 may also be provided by a single legally binding instrument between the processor and another processor that impose substantively the same obligations on the sub processor as the EU standard data protection clauses adopted by the

Commission where a processor is engaged by multiple controllers to carry out substantively similar processing operations in relation to their respective personal data and such personal data of multiple controllers are transferred to another processor in a third country:

a) by the processor and/or

b) by the controller

Proposal for a regulation

Article 42, Paragraph 4

Text proposed by the Commission

4. Where a transfer is based on contractual clauses as referred to in point (d) of paragraph 2 of this Article the controller or processor shall obtain prior authorisation of the contractual clauses according to point (a) of Article 34(1) from the supervisory authority. If the transfer is related to processing activities which concern data subjects in another Member State or other Member States, or substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57.

AmCham EU Amendment

4. Where a transfer is based on contractual clauses as referred to in point (d) **or (e)** of paragraph 2 of this Article the controller or processor shall obtain prior authorisation of the contractual clauses according to point (a) of Article 34(1) from the **lead** supervisory authority. If the transfer is related to processing activities which concern data subjects in another Member State or other Member States, or substantially affect the free movement of personal data within the Union, the **lead** supervisory authority shall apply the consistency mechanism referred to in Article 57.

Justification

This provision is meant to clarify the implementation of the “one-stop shop” concept referred to in recital 98.

Proposal for a regulation
Article 42, Paragraph 5

Text proposed by the Commission

5. Where the appropriate safeguards with respect to the protection of personal data are not provided for in a legally binding instrument, the controller or processor shall obtain prior authorisation for the transfer, or a set of transfers, or for provisions to be inserted into administrative arrangements providing the basis for such transfer. Such authorisation by the supervisory authority shall be in accordance with point (a) of Article 34(1). If the transfer is related to processing activities which concern data subjects in another Member State or other Member States, or substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57. Authorisations by a supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid, until amended, replaced or repealed by that supervisory authority.

AmCham EU Amendment

5. Where the appropriate safeguards with respect to the protection of personal data are not provided for in a legally binding instrument, the controller or processor shall obtain prior authorisation for the transfer, or a set of transfers, or for provisions to be inserted into administrative arrangements providing the basis for such transfer. Such authorisation by the **lead** supervisory authority shall be in accordance with point (a) of Article 34(1). If the transfer is related to processing activities which concern data subjects in another Member State or other Member States, or substantially affect the free movement of personal data within the Union, the **lead** supervisory authority shall apply the consistency mechanism referred to in Article 57. Authorisations by a supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid, until amended, replaced or repealed by that supervisory authority.

Proposal for a regulation
Article 44, Paragraph 1

Text proposed by the Commission

1. In the absence of an adequacy decision pursuant to Article 41 or of appropriate safeguards pursuant to Article 42, a transfer or a set of transfers of personal data to a third country or an international organisation may take place only on condition that:

[...]

AmCham EU Amendment

1. In the absence of an adequacy decision pursuant to Article 41; **or where the Commission decides that a third country, or a territory or a processing sector within that third country, or an international organisation does not ensure an adequate level of protection in accordance with Article 41(5); or in the absence** of appropriate safeguards pursuant to Article 42, a transfer or a set of transfers of personal data to a third country or an international organisation may take place only on condition that:

[...]

Justification

The wording of the Draft could rule out all forms of data transfers to the country, territory, sector or international organization considered as not offering an adequate level of protection regardless of whether other appropriate safeguards are put in place. Article 41(6) of the Draft indeed provides that the prohibition to

transfer personal data in case of inadequacy decided by the Commission is “without prejudice to Articles 42 to 44” while Articles 42(1) and 44(1) mention that they apply only if the Commission has not taken any decision on adequacy.

Proposal for a regulation
Article 44, Paragraph 1 (h)

Text proposed by the Commission

h) the transfer is necessary for the purposes of the legitimate interests pursued by the controller or the processor, which cannot be qualified as frequent or massive, and where the controller or processor has assessed all the circumstances surrounding the data transfer operation or the set of data transfer operations and based on this assessment adduced appropriate safeguards with respect to the protection of personal data, where necessary.

AmCham EU Amendment

h) the transfer is necessary for the purposes of the legitimate interests pursued by the controller or the processor, which cannot be qualified as frequent or massive **or where, prior to such transfer, the personal data is already made lawfully public in the third country**, and where the controller or processor has assessed all the circumstances surrounding the data transfer operation or the set of data transfer operations and based on this assessment adduced appropriate safeguards with respect to the protection of personal data, where necessary.

Justification

What this proposal acknowledges is that a data controller exporting public domain information back into a third country where it is already publicly available must remain responsible for adducing appropriate safeguards. However it also acknowledges that as the information is already widely known in that third country, the export poses a different level of risk for the data subject when compared to an export of consumer provided data. As the result of such reduced risk, it is not appropriate to impose the full requirements of Article 42 but instead the proposal provides the data controller with a degree of discretion around how it discharges its legal responsibilities.

Proposal for a regulation
Recital 84

Text proposed by the Commission

(84) The possibility for the controller or processor to use standard data protection clauses adopted by the Commission or by a supervisory authority should neither prevent the possibility for controllers or processors to include the standard data protection clauses in a wider contract nor to add other clauses as long as they do not contradict, directly or indirectly, the standard contractual clauses adopted by the Commission or by a supervisory authority or prejudice the fundamental rights or freedoms of the data subjects.

AmCham EU Amendment

(84) The possibility for the controller or processor to use standard data protection clauses adopted by the Commission or by a supervisory authority should neither prevent the possibility for controllers or processors to include the standard data protection clauses in a wider contract nor to add other clauses as long as they do not contradict, directly or indirectly, the standard contractual clauses adopted by the Commission or by a supervisory authority or prejudice the fundamental rights or freedoms of the data subjects. ***In some scenarios, it may be appropriate to encourage controllers and processors to provide even more robust***

safeguards via additional contractual commitments that supplement standard data protection clauses.

Proposal for a regulation

Recital 85

Text proposed by the Commission

AmCham EU Amendment

(85) A corporate group should be able to make use of approved binding corporate rules for its international transfers from the Union to organisations within the same corporate group of undertakings, as long as such corporate rules include essential principles and enforceable rights to ensure appropriate safeguards for transfers or categories of transfers of personal data.

(85) A corporate group should be able to make use of approved binding corporate rules for its international transfers from the Union to organisations within the same corporate group of undertakings, ***as well as to processors acting under its instructions***, as long as such corporate rules include essential principles and enforceable rights to ensure appropriate safeguards for transfers or categories of transfers of personal data.

Justification

Realities of data processing today require the recognition of the variety of actors participating in the data processing. This is needed not to water down the provisions of this regulation but to reinforce them. Therefore the legal recognition of different actors can only increase the levels of efficiency and enforceability of data protection by extending these to agents acting on behalf of controllers and processors that are engaged in different phases of the processing of personal data. Finally, the provision on binding corporate rules (article 43) indicates that binding corporate rules are binding not only internally (ie within the group of undertakings, but also externally, and that the controller or processor signing the BCR remains liable; therefore it is not justified to exclude agents on behalf of the controller or processor.

Proposal for a regulation

Article 42, Paragraph 4

Text proposed by the Commission

AmCham EU Amendment

4. Where a transfer is based on contractual clauses as referred to in point (d) of paragraph 2 of this Article the controller or processor shall obtain prior authorisation of the contractual clauses according to point (a) of Article 34(1) from the supervisory authority. If the transfer is related to processing activities which concern data subjects in another Member State or other Member States, or substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57.

4. Where a transfer is based on contractual clauses as referred to in point (d) ***or (e)*** of paragraph 2 of this Article the controller or processor shall obtain prior authorisation of the contractual clauses according to point (a) of Article 34(1) from the ***lead*** supervisory authority. If the transfer is related to processing activities which concern data subjects in another Member State or other Member States, or substantially affect the free movement of personal data within the Union, the ***lead*** supervisory authority shall apply the consistency mechanism referred to in Article 57.

Proposal for a regulation
Article 42, Paragraph 4 (a) (new)

Text proposed by the Commission

AmCham EU Amendment

4(a) (new) To encourage the use of supplemental contractual clauses as referred to in point (e) of paragraph 2 of this Article, lead authorities may offer a data protection seal, mark or mechanism, adopted pursuant to Article 39, to controllers and processors who adopt these safeguards.

Justification

This amendment encourages data controllers and processors to apply the strongest protections possible to data they transfer outside of the Union.

With the increasing globalisation of business and the evolution of computing models like the cloud, cross-border flows of personal data have become routine. In this environment, it is critical that controllers and processors apply strong safeguards to personal data regardless of where that data is located. Users will only have confidence in cloud computing if they know that their data is safe in the cloud.

The current Directive (95/46) generally prohibits transfers of data outside of the Union, however, unless the receiving country has been deemed by the Commission to offer “an adequate level” of data protection. Where a country has not been deemed “adequate”, a company can only transfer data if it can rely on an exception in the Directive, such as using “standard contractual clauses” that the Commission or national DPAs have approved.

Standard clauses are widely used today by organisations that transfer data. Effectively, they impose a legally binding obligation on organisations outside of the Union to apply certain “baseline” protections to data that has been transferred from the Union, including requirements to implement adequate security measures to protect data. The clauses also regulate liability for any damages suffered by individuals between the companies that export and import the data, and enable individuals whose data has been transferred to enforce certain provisions.

In many cases, it may be appropriate for organisations to apply additional safeguards to protect data being transferred out of Europe -- i.e. to supplement the standard clauses with even more robust protections. The amendment above makes clear that organisations can do this, and also creates an incentive to adopt these supplemental protections in the form of a data protection seal or trust mark, which would foster innovation in privacy.

Specifically, the amendment proposed above would do two things:

(1) make clear that controllers and processors may supplement standard contractual clauses under Articles 42(2)(b) and 42(2)(c) of the Regulation with additional contractual commitments, thereby offering stronger protections to customers; and

(2) encourage controllers and processors to adopt these heightened commitments by offering them a data protection “seal of approval”. The seal or trust mark could be adopted pursuant to Article 39 of the Regulation.

Proposal for a regulation
Article 42, Paragraph 5(a) (new)

Text proposed by the Commission

AmCham EU Amendment

5(a) (new) In the event of a discrepancy between the Regulation and the legal requirements of the requesting third country, the Commission will strive to resolve the conflicting legal situation during which the data controller or processor cannot be held liable.

Justification

Private organisations should not be put in the middle of conflicting legal requirements within the European Union or between the EU and third countries.

9. Definition of a Child

Proposal for a regulation

Article 6 (f)

Text proposed by the Commission

(f) Processing is necessary for the purposes of the legitimate interests pursued by a controller, except where such interests are overridden by the interests or fundamental rights or freedoms of the data subject which require protection of personal data, ***in particular where the data subject is a child.***

AmCham EU Amendment

(f) Processing is necessary for the purposes of the legitimate interests pursued by a controller, except where such interests are overridden by the interests or fundamental rights or freedoms of the data subject which require protection of personal data-

Proposal for a regulation

Recital 38

Text proposed by the Commission

(38) The legitimate interests of a controller may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding. ***This would need careful assessment in particular where the data subject is a child, given that children deserve specific protection.*** The data subject should have the right to object the processing, on grounds relating to their particular situation and free of charge. To ensure transparency, the controller should be obliged to explicitly inform the data subject on the legitimate interests pursued and on the right to object, and also be obliged to document these legitimate interests. Given that it is for the legislator to provide by law the legal basis for public authorities to process data, this legal ground should not apply for the processing by public authorities in the performance of their tasks.

AmCham EU Amendment

(38) The legitimate interests of a controller may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding. The data subject should have the right to object the processing, on grounds relating to their particular situation and free of charge. To ensure transparency, the controller should be obliged to explicitly inform the data subject on the legitimate interests pursued and on the right to object, and also be obliged to document these legitimate interests. Given that it is for the legislator to provide by law the legal basis for public authorities to process data, this legal ground should not apply for the processing by public authorities in the performance of their tasks.

Proposal for a regulation

Article 33, Paragraph 2 (d)

Text proposed by the Commission

2 (d) The following processing operations in particular present specific risks referred to in paragraph 1: (...) (d) personal data in large scale filing systems on ***children,***

AmCham EU Amendment

2 (d) The following processing operations in particular present specific risks referred to in paragraph 1: (...) (d) personal data in large scale filing systems on genetic data, or biometric data.

genetic data, or biometric data.

Proposal for a regulation

Recital 29

Text proposed by the Commission

(29) Children deserve specific protection of their personal data, as they may be less aware of risks, consequences, safeguards and their rights in relation to the processing of personal data. **To determine when an individual is a child, this Regulation should take over the definition laid down by the UN Convention on the Rights of the Child. This Regulation should define a child as an individual under the age of 13.**

AmCham EU Amendment

(29) Children deserve specific protection of their personal data, as they may be less aware of risks, consequences, safeguards and their rights in relation to the processing of personal data. **For the purpose of this Regulation a child should be defined** as an individual under the age 13.

Proposal for a regulation

Article 4, Paragraph 4 (18)

Text proposed by the Commission

4 (18) 'child' means any person below the age of **18** years;

AmCham EU Amendment

4 (18) 'child' means any person below the age of **13** years;

Justification

A threshold of 13 years of age for a child reflects more accurately the prevailing standard in Europe (though there are some variations). This prevailing standard has already been reflected in the Regulation's Article 8, which specifies that the processing of the data of a child under 13 shall be lawful only with parental consent. This general threshold should be consistent with the consent threshold already established in the Regulation.

10. Data Breach

Proposal for a regulation

Recital 67 - Security Breach Notification

Text proposed by the Commission

(67) A personal data breach may, if not addressed in an adequate and timely manner, result in substantial economic loss and social harm, including identity fraud, to the individual concerned. Therefore, as soon as the controller **becomes aware** that such a breach has occurred, the controller should notify the breach to the supervisory authority without undue delay **and, where feasible, within 24 hours. Where this cannot be achieved within 24 hours, an explanation of the reasons for the delay should accompany the notification.** The individuals whose personal data could be adversely affected by the breach should be notified without undue delay in order to allow them to take the necessary precautions. A breach should be considered as adversely affecting the personal data or privacy of a data subject where it could result in, for example, identity theft or fraud, physical harm, significant humiliation or damage to reputation. The notification should describe the nature of the personal data breach as well as recommendations as well as recommendations for the individual concerned to mitigate potential adverse effects. Notifications to data subjects should be made as soon as reasonably feasible, and in close cooperation with the supervisory authority and respecting guidance provided by it or other relevant authorities (e.g. law enforcement authorities). For example, the chance for data subjects to mitigate an immediate risk of harm would call for a prompt notification of data subjects whereas the need to implement appropriate measures against continuing or similar data breaches may justify a longer delay.

AmCham EU Amendment

(67) A personal data breach may, if not addressed in an adequate and timely manner, result in substantial economic loss and social harm, including identity fraud, to the individual concerned. Therefore, as soon as the controller **has confirmed with a reasonable degree of certainty** that such a breach has occurred, the controller should notify the breach to the supervisory authority without undue delay. **This means that notification is not immediately required after an incident has occurred but only once the controller has been able to determine with a reasonable degree of certainty that the incident is a personal breach.** The individuals whose personal data could be adversely affected by the breach should be notified without undue delay in order to allow them to take the necessary precautions. A breach should be considered as adversely affecting the personal data or privacy of a data subject where it could result in, for example, identity theft or fraud, physical harm, significant humiliation or damage to reputation. The notification should describe the nature of the personal data breach as well as recommendations as well as recommendations for the individual concerned to mitigate potential adverse effects. Notifications to data subjects should be made as soon as reasonably feasible, and in close cooperation with the supervisory authority and respecting guidance provided by it or other relevant authorities (e.g. law enforcement authorities). For example, the chance for data subjects to mitigate an immediate risk of harm would call for a prompt notification of data subjects whereas the need to implement appropriate measures against continuing or similar data breaches may justify a longer delay.

Justification

The requirement to notify within 24 hours is unrealistic and may prejudice investigations and cause unnecessary distress to consumers. The priority should be to investigate a breach and take appropriate action to limit any loss or damage to consumers.

Proposal for a regulation

Recital 68 - Confirmation of security measures taken following security breach

Text proposed by the Commission

AmCham EU Amendment

(68) In order to determine whether a personal data breach is notified to the supervisory authority and to the data subject without undue delay, it should be ascertained whether the controller has implemented and applied appropriate technological protection and organisational measures to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject, before a damage to personal and economic interests occurs, taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject.

(68) In order to determine whether a personal data breach is notified to the supervisory authority and to the data subject without undue delay, it should be ascertained whether the controller has implemented and applied appropriate technological protection and organisational measures to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject, before a damage to personal and economic interests occurs, taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject. ***In order to avoid over-notification to individuals and supervisory authorities and to ensure efficient use of resources, only those breaches identified as having negative and harmful consequences should be notified.***

Justification

Not all breaches threaten user privacy. For example, the loss of a file containing the names and addresses of data subjects that are in the public domain, would not lead to harm for the consumers concerned as the data are publicly available. Reporting the loss to consumers and supervisory authorities is unwarranted in such cases. In order for the EU's regime to be workable, the notification must focus on personal data breaches that are likely to have serious and negative consequences rather than all breaches.

Proposal for a regulation

Article 31, Paragraph 1

Text proposed by the Commission

AmCham EU Amendment

1. In the case of a personal data breach, the controller shall without undue delay and, ***where feasible, not later than 24 hours after having become aware of it,*** notify the personal data breach to the supervisory authority. ***The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within 24 hours.***

1. In the case of a personal data breach ***that is likely to lead to significant risk of substantial harm to a data subject,*** the controller shall without undue delay notify the personal data breach to ***its lead*** supervisory authority.

Proposal for a regulation
Article 31 (a) (new)

Text proposed by the Commission

AmCham EU Amendment

31 (a) (new) Notification of a personal data breach shall not be required if the controller demonstrates to the satisfaction of the lead authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the security breach. Such technological protection measures shall render the data unintelligible or unusable to any person who is not authorised to access it.

Proposal for a regulation
Article 31, Paragraph 5

Text proposed by the Commission

AmCham EU Amendment

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for establishing the data breach referred to in paragraphs 1 and 2 and for the particular circumstances in which a controller and a processor is required to notify the personal data breach.

5. deleted

Proposal for a regulation
Article 32, Paragraph 1

Text proposed by the Commission

AmCham EU Amendment

1. When the personal data breach is likely to adversely affect the protection of the personal data or privacy of the data subject, the controller shall, after the notification referred to in Article 31, communicate the personal data breach to the data subject without undue delay.

1. **Upon determination by the lead supervisory authority**, when the personal data breach is likely to **lead to significant risk of substantial harm to** the data subject, the controller shall, after the notification referred to in Article 31, communicate the personal data breach to the data subject without undue delay.

Justification

Breach notice obligations provide important incentives to data controllers to be responsible in their management of data, and will help to drive a higher standard of data security across industry. Requiring notice of breaches also fosters confidence of data subjects in third party processing.

To be effective, the breach notice regime must be practical and workable. The regime should not overly burden DPAs nor should it require that controllers notify breaches that prove harmless, which could lead data subjects to suffer from “notification fatigue”. To achieve these ends, the amendments above make three important changes to the proposed Regulation:

- ***First, the amendments would eliminate the obligation to notify within 24 hours.*** *There is significant consensus among industry and regulators that notice within 24 hours is not feasible. Controllers need more time to understand the nature of the breach, who is affected, and whether the breach poses harm to the data subjects involved.*
- ***Second, the amendments make clear that notice is required only where the breach threatens significant risk of serious harm to the data subject.*** *Notifying harmless breaches could have unintended effects: to begin with, it is likely to cause unwarranted anxiety among data subjects, but ultimately may lead to data subjects ignoring all notices. A requirement to notify harmless breaches would also burden data controllers and DPAs unnecessarily, leading to increased costs for European businesses. In addition, lacking resources to deal with these notifications, DPAs may miss important data breaches. In order to ensure a healthy and trustworthy environment, data breaches should be treated appropriately based on the likelihood of harm resulting from the breach.*
- ***Third the usability of the data and the circumstances in which the data was lost should also be considered in determining whether notification is needed.*** *If data was accidentally destroyed or was lost inadvertently (i.e., no one hacked into the system where the information resided, or stole physical data), those facts in the context of an event should bear on the likelihood that the data has fallen into the hands of an unauthorized person whose possession of the data gives rise to the risk of harm. It does not make sense to treat a minor breach that threatens little or no damage to an individual -- for example, where an online computer gaming account is hacked and a hacker gains access to a player’s game achievements or where a storage company misplaces internally a storage box but re-locates it shortly thereafter -- the same way as a breach that is likely to create a significant risk of substantial harm, such as a breach involving sensitive personal data (e.g., an electronic medical record).*
- ***Finally, the amendments delete references to delegated acts.*** *Given the essential nature of breach obligations to the Union’s data protection framework, the rules on breach should be addressed in the Regulation itself -- and not left to secondary rulemaking.*

AmCham EU's response to the Commission communication on a comprehensive approach on data protection in the European Union

American Chamber of Commerce to the European Union
Avenue des Arts/Kunstlaan 53, 1000 Brussels, Belgium
Telephone 32-2-513 68 92 Fax 32-2-513 79 28
Register ID: 5265780509-97
Email: info@amchameu.eu

Secretariat Point of Contact: Shannon Petry, shannon.petry@amchameu.eu
Tel: 02 289 10 36

Introduction.....	3
Executive Summary	5
1 One comprehensive framework	11
1.1 Architecture	11
1.2 Applicable law	11
2 Principles.....	13
2.1 Technological neutrality	13
2.2 Accountability	14
2.2.1 Accountability is not a new concept.....	14
2.2.2 Privacy culture	15
2.2.3 Accountability in practice	15
2.2.4 Existing components of accountability	16
(i) Training and policies.....	16
(ii) Data Protection Officers.....	16
(iii) Binding Corporate Rules.....	16
2.2.5 Privacy by Design Process	16
2.3 The importance of context	18
2.3.1 Context provides meaning.....	18
2.3.2 Context for what?.....	18
2.3.3 Opt-in vs. Opt-out	20
2.3.4 Legislating for context	20
2.4 Data breach notifications	21
3 Data subjects' rights.....	22
3.1 Data portability	22
3.2 The right to be forgotten.....	23
4 Enhancing the Internal Market and Promoting Competitiveness.....	25
4.1 Better harmonisation: increase legal certainty	25
4.1.1 Definitions.....	25
(i) Personal data	25
(ii) Consent.....	27
4.2 Reducing the administrative burden	27
4.2.1 Notifications.....	27
4.2.2 Privacy notices	28
4.3 Self-regulation	29
4.4 Promoting Competitiveness.....	31
4.4.1 Promoting dialogue between regulators and industry	31
4.4.2 Accountability for economic development in policy making.....	32
5 Addressing globalisation and international data flows.....	32
5.1 Cloud computing	32
5.2 International data flows	35
5.2.1 Adequacy vs. adequate safeguards.....	35
5.2.2 Binding Corporate Rules.....	36
5.2.3 Binding Safe Processor Rules	38
5.2.4 Safe Harbor	38
5.2.5 Standard Contractual Clauses.....	39
5.3 Universal principles.....	40
6 Cooperation and enforcement	40
6.1 Better cooperation between DPAs and EU authorities	40
6.2 Harm-based enforcement.....	41
6.3 Class actions	41
7 Conclusion	42

14 January 2011

Introduction

This document contains the response of the American Chamber of Commerce to the European Union (AmCham EU) to the Consultation on the European Commission's comprehensive approach on personal data protection in the European Union. It follows the Position Statement and Information Paper submitted for consideration during the previous round of consultations on data protection.¹

AmCham EU recognises that the two main purposes of Directive 95/46 (to protect the fundamental rights and freedoms of natural persons, in particular their right to privacy with respect to the processing of personal data, and to ensure the free flow of personal data between Member States) remain sound and should always be kept in mind in the preparation of the comprehensive approach on personal data protection currently being suggested.

While the Commission's Communication adequately portrays the challenges posed by innovation and advancing technological changes to application of the Directive, it seems to overplay the utility of increased transparency and enforcement alone to address these challenges. The Communication highlights the need for harmonisation among a myriad of national interpretations of the Directive, including the minimisation of national gold-plating of data protection requirements, increased emphasis on flexible cross-border compliance solutions and consideration of broader global trade implications from EU rules, but does not develop significant discussion to address these 'growing pains' under the Directive commensurate to their importance.

Our comments below – particularly in the areas of better harmonisation, accountability, data portability, notifications and international data flows – focus on the environment in which the Directive operates today, one of increasingly globalised commerce and transactions of personal information. Addressing the 'growing pains' highlighted above will be key to the meaningful transparency and effective enforcement that the Commission seeks in this new environment, not only for the betterment

¹ See 'AmCham EU Position Statement on the Commission consultation on protection of personal data', 19 January 2010 and 'AmCham EU response to the Commission consultation on protection of personal data', 19 January 2010, www.amchameu.eu.

of data subjects and the protection of their data, but also in terms of the proportionality of compliance burdens for controllers and processors.

In a world where information has become a valuable resource in society and where information sharing that serves legitimate purposes is general practice, AmCham EU would like to note that ensuring appropriate protection for collected and processed information is a priority. AmCham EU member companies take data protection seriously and it is an essential element of maintaining user trust and confidence. AmCham EU finds that too often discussions of data protection begin with the false assumption that, in general, personal data is not appropriately protected.

The data minimisation principle, which is based on the assertion that there is no need to protect what has not been collected, can be a useful part of a Privacy by Design approach to protecting personal data. However, it should not be elevated to an obligation, because it might in practice prevent consumers from reaping the benefits that secure collection of personal data can yield. Furthermore, determining the appropriate ‘minimum’ would be highly subjective and therefore impossible to effectively regulate. Therefore, more emphasis should be placed on determining whether the purposes for data collection are legitimate and specified in ways that are meaningful and understood by data subjects.

AmCham EU believes that the EU should be more ambitious when seeking to reconcile effective protection of privacy and personal data with its economic needs. In a knowledge-based society where ‘every European is digital’, it is critically important that data protection rules are interpreted and implemented in a way that is respectful of European citizens’ legitimate expectation that the EU will protect their prosperity as well as their privacy. This is not just about ensuring the coherence of the Single Market; it is essential to ensuring that the Single Market remains competitive.

A right balance between the protection of personal information and the free flow of information as inspired by Directive 95/46 should remain a key driver of the comprehensive approach on personal data protection in the European Union to the benefit of EU citizens.



Executive Summary

	Issue	AmCham EU's Position
One Comprehensive Framework	<i>Architecture</i>	AmCham EU is strongly opposed to a regime where various data protection rules apply per sector and/or per Member State and would not support the introduction of any specific rules that do not fit with the notion of a comprehensive framework.
	<i>Applicable Law</i>	A comprehensive approach on data protection should enable companies operating within various EEA Member States to be subject to one set of data protection rules and therefore concentrate their compliance efforts in a consistent and effective way with one regulator. This would allow businesses operating across borders to save enormous resources without infringing on data subjects' right to privacy.
Principles	<i>Technological Neutrality</i>	Retaining the technological neutrality principle throughout the legal framework will enable both Member States and industry to address issues as and when appropriate. Consumers also benefit from technology neutrality, as they will be able to understand the privacy framework and protections regardless of the specific type of device or technology being used, increasing consumer confidence and promoting economic growth. This will ensure that the EU's legal framework for data protection can remain appropriate and effective in the long term.
	<i>Accountability</i>	AmCham EU supports including

		<p>the principle of accountability in new legislation provided accountability is interpreted as a concept underscoring the renewed focus of the legislative proposals on a results-based system. The legislation should also provide the right incentives to organisations to implement the necessary procedures while rewarding those that have taken these steps already.</p>
	<i>Privacy by Design Process</i>	<p>AmCham EU believes that a Privacy by Design Process concept should focus on making sure that organisations (public and private) have implemented privacy protection into training programmes for people and have embedded it in processes. It should not take the form of design mandates or technology preferences, nor focus on prescriptive details regarding services and/or products.</p>
	<i>Context</i>	<p>AmCham EU believes that EU legislators should enable data controllers to take context into account when selecting the most appropriate way of providing information, obtaining consent and offering control.</p>
	<i>Data Breach Notifications</i>	<p>AmCham EU believes that the wider introduction of any data breach notifications needs to be carefully assessed; if the requirements are too broad, breach notifications could be very burdensome to businesses and confusing for/ignored by citizens. AmCham EU recommends that a specific threshold, such as a requirement of a significant risk of harm to the user, be set to</p>

		ensure that notices are effective. AmCham EU also favours a standardised EU data breach notification over a range of different notification obligations across the Member States.
Data Subjects' Rights	<i>Data Portability</i>	AmCham EU is concerned about the implementation of an explicit right to data portability in practice and would like to ensure that such a possibility is granted only to the extent it is reasonably technically feasible and that no specific interoperability standards would be imposed on data controllers.
	<i>The Right to Be Forgotten</i>	AmCham EU believes that there needs to be a more open and in-depth debate between stakeholders and policy-makers on a possible legal definition of a 'right to be forgotten' before its introduction into EU law is considered.
Enhancing the Internal Market and Promoting Competitiveness	<i>Better Harmonisation</i>	The new framework should address harmonisation issues to enable businesses to take a Europe-wide view of data protection compliance.
	<i>Reducing the Administrative Burden</i>	AmCham EU applauds the intended simplification of the notification regime and the harmonisation of content of information notices. In particular, with respect to notifications, AmCham EU believes that the European Commission should evaluate the need and rationale for <i>ex ante</i> notifications and weigh that against the significant and time-consuming burden this creates for controllers and Data Protection Authorities who need to review the large quantities of

		<p>notifications that are filed. For ‘riskier’ or more sensitive data processing where notifications may be warranted, AmCham EU urges the European Commission to work with Data Protection Authorities to develop harmonised and simplified filing templates at the EU level. Any templates developed should be given mutual recognition across all Member States in order to reduce administrative burdens if or when notification is required. While guidelines regarding privacy notices for users/consumers would be welcomed, AmCham EU would like to caution against standardised compulsory privacy notices drafted without stakeholders’ involvement or outside their control.</p>
	<i>Self-regulation</i>	<p>AmCham EU recommends that the Commission take a much more active role in promoting self-regulatory and co-regulatory mechanisms.</p>
	<i>Promoting Competitiveness</i>	<p>In order to promote the EU’s competitiveness, the Commission should be given explicit responsibility for ensuring compatibility of the implementation and interpretation of EU data protection law with EU economic and other policy objectives.</p>
International Data Flows	<i>Accountability-based Regime</i>	<p>AmCham EU would welcome the opportunity to explore the concept of an accountability-based transfer regime, providing sufficient safeguards and replacing adequacy for international data flows, in more</p>

		detail with the Commission.
	<i>Binding Corporate Rules</i>	AmCham EU believes that, in general, the BCR process can be a useful tool, but calls upon the EU to promote a less burdensome process and a broadening of their scope of application (e.g. not limited to intra-group transfers and coverage of transfers to processors) in order to realise the full potential of this data transfer solution and accountability tool.
	<i>Binding Safe Processor Rules</i>	AmCham EU calls for a flexible internal governance model for data transfers to processors. AmCham EU sees BSPRs as a potentially useful tool in this respect and is ready to contribute to and discuss the outcome of the current work undertaken by European authorities. However, care must be taken to avoid a BSPR procedure that would maintain the complexities and costs associated with today's BCR approval process.
	<i>Safe Harbor</i>	AmCham EU would like to see the Safe Harbor programme recognised as a successful tool in this revision.
	<i>Standard Contractual Clauses</i>	The utility of SCCs could be further improved by giving the parties more flexibility to make changes to SCCs as long as the parties to the SCCs remain the same and there are no amendments to clauses made mandatory by the European Commission.
Cooperation and Enforcement	<i>Cooperation</i>	AmCham EU welcomes the work currently being undertaken by the Article 29 Working Party in relation to cooperation between DPAs. It is crucial that DPAs

		better coordinate their activities and cooperate more closely, especially with respect to cross-border matters.
	<i>Harm-based Enforcement</i>	AmCham EU believes that formal considerations of harm to data subjects should be a prerequisite for modern legislation as well as for any enforcement action, most notably for imposing fine.
	<i>Class Actions</i>	AmCham EU cannot support any language that leaves open the possibility of class action suits.

1 One comprehensive framework

1.1 Architecture

AmCham EU recognises the need for a comprehensive and coherent approach to data protection in the EU and welcomes the new consultation issued by the European Commission in this respect.

Given the lack of harmonisation between Member States in this matter after 15 years of implementation of Directive 95/46, AmCham EU is open to the Commission examining the possibility of proposing a Regulation, rather than a new Directive, to develop the new comprehensive framework in a single instrument. This would avoid the risks created by varying implementation among Member States as the same rules would then be directly applicable in all Member States. However, AmCham EU is mindful of the fact that the content of the legislation will be a relevant factor when determining the most appropriate legal instrument. We believe that the most appropriate choice will become clearer as the text materialises.

AmCham EU suggests that EU authorities examine the possibility of an opt-for regime, available to companies that operate across the EU. This regime would enable companies to have a single set of rules applicable across all their EU activities, as is the case of the alternative method for harmonising national laws (known as the 28th regime) which has recently been referred to in the context of the revision of the draft Consumer Rights Directive.

AmCham EU is strongly opposed to a regime where various data protection rules apply per sector and/or per Member State and would not support the introduction of any specific rules that do not fit with the notion of a comprehensive framework.

1.2 Applicable law

The applicable law rule set forth in Article 4 of Directive 95/46 has proved difficult to apply in practice, particularly when several Member States are concerned or when ‘equipment’ is used in the EEA by a data controller that is not established in the EEA.

Under the current framework, when data collection by one company takes place in various EEA Member States with the

involvement of its European affiliates or equipment in the EEA, that company may have to comply with the rules applicable in each country where data collection takes place. This creates uncertainty as well as adding to the compliance burden.

AmCham EU calls for a review of the applicable law principle whereby the applicable rules should only be those of the EEA country where the company's 'main establishment' is located.²

Such a principle would mean that a multinational company is subject only to the law and enforcement agency of its 'main establishment's' home state. Only that Member State's law would be applicable to the EEA operations and to any EEA subsidiary (assuming majority ownership and control of that entity) and only the multinational's EEA home state data protection authority should have the ability to take action against that company (regardless of the location of any individual subsidiary location, if any). Such a principle would be of huge benefit to the data protection regime overall, bringing greater legal certainty to companies and end users.

AmCham EU believes that a clear definition of the concept of 'main establishment' of a company must be provided in the new framework. AmCham EU is ready to work with the Commission to identify the considerations that may be relevant to define a 'main establishment' (e.g. main operations in the EEA, main location for business purposes in the EEA, where the physical operations are based, where personal data is processed and/or where decisions about data processing are made).

To create greater legal certainty for both users and companies, it is essential that the overall regime be harmonised. Greater consistency across the EEA would give national data protection authorities the confidence that the application of another Member State's law adequately protects the personal data of their own citizens.

A comprehensive approach on data protection should enable companies operating within various EEA Member States to be subject to one set of data protection rules and therefore concentrate their compliance efforts in a consistent and effective way with one regulator. This would allow businesses operating

² The Article 29 Working Party also supports such a principle, as indicated in its Opinion 8/2010 on applicable law adopted on 16 December 2010.

across borders to save enormous resources without infringing on data subjects' right to privacy.

2 Principles

In addition to the key principles already set forth in Directive 95/46, AmCham EU believes that the following principles should be included in the comprehensive legal framework: technological neutrality, accountability, the importance of context and data breach notifications.

2.1 Technological neutrality

In its Communication, the Commission recognises that any changes to be made to the legislative framework in this current review will have to “stand the test of time”, just as Directive 95/46 has. AmCham EU agrees with the Commission that the legal framework must provide legal certainty to citizens of future generations regardless of how sophisticated technology may become. To ensure this is possible, it is important that the technology-neutral approach that has been shown to be effective is maintained and is neither removed nor unintentionally called into question.

While AmCham EU finds it appropriate for the current review to consider the challenges of today's technology, such as social networks and cloud computing, we suggest that the review also look beyond current technologies in order to ensure that the legal framework will be appropriate regardless of specific technologies that might come of age in the future. This requires the retention of the technological neutrality principle as well as the avoidance of any introduction of requirements focused on a specific technology or possible technology mandates.

For example, while Privacy by Design is a concept that AmCham EU supports in principle, it is important that this concept not be defined in the legal framework in a way that demands technology-specific requirements for the design and deployment of IT products or solutions. A definition that goes into details and specifics as to the technology that should be embedded or bundled into IT equipment could tie the hands of industry, preventing it from developing innovative privacy tools and solutions to address threats and risks to data protection, security and privacy that may not even be envisaged today.

It should be remembered that information is a key target for criminals, whose activities evolve and adapt much more quickly than legislation can be changed. Prescriptive requirements could impede industry efforts to counteract criminal activity and, in the end, would be counterproductive.

Retaining the technological neutrality principle throughout the legal framework will enable both Member States and industry to address issues as and when appropriate. Consumers also benefit from technology neutrality, as they will be able to understand the privacy framework and protections regardless of the specific type of device or technology being used, increasing consumer confidence and promoting economic growth. This will ensure that the EU's legal framework for data protection can remain appropriate and effective in the long term.

2.2 Accountability

2.2.1 Accountability is not a new concept

Accountability refers to the ability of company to demonstrate its capacity to achieve specified privacy practices and to have that capacity objectively measured by regulators or internal/external auditors. The concept of accountability already exists and is used today; a limited example is Binding Corporate Rules (BCRs), where companies (data controllers) show regulators how their internal rules protect personal data and be measured on how these rules are upheld.

Accountability also applies with respect to security measures to be implemented by data controllers and processors and to the appointment of data protection officers pursuant to the current data protection directive.³

³ One example can be found in Canadian legislation: 'Canada has, through the Personal Information Protection and Electronic Documents Act (PIPEDA), chosen an organization-to-organization approach that is not based on the concept of adequacy. PIPEDA does not prohibit organizations in Canada from transferring personal information to an organization in another jurisdiction for processing. However under PIPEDA, organizations are held accountable for the protection of personal information transfers under each individual outsourcing arrangement. The Office of the Privacy Commissioner of Canada can investigate complaints and audit the personal information handling practices of organizations'. *See* www.priv.gc.ca/information/guide/2009/gl_dab_090127_e.cfm.

The European Commission should examine how these tools can be used in a more harmonised and predictable fashion.⁴

2.2.2 Privacy culture

AmCham EU calls for the regulatory framework to move from a procedure-based regime to a results-based legal system. In such a system, legislation should establish general guidelines for the outcome to be achieved; it should not focus on the precise means for achieving this via administrative and overly prescriptive processes that do not necessarily lead to increased data protection.

In a results-based system, public and private organisations are accountable for handling data wherever that data travels. This will allow them to focus on the core objective of the legal framework instead of merely seeking legal compliance.

Additionally, accountability and liability should be recognised as distinct principles. Accountability should not result *a priori* in liability; additional legal steps should be necessary to establish liability on a case-by-case basis beyond demonstrations of accountability mechanisms.

An improved legal framework should encourage and give incentives for organisations to be held accountable. Such organisations should set the protection of individuals' rights as a recognised corporate objective, while seeking and achieving legal compliance. This will enable data protection to become a proactive part of all businesses rather than a reactive compliance function. Ensuring that this accountability follows the data, regardless of where it is controlled or processed, will ultimately increase data protection and benefit all consumers.

2.2.3 Accountability in practice

AmCham EU favours the introduction of accountability principles. The concept of accountability that AmCham EU calls for is, however, broader than that mentioned in the Communication, which is only focused on increasing the responsibility of data controllers. Rather, we believe accountability is a concept that should be the foundation of the

⁴At the international level, the accountability principle has already been recognised in the OECD Privacy Guidelines first established in 1980 and the Asia-Pacific Economic Cooperation (APEC) Privacy Framework.

legal framework in its totality, of how we look at data protection, of how we enforce it and of how we supervise it.

We also stress the need to allow companies the flexibility to determine how accountability should be demonstrated depending on the business model, sector or systems already in place.

AmCham EU supports including the principle of accountability in new legislation provided accountability is interpreted as a concept underscoring the renewed focus of the legislative proposals on a results-based system. The legislation should also provide the right incentives to organisations to implement the necessary measures while rewarding those that have taken these steps already.

2.2.4 Existing components of accountability

(i) Training and policies

AmCham EU believes that staff training and policies could be part of an accountability model.

(ii) Data Protection Officers

AmCham EU recognises that the appointment of an internal Data Protection Officer within a group of companies can conform with the accountability model. However, a strict obligation to appoint a Data Protection Officer may not be implementable; there is immense variation across companies' internal structures and business models. In some cases, companies may be able to find ways to protect personal data that are more effective than the appointment of a Data Protection Officer.

(iii) Binding Corporate Rules

Possibly the best (albeit of limited application) example to date of an accountability-based mechanism founded on an internal governance approach across the organisation in the framework of Directive 95/46 is the Binding Corporate Rules data transfer solution which some AmCham EU members currently have in place.

2.2.5 Privacy by Design Process

AmCham EU underlines the importance of implementing and integrating accountability in the development of organisational systems and processes. Privacy by Design Process (PbDP) is a concept that should be part of an accountable company's overall approach to supporting privacy in an environment of

technological change and information-intensive innovation. AmCham EU is supportive of a drive for organisations to embed PbDP into their processes and people.

To date there is only a vague definition of PbDP available in the EEA and all stakeholders would need to be involved in fully defining the concept. Indeed while PbDP has become a popular term in the privacy community, it means different things to different people.

There is a clear need to look at the issue of data protection with a global perspective to avoid further fragmentation, taking stock of industry's own efforts and taking into account technological developments. Although every organisation should integrate privacy into its processes, the rules should allow for flexibility and leave room for adaptation in how this is done. This is especially the case with respect to small and medium-sized enterprises (SMEs) given their specific business processes and resources. One should keep in mind that there is not one single way of implementing Privacy by Design Process and that the different elements of a company's process should be taken into account. PbDP does not just describe how the products are built; it reflects how services operate and how business is conducted.

In that context, AmCham EU supports the concept of Privacy by Design but thinks any reflection on the concept in legislative proposals should provide the flexibility necessary to account for different business models and organisational needs. It should focus on designing privacy into processes and people and should not impose 'privacy by default' or any technology mandate. AmCham EU would like to work with all stakeholders to further define the concept and provide the European Commission with input regarding its implications.

We would further like to stress that all legitimate businesses already have processes in place that would fall under the concept of Privacy by Design Process (ranging from more formal and documented procedures such as Privacy Impact Assessments to internal controls, regular interactions between the legal department and the technology developers or simply the existence of privacy officers). These should be acknowledged, allowed and encouraged if any PbDP concept is introduced with the legislative revision. The most appropriate specific mechanisms to ensure effective PbDP measures within a business (and ultimately a high level of data protection for data subjects) will always be best

determined by the business itself depending on factors such as the type of personal data processed as well as the business model, sector and size of the company.

AmCham EU believes that a Privacy by Design Process concept should focus on making sure that organisations (public and private) have implemented privacy protection into training programmes for people and have embedded it in processes. It should not take the form of design mandates or technology preferences, nor focus on prescriptive details regarding services and/or products.

2.3 The importance of context

Since 1995, a significant transformation of society and the global economy has led to an explosion of the number of contexts in which data, including personal data, is collected and processed. This proliferation of contexts is one of the main drivers for change in the legislative framework. It is therefore important that legislators take the issue of context into account when drafting new texts.

2.3.1 Context provides meaning

Effective communication is at the heart of economic and social progress, and effective communication is impossible without a mutually understood context. This is a reality that we experience in everyday life. Context is what makes a joke funny for those who share it. The importance of context is also something keenly understood by anyone who has been quoted out of context in the media. Interactions between data subjects and data controllers are not an exception to this – effective protection of privacy is therefore also heavily dependent on context.

2.3.2 Context for what?

Data subjects must understand the context in which they are *provided information* by data controllers about the collection and use of data. This might be as simple as seeing the logo or brand of a data controller on a letterhead (for example, most people will immediately understand the context of a bill from a utility company before even opening the envelope). It could also be a more complex situation, such as the collection of data by a familiar data controller (e.g. employers, websites, retailers) for a previously unspecified purpose. In some cases, context for

data collection and use is particularly hard to explain. This can be the case, for example, when an unfamiliar party seeks to collect data. In such cases, providing notice and transparency in context is arguably even more important, since the data subject is otherwise unlikely to understand. Seen from another angle, transparency and information-sharing are worth nothing if provided out of context. An employee cannot be expected to understand information provided by his or her employer if it is provided in the street on a holiday.

According to Directive 95/46, *consent* must be freely given, specific and *informed* in order to be valid. This last characteristic is the one that is most dependent on context. As described above, information provided out of context is unlikely to be a basis for valid consent. The concept of *implicit consent* is also heavily dependent on context. It should also be noted that the validity of consent may or may not have a temporal dimension (e.g. in some contexts, consent for use of data collected can conceivably be valid if it is given before, during or after data collection, especially if the data is collected for other purposes). In a fast-moving world of innumerable data-enabled transactions, context has become an essential element for providing valid consent.

The Article 29 Working Party (A29WP) has already acknowledged the importance of context in relation to consent in its work on consent provided in the context of an employment relationship.⁵ Consent in a particular context is often linked to the desire to ensure a certain ‘benefit’ within that context; and this should not be understood as ‘trading’ privacy. A good example is healthcare: if a patient can receive better, more accurate and more effective treatment with the use and processing of their personal data combined with hospital data and research data, they may want to consent to that data being used as long as security safeguards are in place. Today, interpretation of this part of Directive 95/46 varies across the Member States, and improved consistency is needed.

The logic of context also applies to data subjects’ *control* over their data. Like any other type of communication, an opportunity for data subjects to affirm or refuse the

⁵ Opinion 8/2001 on the processing of personal data in the employment context, DG MARKT 5062/01, 13 September 2001.

collection and use of data needs to be done at a time and in a place that makes sense and is in line with the data subject's reasonable expectations.

2.3.3 Opt-in vs. Opt-out

It is an unfortunate fact that the old framework, with its insufficient emphasis on context, has created a polarised debate between those in favour of 'opt-in' approaches to consent and control (broadly defined as ruling something out unless the data subject has expressly chosen to accept it) and those in favour of 'opt-out' (broadly defined as a situation where the data subject is allowed to stop something that would otherwise proceed). 'Opt-in' has come to be perceived as more protective of users' privacy than 'opt-out'. The result has been a drive by privacy advocates (and indeed by many legislators) to push for 'opt-in' approaches to data protection to become the norm. In recent years, however, it has become clear that a poorly designed 'opt-in' (for example, one provided out of context) is less protective of privacy than a well-designed 'opt-out'. Indeed, there is currently a wide range of mechanisms that enable users to control and consent to use of their information; some of the more robust opt-out mechanisms in fact do a better job of protecting privacy than do weaker opt-in mechanisms.

A good example of this would be the transparency and control tools that are being developed by the online advertising industry specifically for behaviourally targeted ads. Both transparency and control will be provided contextually where the user would intuitively expect and understand them – in the ads themselves. By clicking on a globally standardised icon located in or around the ad, users will be able to access detailed information about behavioural advertising and exercise control over it via an industry-wide tool that will stop the delivery of such ads to that user's browser. This kind of context-sensitive approach potentially frees us from the sterile 'opt-in vs. opt-out' debate by both better protecting the data subject and allowing for new business models to develop responsibly.

AmCham EU believes that EU legislators should enable data controllers to take context into account when selecting the most appropriate way of providing information, obtaining consent and offering control.

2.3.4 Legislating for context

The challenge of context for legislators is that it is so infinitely varied, intangible and changing that it is actually impossible to lay down detailed rules for a case-by-case analysis of its impact. Thankfully, the legislative framework is principles-based and provides the flexibility needed to apply rules with common sense to the relevant situation. The principles-based approach must continue in order to provide the necessary flexibility. However, this flexibility must not be seen as a license for data controllers to act irresponsibly. Effective self-regulation is needed in many areas where context has a particular impact, such as in the example of behavioural advertising addressing in section 2.3.3.

AmCham EU urges the European Commission to explicitly recognise the role and importance of context as a critical factor for data controllers to take into account.

2.4 Data breach notifications

AmCham EU sees the introduction of a data breach notification provision across all sectors as a tool for increasing transparency and consumer understanding. Introducing a requirement in the legal framework to notify users if data has been lost or stolen can empower consumers to take action if they want or need to.

It is important, though, to consider the threshold above which the need to notify would apply when drafting an appropriate and workable notification framework. Determining the level at which a breach would be serious enough to trigger a notification provides clarity to organisations in terms of what action is expected of them and when. It can also help address concerns with respect to possible over-notification of citizens. AmCham EU suggests that, moving forward, the Commission considers introducing the principle of a 'significant risk of harm' threshold.

However, AmCham EU would like to caution that the details and specific procedures to be followed should a horizontal data breach notification requirement be introduced need to be discussed in detail with stakeholders. If notice obligations apply to data or events that do not constitute a significant risk of harm, over-provision of notices could confuse consumers and, with time, potentially lead them to ignore important notices. Notifications can be a burdensome, complex and costly procedure for businesses, data protection authorities (DPAs) and citizens so the modalities need to be well thought-through (especially if such an obligation were to apply across the public and private sectors).

The legislative framework should also explicitly recognise the important role that privacy and security technologies can play in protecting data that is lost or stolen. For example, if the data lost is encrypted, the notification requirements associated with that breach could be adjusted accordingly to account for the reduced risk of harm.

The right balance must be found between breach notification as a means to improve appropriate security measures or sanctions and any remedial actions implemented in order to minimise harm, disruption and reputational consequences. In this context, entity or group internal disclosures should not be considered unauthorised disclosures (unless they relate to a specific individual and therefore could be subject to a data subject request).

AmCham EU believes that the wider introduction of any data breach notifications needs to be carefully assessed; if the requirements are too broad, breach notifications could be very burdensome to businesses and confusing for/ignored by citizens. AmCham EU recommends that a specific threshold, such as a requirement of significant risk of harm to the user, be set to ensure that notices are effective. AmCham EU also favours a standardised EU data breach notification over a range of different notification obligations across the Member States.

3 Data subjects' rights

In addition to the rights already granted to data subjects by Directive 95/46, which are already effectively implemented in practice by AmCham EU members, two 'new' data subjects' rights are mentioned in the Communication: data portability and the right to be forgotten.

3.1 Data portability

AmCham EU understands the interest data subjects have in the possibility of withdrawing their data from one application or service in order to transfer this withdrawn data into another application or service. Some companies already voluntarily provide this as a service.

AmCham EU is concerned about the implementation of an explicit right to data portability in practice and would like to ensure that such a possibility is granted only to the extent it is

reasonably technically feasible and that no specific interoperability standards would be imposed on data controllers.

3.2 The right to be forgotten

The Communication calls for clarification of the ‘right to be forgotten’, i.e. the right of individuals to have their data no longer processed and deleted when it is no longer needed for legitimate purposes.

AmCham EU notes that the elements of the so-called ‘right to be forgotten’ are already enshrined in the current Directive, in so far as this concept is considered from a privacy and data protection perspective. Indeed, the obligation to keep data only as long as necessary for the purposes for which the data has been collected, along with the right to have data deleted and the right to withdraw consent, are components of the ‘right to be forgotten’.

These provisions may not yet have lived up to expectations due to implementation and enforcement failures, but AmCham EU does not believe that this justifies the introduction of a ‘right to be forgotten’, which inherently carries much wider ethical and philosophical connotations.

AmCham EU agrees that there may be a need to reinforce the existing rules, but argues that the ‘right to be forgotten’ seems to have introduced a debate that deviates from the heart of the problem. AmCham EU would like to caution against an attempt to address all the societal challenges of the ‘right to be forgotten’ exclusively through creation of unjustified obligations on data controllers and processors. For instance, some lines of thought currently being developed at the Member State level would inevitably lead to a general obligation to monitor the Internet, undermining the strong foundations on which the Internet was developed in the first place and the basis on which democratic societies operate. Such a debate may be valid as technology has penetrated every aspect of our lives, but certainly should not be held in the context of the revision of the EU legal framework on data protection. In fact, it has already been addressed in the Commission’s recent consultation on e-commerce. It should be noted that the e-Commerce Directive prevents the imposition of a general obligation to monitor on website providers, and that this provision was an integral part of the excellent balance of rights and responsibilities that was struck at the time.

AmCham EU believes that it would be useful for the European Commission to focus on substance rather than joining a rhetorical debate. A clarification of the ‘right to be forgotten’ as meaning that individuals have the right ‘to have the data they provide no longer processed and deleted when it is no longer needed for legitimate purposes’ would be welcome.

To be workable, the rights to data portability and deletion must clearly distinguish between data directly inputted by the user (e.g. photos or names of friends) and data created by the service provider. The scope of “user data” will need to be clearly delineated in close consultation with industry in order to avoid differences of interpretation and approach across the Member States.

AmCham EU believes that there needs to be a more open and in-depth debate between stakeholders and policy-makers on a possible legal definition of a ‘right to be forgotten’ before its introduction into EU law is considered.

At this stage, we see that such a right may lead to serious practical difficulties and undesirable or unintended consequences. Many questions remain unanswered, including:

- What types of data should fall under such a right? Introduction of the right may be triggered by current privacy concerns (particularly related to social networks) but how would it apply to the rest of the online (and even offline) world?
- What would happen with metadata or back-up systems if a ‘right to be forgotten’ is introduced in EU law?
- What level of anonymisation would be acceptable for the right to be inapplicable?
- How would the ‘right to be forgotten’ be enforced in the public sector?
- How would it be reconciled with other legal requirements relevant to law enforcement, such as data retention requirements?
- How can both the public and private sectors handle the legal, financial and technical complexities that such a right would entail?

One suggestion recently raised to address technical complexity, expiration dates for information, at this stage seems entirely unworkable and does not at all take into account the societal and economic benefits that derive from the analysis and secondary uses

of the vast amounts of data produced in our daily activities (not to mention the technical challenges it entails).

Finally, AmCham EU strongly supports Commissioner Kroes' views on this topic, as expressed in her speech of 25 November 2010 on cloud computing and data protection: 'Just like in real life, when you present yourself on the net, you cannot assume no records exist of your past actions'.

4 Enhancing the Internal Market and Promoting Competitiveness

4.1 Better harmonisation: increase legal certainty

Personal data processing is currently regulated in fragmented ways across the EEA due to differing implementations and/or interpretations. Each Data Protection Authority has their own interpretation of the broad principles of the Directive, based on their local legal and cultural expectations. There has been a growing lack of legal certainty regarding how Member States are interpreting fundamental core principles of the Directive, such as the definitions of personal data and consent.

The new framework should address harmonisation issues to enable businesses to take a Europe-wide view of data protection compliance.

4.1.1 Definitions

Some existing definitions in Directive 95/46 may need to be revised to ensure a better harmonisation and increase legal certainty.

(i) Personal data

The concept of personal data is at the forefront of the discussion of the review of the data protection Directive. Indeed, the presence and processing of data that is considered personal in accordance with the definition spelled out in the Directive triggers the application of the set of rights and obligations outlined in the Directive. The broad and imprecise character of the current definition creates a level of uncertainty regarding the extent to which those rights and obligations apply to particular cases. This

lack of clarity is highlighted in the Communication as well.

A more nuanced approach to the concept of personal data is needed, going beyond the binary system currently in place. The key is to determine a system that addresses what rights and obligations are necessary (appropriate and proportionate) to protect the information processed. AmCham EU suggests a few concrete alternatives that may deserve consideration when drafting the proposal to review the Directive:

- Creation of objective criteria that, if met, would determine not only if data is personal but also the context in which data becomes personal. This concept is already enshrined in Austrian law.⁶
- Maintenance of the current definition, complemented by the creation of a gradation system of obligations based on the risks of harm to individuals through the processing of information related to them.

Additionally, AmCham EU asks the Commission to explicitly exclude business contact information (names, office addresses, email addresses and telephone information – and, as the case may be, company names) from the definition of personal data. Contact information should not be qualified as personal data. Enterprises need to use business contact information to conduct business; it is indispensable to reach their customers, to coordinate with their suppliers and to work with business partners. Currently, enterprises must obtain consent for the processing of such data. The Spanish Data Protection Authority has recognised that this is an excessively cumbersome requirement and has excluded business contact information from the scope of personal data in Spain. AmCham EU encourages the Commission to ensure that this exclusion is applied across the EU. This simple step

⁶ See the definition of ‘only indirectly personal data’ used to refer to data which relate to the subject in such a manner that the controller, processor or recipient of a transmission cannot establish the identity of the data subject by legal means, available at <http://www.ics.uci.edu/~kobsa/privacy/Austrian-english.htm#E1>

would immediately reduce the burden of compliance at little real cost to personal privacy, as the data relates only to contact information of individuals at their places of business.

(ii) Consent

Directive 95/46 describes consent as ‘freely given, specific, and informed’. AmCham EU believes that this definition remains entirely appropriate, and allows for the flexibility that is necessary in the modern world.

However, the existing framework insufficiently emphasises the importance of context (see section 2.3 above). Traditional interpretations of consent have tended to give primary importance to the temporal aspect of consent at the expense of other crucially important contextual factors. This emphasis is based on an assumption that has fed the polarisation of the “opt-in vs. opt-out” debate, but which has not actually protected or empowered data subjects.

AmCham EU calls on the Commission to clarify that the validity of consent depends heavily on context. EU legislators should seek a modern approach to consent that allows data controllers to select the most contextually appropriate way of providing information, obtaining consent and offering control. This could allow the debate to move on from “opt-in vs. opt-out” while better protecting the data subject and allowing new business models to develop responsibly.

4.2 Reducing the administrative burden

AmCham EU applauds the intended simplification of the notification regime and the harmonisation of content of information notices.

4.2.1 Notifications

It is widely recognised that the current notification system needs to be revised and simplified. The significant differences that exist across the 27 Member States, such as the amount of detail required and the type of forms to be used, lead to significant compliance costs and result in

unequal enforcement. As a result, any organisation operating across the EU Member States needs to file separate registrations and consequently cannot benefit from economies of scale.

AmCham EU believes that the European Commission should evaluate the need and rationale for *ex ante* notifications and weigh that against the significant and time-consuming burden this creates for controllers and data protection authorities who need to review the large quantities of notifications that are filed.

Instead, both controllers and data protection authorities would benefit from *ex post* controls which would lead to a system based on compliance and accountability for the protection of personal data.

For ‘riskier’ or more sensitive data processing where notifications may be warranted, AmCham EU urges the European Commission to work with Data Protection Authorities to develop harmonised and simplified filing templates at the EU level. Any templates developed should be given mutual recognition across all Member States in order to reduce administrative burdens if or when notification is required.

4.2.2 Privacy notices

Transparency is essential to allowing users to make informed and meaningful choices about the processing of personal information related to them. The existing EU data protection Directive lays down the main elements to be contained in privacy notices. However, because of the leeway afforded to Member States in implementing the Directive, there are often additional and differing national requirements to be considered. This means that companies must sometimes have different privacy notices in different Member States, creating an additional administrative burden. It may also prove difficult to ensure complete compliance with the differing rules from a technical point of view.

Nevertheless, AmCham EU would like to caution against any static, detailed provisions in the forthcoming legislative proposal that would impair the creativity and communication of companies’ privacy practices. Indeed, AmCham EU believes that the transparency principle should remain as flexible as possible, allowing companies

to *realise* it in their product and service policies in ways that are meaningful to their particular audiences (e.g. consumers and users of a particular product or service). There should be no rigid standardisation of what information is disclosed and how, and security aspects should not be put at risk; if standard privacy notices are drawn up, their use should be left voluntary.

While guidelines regarding privacy notices for users/consumers would be welcomed, AmCham EU would like to caution against standardised compulsory privacy notices drafted without stakeholders' involvement or outside their control.

4.3 Self-regulation

In recent years, the European Commission has increasingly resorted to softer legal instruments such as recommendations as an alternative or ancillary to traditional authoritative legislation. This approach has led to more effective, pragmatic and business-minded actions. Similarly, the European Commission has supported industry initiatives for self-regulation, especially in fast-developing areas of industry.⁷

In order to ensure effective data protection in a rapidly evolving environment, self-regulation is a very effective tool to help data controllers comply with legal rules in practice. It also helps regulators gain a better understanding of how rules should apply in a concrete situation.

Article 27 of the Directive already contains provisions encouraging the adoption of codes of conduct for the proper implementation of legal rules in specific sectors. However, to date, very few industry codes have been developed pursuant to Article 27 of the Directive, even though such mechanisms could play an important role in ensuring strong privacy protection in an era when data routinely moves across jurisdictional boundaries, complicating regulatory efforts by national authorities.

The current system— with detailed national implementation of the Directive in each Member State – has not left much room for the promotion of effective self-regulation. This is presumably because

⁷ See for example, the Safer Social Networking Principles for EU and the European Framework for Safer Mobile use by Young Teenagers and Children (http://ec.europa.eu/information_society/activities/sip/self_reg/index_en.htm).

conscientious Member States prefer to prescribe all means to comply with legal rules rather than leave them to self-regulation by the industry in general or data controllers in particular.

An efficient way to foster effective self-regulation would be to revisit Article 27 in a way that would encourage Member States to support self-regulation as a valid means of compliance with EU law. Revisions could also consider promoting pan-European self-regulation in order to strengthen the Single Market.

In practical terms, the changes to the current provisions of Article 27 would be as follows:

First, the first paragraph of Article 27 should be supplemented to cover European-level codes of conduct, taking into consideration the recognised need for a more harmonised implementation of data protection rules in each Member State. The process described in the third paragraph of Article 27 as regards Community codes echoes this wider approach and should be reinforced so as to encourage and support pan-European solutions adopted by industry operators.

Second, the roles of the national and EU-wide authorities (such as the A29WP) should be more clearly defined and, given the nature of self-regulation, data controllers, trade associations and other bodies should be able to consult them on a voluntary basis. Self-regulation should indeed remain a voluntary act by operators and should not depend on regulatory approval at the national or European level that could hamper development and effectiveness with complicated and time-consuming procedures. In that respect, according to the current third paragraph of Article 27, approval by the A29WP is based on analysis of compatibility with national laws, a stipulation that seems to actually duplicate the work responsibilities that individual DPAs already have to measure compliance with their national laws.

Third, it should also be made clear that regulators' approval (or not) of codes of conduct is a separate matter from determinations of individual operators' compliance with the law.

Lastly, Article 27 should also be supplemented to incentivise effective self-regulation, for example by acknowledging a limited legal exposure for operators participating in approved self-regulation schemes.

AmCham EU strongly believes that the above changes should be seriously considered. Implementation could be ensured by assigning responsibility for supporting self-regulation from the standpoint of its economic benefits to a section of the Commission or to a new body at the European level.

Besides the above submission procedures of codes of conduct to the regulatory authorities, AmCham EU also favours industry-developed and managed certifications provided they remain voluntary and affordable. Such certifications should be open to companies both inside and outside the EEA in order to facilitate international data flows. Indeed, industry is able to adapt to new market realities at a faster pace than government, and government does not have the same competitive incentive to enforce proper use of certifications (e.g. icons or seals on web pages) as industry does. In the long term, an industry-developed and managed certification that is endorsed by both EU and non-EU regulators would help reduce compliance burdens on operators and foster competitiveness.

AmCham EU recommends that the Commission take a much more active role in promoting self-regulatory and co-regulatory mechanisms.

4.4 Promoting Competitiveness

The current legislative framework created strong institutions whose primary responsibility is to protect privacy. These include the national Data Protection Authorities (DPAs), the European Data Protection Supervisor (EDPS) and his office, and the Article 29 Working Party. These institutions have done stellar work in privacy protection, and are to be commended. However, AmCham EU believes that the EU should always seek to balance complementary policy objectives.

4.4.1 Promoting dialogue between regulators and industry

DPAs and the A29WP are rightly focused on protecting citizens' privacy. Unfortunately, the way these institutions have interpreted the law and the approaches to compliance they have recommended or required have often failed to reflect technological, commercial or economic realities. We believe this is due in part to the A29WP's failure to adequately consult industry during preparation of its opinions and recommendations.

The Commission should therefore propose that Article 30 be amended to include an obligation for the A29WP to consult industry in the preparation of its opinions and recommendations.

4.4.2 Accountability for economic development in policy making

AmCham EU believes that the respective roles and responsibilities of the A29WP and the Commission as described in Article 30 have not been reflected in practice. Accordingly, these provisions on roles and responsibilities should be strengthened and clarified to require the Commission to assess whether the work of the A29WP has potential economic impacts or impacts other EU policy priorities (including industry consultation, effects on competition, the coherence of the Single Market, or the growth of a specific sector or activity). Further, the Commission should respond to the A29WP's opinions or recommendations in cases where it believes they have such an impact. The A29WP should be given the opportunity to revise its opinions or recommendations in light of the Commission's response. If the Commission believes there is sufficient need to clarify or promote a common approach, it should adopt a Commission Recommendation on the subject.

In addition, the Commission should proactively monitor any Member State's transposition and implementation of the legislative framework, with a view to ensuring a consistent and coherent approach across the EU.

The Commission should present an annual report to the European Parliament on Member States' implementation of the legislative framework and its work on ensuring an appropriate balance between the framework's security, economic and privacy objectives.

In order to promote the EU's competitiveness, the Commission should be given explicit responsibility for ensuring compatibility of the implementation and interpretation of EU data protection law with EU economic and other policy objectives.

5 Addressing globalisation and international data flows

5.1 Cloud computing

Cloud computing solutions are currently growing steadily and should grow even more in the coming years, holding great promise for Europe. Cloud computing also offers innovative ways to enhance data privacy and security. However, these technologies also raise a new set of questions about how to best protect user privacy while simultaneously enabling innovation.

AmCham EU agrees with the European Commission that high standards of data protection are needed within cloud computing. Many AmCham EU members are developing cloud services. Without high standards of data protection these services will not be taken up by customers around Europe, meaning the potential of cloud computing will not be fulfilled. However, there are many open questions about cloud computing and its regulation and these cannot all be addressed in the data protection directive review.

Data protection law is based on protecting data in a given physical infrastructure in a fixed location that can be identified and protected. By definition, current data protection rules will struggle to deal with the realities of cloud computing.

Cloud computing is a technology with many definitions, but it is generally understood as referring to computing services provided to customers through the internet. The Commission's Communication uses the definition 'Internet-based computing whereby software, shared resources and information are on remote servers ('in the cloud')'. AmCham EU would agree with this definition but further nuance it by noting that cloud computing can be either Infrastructure as a Service (IaaS), Software as a Service (SaaS) or Platform as a Service (PaaS). These are, broadly, the main service models of cloud computing. In addition not all clouds are the same. There are public clouds, private clouds and hybrid clouds. Some companies have their own private cloud infrastructure behind their own firewall and governments in Europe are considering this option.

While cloud computing itself is not an entirely new model of computing, its potential is only just being understood. The ability for companies to scale up their computing needs quickly will mean that they can have the processing power they require without having to maintain or purchase infrastructure. Cloud computing, it should be noted, can give access to more expertise as companies can purchase IT security services and have access to

teams of security professionals that the cloud service providers need in order to protect data.

With regard to the Commission's Communication, the main challenge highlighted is the fact that using cloud computing could lead to international transfer of data without the data subject realising that their data has left the country. This touches upon the issue of data transfer outside the EEA that will be discussed in Section 5.2.

Indeed, cloud providers often offer services that transcend geographic boundaries, with data stored on servers in multiple markets, belonging to customers in various jurisdictions and routinely moving across national borders. Differences in national rules on data privacy and security mean that a patchwork of protections, some stronger and some weaker, apply to cloud data. This undermines users' confidence that their data is safe while occasionally creating conflicts between substantive legal obligations imposed on cloud providers.

Several models are available today for the transfer of data outside the EEA. The review of the legal framework is an opportunity to evaluate existing models such as Binding Corporate Rules, the Safe Harbor programme or other international agreements and Standard Contractual Clauses vis-à-vis the cloud and other new challenges, and to propose new ones⁸ to ensure that data is transferred with adequate protection.

Another option for managing international data transfers and cloud computing would be to recognise that companies can move data controlled within their own company or corporate group across international borders. Should a company or a cloud service provider undertake to manage data protection for their own data or for a customer's data within their own IT infrastructure, then they should be allowed to move data internationally. The company providing the service would take on responsibility for ensuring data protection wherever the data is stored globally. This also fits with the principle of accountability, where companies have to be accountable for data protection. This model has been recognised in other countries around the world.⁹ This would allow cloud computing to develop without obliging governments to redraft complex international data transfer rules.

⁸ See discussion of international data flows in section 5.2.

⁹ See, *inter alia*, the APEC Privacy Framework, Asia-Pacific Economic Cooperation Secretariat, 2005.

The review of the data protection Directive also affords an opportunity to remove additional requirements for data transfers. A company doing business in the EEA should be subject to one standard in this area, not a range of them as is currently the case. AmCham EU believes that solutions can be found during review of the data protection Directive that will allow the continued development of cloud services with strong data protection requirements.

5.2 International data flows

The possibility of transferring personal data within globally operating companies and the possibility of involving service providers that may be located in- or outside the EEA is a key requirement of the business community. In many cases it will be far more efficient to involve global service providers, which will require personal data to be transferred, stored and processed in third countries.

Companies are sensitive to the need to provide proper protection of the personal data that they process for their customers and employees. Over the last decade, sensitivity both of the public and of company employees as to how their personal data is collected and processed has significantly increased. Companies have both legal and commercial reasons to comply with data protection laws, including a desire to be successful in the marketplace and to be seen as an employer of choice by employees. Although the current text of Article 26 of the Directive allows for a range of derogations, it would be good to take advantage of the opportunity offered by amending the Directive to introduce improvements.

5.2.1 Adequacy vs. adequate safeguards

The Communication highlights a number of inconsistencies which currently exist in the rules regarding international data transfers and which could be addressed by the new comprehensive framework. The recognition of these problems is welcomed. However, AmCham EU regards the proposal to only examine how the adequacy principle could be further clarified and enhanced as a missed opportunity to reconsider whether the adequacy principle is itself adequate and whether it will still have a role to play in the future legal framework.

Information is already being transferred (under contractual arrangements as allowed by the Directive) to non-EU countries that may in fact fail the adequacy test. We believe that the adequacy principle is itself not working. Therefore, the Commission should reassess the need to ‘clarify’ adequacy procedures and instead examine other means of ensuring data remains protected when transferred internationally.

AmCham EU believes that the adequacy principle could be replaced by the extension of the principle of accountability to international data transfers. A move towards accountability instead of adequacy would mean that a duty of care is placed on all those processing European citizens’ data. Steps would have to be taken to demonstrate that the measures in place ensure a level of security based on the risks that data may face when it is being transferred outside the EEA. For example, in the UK, the Information Commissioner already allows data controllers to make their own assessment of whether personal data would be protected once transferred to a given third country.

Clearly, however, it would be important that a move towards accountability in the international context does not simply become an exercise in form-filling to demonstrate compliance.

The Commission should fully examine how accountability can be operationalised to make it an ongoing responsibility and part of the day-to-day operations of data controllers according to the internal governance models of companies in the EU and beyond.

AmCham EU would welcome the opportunity to explore the concept of an accountability-based transfer regime, providing sufficient safeguards and replacing adequacy for international data flows, in more detail with the Commission.

5.2.2 Binding Corporate Rules

Today, Binding Corporate Rules (BCRs) are a way in which some companies, as accountable data controllers, can transfer some data on a global basis outside the EEA.

The Commission has highlighted the role BCRs can play as a self-regulatory solution that enables organisations to demonstrate

their compliance with data protection requirements. On one hand, BCRs are a good example of a current mechanism that can demonstrate accountability while seeking to reduce administrative burdens. Further, they can encourage harmonisation by seeking mutual recognition by authorities. On the other hand, even though BCRs reflect the principle of accountability, they are currently too narrow in scope (e.g. they are limited to intra-group transfers and do not cover data transfers to data processors) and too burdensome for many companies to implement.

It must indeed be recognised that BCRs are a process that requires a great deal of time, resources and money. Securing approval from all EU data protection regulators with jurisdiction over the relevant data transfers can take from 1.5 to 3 years. Many AmCham EU members have not been in a position to make the necessary investment in applying for BCRs and have chosen other tools to enable international data transfers.

Nevertheless, during the past eight years the processes and procedures put in place to facilitate the drafting and obtaining of BCRs approvals have significantly improved; this has improved the ways in which companies can transfer data on a global basis outside the EEA. The fact that a majority of DPAs have acknowledged that this is one of the most viable transfer tools, that a BCR mutual recognition procedure has been introduced and that the time required to obtain approval of BCRs has been reduced are a few examples of the positive developments in relation to the BCRs process over the past years.

The recently built EU BCRs webpage, with an overview of procedures and national requirements, is also a useful tool. There is of course still room for improvement, including having more countries sign up to the mutual recognition system and further simplifying the approval process. It is also imperative that BCRs be added as a separate legal ground for derogation under Article 26 or at least formally recognised as providing adequate safeguards.

AmCham EU believes that, in general, the BCR process can be a useful tool, but calls upon the EU to promote a less burdensome process and a broadening of their scope of application (e.g. not limited to intra-group transfers and coverage of transfers to processors) in order to realise the full potential of this data transfer solution and accountability tool.

5.2.3 Binding Safe Processor Rules

The BCR model is currently mainly used in cases where companies are controllers of the information they process. It does not cover situations where companies are data processors.

AmCham EU would welcome a pragmatic data transfer solution for processors that would be recognised as providing adequate safeguards. We are therefore interested in contributing to and discussing the outcome of the work undertaken with respect to Binding Safe Processor Rules (BSPRs) in the framework of the formal mandate given to the BCR sub-group during a recent A29WP plenary session. AmCham EU believes that, in principle, the idea of an internal governance model for the processing of personal data by multinational companies that would also cover organisations when they act as processors would be worthwhile to explore.

However, AmCham EU would like to caution that BSPRs could only be considered valuable if mechanisms are put into place to avoid the complexity and considerable resources required by the BCR approval process. Otherwise, companies without BCR experience (or without the means to invest the time, resources and money associated with the complex BCR approval process) would be put at a competitive disadvantage.

AmCham EU calls for a flexible internal governance model for data transfers to processors. AmCham EU sees BSPRs as a potentially useful tool in this respect and is ready to contribute to and discuss the outcome of the current work undertaken by European authorities. However, care must be taken to avoid a BSPR procedure that would maintain the complexities and costs associated with today's BCR approval process.

5.2.4 Safe Harbor

The Safe Harbor programme introduced in 2000 has become a widely-used derogation (more than 2,000 certified organisations) for transferring personal data from Europe to Safe Harbor participants in the U.S. Many AmCham EU members have found this a useful tool that provides legal certainty and enables transatlantic business.

AmCham EU members believe that the protection offered to data subjects via Safe Harbor is as robust as that afforded by national data protection enforcement regimes in the EU. Moreover, its

success and popularity have led to a much greater awareness of EU data protection laws in the U.S. It is therefore unfortunate that the process has recently been subject to some ill-informed criticism. The vast majority of the companies that have certified are aware of their responsibilities and have internal or external compliance programs.

Going forward, improvements could be made that would further increase the value of Safe Harbor. One aspect that could be clarified is that data processors established in the US can also certify for Safe Harbor. Data processors' certifications apply the principle of data security, which is something they can control themselves. To comply with the other Safe Harbor principles they require the cooperation of the European data controller (their client). Such a certification by a data processor can be very practical for American IT vendors which receive personal data from their clients located in the EU and need to process it. For this purpose Safe Harbor can be an alternative to entering into Standard Contractual Clauses.

Onward transfer to other (sub)-data processors can be enabled by putting service agreements in place between the data processor that certified for Safe Harbor and its subcontractors that have data protection clauses that at least equal the level of data security as described in the Safe Harbor principles.

AmCham EU would like to see the Safe Harbor programme recognised as a successful tool in this revision.

5.2.5 Standard Contractual Clauses

The Standard Contractual Clauses (SCCs), including one for transfers between data controllers and a recently updated one for transfers from data controllers and data processors, are by now well-known and are used on a wide scale. Many companies have found them useful tools that require less investment than other options, but they are unfortunately not an effective long-term solution to facilitating international data transfers.

An important road block for an even wider use of these SCCs is that many DPAs want to pre-approve every new set of SCCs even when the parties do not deviate from the standard template of the SCCs. This requirement is cumbersome and does not add any practical value. For some countries, it is even unclear whether their DPA requires prior submission or prior approval of new

SCCs. In case such a prior review is requested, the DPAs should act promptly to make a decision. In some countries this process takes several months. AmCham EU recommends the Commission propose a new framework in such a way that no further national review or approval would be required by national DPAs as long as the parties do not deviate from the template text of the SCC.

The utility of Standard Contractual Clauses could be further improved by giving the parties more flexibility to make changes to SCCs as long as the parties to the SCCs remain the same and there are no amendments to clauses made mandatory by the European Commission.

As long as amendments to SCCs are properly signed by the parties, a further review, with its corresponding delay, would not be required.

Finally, currently there is no clear answer as to which type of SCC needs to be used in cases where the data processor is located in the EEA and the client (the data controller) is located in a third country. When personal data is collected in one or more third countries, which may lack a data protection regime or have one that has lower standards than that of the EEA, the conclusion should be that the Directive (and as a consequence the respective national data protection law) does not apply when these data are processed in the EU (in accordance with the instructions of the client) and after processing in the EU are transferred back to the client.

5.3 Universal principles

Universal principles of data protection should be developed to respond to the challenges raised by global data processing. AmCham EU believes that the EU should continue to play a leadership role in working towards a set of universal data protection principles and welcomes the fruitful dialogue established with U.S. authorities regarding data protection.

6 Cooperation and enforcement

6.1 Better cooperation between DPAs and EU authorities

AmCham EU welcomes the work currently being undertaken by the Article 29 Working Party in relation to cooperation between DPAs. It is crucial that DPAs better coordinate their activities and

cooperate more closely, especially with respect to cross-border matters.

AmCham EU also recognises the need for the work of the A29WP to be more transparent. The European Commission could have an oversight and supervisory role in order to ensure consistency and enable mutual recognition wherever possible.

6.2 Harm-based enforcement

The Directive has an insufficient focus on harms and risks and lacks consistent, practical enforcement mechanisms. With the exceptions of some specific provisions, the Directive does not take a harm-based approach or measure degrees of harm to guide consideration of preventative measures, penalties or effective enforcement mechanisms. Taking a harm-based approach may result in better privacy outcomes and is consistent with the human rights approach of the Directive.

AmCham EU believes that enforcement measures are inconsistently applied. Enforcement action should be robust, harmonised and predictable (to the extent possible) and reflect the responsibility of each party. To the extent that one party is processing on the instructions of another party, that other party should be primarily liable in any enforcement action. The parties should be able to contractually allocate risk. If one party is concerned about data protection liability caused by the other, it can seek an indemnity from that other party. To ensure consistency, Member States should adopt a common approach and multiple laws should not apply to the same process. Revenues obtained should be returned to those affected where identification is possible and should not be used to fund the regulator as this distorts the incentive for pursuing sanctions.

AmCham EU believes that formal considerations of harm to data subjects should be a prerequisite for modern legislation as well as for any enforcement action, most notably for imposing fines.

6.3 Class actions

While AmCham EU supports the need to make remedies and sanctions more effective and believes that this can be done by making them more harmonised and predictable. We do not support the introduction of class action procedures, as suggested by the

A29WP document on “The Future of Privacy” as adopted on 1 December 2009, nor the Communication’s suggestion¹⁰ of “extending the power of data protection authorities, civil society authorities or other associations to bring an action relating to a number of individuals before the national courts”.

AmCham EU cannot support any language that leaves open the possibility of class action suits.

7 Conclusion

AmCham EU looks forward to working with European Union authorities to provide input, expertise and recommendations as the approach to protection of personal data in the EU is reviewed.

* * *

AmCham EU speaks for American companies committed to Europe on trade, investment and competitiveness issues. It aims to ensure a growth-orientated business and investment climate in Europe. AmCham EU facilitates the resolution of transatlantic issues that impact business and plays a role in creating better understanding of EU and US positions on business matters. Aggregate US investment in Europe totalled €1.2 trillion in 2008 and currently supports 4.8 million direct jobs in Europe.

* * *

¹⁰ See section 2.1.7, page 9 of the Communication.

EUROPEAN BANKING FEDERATION (EBF) POSITION ON THE JURI DRAFT OPINION ON THE EUROPEAN COMMISSION PROPOSAL FOR A REGULATION ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA AND THE FREE MOVEMENT OF SUCH DATA

The European Banking Federation supports the objectives of the current review and welcomes the JURI draft opinion on the European Commission proposal for a General Data Protection Regulation as it rightly identified some of the key concerns for the European banking industry.

However, some provisions of the EC proposal remains to be amended and we are therefore pleased to submit to you: a summary of the EBF key priorities (I) the JURI amendments supported by the EBF (II) and the EBF amendments proposed on the Regulation (III).

I. EBF KEY PRIORITIES

A. Data breach notification

- **Introducing an obligation to notify personal data breaches in 24 hours for other sectors than the telecommunications sectors appears disproportionate to the EBF.**
- At present, banks notify their customers for instance if their credit card has been skimmed (i.e. information about a card and the associated PIN-code is copied for the purpose of manufacturing a fake card). It is also in the bank's interest to protect their customers against fraud and sustain a very high level of security. The banks can also be held liable for damages their customers may suffer due to deficiencies in their IT- security systems. The banks test and update their systems and security solutions regularly to make sure that the information in the bank's system is always well-protected and secure. The transfer of information between the customer's computer and the online banking system is always encrypted. The customer must also make sure that his/her computer, codes and personal information are protected to prevent the possibility of fraud. **To avoid "data breaches" it would be more effective to inform customers on how to protect their own computers, never disclose their bank account details to unknown persons etc.**
- A mandatory personal data breach notification system could first give rise to organizational concerns since the implementation of such a system of notification could burden and delay the process of information to the customers.
- Attention should be paid to the criteria which trigger the obligation to notify: **The notification requirement should be limited to serious breaches affecting more than one individual.** There is otherwise a danger of triggering an avalanche of notifications with the potential to confuse unnecessary alarm individuals or desensitise affected data subjects (where notifications are so commonplace they are to a large extent ignored by the recipient, thereby rendering the notification worthless).

- **Exemptions from data breach provisions should be awarded where sophisticated encryption is used.** This will encourage the practice of encrypting personal data, especially prior to their transmission. It should also be possible to dispense with notification if measures are taken to adequately compensate those affected, e.g. by issuing new credit cards to replace cards whose details have been compromised.

A framework where notification is made in the most expedient time possible would achieve the goal of ensuring regulators and data subjects are well informed without causing unnecessary burden for regulators or alarm to victims of breaches. In addition, especially for the banking sector, notification to data subjects at all times may enable certain forms of fraud.

B. Consent

- **Consent given by consumers in a tacit way should be allowed. The word “explicit” should indeed be deleted** as we believe that certain conditions (e.g. definition of certain period of time to opt-out) should be set to constitute a framework to allow for the practice of tacit consent as is already the case in some jurisdictions (e.g. Spain, Austria).
- A typical consent situation within the banking industry is the transfer of data to credit agencies. This consent may under the regulation not be deemed as freely given as almost all banks require customers to sign credit agency consent. However, it is in the interest of the financial marketplace, the very financial institution and the data subject (prevent excessive indebtedness, insolvency) that there is a working credit information system.
- Often customers may be perceived as being in a situation of imbalance with respect to companies that process personal data. It will be difficult to ascertain what “significant imbalance” may mean.

C. Right to data portability - Article 18

- **The portability principle seems to be designed for new technology / information society industry.** Therefore **the EBF would like to limit the scope of Article 18 to storage of data in online-databases.** Indeed, the extension of such a right to the financial sector seems inappropriate considering the nature of the data kept in bank servers, their sensitiveness and their variety. Should the scope of this provision not be limited, we are indeed concerned that the right to data portability increases the risk of disclosure of personal data to third parties.
- The EBF also would like to stress that the exercise of this right could require organizations to disclose information on trade secrets or information on other customers. The banking industry has to comply with retention requirements deriving from commercial and tax law. The obligation to bank secrecy should be taken into account.
- If we take the example of a customer with a real estate loan. The data held about this customer including his financial credit worthiness represents at the same time intellectual property of the very financial institution, which is protected by constitutional rights as well.
- This principle cannot lead to a completely imbalanced between claimant and defendant in case of a civil litigation as the data subject may be in the position to extract all data from the affected company or extract at least information which would have to be provided under the very civil procedure rules.

D. Profiling - Article 20

- Profiling is a typical technique used in the area of Anti Money Laundering to identify unusual financial transactions which might not fit in the financial profile of the customer. This is required by the Anti Money Laundering laws and it is also in the interest of the very financial institution not to be misused by criminal actions. It is therefore based on the balance of interests.
- It is important to stress that it might be an information overload for the customers if this information have to be given in advance of an e.g. current account contract.
- In addition, as not all requirements regarding Anti Money Laundering derive from the law itself but from supervisory authority circulars we believe that it is imperative to resolve the relationship of draft regulation and the Anti Money Laundering Directive, local implementations and deduced circulars.
- Furthermore, it can be noted that the draft regulation extends the restrictions of the 1995 Directive to practices that do not necessarily have a negative effect for people if they are intended to make information more relevant and more useful for the individual. The new rules could compromise the effort made by companies to offer their customers "customised" products and services and degrade the quality of services offered to European citizens. Moreover, provisions on profiling need to allow profiling for legitimate interests and purposes that are for example intended to respond to consumer demands. In other words, there is no need to require additional and specific conditions for this type of profiling.

E. Fraud - Notably Article 6, 9, 20 and Lawfulness of processing - Article 6.1

- The EBF suggests adding particular cases of lawful processing of data. The EBF considers that detecting and preventing fraud in consumer lending is of significant importance, not only to financial institutions, but can help to protect consumers from identity theft. Therefore, fraud prevention and detection should be explicitly recognised as a legitimate purpose for data processing.
- Banks are entitled to process fraud data in order to prevent frauds and minimize risks related to the granting of credits and undertakings. The processing of this kind of sensitive data is currently possible if data protection authorities issue permission for reason for pertaining to an important public interest. **The EBF wonders whether the restrictions of Article 9 of the proposed regulation will still allow the maintenance of such databases in the future.**
- The EBF thinks that Article 6.1.c should be widened-up to include orders, recommendations of competent organizations as well as the requirements of supervisory authorities. In an on-line world and a global economy, international standards of supervisory bodies should indeed be recognized.

II. JURI AMENDMENTS SUPPORTED BY THE EBF

The European Banking Federation (EBF) welcomes the following changes which have been made to the draft text in the JURI draft opinion:

- Amendment 4 to Recital 27 containing a precise definition of main establishment is welcome for financial institutions operating in several Member States.
- Amendment 12 to Recital 67 where it is recognized that substantial breaches only should be notified.
- Amendment 13 to Recital 82 which brings clarity to the issue of the transfer of data to third countries.
- Amendment 22 to Article 4.2 bis that defines the concept of anonymous data which helps giving more legal certainty.
- Amendment 24 to Article 6.1.f where maintain the wording of Directive 95/46/EC authorises the use of third parties (e.g. credit bureaux).
- Amendment 34 to Article 15.2 which enables to verify the identity of the person requesting access in order to avoid abuses.
- Amendment 36 to Article 18 and the deletion of the right to portability which the EBF found specific to the social networks but irrelevant for the banking sector.
- Amendments 25, 29, 30, 40, 41,47, 60, 67
- Amendment 43 which helps defining clearly the information that the documentation shall contain.
- Amendment 48 to Article 31.1 which recognizes to concentrate on the measures to prevent a breach and not on minor breaches.
- Amendment 50 to Article 33 paragraph 4 which recognizes the disproportion of the EC proposal regarding the requirement of an impact assessment.
- Amendment 71 and the call for technological neutrality.

However, the EBF believes that the draft JURI opinion still requires further improvements and would strongly recommend a number of additional amendments as detailed in the attached table.

III. EBF PROPOSED AMENDMENTS TO JURI DRAFT OPINION ON THE EC PROPOSAL FOR A GENERAL DATA PROTECTION REGULATION

- Recital 25 on the conditions of consent

EC proposal	JURI amendment 3	EBF proposed amendment
<p>(25) Consent should be given explicitly by any appropriate method enabling a freely given specific and informed indication of the data subject's wishes, either by a statement or by a clear affirmative action by the data subject, ensuring that individuals are aware that they give their consent to the processing of personal data, including by ticking a box when visiting an Internet website or by any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data. Silence or inactivity should therefore not constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. If the data subject's consent is to be given following an electronic request, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.</p>	<p>(25) Consent should be given explicitly by any methods appropriate to the media used enabling a freely given specific and informed indication of the data subject's wishes, either by a statement or by a clear affirmative action by the data subject, ensuring that individuals are aware that they give their consent to the processing of personal data, including by ticking a box when visiting an Internet website or by any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data. Silence or inactivity should therefore not constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. If the data subject's consent is to be given following an electronic request, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.</p>	<p>(25) Consent should be given explicitly by any appropriate method enabling a freely given specific and informed indication of the data subject's wishes, either by a statement or by a clear affirmative action by the data subject, ensuring that individuals are aware that they give their consent to the processing of personal data, including by ticking a box when visiting an Internet website or by any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data. Silence or inactivity should therefore not constitute consent.</p>
<p>Justification</p> <p>Consent given by consumers in a tacit way should be allowed. The word “explicit” should indeed be deleted as we believe that certain conditions (e.g. definition of certain period of time to opt-out) should be set to constitute a framework to allow for the practice of tacit consent as is already the case in some jurisdictions (e.g. Spain, Austria).</p> <ul style="list-style-type: none"> A typical consent situation within the banking industry is the transfer of data to credit agencies. This consent may under the regulation not be deemed as freely given as almost all banks require customers to sign credit agency consent. However, it is in the interest of the financial marketplace, the various financial institutions and the data subject (prevent excessive indebtedness, insolvency) that there is a working credit information system. 		

- Article 6 1. f on the Lawfulness of processing

EC proposal	JURI amendment 24	EBF proposed amendment
<p>(f) processing is necessary for the purposes of the legitimate interests pursued by a controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks</p>	<p>(f) processing is necessary for the purposes of the legitimate interests pursued by a controller or by a third party or third parties to whom the data are communicated, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks.</p>	<p>(f) processing is necessary for the purposes of the legitimate interests pursued by a controller, or by the third party or parties to whom the data are disclosed except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks.</p> <p>(g) the data are collected from public registers, lists or documents accessible by everyone;</p> <p>(h) the processing is necessary to defend an interest, collecting evidences as judicial proofs or file an action.</p>
<p style="text-align: center;">Justification</p> <ul style="list-style-type: none"> The EBF agrees with the approach proposed by the draft opinion of the JURI Committee mentioning that “processing is necessary for the purposes of the legitimate interests pursued by a controller or by a third party or third parties to whom the data are communicated”. Indeed, the lawfulness of processing based on the legitimate interest must be extended to legitimate interests pursued by third parties to whom the data are disclosed by a controller as otherwise, the consequences could be to exclude the possibility for data suppliers to supply on a legitimate basis data to final users of such data even if the legitimate interest is recognized and justified. In addition, the EBF suggests adding particular cases of lawful processing of data. Processing of personal data shall be lawful if the data are collected from public registers, lists or documents accessible by everyone and if the processing is necessary to defend an interest, collecting evidences as judicial proofs or file an action. 		

- Article 7 on the conditions for consent (right of withdrawal)

EC proposal	JURI amendment 26	EBF proposed amendment
<p>3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.</p> <p>4. Consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller.</p>	-	<p>3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal or in cases where a minimum mandatory term of storage is provided by a European or national law, or data are processed according to European and national regulatory provisions, or for anti-fraud or legal purposes. The data subject has to communicate his willingness to withdraw his or her consent to the processor. The withdrawal of the consent is effective 30 days after the receipt of the declaration.</p> <p>4. Consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller.</p>
<p style="text-align: center;">Justification</p> <ul style="list-style-type: none"> Often customers may be perceived as being in a situation of imbalance with respect to companies that process personal data. It will be difficult to ascertain what “significant imbalance” may mean. If one argues that customers are often in a situation of imbalance with respect to companies, consent will never be a legitimate ground to base data processing. This collides with the principle that there are six legitimate grounds for the processing of data in Article 6.1 of the draft Regulation, consent being one of them. In addition, there are situations where data subjects will be confronted with the choice of granting or not consent with negative consequences if they do not provide it. In these situations such choice will bring data subjects in a situation of imbalance. This provision is likely to negatively affect the banking sector. Some may argue for instance that banks and their customers may be in a situation of imbalance. This may lead 		

banks not being able to rely on consent.

The banking sector is subject to worldwide heavy regulators’ controls, which may require the processing of personal data for numerous specific situations to meet legal and regulatory obligations. In certain circumstances, well informed consent may be the sole adequate ground for processing data in order to meet the privacy rights of data Subjects. If article 7.4 remains, the banking sector will be detrimentally affected and will be indirectly put in a situation of inequality with respect to other sectors.

The EBF would therefore suggest deleting the entire paragraph 4 of Article 7.

- The right of data subject to withdraw their consent at any time can actually prevent the performance of legal requirements such as those of responsible lending. It may become very difficult for financial institutions to find appropriate information in clients’ databases (collecting either negative or positive information) to assess their creditworthiness when the clients may withdraw their consent whenever they feel like (for example at their very moment when their debts become overdue). The compliance with the Consumer Credit Directive Requirements (and future Mortgage Credit Directive as well) can hardly be assured and the effectiveness of creditworthiness assessment diminished.
- In the employment context, it may be appropriate that the employer can process health information concerning the employee's sick leave or data of employees covered by the collective agreements social chapters. It is also very uncertain whether an employer can process personal data concerning health at all, when the nature of art. 7, 9 and 81 is compared. If the employer cannot process health information it will complicate efforts to maintain the employee's relationship with the company and the labour market.
- It would also be extremely intrusive, if the employers no longer can process criminal records in employment. In the financial sector, it is very important that the employer is able to do so. For example, it is not reassuring that employers in connection with employment, of employees that handle the customers' money transactions, does not have the possibility to determine whether, the employee previously has been convicted of financial crimes. This process is also here governed by the general principles of treatment in Article 5 which is sufficient.
- The continued processing should be permitted in order to continue the contractual relationship that may exist between the controller and the data subject, or to allow the fulfillment of any obligation of the controller, or to respect legal basis.

• Article 12, paragraph 1, 2 and 4 Procedures and mechanisms for exercising the rights of the data subject

EC proposal	JURI amendment	EBF proposed amendment
1. The controller shall establish procedures for providing the information referred to in Article 14 and for the exercise of the rights of data subjects referred to in Article 13 and Articles 15 to 19. The controller shall provide in particular	-	1. The controller shall establish procedures for providing the information referred to in Article 14 and for the exercise of the rights of data subjects referred to in Article 13 and Articles 15 to 19. The controller shall provide in particular mechanisms for

<p>mechanisms for facilitating the request for the actions referred to in Article 13 and Articles 15 to 19. Where personal data are processed by automated means, the controller shall also provide means for requests to be made electronically.</p> <p>2. The controller shall inform the data subject without delay and, at the latest within one month of receipt of the request, whether or not any action has been taken pursuant to Article 13 and Articles 15 to 19 and shall provide the requested information. This period may be prolonged for a further month, if several data subjects exercise their rights and their cooperation is necessary to a reasonable extent to prevent an unnecessary and disproportionate effort on the part of the controller. The information shall be given in writing. Where the data subject makes the request in electronic form, the information shall be provided in electronic form, unless otherwise requested by the data subject.</p> <p>3. If the controller refuses to take action on the request of the data subject, the controller shall inform the data subject of the reasons for the refusal and on the possibilities of lodging a complaint to the supervisory authority and seeking a judicial remedy.</p> <p>4. The information and the actions taken on requests referred to in paragraph 1</p>		<p>facilitating the request for the actions referred to in Article 13 and Articles 15 to 19. Where personal data are processed by automated means, the controller shall may also provide means for requests to be made electronically.</p> <p>2. The controller shall inform the data subject without delay and, at the latest within two months of receipt of the request, whether or not any action has been taken pursuant to Article 13 and Articles 15 to 19 and shall provide the requested information. This period may be prolonged for a further month, if several data subjects exercise their rights and their cooperation is necessary to a reasonable extent to prevent an unnecessary and disproportionate effort on the part of the controller. The information shall be given in writing. Where the data subject makes the request in electronic form, the information shall be provided in electronic form through a secure procedure, unless otherwise requested by the data subject. Before providing any data and in order to prevent any data breach possibilities, a proper identification of the data subject is needed.</p> <p>3. If the controller refuses to take action on the request of the data subject, the controller shall inform the data subject of the reasons for the refusal and on the possibilities of lodging a complaint to the supervisory authority and seeking a judicial remedy.</p> <p>4. The information and the actions taken on requests referred to in paragraph 1 shall be</p>
---	--	--

<p>shall be free of charge. Where requests are manifestly excessive, in particular because of their repetitive character, the controller may charge a fee for providing the information or taking the action requested, or the controller may not take the action requested. In that case, the controller shall bear the burden of proving the manifestly excessive character of the request.</p>		<p>free of charge once a year. Where requests are manifestly excessive, in particular because of their repetitive character, the controller may charge a fee for providing the information or taking the action requested, or the controller may not take the action requested. In that case, the controller shall bear the burden of proving the manifestly excessive character of the request.</p>
--	--	---

Justification

- The delay to inform the data subject is too short.
- The EBF considers that the controller should remain free to provide means to individuals for exercising their rights. We acknowledge the fact that data subjects may request information electronically. However, the EBF believes that a secure way is needed to be able to provide the said data. **A proper identification of the subject is needed before providing any data and to prevent any data breach possibilities. Furthermore the data subject has to support a secure procedure for the transmission of the data via Internet**, e.g. encryption mechanism.
- Providing the required information implies administrative expenses (not for profit) for European banks. Therefore, **the EBF considers that data controllers should be permitted to request an appropriate (not for profit) contribution in order to cover the administrative costs of providing that information.** In case the Commission considers this opportunity of paramount importance the EBF would **suggest limiting the free of charge only if the access is exercised once a year.**
- The EBF objects to the idea of giving the Commission the mandate to lay down standard forms and standard procedures for the communication, including the electronic format. It should be up to the bank and the customer to decide on how to communicate. **The EBF therefore welcomes the amendments suggested by the JURI draft opinion.**

- Article 17, paragraph 1(a) Right to be forgotten and to erasure

EC proposal	JURI amendment	EBF proposed amendment
<p>1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available</p>	-	<p>1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data</p>

<p>by the data subject while he or she was a child, where one of the following grounds applies:</p> <p>(a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; (...)</p>		<p>subject while he or she was a child, where one of the following grounds applies:</p> <p>(a) the data are no longer necessary in relation to the purposes for which they were collected or further processed and the legally mandatory minimum retention period has expired (...)</p>
--	--	--

Justification

The EBF is convinced that this article designed to protect internet social media users, may be extremely difficult to execute in the banking sector. Banks are obliged to store some data. For instance, for statistics purposes to process credit applications and assess objectively the creditworthiness of customers. As identified in others amendments the right to be forgotten and erasure should be limited in particular taking in consideration the data held by credit reference bureau. It should be paid attention to the misuse of this right in the field of credit.

Meeting the obligations the 3rd EU Anti-Money Laundering (AML) Directive also implies the storage of data for a long period of time. Article 30 of the 3rd AML Directive provides for instance that in the case of the customer due diligence the record keeping of documents and information is required for a period of **at least five years** after the business relationship with their customer has ended.

In the majority of cases, banks shall therefore not be able to erase all the data processed – on request of the data subject.

The term ‘further processed’ strikes a better balance regarding the Articles 6.4 and 5 b of the European Commission’s proposal

- **Article 20.2.c Measures based on profiling**

EC proposal	JURI amendment	EBF proposed amendment
<p>1. Every natural person shall have the right not to be subject to a measure which produces legal effects concerning this natural person or significantly affects this natural person, and which is based solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health,</p>	<p style="text-align: center;">-</p>	<p>1. Every natural person shall have the right not to be subject to a measure decision which produces legal effects concerning this natural person or significantly affects this natural person, and which is based solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences,</p>

<p>personal preferences, reliability or behaviour.</p> <p>2. Subject to the other provisions of this Regulation, a person may be subjected to a measure of the kind referred to in paragraph 1 only if the processing:</p> <p>(a) is carried out in the course of the entering into, or performance of, a contract, where the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or where suitable measures to safeguard the data subject's legitimate interests have been adduced, such as the right to obtain human intervention; or</p> <p>(b) is expressly authorized by a Union or Member State law which also lays down suitable measures to safeguard the data subject's legitimate interests; or</p> <p>(c) is based on the data subject's consent, subject to the conditions laid down in Article 7 and to suitable safeguards.</p> <p>3. Automated processing of personal data intended to evaluate certain personal aspects relating to a natural person shall not be based solely on the special categories of personal data referred to in Article 9.</p> <p>4. In the cases referred to in paragraph 2, the information to be provided by the controller under Article 14 shall include information as to the existence of</p>		<p>reliability or behaviour.</p> <p>2. Subject to the other provisions of this Regulation, a person may be subjected to a measure of the kind referred to in paragraph 1 only if the processing:</p> <p>(a) is carried out in the course of the entering into, or performance of, a contract, where the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or where suitable measures to safeguard the data subject's legitimate interests have been adduced, such as the right to obtain human intervention; or</p> <p>(b) is necessary to comply with expressly authorized by a Union or Member State law which also lays down suitable measures to safeguard the data subject's legitimate interests; or</p> <p>(c) is based on the data subject's consent, subject to the conditions laid down in Article 7 and to suitable safeguards.</p> <p>3. Automated processing of personal data intended to evaluate certain personal aspects relating to a natural person shall not be based solely on the special categories of personal data referred to in Article 9.</p> <p>4. In the cases referred to in paragraph 2, the information to be provided by the controller under Article 14 shall include information as to the existence of</p>
--	--	--

<p>processing for a measure of the kind referred to in paragraph 1 and the envisaged effects of such processing on the data subject.</p> <p>5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for suitable measures to safeguard the data subject's legitimate interests referred to in paragraph 2.</p>		<p>processing for a measure of the kind referred to in paragraph 1 and the envisaged effects of such processing on the data subject.</p> <p>5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for suitable measures to safeguard the data subject's legitimate interests referred to in paragraph 2.</p>
---	--	---

Justification

- The EBF is concerned on the impact of the provisions concerning profiling to the European banking industry. The definition being too broad should be adapted as only decision having legal effect can be taken into consideration.
- Profiling is a typical technique used in the area of Anti Money Laundering to identify unusual financial transactions which might not fit in the financial profile of the customer. This is required by the Anti Money Laundering laws and it is also in the interest of the various financial institutions not to be misused by criminal actions. It is therefore based on the balance of interests.
- It is important to stress that it might be an information overload for the customers if this information have to be given in advance of an e.g. current account contract.
- In addition, as not all requirements regarding Anti Money Laundering (AML) derive from the law itself but from supervisory authority circulars we believe that it is imperative to resolve the relationship of draft regulation and the AML Directive, local implementations and deduced circulars.
- Furthermore, the rules on profiling should not prohibit or restrict risk assessment as part of lending practices as foreseen for example in the EU Consumer Credit Directive and in banking supervisory law (risk-based approach by “Basel II”). The draft Regulation extends the restrictions of Directive 95/46 to practices that do not necessarily have a negative effect for people if they are intended to make information more relevant and more useful for the individual. By encompassing all forms of personalisation, whatever the possible impact on users, the new rules could compromise the effort made by companies to offer their customers "customised" products and services and degrade the quality of services offered to European citizens.
- Delegated acts for this purpose are not necessary: paragraph 2 is sufficient.

- Article 79 Administrative sanctions

EC proposal	JURI amendment 63	EBF proposed amendment
<p>3. In case of a first and non-intentional non-compliance with this Regulation, a warning in writing may be given and no sanction imposed, where:</p> <p>(a) a natural person is processing personal data without a commercial interest; or</p> <p>(b) an enterprise or an organisation employing fewer than 250 persons is processing personal data only as an activity ancillary to its main activities.</p>	<p>3. <i>The supervisory authority may give a written warning without imposing a sanction. The supervisory authority may impose a fine of up to EUR 1 000 000 for repeated, deliberate breaches or, in the case of a company, of up to 2 % of its annual worldwide turnover.</i></p>	<p>3. The supervisory authority may give a written warning without imposing a sanction. The supervisory authority may impose a fine of up to EUR 1 000 000 for repeated, deliberate breaches or, in the case of a company, of up to 2 % of its annual worldwide turnover.</p>
<p>Justification</p> <ul style="list-style-type: none"> Article 79 use a mandatory language and states that supervisory authorities “shall impose a fine” in the situations described. This leads to a situation where very little margin of appreciation is left to the supervisory authorities. In this regard, EBF would like to stress, at the outset, the importance of the clarity and certainty of the obligations set out in the proposed Regulation. <p>The EBF members believes that generally sanctions should not be systematically imposed and a margin of discretion in deciding when to impose a fine should be left to the supervisory authority since many factors influence the nature of the infringement (EDPS opinion, paragraph 266; Working Party Article 29 opinion, page 23).</p> <p>In this perspective, the EBF is more in favor of the JURI draft opinion mentioning that “The supervisory authority may impose a fine” instead of “shall impose a fine” mentioned in the Commission’s proposal and welcome the deletion of the other articles relating to the administrative sanctions.</p> <ul style="list-style-type: none"> In addition, the EBF would like to stress that according to the subsidiarity principle usually regulation in the area of administrative proceedings and the imposition of administrative fines fall within the competences of the Member States. <p>The EBF considers that the sole criteria of the annual worldwide turnover of enterprises could lead to very disproportionate amounts of fines; therefore the administrative sanctions should be limited to a fixed amount.</p>		

We hope that you will find these remarks helpful and thank you in advance for taking them into consideration for your future work on the Regulation.

Contact persons:

Séverine Anciberro: s.anciberro@ebf-fbe.eu;

Fanny Derouck: f.derouck@ebf-fbe.eu;

Noémie Papp : noemie.papp@ebf-fbe.eu

Implementing the Accountability Concept in the Data Protection Regulation

Accountability principles and implementing accountability concept

Accountability is a well-established principle of data protection, found in existing guidance such as the OECD Guidelines¹ and APEC Privacy Framework² and in the laws of for example Canada and Mexico. Regulators, industry and advocacy groups have further defined the essential elements of accountability³. According to the accountability principle, all organizations engaged in the processing of personal data, including controllers and processors irrespective of their size, should be held accountable for implementing appropriate, demonstrable and effective technical and organizational measures by means of a privacy program to ensure proper protection of personal data. Essential elements of effective privacy programs include:

1. Sufficient management oversight;
2. Policies, processes and practices to make the policies effective;
3. Risk assessment and mitigation planning procedures;
4. Adequately skilled data protection staff;
5. Awareness and training of staff;
6. Internal enforcement;
7. Issue response; and
8. Remedies to those whose privacy has been put at risk.

Privacy programs should be tailored having regard to the type of the organization, the nature of the processed personal data and the state of the art of technologies and available methodologies, for example to carry out a data protection impact assessment. Implementing the superior Accountability concept in the Data Protection Regulation instead of opting for the antiquated prescriptive and straight-jacked set of compliance requirements as currently proposed would in practice lead to improved data protection. Accordingly, a flexible, yet clear requirement of an effective data protection program could be established in the Regulation. Other administrative requirements, such as the overly prescriptive documentation requirements contained in the proposal, should in return be reduced.

Data Protection Impact Assessment (DPIA) and prior consultation.

According to the Accountability concept, all processing of personal data should be planned appropriately, including the carrying out of risk assessments prior to commencing the processing. No specific type of DPIA should be mandated nor should the assessment obligation be reserved to any specific type of processing. Prior consultation should only take place when the processing is based on the legal grounds of either 'exercise of public authority' (art. 6.1 e) or the 'legitimate interests test' (art. 6.1 f) *and* the processing in question is likely to present specific significant risks to data subjects. This means for instance that a prior consultation should not be required when the processing is based on 'consent' (art. 6.1 a) or 'contract' (art. 6.1 b). The activity of supervisory authorities can consequently altogether be much more focused on ex-post controls rather than ex-ante clearance of processing operations.⁴

Implications to the Regulation

This approach, including the new article 22 would effectively codify in a single article the main structural and organizational requirements necessary to effectively comply with the Regulation; it would therefore entail amending and simplifying articles 23, 28, and 33-37.

¹ http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1_00.html

² http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx

³ http://www.informationpolicycentre.com/accountability-based_privacy_governance/

⁴ Recommendations of the Article 29 Data Protection Working Party in its Opinion 3/2010, par. 54 and 63

Set of Amendments implementing the Accountability Principle into Law

Article 22 (Responsibility of the controller)	
Commission proposal	Proposed amendment
<p>1. The controller shall adopt policies and implement appropriate measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation.</p> <p>2. The measures provided for in paragraph 1 shall in particular include:</p> <p>(a) keeping the documentation pursuant to Article 28;</p> <p>(b) implementing the data security requirements laid down in Article 30;</p> <p>(c) performing a data protection impact assessment pursuant to Article 33;</p> <p>(d) complying with the requirements for prior authorisation or prior consultation of the supervisory authority pursuant to Article 34(1) and (2);</p> <p>(e) designating a data protection officer pursuant to Article 35(1).</p> <p>3. The controller shall implement mechanisms to ensure the verification of the effectiveness of the measures referred to in paragraphs 1 and 2. If proportionate, this verification shall be carried out by independent internal or external auditors.</p>	<p><i>1. Having regard to the state of the art, the nature of personal data processing and the type of the organization, both at the time of the determination of the means for processing and at the time of the processing itself, the controller and processor shall implement appropriate and demonstrable technical and organizational measures in such a way that the processing will meet the requirements of this Regulation and ensures the protection of the rights of the data subject by design.</i></p> <p><i>2. Such measures include, without limitation,</i></p> <p><i>(a) Sufficiently independent management oversight of processing of personal data to ensure the existence and effectiveness of the technical and organizational measures;</i></p> <p><i>(b) Existence of proper policies, instructions or other guidelines to guide data processing needed to comply with the Regulation as well as procedures and enforcement to make such guidelines effective;</i></p> <p><i>(c) Existence of proper planning procedures to ensure compliance and to address potentially risky processing of personal data prior to the commencement of the processing;</i></p>

<p>4. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures referred to in paragraph 1 other than those already referred to in paragraph 2, the conditions for the verification and auditing mechanisms referred to in paragraph 3 and as regards the criteria for proportionality under paragraph 3, and considering specific measures for micro, small and medium-sized-enterprises.</p>	<p><i>(d) Existence of appropriate documentation of data processing to enable compliance with the obligations arising from the Regulation;</i></p> <p><i>(e) Existence of adequately skilled data protection organization or data protection officer or other staff supported with adequate resources to oversee implementation of measures defined in this article and to monitor compliance with this Regulation, having particular regard to ensuring sufficient organizational independence of such data protection officer or other staff to prevent inappropriate conflicts of interest. Such a function may be fulfilled by way of a service contract;</i></p> <p><i>(f) Existence of proper awareness and training of the staff participating in data processing and decisions thereto of the obligations arising from this Regulation;</i></p> <p><i>3. Upon request by the competent data protection authority, the controller or processor shall demonstrate the existence of technical and organizational measures.</i></p> <p><i>4. Group of undertakings may apply joint technical and organizational measures to meet its obligations arising from the Regulation.</i></p> <p><i>5. This article does not apply to a natural person processing personal data without commercial interest.</i></p>
---	--

Justification

We believe all organizations engaged in the processing of personal data, including controllers and processors irrespective of their size, should be held accountable for implementing appropriate, demonstrable and effective technical and organizational measures to ensure compliance with the Regulation. Accountability is a well-established principle of data protection, found in existing guidance such as the OECD Guidelines¹ and APEC Privacy Framework² and in the laws of for example Canada and Mexico.

Implementing such Accountability concept in the Data Protection Regulation instead of opting for the antiquated prescriptive and straight-jacked set of detailed and prescriptive compliance requirements as currently proposed would in practice allow controllers, processors and DPAs to focus their attention on what is really necessary to deliver optimal data protection. This will result in improved data protection and avoid unnecessary burden for all parties involved.

Amendment

Art 23 (Data Protection by Design/Default)	
Commission proposal	Proposed amendment
<p>1. Having regard to the state of the art and the cost of implementation, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.</p>	<p>1. Having regard to the state of the art and, the cost of implementation and international best practices, appropriate measures and procedures shall be implemented where technically feasible to ensure the processing operation meets, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensures the protection of the rights of the data subject.</p>

¹ http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html

² http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/_media/Files/Groups/ECSG/05_ecsq_privacyframewk.ashx

<p>2. The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals.</p>	<p>2. <i>Such measures and procedures shall:</i></p> <ul style="list-style-type: none"> (a) <i>follow the principle of technology, service and business model neutrality</i> (b) <i>be based on global industry-led efforts and best practices</i> (c) <i>be flexible based on an entities' business model, size, and level of interaction with personal data</i> (d) <i>take due account of existing technical standards and regulations in the area of public safety and security</i> (e) <i>take due account of international developments</i> <p>2. The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals.</p>
<p>3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures and mechanisms referred to in paragraph 1 and 2, in particular for data protection by design</p>	<p>3. <i>In implementing the provisions of this Regulation, it shall be ensured that no mandatory requirements for specific technical features are imposed on products and services, including terminal or other electronic communications equipment, which could impede the placing of equipment on the market</i></p>

<p>requirements applicable across sectors, products and services.</p> <p>4. The Commission may lay down technical standards for the requirements laid down in paragraph 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>	<p><i>and the free circulation of such equipment in and between Member States.</i></p> <p><i>The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures and mechanisms referred to in paragraph 1 and 2, in particular for data protection by design requirements applicable across sectors, products and services.</i></p> <p><i>4. The Commission may lay down technical standards for the requirements laid down in paragraph 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</i></p>
--	--

Justification

Privacy by design is an important concept. Having in place technical and organizational measures helps to ensure data protection is at the heart of privacy by design. However, art. 23 appears to be a generic definition, while other articles include further and more detailed data protection by design –type of obligations. For example, the current proposed art. 23 to a large extent overlaps with art. 22 and art. 5 c). In addition, some of the needed technical and organizational measures are actually those defined in, for example, in the following articles: Art. 26 (processor agreements), art. 28 (documentation), art. 30 (security), art. 33 (data protection impact assessment) and art. 35 (data protection officer). We believe that such repetition is likely to lead to confusion and does not add value. A better result is achieved through an improved art. 22 as suggested by amendment 30 introducing the Accountability concept and by adding the last sentence of proposed art. 23.2 to art. 5 b) (principles relating to personal data processing).

Amendment

Article 28 (documentation)	
Commission proposal	Proposed amendment
<p>1. Each controller and processor and, if any, the controller's representative, shall maintain documentation of all processing operations under its responsibility.</p> <p>2. The documentation shall contain at least the following information:</p> <p>(a) the name and contact details of the controller, or any joint controller or processor, and of the representative, if any;</p> <p>(b) the name and contact details of the data protection officer, if any;</p> <p>(c) the purposes of the processing, including the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);</p> <p>(d) a description of categories of data subjects and of the categories of personal data relating to them;</p> <p>(e) the recipients or categories of recipients of the personal data, including the controllers to whom personal data are disclosed for the legitimate interest pursued by them;</p>	<p>1. Each controller and processor and, if any, the controller's representative, shall maintain documentation of <i>all the main categories of</i> processing operations under its responsibility.</p> <p>2. Such documentation shall contain at least the following information:</p> <p>(a) the name and contact details of the, or any joint controller or processor, and of the representative, if any;</p> <p>(b) the name and contact details of the data protection organization or data protection officer, if any;</p> <p>(c) the generic purposes of the processing including the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);</p> <p>(d) a description of categories of data subjects and of the categories of personal data relating to them;</p> <p>(e) the categories of recipients of the personal data, including the controllers to whom personal data are disclosed for the legitimate interest pursued by them;</p>

<p>(f) where applicable, transfers of data to a third country or an international organisation, including the identification of that third country or international organisation and, in case of transfers referred to in point (h) of Article 44(1), the documentation of appropriate safeguards;</p> <p>(g) a general indication of the time limits for erasure of the different categories of data;</p> <p>(h) the description of the mechanisms referred to in Article 22(3).</p> <p>3. The controller and the processor and, if any, the controller's representative, shall make the documentation available, on request, to the supervisory authority.</p> <p>4. The obligations referred to in paragraphs 1 and 2 shall not apply to the following controllers and processors:</p> <p>(a) a natural person processing personal data without a commercial interest; or</p> <p>(b) an enterprise or an organisation employing fewer than 250 persons that is processing personal data only as an activity ancillary to its main activities.</p> <p>5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the documentation</p>	<p>(f) where applicable, transfers of personal data to a third country or an international organisation, and, in case of transfers referred to in point (h) of Article 44(1), a reference to safeguards employed;</p> <p>(g) a general indication of the time limits for erasure or data retention policy applicable to the different categories of data;</p> <p>(h) the description of the mechanisms referred to in Article 22(3).</p> <p>3. The controller and the processor and, if any, the controller's representative, shall make the documentation available, on the basis of a request outlining the reasons for requiring access to the documents, to the supervisory authority.</p> <p>4. The obligations referred to in paragraphs 1 and 2 shall not apply to the following controllers and processors:</p> <p>(a) a natural person processing personal data without a commercial interest; or</p> <p>(b) an enterprise or an organisation employing fewer than 250 persons that is processing personal data only as an activity ancillary to its main activities.</p> <p>5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the documentation referred to in paragraph 1, to take account of in particular the</p>
--	--

referred to in paragraph 1, to take account of in particular the responsibilities of the controller and the processor and, if any, the controller's representative.	responsibilities of the controller and the processor and, if any, the controller's representative.
6. The Commission may lay down standard forms for the documentation referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	6. To ensure harmonized requirements within Europe , the Commission may lay down standard forms for the documentation referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Justification

Effective data protection requires that organizations have a sufficiently documented understanding of their data processing activities. The documentation requirement in art 28.2 appears to largely duplicate the notification provisions in art. 14, is unnecessarily burdensome and even empowers the Commission to provide even more detailed documentation requirements. Instead of satisfying bureaucratic needs, the aim of the documentation should be to help controllers and processors meet their obligations and the lead DPA to effectively enforce the Regulation. Companies have many ways of documenting their data processing environment and no specific method should be mandated. Often such documentation exists through multiple means. A very detailed documentation would remain an almost instantly outdated snapshot of a constantly changing reality characterized by complex data processing arrangements in a multiparty environment. It should be left to the controllers and processors – in agreement with the lead DPA - based on the Accountability principle to determine which documentation is adequate and best suited for specific processing activities to comply with this Regulation and achieve the desired protection. Finally, art. 28.3 is unnecessary because of art. 29.

Amendment

Article 33 (Data protection impact assessment)	
Commission proposal	Proposed amendment
1. Where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller or the processor acting on the controller's behalf shall carry out an assessment of the impact	1. Where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller shall carry out an assessment of the impact of the envisaged processing operations on the

<p>of the envisaged processing operations on the protection of personal data.</p> <p>2. The following processing operations in particular present specific risks referred to in paragraph 1:</p> <p>(a) a systematic and extensive evaluation of personal aspects relating to a natural person or for analysing or predicting in particular the natural person's economic situation, location, health, personal preferences, reliability or behaviour, which is based on automated processing and on which measures are based that produce legal effects concerning the individual or significantly affect the individual;</p> <p>(b) information on sex life, health, race and ethnic origin or for the provision of health care, epidemiological researches, or surveys of mental or infectious diseases, where the data are processed for taking measures or decisions regarding specific individuals on a large scale;</p> <p>(c) monitoring publicly accessible areas, especially when using optic-electronic devices (video surveillance) on a large scale;</p> <p>(d) personal data in large scale filing systems on children, genetic data or biometric data;</p> <p>(e) other processing operations for which the consultation of the supervisory authority is required pursuant to point (b) of Article 34(2).</p> <p>3. The assessment shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data</p>	<p>protection of personal data.</p> <p>2. The following processing operations in particular present specific risks referred to in paragraph 1:</p> <p>(a) a systematic and extensive evaluation of personal aspects relating to a natural person or for analysing or predicting in particular the natural person's economic situation, location, health, personal preferences, reliability or behaviour, which is based on automated processing and on which measures are based that produce legal effects concerning the individual or significantly affect the individual;</p> <p>(b) information on sex life, health, race and ethnic origin or for the provision of health care, epidemiological researches, or surveys of mental or infectious diseases, where the data are processed for taking measures or decisions regarding specific individuals on a large scale;</p> <p>(c) monitoring publicly accessible areas, especially when using optic-electronic devices (video surveillance) on a large scale;</p> <p>(d) personal data in large scale filing systems on children, genetic data or biometric data;</p> <p>(e) other processing operations for which the consultation of the supervisory authority is required pursuant to point (b) of Article 34(2).</p> <p>3. The assessment shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data</p>
--	--

<p>subjects, the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned.</p>	<p>subjects, the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned.</p>
<p>4. The controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations.</p>	<p>4. The controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations.</p>
<p>5. Where the controller is a public authority or body and where the processing results from a legal obligation pursuant to point (c) of Article 6(1) providing for rules and procedures pertaining to the processing operations and regulated by Union law, paragraphs 1 to 4 shall not apply, unless Member States deem it necessary to carry out such assessment prior to the processing activities.</p>	<p>5. Where the controller is a public authority or body and where the processing results from a legal obligation pursuant to point (c) of Article 6(1) providing for rules and procedures pertaining to the processing operations and regulated by Union law, paragraphs 1 to 4 shall not apply, unless Member States deem it necessary to carry out such assessment prior to the processing activities.</p>
<p>6. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the processing operations likely to present specific risks referred to in paragraphs 1 and 2 and the requirements for the assessment referred to in paragraph 3, including conditions for scalability, verification and auditability. In doing so, the Commission shall consider specific measures for micro, small and medium-sized enterprises.</p>	<p>6. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the processing operations likely to present specific risks referred to in paragraphs 1 and 2 and the requirements for the assessment referred to in paragraph 3, including conditions for scalability, verification and auditability. In doing so, the Commission shall consider specific measures for micro, small and medium-sized enterprises.</p>
<p>7. The Commission may specify standards and procedures for carrying out and verifying and auditing the assessment referred to in paragraph 3. Those implementing acts shall</p>	<p>7. The Commission may specify standards and procedures for carrying out and verifying and auditing the assessment referred to in paragraph 3. Those</p>

be adopted in accordance with the examination procedure referred to in Article 87(2).	implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).
---	--

Justification

The DPIA obligation is seriously flawed as it is currently proposed. The approach to single out certain types of processing, brand them as risky and treat them differently from supposedly non-risky processing is dangerous and will not produce the desired results. We believe all processing of personal data should be planned appropriately prior to commencing the processing to ensure compliance with the Regulation. Organizations should be held accountable for applying risk identification and mitigation planning methodologies that are appropriate for the processing at hand. No specific type of DPIA should be mandated nor should the assessment obligation be reserved to any specific type of processing. Some of the activities listed in article 33 are standard processing for which such an assessment should not need to be submitted to a DPA for prior authorization or consultation. In the current online reality, processing of e.g. location data, user segmentation and other such practices described as potentially risky in the proposal, are the norm rather than exception and do not necessarily pose any significant risk to individuals.

Furthermore, DPIA's are only one specific method, among others (constantly evolving methodologies), to achieve the ultimate objective of ensuring that risks to privacy have been identified and proper mitigations planned in a timely fashion. It therefore does not make sense to regulate DPIAs in a strict manner while ignoring the broader picture of the risk assessing and mitigation toolkit. Risk assessment and mitigation should be the responsibility of the controller according to the Accountability Principle implemented via the amendment to article 22.

Amendment

Article 34 (Prior authorisation and prior consultation)	
Commission proposal	Proposed amendment
1. The controller or the processor as the case may be shall obtain an authorisation from the supervisory authority prior to the processing of personal data, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where a controller or processor	1. The controller or the processor as the case may be shall obtain an authorisation from the supervisory authority prior to the processing of personal data, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where a controller or processor

<p>adopts contractual clauses as provided for in point (d) of Article 42(2) or does not provide for the appropriate safeguards in a legally binding instrument as referred to in Article 42(5) for the transfer of personal data to a third country or an international organisation.</p> <p>2. The controller or processor acting on the controller's behalf shall consult the supervisory authority prior to the processing of personal data in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where:</p> <p>(a) a data protection impact assessment as provided for in Article 33 indicates that processing operations are by virtue of their nature, their scope or their purposes, likely to present a high degree of specific risks; or</p> <p>(b) the supervisory authority deems it necessary to carry out a prior consultation on processing operations that are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope and/or their purposes, and specified according to paragraph 4.</p> <p>3. Where the supervisory authority is of the opinion that the intended processing does not comply with this Regulation, in particular where risks are insufficiently identified or mitigated, it shall prohibit the intended processing and make appropriate proposals to remedy such non-compliance.</p>	<p>adopts contractual clauses as provided for in point (d) of Article 42(2) or does not provide for the appropriate safeguards in a legally binding instrument as referred to in Article 42(5) for the transfer of personal data to a third country or an international organisation.</p> <p>2. The controller or processor acting on the controller's behalf shall consult the supervisory authority prior to the processing of personal data in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where:</p> <p>(a) a data protection impact assessment as provided for in Article 33 indicates that the processing is based on point (e) or (f) of Article 6(1) and the processing operations are by virtue of their nature, their scope or their purposes, likely to present a high degree of specific risks; or</p> <p>(b) the supervisory authority deems it necessary to carry out a prior consultation on processing operations that are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope and/or their purposes, and specified according to paragraph 4.</p> <p>3. Where the supervisory authority is of the opinion that the intended processing does not comply with this Regulation, in particular where risks are insufficiently identified or mitigated, it shall prohibit the intended processing and make appropriate proposals to remedy such non-compliance. Such a decision shall be</p>
--	---

<p>4. The supervisory authority shall establish and make public a list of the processing operations which are subject to prior consultation pursuant to point (b) of paragraph 2. The supervisory authority shall communicate those lists to the European Data Protection Board.</p>	<p><i>subject to appeal in a competent court and it may not be enforceable while being appealed unless the processing would result in immediate serious harm suffered by data subjects.</i></p> <p>4. The supervisory authority shall establish and make public a list of the processing operations which are subject to prior consultation pursuant to point (b) of paragraph 2. <i>The following processing operations are likely to present specific risks:</i></p> <p><i>(a) a systematic and extensive evaluation of personal aspects relating to a natural person or for analysing or predicting in particular the natural person's economic situation, location, health, personal preferences, reliability or behaviour, which is based on automated processing and on which measures are based that produce legal effects <u>that gravely and adversely affect the individual's fundamental rights</u>;</i></p> <p><i>(b) information on sex life, health, race and ethnic origin or for the provision of health care, epidemiological researches, or surveys of mental or infectious diseases, where the data are processed for taking measures or decisions regarding specific individuals on a large scale;</i></p> <p><i>(c) monitoring publicly accessible areas, especially when using optic-electronic devices (video surveillance) on a large scale;</i></p> <p><i>(d) personal data in large scale filing systems on children, genetic data or</i></p>
--	---

<p>5. Where the list provided for in paragraph 4 involves processing activities which are related to the offering of goods or services to data subjects in several Member States, or to the monitoring of their behaviour, or may substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57 prior to the adoption of the list.</p> <p>6. The controller or processor shall provide the supervisory authority with the data protection impact assessment provided for in Article 33 and, on request, with any other information to allow the supervisory authority to make an assessment of the compliance of the processing and in particular of the risks for the protection of personal data of the data subject and of the related safeguards.</p> <p>7. Member States shall consult the supervisory authority in the preparation of a legislative measure to be adopted by the national parliament or of a measure based on such a legislative measure, which defines the nature of the processing, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects.</p>	<p><i>biometric data;</i></p> <p><i>The supervisory authority shall communicate those lists to the European Data Protection Board.</i></p> <p>5. Where the list provided for in paragraph 4 involves processing activities which are related to the offering of goods or services to data subjects in several Member States, or to the monitoring of their behaviour, or may substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57 prior to the adoption of the list.</p> <p>6. The controller or processor shall provide the supervisory authority with the data protection impact assessment provided for in Article 33, and with any other information to allow the supervisory authority to make an assessment of the compliance of the processing and in particular of the risks for the protection of personal data of the data subject and of the related safeguards.</p> <p>7. Member States shall consult the supervisory authority in the preparation of a legislative measure to be adopted by the national parliament or of a measure based on such a legislative measure, which defines the nature of the processing, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects.</p>
--	---

<p>8. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for determining the high degree of specific risk referred to in point (a) of paragraph 2.</p>	<p>8. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for determining the high degree of specific risk referred to in point (a) of paragraph 2.</p>
<p>9. The Commission may set out standard forms and procedures for prior authorisations and consultations referred to in paragraphs 1 and 2, and standard forms and procedures for informing the supervisory authorities pursuant to paragraph 6. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>	<p>9. The Commission may set out non mandatory standard forms and procedures for prior authorisations and consultations referred to in paragraphs 1 and 2, and standard forms and procedures for informing the supervisory authorities pursuant to paragraph 6. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</p>

Justification

Mandatory prior consultation should take place between supervisory authorities and data controllers and processors where needed, i.e. in exceptional cases which present specific risks and where the processing is not being carried out based on the data subject’s consent but on other grounds (contract, legal obligation). In all other cases, the supervisory authorities should concentrate their limited resources on ensuring an effective and consistent (‘ex-post’) enforcement of the law, similar to other regulatory areas, including health and safety regulations. See also the recommendation of the Article 29 Working Party in its Opinion 3/2010 paragraph 63.

Amendment

Article 35 (Designation of Data Protection Officer)	
Commission proposal	Proposed amendment
<p>1. The controller and the processor shall designate a data protection officer in any case where:</p> <p>(a) the processing is carried out by a public authority</p>	<p>1. The controller and the processor shall designate a data protection organization or data protection officer in any case where:</p> <p>(a) the processing is carried</p>

<p>or body; or</p> <p>(b) the processing is carried out by an enterprise employing 250 persons or more; or</p> <p>(c) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects.</p> <p>2. In the case referred to in point (b) of paragraph 1, a group of undertakings may appoint a single data protection officer.</p> <p>3. Where the controller or the processor is a public authority or body, the data protection officer may be designated for several of its entities, taking account of the organisational structure of the public authority or body.</p> <p>4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may designate a data protection officer.</p> <p>5. The controller or processor shall designate the data protection officer on the basis of professional qualities and, in particular, expert knowledge of</p>	<p>out by a public authority or body; or</p> <p>(b) the processing is carried out by an enterprise employing 250 persons or more; or</p> <p>(c) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects.</p> <p>2. In the case referred to in point (b) of paragraph 1, a group of undertakings may appoint a single data protection officer.</p> <p>3. Where the controller or the processor is a public authority or body, the data protection organization or data protection officer may be designated for several of its entities, taking account of the organisational structure of the public authority or body.</p> <p>4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may designate a data protection officer.</p> <p>5. The controller or processor shall designate the data protection organization or data protection</p>
---	--

<p>data protection law and practices and ability to fulfil the tasks referred to in Article 37. The necessary level of expert knowledge shall be determined in particular according to the data processing carried out and the protection required for the personal data processed by the controller or the processor.</p> <p>6. The controller or the processor shall ensure that any other professional duties of the data protection officer are compatible with the person's tasks and duties as data protection officer and do not result in a conflict of interests.</p> <p>7. The controller or the processor shall designate a data protection officer for a period of at least two years. The data protection officer may be reappointed for further terms. During their term of office, the data protection officer may only be dismissed, if the data protection officer no longer fulfils the conditions required for the performance of their duties.</p> <p>8. The data protection officer may be employed by the controller or processor, or fulfil his or her tasks on the basis of a service contract.</p> <p>9. The controller or the processor shall communicate the name and contact details of the data protection officer to the supervisory authority and to</p>	<p>officer on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and ability to fulfil the tasks referred to in Article 37. The necessary level of expert knowledge shall be determined in particular according to the data processing carried out and the protection required for the personal data processed by the controller or the processor.</p> <p>6. The controller or the processor shall ensure that any other professional duties of the data protection organization or data protection officer are compatible with the person's tasks and duties as data protection officer and do not result in a conflict of interests.</p> <p>8. The data protection officer may be employed by the controller or processor, or fulfill his or her tasks on the basis of a service contract.</p> <p>9. The controller or the processor shall communicate the contact details of the data protection organization or data protection officer to the supervisory authority and to the public.</p> <p>10. Data subjects shall have the right to contact the data protection organization on all issues related to the processing of the data subject's data and to request exercising the rights under this Regulation.</p> <p>11. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the core</p>
---	---

<p>the public.</p> <p>10. Data subjects shall have the right to contact the data protection officer on all issues related to the processing of the data subject's data and to request exercising the rights under this Regulation.</p> <p>11. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the core activities of the controller or the processor referred to in point (c) of paragraph 1 and the criteria for the professional qualities of the data protection officer referred to in paragraph 5.</p>	<p>activities of the controller or the processor referred to in point (c) of paragraph 1 and the criteria for the professional qualities of the data protection officer referred to in paragraph 5.</p>

Justification

There are clear benefits in having in place roles and responsibilities to ensure compliance. The proposal, however, appears overly detailed in describing the tasks of a data protection officer and it also fails to recognize that also other organizational structures may result in equally or even more effective data protection. Here again it will be much more effective to take the Accountability principle into account and legislate accordingly. In larger organizations it is not reasonable to expect that a single data protection officer would be involved in all issues relating to the protection of personal data. Often in larger organizations the data protection roles and responsibilities, ranging from requirements setting, implementation, training and awareness, incident response and oversight and reporting are rightfully decentralized across the organizations, while being bound together by a comprehensive data protection program. Without senior management support and a systematic management approach, it is unlikely that such a mandatory advisory and monitoring role envisaged by the proposal will lead to desired outcomes.

Some requirements for data protection officers in the proposal may even be counterproductive. For example, creating a two year protected term in form of a job guarantee for a data protection officer creates incentives to outsource the role to an external service provider to balance the risk of an unsuccessful recruitment. As in-depth knowledge of the organization is often a prerequisite for successful data protection, outsourcing can hardly be seen as a desired outcome in all cases. Also, some organizational flexibility will lead to a better organisation of the data protection resources: often, a member of the organizations senior management responsible according to the Accountability principle (and being an element of it) will achieve better data protection results than a data protection officer with a rather procedural role.

Amendment

Article 36 (position of the data protection officer)	
Commission proposal	Proposed amendment
<p>1. The controller or the processor shall ensure that the data protection officer is properly and in a timely manner involved in all issues which relate to the protection of personal data.</p> <p>2. The controller or processor shall ensure that the data protection officer performs the duties and tasks independently and does not receive any instructions as regards the exercise of the function. The data protection officer shall directly report to the management of the controller or the processor.</p> <p>3. The controller or the processor shall support the data protection officer in performing the tasks and shall provide staff, premises, equipment and any other resources necessary to carry out the duties and tasks referred to in Article 37.</p>	<p>1. The controller or the processor shall ensure that the data protection organization or data protection officer is properly and in a timely manner involved in all significant issues which relate to the protection of personal data.</p> <p>2. The controller or processor shall ensure that The data protection organization or data protection officers shall performs the their duties and tasks independently and does not receive any instructions as regards the exercise of the function. The data protection officer shall directly report to the management of the controller or the processor.</p> <p>3. The controller or the processor shall support the data protection organization or data protection officer in performing the tasks and shall provide staff, premises, equipment and any other resources necessary to carry out the duties and tasks referred to in Article 37.</p>

Justification

It is not possible for a company to ensure that someone act “independently” just as much as it is impossible for a company to ensure that someone act honestly. Instead, this should be an obligation on the DPO.

Amendment

Article 37 (Tasks of the data protection organization or data protection officer)	
Commission proposal	Proposed amendment
<p>1. The controller or the processor shall entrust the data protection officer at least with the following tasks:</p> <p>a) to inform and advise the controller or the processor of their obligations pursuant to this Regulation and to document this activity and the responses received;</p> <p>b) to monitor the implementation and application of the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, the training of staff involved in the processing operations, and the related audits;</p> <p>c) to monitor the implementation and application of this Regulation, in particular as to the requirements related to data protection by design, data protection by default and data security and to the information of data subjects and their requests in exercising their rights under this Regulation;</p>	<p>1. The controller or the processor shall entrust the data protection organization or data protection officer at least with the following tasks:</p> <p>a) to inform and advise the controller or the processor of their obligations pursuant to this Regulation and to document this activity and the responses received;</p> <p>b) to develop, support and monitor the implementation of measures referred to in Article 22, in particular to monitor the implementation and application of the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, the training of staff involved in the processing operations, and the related audits;</p> <p>c) to monitor compliance with the Regulation. the implementation and application of this Regulation, in particular as to the requirements related to data protection by design, data protection by default and data security and to the information of data subjects</p>

	and their requests in exercising their rights under this Regulation;
--	---

Justification

In today's organizational reality a lot of everyday advice is given over the phone, in meetings, through email or instant messaging. Having an obligation to systematically document one's everyday interaction with supported business operations would generate a massive and disproportionate administrative burden. However, actual privacy impact assessments and similarly structured privacy reviews need to be documented.

It should be up to the organization to define how they decide to organize their data protection organization and business in general. The proposed regulation appears to envision a centralized organization with full and sole control over its resources and organization, which is just one approach to reach compliance.

MEP Amelia Andersdotter
Parlement européen
Bât. Altiero Spinelli 06E264
60, rue Wiertz B-1047 Bruxelles/Brussel

November 26th 2012

Dear Mrs. Andersdotter,

Nokia is very interested in the draft Data Protection Regulation. The legislation will heavily impact on our ability to seek for optimal protection of our customer's data, our possibilities to successfully offer location-based services, and it will determine whether a globally competitive digital marketplace can develop in Europe.

As the political work on the proposed Data Protection Regulation advances, we understand that key issues are being singled out by the rapporteur, shadows and other interested Members of Parliament, for being made subject to amendments. On the basis of our solid and long-term data protection experience, we would like to recommend that the 'Accountability' principle receives high attention in the parliamentary work and be implemented in the Regulation.

The Accountability concept lays down essential elements of an effective privacy program that all data controllers need to implement, rather than being confronted with old-fashioned static and detailed compliance requirements. This allows controllers to operate according to the best suited up-to-date tools to deliver optimal data protection. It is through the implementation of the accountability concept that Nokia managed to undergo a real transformation towards embracing a true privacy culture. The company is now pro-actively integrating privacy solutions at early stages and in a horizontal fashion into all products and processes instead of perceiving data protection merely as a compliance-led ex-post audit activity.

The Regulation will have to strike a balance between the effective protection of private data and not over-burdening SMEs with obligations. And also in this respect, it would be better to opt for the flexible and size-adaptable Accountability approach rather than working with multiple exceptions for SMEs which complicate the legislation and ultimately reduce protection of data subjects.

Nokia supports the harmonization approach and a sufficient level of detail where this is appropriate (definitions, privacy principles, conditions for processing). But over-prescriptive and inflexible requirements in other sections (art. 28 'documentation', art. 33 'data protection impact assessment' and 34 (prior authorization and consultation etc.)) will lead to burdensome compliance-driven approaches within companies and turn the focus away from implementing optimal protection according to the Accountability principle. Mandating data protection impact assessments for

instance for an arbitrarily selected 'rough' category of processing operations and obliging controllers to await reviews by DPAs of the considerable amounts of assessments that will be submitted every week will not be the best way to identify and mitigate risks.

Please find attached to this letter a one pager describing the Accountability concept in further detail and a set of draft amendments which would implement the concept in the draft Regulation. Please do not hesitate to contact us if you have questions or if you would like to discuss this issue in more detail.

Best regards,



Mikko Niva

MEP Christian Engström
Parlement européen
Bât. Altiero Spinelli 08G153
60, rue Wiertz B-1047 Bruxelles/Brussel

November 19th, 2012

Dear Mr. Engström,

Nokia is very interested in the draft Data Protection Regulation. The legislation will heavily impact on our ability to seek for optimal protection of our customer's data, our possibilities to successfully offer location-based services, and it will determine whether a globally competitive digital marketplace can develop in Europe.

As the political work on the proposed Data Protection Regulation advances, we understand that key issues are being singled out by the rapporteur, shadows and other interested Members of Parliament, for being made subject to amendments. On the basis of our solid and long-term data protection experience, we would like to recommend that the 'Accountability' principle receives high attention in the parliamentary work and be implemented in the Regulation.

The Accountability concept lays down essential elements of an effective privacy program that all data controllers need to implement, rather than being confronted with old-fashioned static and detailed compliance requirements. This allows controllers to operate according to the best suited up-to-date tools to deliver optimal data protection. It is through the implementation of the accountability concept that Nokia managed to undergo a real transformation towards embracing a true privacy culture. The company is now pro-actively integrating privacy solutions at early stages and in a horizontal fashion into all products and processes instead of perceiving data protection merely as a compliance-led ex-post audit activity.

The Regulation will have to strike a balance between the effective protection of private data and not over-burdening SMEs with obligations. And also in this respect, it would be better to opt for the flexible and size-adaptable Accountability approach rather than working with multiple exceptions for SMEs which complicate the legislation and ultimately reduce protection of data subjects.

Nokia supports the harmonization approach and a sufficient level of detail where this is appropriate (definitions, privacy principles, conditions for processing). But over-prescriptive and inflexible requirements in other sections (art. 28 'documentation', art. 33 'data protection impact assessment' and 34 (prior authorization and consultation etc.)) will lead to burdensome compliance-driven approaches within companies and turn the focus away from implementing optimal protection according to the Accountability principle. Mandating data protection impact assessments for

instance for an arbitrarily selected 'rough' category of processing operations and obliging controllers to await reviews by DPAs of the considerable amounts of assessments that will be submitted every week will not be the best way to identify and mitigate risks.

Please find attached to this letter a one pager describing the Accountability concept in further detail and a set of draft amendments which would implement the concept in the draft Regulation. Please do not hesitate to contact us if you have questions or if you would like to discuss this issue in more detail.

Best regards,



Mikko Niva