

Freie und Hansestadt Hamburg
Der Hamburgische Beauftragte für
Datenschutz und Informationsfreiheit
Klosterwall 6 (Block C)
20095 Hamburg
DEUTSCHLAND

Mag. Maximilian Schrems

████████████████████

██████████

ÖSTERREICH

Wien, 1. Dezember 2015

Beschwerde gegen „Facebook Ireland Ltd“, „Facebook Inc“ und/oder die „Facebook Germany GmbH“

Sehr geehrte Damen und Herren,

Angesichts der umfangreichen Berichterstattung rund um eine mögliche Zusammenarbeit von „Facebook Ireland Ltd“ mit diversen US-Behörden (insb der amerikanischen „National Security Agency“ im Rahmen des „PRISM“ Programms) und dem Urteil C-362/14 des EuGH, ist davon auszugehen, dass meine Daten entgegen den europäischen Gesetzen verarbeitet werden.

Entsprechend bringe ich diese Beschwerde ein und bitte Sie diesen Sachverhalt genauer zu überprüfen und ggf den Datentransfer von „Facebook Ireland Ltd“ an „Facebook Inc“ in den Vereinigten Staaten von Amerika („USA“) zu unterbinden.

A. ZUR ZUSTÄNDIGKEIT

Die „Facebook Ireland Ltd“ wird im deutschsprachigem Raum (Deutschland, Österreich und Schweiz) durch die „Facebook Germany GmbH“ (Caffamacherreihe 7, 20355 Hamburg, Deutschland) vertreten, welche ua den Vertrieb der Werbemöglichkeiten auf „facebook.com“ übernimmt und „Facebook Ireland Ltd“ auch in anderen Belangen entsprechend vertritt.

Schon aus dem klaren Wortlaut der RL 95/46/EG ergibt sich Ihre Zuständigkeit in Hinblick auf die (für diese Beschwerde nur teilweise relevante) „Facebook Germany GmbH“.

Im Lichte der Urteile C-230/14 („Weltimmo“) und C-131/12 („Google Spain“) ist, angesichts der Tätigkeit der „Facebook Germany GmbH“ im Rahmen des Facebook-Konzerns auch eine Zuständigkeit Ihrer Behörde für „Facebook Ireland Ltd“ und ggf für „Facebook Inc“ gegeben.

B. ZUM SACHVERHALT

Angesichts der umfangreichen Berichterstattung und Debatten innerhalb der europäischen Datenschutzbehörden und dem Urteil C-362/14 des EuGH gehe ich davon aus, dass Ihrer Behörde die Eckpunkte des US-Überwachungsskandals bekannt sind und ich den Sachverhalt entsprechend gedrängt darstellen kann. Falls sich jedoch weitere Detailfragen ergeben, bin ich natürlich jederzeit gerne mit weiteren Ausführungen behilflich.

1. Kundenbeziehung zum Facebook-Konzern

Ich bin seit 2008 ein Nutzer von „facebook.com“, einem Dienst von „Facebook Ireland Ltd“ (Hanover Reach 5-7, Hanover Quay, 2. Dublin, Irland). Mein Facebook-Profil ist unter der URL [REDACTED] (zum Teil) öffentlich abrufbar. Die entsprechenden Daten werden jedoch auch von „Facebook Inc“ als verantwortliche Stelle in den USA verarbeitet (zB bei der Datenverarbeitung die mit meinen 28 amerikanischen „Facebook-Freunden“ anfällt).

Weiter habe ich mich zu diversen Werbemöglichkeiten auf facebook.com wiederholt informiert und dabei auch meine persönlichen Daten für „Gutscheine“ und „Trainings“ auf den Business-Seiten von facebook.com angegeben. Diesbezüglich erhielt ich auch mehrere Anrufe durch die „Facebook Germany GmbH“ auf mein privates Mobiltelefon, welche mich ermutigten unter anderem die Facebook-Seite „evf“ (europe-v-facebook) mittels bezahlten Einschaltungen zu bewerben, da (so die damaligen telefonischen Angaben der „Facebook Germany GmbH“) Facebook derartigen Seiten, bei entsprechender Bezahlung, garantiert zu sehr großen Erfolge verhelfen kann. Die „Facebook Germany GmbH“ hat verarbeitet meine Daten daher auch direkt.

2. „Facebook Ireland Ltd“ und die „Facebook German GmbH“ übermittelt meine Daten an „Facebook Inc“

Auch aufgrund der weiteren Angaben von „Facebook Ireland Ltd“ und der Rolle der „Facebook German GmbH“ ist klar, dass meine Daten nicht nur von „Facebook Ireland Ltd“, sondern auch von „Facebook Inc“ verarbeitet werden und dabei in die USA übermittelt werden. Dies ergibt sich aus den gemeinsamen Datenschutzbestimmungen „Facebook Ireland Ltd“ unter <https://www.facebook.com/privacy/explanation>:

„Wir teilen Informationen, die wir über dich haben, innerhalb der Gruppe von Unternehmen, die zu Facebook gehören.“

„Für die in dieser Richtlinie beschriebenen Zwecke kann Facebook Informationen intern innerhalb seiner Unternehmensgruppe oder an Dritte weitergeben. Informationen, die im Europäischen Wirtschaftsraum („EWR“) gesammelt werden, können für die in dieser Richtlinie beschriebenen Zwecke beispielsweise in Länder außerhalb des EWR übertragen werden.“

3. „Facebook Inc“ fällt unter US-Überwachungsgesetze

„Facebook Inc“ fällt unter diverse bekannte und geheime amerikanische Gesetze, Regeln, Gerichtsentscheidungen und Verwaltungsentscheidungen („Executive Orders“), die „Facebook Inc“ dazu verpflichten persönliche Daten den US-Behörden, wie zB der „National Security Agency“ (NSA) oder dem „Federal Bureau of Investigations“ (FBI) zur Verfügung zu stellen und/oder diese zu übermitteln. Diese Rechtsgrundlagen finden sich zB in 50 USC § 1881a, der auf jeden „Electronic Communication Provider“ anwendbar ist und diesen verpflichtet Zugang zu jeglicher „Foreign Intelligence Information“ zu ermöglichen oder Executive Order 12.333, neben vielen ähnlichen Rechtsgrundlagen.

Meine persönlichen Daten, ebenso wie alle Informationen in diesem Verfahren vor Ihrer Behörde erfüllen mitunter die Definition der „Foreign Intelligence Information“ (zB weil meine Tätigkeiten in diesem und anderen Verfahren für die US-Regierung relevant sein könnten).

Doch selbst wenn meine persönlichen Daten nicht unter diese Definition fallen würden, wären meine Daten unter diesem Gesetz abrufbar, den US-Gesetze zielen auf Daten ab – nicht auf Personen. Daher muss „Facebook Inc“ einen Zugriff auf alle Daten zur Verfügung stellen, solange es irgendwo irgendwelche relevanten Informationen in seinen Systemen speichert. Dies ist unabhängig von der Relevanz der jeweiligen spezifischen Daten und der zugehörigen Person. Mit anderen Worten: US-Gesetze, wie zB § 1881a ist auf alle Daten anwendbar die ein „Electronic Communication Provider“ speichert, nicht nur auf spezifische Daten einer Zielperson. Entsprechend basiert der US-Zugriff auch auf jährlichen „Zertifikaten“ und „Direktiven“ die sich nicht an eine bestimmte Person richten, sondern auf alle Daten die ein Provider verarbeitet.

Nachdem US-Recht auf Informationen und nicht auf Personen abzielt, gibt es auch keinen Rechtsweg der einem Betroffenen erlauben würde seine Rechte durchzusetzen. Personen die weder eine US-Staatsbürgerschaft besitzen, noch dauerhaft in den USA aufhältig sind, haben auch keine Bürgerrechte unter der US-Verfassung. Der zuständige „United States Foreign Intelligence Surveillance Court“ tagt geheim und entscheidet auf Basis eines einseitigen Antrags der US-Regierung. Die Richter werden allein von der US-Regierung ernannt. Seit 1979 hat das Gericht nur 12 von mehr als 35.000 Anträgen abgelehnt. Das Gericht ist damit *de facto* eher eine „Abnickungsmaschine“ als ein „Gericht“, da fast alle relevanten Elemente eines „Gerichts“ fehlen. Zusammenfassend erfüllt dieses Gericht niemals die Vorgaben eines „Gerichts“ in einem „demokratischen Staat“ (Artikel 6 EMRK und/oder Artikel 47 EU-Grundrechtecharta).

4. „Facebook Inc“ fällt unter US “Gag Orders”

„Facebook Inc“ fällt unter amerikanische “gag orders” (wörtlich “Knebel-Anordnung”) die „Facebook Inc“ dazu verpflichten alle Fakten zum US-Überwachungsskandal geheim zu halten und zu leugnen. Nur bestimmte Personen mit der notwendigen Sicherheitsfreigabe dürfen von diesen Systemen wissen.

Es ist daher klar, dass jede Stellungnahme von “Facebook Inc” im Lichte dieser rechtlichen Pflichten gesehen werden muss. Selbst hohe Manager innerhalb des Konzerns haben vermutlich meist nicht die notwendige Sicherheitsfreigabe um wissen zu dürfen, was im eigenen Unternehmen passiert. Eine Stellungnahme einer Person, die nach nationalem Recht dazu verpflichtet ist zu lügen, hat praktisch keinen Wert, insbesondere da eine derartige

Falschaussage zu keinerlei Verantwortlichkeit führt, eine korrekte Aussage jedoch zu massiven persönlichen Konsequenzen nach US-Recht führen kann.

Dieses Problem betrifft auch US-Beamte, Rechtsanwälte und Vertreter von „Facebook Inc“ und insbesondere „Facebook Ireland Ltd“ und die „Facebook Germany GmbH“, die aufgrund des US-Rechts durchgängig entweder keinen Zugang zu den relevanten Informationen haben können oder aber zur Falschaussage verpflichtet sind.

Dass „Facebook Inc“ nicht frei über diverse Zugriffsformen der US-Regierung sprechen kann, hat der Konzern auch schon in einem Brief an „Facebook Ireland Ltd“ vom 8. Juli 2013 zugestanden in dem „Facebook Inc“ dem Tochterunternehmen in Irland mitteilte, dass es nach US-Recht „significant constraints“ (auf Deutsch etwa „signifikante Beschränkungen“) gibt, die es „Facebook Inc“ verunmöglichen über diese Programme zu informieren.

Dass derartige „Gag Orders“ in den USA üblich sind, ist auch aus diversen Veröffentlichungen und geleakten Gerichtsentscheidungen nach 50 USC Kapitel 36 (siehe zB FISA-Gerichtsbeschluss vom 25. April 2013¹) bekannt.

5. „Facebook Inc“ kooperiert auch faktisch mit US-Überwachungsgesetzen

Die Aufdeckungen von Edward Snowden haben bewiesen, dass „Facebook Inc“ (neben vielen anderen US-Unternehmen) nicht nur abstrakt unter diverse US-Überwachungsgesetze fällt, sondern auch faktisch an Programmen wie „PRISM“ oder „XKeyscore“ teilnimmt – um nur zwei der unzähligen Programme zu nennen.

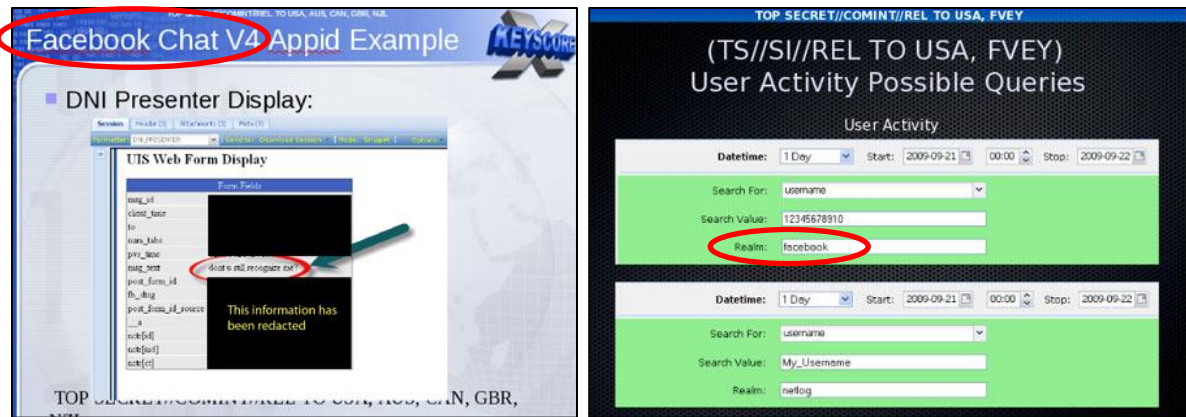
Diese relativ umfangreichen Snowden-Dokumente sind Ihrer Behörde sicherlich bekannt und auch öffentlich im Internet abrufbar. Als reine Beispiele würde ich gerne die folgenden Präsentations-Seiten, die Edward Snowden geleakt hat vorbringen, die (wie viele andere Dokumente) klarmachen, dass „Facebook Inc“ auch faktisch Teil des „PRISM“-Systems oder des „xKeyscore“-Systems ist – um nur zwei von vielen US-Überwachungsprogramme zu nennen.

The image contains two screenshots of PRISM program documentation. The left screenshot, titled "PRISM Collection Details", shows a list of "Current Providers" including Microsoft (Hotmail, etc.), Google, Yahoo!, Facebook, PalTalk, YouTube, Skype, AOL, and Apple. A green arrow points from this list to a box titled "What Will You Receive in Collection (Surveillance and Stored Comms?)". This box lists various types of data collected, such as E-mail, Chat, Videos, Photos, Stored data, VoIP, File transfers, Video Conferencing, and Notifications of target activity. The right screenshot, titled "PRISM Case Notations", shows a specific case ID "P2ESQC120001234". It breaks down this ID into components: "Fixed trigraph, denotes PRISM source collection", "Year CASN established for selector", and "Serial #". Below this, it lists "Content Type" codes: A: Stored Comms (Search), B: IM (chat), C: RTN-EDC, D: RTN-IM, E: E-Mail, F: VoIP, G: Full (WebForum), H: OSN Messaging, I: OSN Basic Subscriber Info, J: Videos. Both screenshots have "TOP SECRET//SI//ORCON//NOFORN" markings.

¹ Voller Titel der Entscheidung "IN RE APPLICATION OF THE FEDERAL BUREAU OF INVESTIGATION FOR AN ORDER REQUIRING THE PRODUCTION OF TANGIBLE THINGS FROM VERIZON BUSINESS NETWORK SERVICES, INC. ON BEHALF OF MCI COMMUNICATION SERVICES, INC. D/B/A VERIZON BUSINESS SERVICES."

Die Präsentationen machen auch klar, dass „Facebook Inc“ nicht nur eine „kleine Quelle“ für individuelle Abfragen der Behörden ist, sondern eine Hauptquelle („PRISM-Provider“) mit einer eigenen Identifikationsnummer („P4“) ist.

Ebenso ist Facebook in den XKeyscore-Dokumenten ausdrücklich genannt, die zeigen wie US-Beamte innerhalb der Facebook-Datensätze nach Informationen „suchen“ können:



Diese Faken werden nur von „Facebook Inc“ bestritten. Keine anderen relevanten Institutionen bestritten diese Fakten (zB die EU-Kommission, der Europäische Parlament, der EuGH, der EDPS, die Artkl-29-Arbeitsgruppe, alle EU-Mitgliedstaaten vor dem EuGH im Fall C-362/14, der Irische High Court im Fall *Schrems -v- Data Protection Commissioner*, die Berichte des amerikanischen „Privacy and Civil Liberties Oversight Board“ und die US-Regierung).

Nachdem ihre Behörde die relevanten Dokumente zu den oben referenzierten Aussagen sicherlich vorliegen hat würde ich uns weitere Ausführungen hierzu ersparen. Ich würde jedoch gerne nochmals darauf hinweisen, dass die US-Regierung (die einzige Organisation neben „Facebook Inc“, die über Informationen aus erster Hand verfügt) wiederholt die oben genannten Fakten bestätigt hat. Als Beispiel:

“The federal government has been secretly collecting information on foreigners overseas for nearly six years from the nation’s largest Internet companies like Google, Facebook and, most recently, Apple, in search of national security threats, the director of national intelligence confirmed Thursday night.” <http://www.nytimes.com/2013/06/07/us/nsa-verizon-calls.html>

Die einzige faktische Meinungsverschiedenheit zwischen der US-Regierung und den europäischen Stellen scheint daher zu sein, ob diese Systeme „*Massenüberwachung*“ darstellen, was jedoch in Wirklichkeit eine juristische und keine faktische Frage ist (siehe hierzu unten). Die Tatsache, dass es tatsächlichen Zugriff auf die „Facebook-Daten“ im Rahmen des „PRISM“-Programms gibt scheint jedoch generell unstrittig zu sein.

6. Feststellungen des irischen High Court

Aufgrund der großen tatsächlichen Überlappung der hier behandelten Fragen, scheint auch das Urteil des irischen High Court in *Schrems -v- Data Protection Commissioner* relevant. Nach einer eingehenden Verhandlung zum „PRISM“-Programm, stellt der irische High Court zB fest:

“4. While it is true that the Snowden disclosures caused – and are still causing – a sensation, only the naïve or the credulous could really have been greatly surprised.”

“5. Yet only the foolish would deny that the United States has, by virtue of its superpower status, either assumed – or, if you prefer, has had cast upon it – far-reaching global security responsibilities.”

“13. While there may be some dispute regarding the scope and extent of some of these programmes, it would nonetheless appear from the extensive exhibits contained in the affidavits filed in these proceedings that the accuracy of much of the Snowden revelations does not appear to be in dispute. The denials from official sources, such as they have been, were feeble and largely formulaic, often couched in carefully crafted and suitably ambiguous language designed to avoid giving diplomatic offence. I will therefore proceed on the basis that personal data transferred by companies such as Facebook Ireland to its parent company in the United States is thereafter capable of being accessed by the NSA in the course of a mass and indiscriminate surveillance of such data. Indeed, in the wake of the Snowden revelations, the available evidence presently admits of no other realistic conclusion.”

Diese Feststellungen wurden auch von EuGH in der Rechtssache C-362/14 überprüft und übernommen. Diese Fakten sind daher höchstgerichtlich geklärt.

7. Tatsächliche Nachteile

Auch wenn dies nach meinem Dafürhalten vollkommen irrelevant ist, würde ich aus Gründen der Vollständigkeit gerne vorbringen, dass [REDACTED]

[REDACTED]

8. Zusammenfassung

Zusammenfassend gibt es daher klare Beweise, dass meine persönlichen Daten die von „Facebook Ireland Ltd“ und der „Facebook Germany GmbH“ als verantwortliche Stelle und von „Facebook Inc“ als Dienstleister verarbeitet werden und diversen US-Behörden unter diversen bekannten und geheimen Rechtsgrundlagen und Überwachungsprogrammen wie „PRISM“ zumindest „bereitgestellt“ werden. Weiter gibt es den begründeten Verdacht, dass auf meine persönlichen Daten auch zusätzlich zugegriffen wurde.

C. ZUM RECHT

Vorab darf ich kurz festhalten, dass ich mich im Weiteren aus Gründen der Praktikabilität auf die entsprechenden Stellen in der RL 95/46/EG beziehe, die je nach Situation im jeweiligen nationalen Datenschutzrecht (zB dem BDSG oder dem irischen DPA) umgesetzt wurden.

1. Definition von „Verarbeiten“

Die meisten Argumente in der Debatte zwischen den USA und Europa drehen sich um die Frage der konkreten Form des Datenzugriffs durch die US-Behörden.

Einige Aussagen und Dokumente lassen den Schluss zu, dass die US-Regierung die relevanten Daten tatsächlich in großen Rechenzentren „speichert“ (wie im medial viel beachteten Datenzentrum in Utah) und wie im Fall des US-Telekomanbieters Verizon Daten von Unternehmen in Speichersysteme der US-Regierung *übermittelt* werden, wo diese ähnlich der EU-Vorratsdatenspeicherung gesammelt werden (siehe hierzu den geleakten Gerichtsbeschluss des FISA-Gerichts vom 25. April 2013).

Andere Aussagen legen den Schluss nahe, dass Anbieter wie „Facebook Inc“ diese Daten nur elektronisch „bereitstellen“ müssen und damit zwar einen Zugriff auf alle Daten erlauben, jedoch nur ein kleiner Teil dieser Daten, dann tatsächlich von US-Behörden abgerufen wird.

Auch wenn dieser Unterschied nach US-Recht relevant sein mag, sind all diese Unterscheidungen nach EU-Recht vollkommen irrelevant. Artikel 2(b) der RL 95/46/EG definiert das „Bereitstellen“ bereits als eine Art der „Verarbeitung“. Wenn also meine persönlichen Daten auch nie von US-Behörden abgerufen wurden, so reicht das reine Faktum, dass meine Daten „bereitgestellt“ werden müssen (zB unter 50 USC, Kapitel 36) aus, um unter den Anwendungsbereich der RL 95/46/EG und des Artikels 8 der EU-Grundrechtecharta (GRC) zu fallen. Auch die GRC nützt die Definition des „Verarbeitens“ in Artikel 2(b) der RL 95/46/EG.

Auch wenn ich ausdrücklich vorbringe, dass ich jeden Grund habe davon auszugehen, dass meine persönlichen Daten die auf den Systemen von „Facebook Inc“ gespeichert wurden, auch tatsächlich abgerufen wurden, würde ich daher gerne hervorheben, dass allein die Tatsache, dass meine Daten „bereitgestellt“ werden müssen relevant scheint um die Situation in den USA im Rahmen dieser Beschwerde zu beurteilen.

Schlussendlich will ich betonen, dass der relevante Verarbeitungsschritt im Rahmen dieser Beschwerde die Übermittlung bzw Überlassung meiner Daten von „Facebook Ireland Ltd“ und der „Facebook Germany GmbH“ an „Facebook Inc“ ist. Die „Massenüberwachung“ in den USA ist daher nur eine sekundäre Verarbeitung die jedoch bei der Beurteilung der Rechtmäßigkeit einer Übermittlung oder Überlassung relevant wird. Für „Facebook Inc“ besteht der Verarbeitungsvorgang ebenfalls aus einer Übermittlung aus dem EWR und einem weiteren Verarbeitungsvorgang im Rahmen des Zugriffs durch die US-Behörden. Beide Schritte sind jedoch an sich strikt zu unterscheiden.

2. EU-Grundrechtecharta (GRC)

Der EuGH hat in der Rechtssache C-362/14 festgestellt, dass „Massenüberwachung“ wie zB unter dem „PRISM“-Programm nicht nur „*unverhältnismäßig*“ sondern sogar eine Verletzung des „*Wesensgehalts*“ des Grundrechts auf Achtung des Privatlebens nach Artikel 7 GRC darstellt (siehe Rz 94 des Urteils).

Im gleichen Urteil hat der EuGH ebenso eine Verletzung des „*Wesensgehalts*“ des Grundrechts auf einen wirksamen Rechtsbehelf nach Artikel 47 GRC durch das Fehlen jeglichen Rechtsbehelfs nach US-Recht erblickt (siehe Rz 95 des Urteils).

Das Urteil des EuGH macht klar, dass meine Daten im gegenständlichen Fall schon auf Basis des europäischen Primärrechts nicht in die USA übermittelt werden dürfen – unabhängig von jeglichem Erlaubnistatbestand und jeglicher Regelung im Sekundärrecht.

Nach der ständigen Rechtsprechung des EuGH muss auch jeder Sekundärrechtsakt (wie zB die RL 95/46/EG aber auch jede Entscheidung der Europäischen Kommission) im Lichte des Primärrechts ausgelegt werden. Im gegenständlichen Fall umfasst dies naturgemäß auch die entsprechende Rechtsprechung des EuGH im Fall C-362/14.

3. Übermittlung in einen Drittstaat nach RL 95/46/EC

Die Artikel 25 und 26 der RL 95/46/EG untersagen eine Übermittlung in einen Drittstaat außerhalb des EWR der kein „angemessenes Schutzniveau“ bietet.

Die USA hatten zu keinem Zeitpunkt ein „angemessenes Schutzniveau“ geboten. Nach dem Urteil C-362/14 ist auch die Entscheidung 2000/520/EG der EU-Kommission hinfällig, wonach bestimmten US-Unternehmen die sich nach „Safe Harbor“ selbst-zertifiziert haben ein „angemessenes Schutzniveau“ bieten, weswegen eine Übermittlung generell verboten ist.

„Facebook Ireland Ltd“ und die „Facebook Germany GmbH“ übermitteln meine Daten weiter an „Facebook Inc“ in den Vereinigten Staaten. Nach dem Gesetz müssen die „Facebook Germany GmbH“ und „Facebook Ireland Ltd“ hierbei sicherstellen und beweisen, dass meine Daten entsprechend den europäischen Gesetzen geschützt sind.

Weiter ist darauf hinzuweisen, dass Artikel 25 und 26 der RL 95/46/EG einer abstrakte Beurteilung des Schutzniveaus in einem Drittstaat folgt, da es zumeist unmöglich ist den faktischen Schutz in einem Drittstaat zu überprüfen.

Nach der aktuellen Rechtslage muss ich daher nur beweisen, dass meine Daten in ein Drittland übermittelt werden, dass generell kein angemessenes Schutzniveau bietet. Ich muss weder beweisen, dass meine Daten den US-Behörden „*bereitgestellt*“ werden (auch wenn das offensichtlich ist) oder von US-Behörden weiter verarbeitet werden (was ebenfalls klar ist). Das Gesetz verlangt auch keinen „Sekundärschaden“ oder eine direkte Konsequenz aus der Übermittlung in einen Drittstaat, wie der EuGH in C-362/14 festgehalten hat.

Mit anderen Worten: Es ist (a) meine Aufgabe in diesem Verfahren zu beweisen, dass meine Daten in einen Drittstaat übermittelt werden der kein angemessenes Schutzniveau bietet (was sich bereits aus dem Gesetz ergibt) und die Aufgabe von „Facebook Ireland Ltd“ und der

„Facebook Germany GmbH“ das Gegenteil zu beweisen. Weiter muss (b) die „Angemessenheit“ allein auf einer abstrakten (rechtlichen) Ebene gegeben sein. Nur in einem zweiten Schritt (etwa durch das faktische Fehlen des rechtlichen Schutzes) ist auch der faktische Schutz beachtlich.

„Facebook Ireland Ltd“ und die „Facebook Germany GmbH“ können damit offensichtlich auf keiner dieser Ebenen durchdringen.

a. Standardvertragsklauseln

Nach einem Brief von „Facebook Ireland Ltd“ basiert die Datenübermittlung zwischen „Facebook Ireland Ltd“ und „Facebook Inc“ auf Standardvertragsklauseln unter der Entscheidung 2010/87/EU.

Die genutzten Klauseln weichen jedoch vom Anhang der Entscheidung 2010/87/EU gravierend ab, da nach Klausel 2 die Standardvertragsklauseln von „intergroup agreements“ und einem anderen geschwärzten Dokument überlagert werden. Eine Abänderung der Klauseln ist jedoch nach Klausel 10 des Anhangs zur Entscheidung 2010/87/EU nicht zulässig. „Facebook Ireland Ltd“ und ggf die „Facebook Germany GmbH“ können sich daher nicht auf die Entscheidung 2010/87/EU berufen.

Insoweit „Facebook Inc“ nicht nur als Dienstleister, sondern selbst als verantwortliche Stelle agiert ist die Entscheidung 2010/87/EU überhaupt die falsche Rechtsgrundlage.

Alle relevanten Kommissions-Entscheidungen haben auch eine entsprechende Ausnahmebestimmung, welche klarstellt, dass die Entscheidung nicht anwendbar ist, wenn *„feststeht, dass der Datenimporteur oder Unterauftragsverarbeiter nach den für ihn geltenden Rechtsvorschriften Anforderungen unterliegt, die ihn zwingen, vom anwendbaren Datenschutzrecht in einem Maß abzuweichen, das über die Beschränkungen hinausgeht, die im Sinne von Artikel 13 der Richtlinie 95/46/EG für eine demokratische Gesellschaft erforderlich sind, und dass sich diese Anforderungen wahrscheinlich sehr nachteilig auf die Garantien auswirken würden, die das anwendbare Datenschutzrecht und die Standardvertragsklauseln bieten“*. Diese Ausnahme wurde dem Artikel 4(1)(a) der Entscheidung 2010/87/EU entnommen, alle anderen relevanten Entscheidungen haben jedoch gleichlautende Ausnahmebestimmungen.

Dass das „PRISM“-Programm gegen den Kernbereich der Artikel 7, 8 und 47 der GRC verstößt wurde vom EuGH in C-362/14 klar festgestellt. Artikel 13 der 95/46/EG auf welche die Entscheidungen der EU-Kommission verweisen müssen im Lichte der Artikel 7, 8 und 47 GRC ausgelegt werden. Die Frage ob die US-Überwachungsprogramme daher über das in Artikel 13 der RL 95/46/EG vorgesehene Niveau hinausgehen, ist daher durch die Entscheidung C-362/14 klar und final beantwortet.

Die Entscheidung verlangt weiter, dass die gesetzlichen Anforderungen im Drittstaat sich negativ auf die Garantien in den Standardvertragsklauseln auswirken. Hierzu ist also darauf hinzuweisen, dass kein faktischer Nachteil, sondern lediglich eine nachteilige Auswirkung auf die rechtlichen Garantien notwendig ist – was in diesem Fall ebenfalls klar gegeben ist.

Kurzum: Allein dass „Facebook Inc“, wie oben ausgeführt, unter die relevanten US-Gesetze fällt (und unabhängig davon ob „Facebook Inc“ mit den US-Behörden tatsächlich kooperiert) macht eine Übermittlung in die USA nach Artikel 4(1)(a) der Entscheidung rechtswidrig.

Zusätzlich würde die tatsächlichen Datenverarbeitungen durch „Facebook Inc“ und auch die vermutlich fehlende Information von „Facebook Ireland Ltd“ und der „Facebook Germany GmbH“ über diverse Arten des Zugriffs durch US-Behörden (neben anderen Verstößen) gegen die Standardverträge verstoßen und damit eine Unterbrechung der Datenübermittlung nach den Klauseln in Artikel 4(1)(b) und (c) der Entscheidung 2010/87/EG (bzw der jeweils genutzten Entscheidung) erlauben.

Zusammengefasst kann und muss ihre Behörde die Ausnahmen in Artikel 4(1) der jeweiligen Kommissions-Entscheidungen nutzen um den europäischen Grundrechtsschutz, wie er vom EuGH in C-362/14 festgelegt wurde, entsprechend Geltung zu verschaffen, wenn die genutzten Klauseln – angesichts der Ausnahmen in Klausel 2 – überhaupt unter diese Entscheidung fallen.

b. Einwilligung

Es ist umstritten ob der Grundrechtsschutz nach Artikel 7, 8 und 47 der GRC überhaupt durch eine Einwilligung umgangen werden kann. Ich bringe daher vor, dass dies nicht möglich ist und sich die Frage nach einer „Zustimmung“ daher *nicht* stellt.

Selbst wenn eine Zustimmung nach der GRC möglich wäre, so müsste diese Zustimmung nach RL 95/46/EG jedenfalls (1) frei, (2) spezifisch, (3) informiert und (4) eindeutig in Hinblick auf die jeweilige Übermittlung erfolgen.

„Facebook Ireland Ltd“ verwendet derzeit folgende Klausel zum Thema Datentransfers in Drittstaaten:

„Für die in dieser Richtlinie beschriebenen Zwecke kann Facebook Informationen intern innerhalb seiner Unternehmensgruppe oder an Dritte weitergeben. Informationen, die im Europäischen Wirtschaftsraum („EWR“) gesammelt werden, können für die in dieser Richtlinie beschriebenen Zwecke beispielsweise in Länder außerhalb des EWR übertragen werden.“

Diese Klausel erfüllt keine der oben ausgeführten vier Voraussetzungen.

Die Zustimmung ist schon deswegen nicht „informiert“ da der Facebook-Konzern öffentlich angibt, dass die relevanten Daten den US-Behörden eben geraden *nicht* zur Verfügung gestellt werden. Eine verantwortliche Stelle die aggressiv argumentiert, dass ein gewisser Verarbeitungsvorgang nicht stattfindet, kann unmöglich vorgeben, dass er den Betroffenen gleichzeitig über diesen Verarbeitungsvorgang informiert hat.

Die Klausel nennt auch keine bestimmten Länder für die Verarbeitung dieser Daten, sondern erlaubt es „Facebook Ireland Ltd“ und der „Facebook Germany GmbH“ die Daten praktisch überall in der Welt zu verarbeiten. Es findet sich auch kein Wort zur relevanten Frage der „Massenüberwachung“ oder zu bestimmten, besonders relevanten US-Gesetzen. Die Klausel lässt auch jede Art der Präzision vermissen, die eine spezifische oder eindeutige Zustimmung ermöglichen würde. Im Prinzip sagt der Facebook-Konzern nur, dass die Daten *irgendwo* in der ganzen Welt verarbeitet werden.

Der Facebook-Konzern ist dabei offensichtlich zwischen EU-Recht, das eine entsprechende Information und Zustimmung erfordert, und dem US-Recht, das genau diese Information verbietet, gefangen. Diese Situation macht eine gültige Einwilligung unmöglich.

c. Andere Rechtsgrundlagen

Jegliche andere Rechtsgrundlage nach Artikel 25 und 26 der RL 95/46/EG bzw der jeweiligen nationalen Umsetzung auf die sich „Facebook Ireland Ltd“ oder die „Facebook Germany GmbH“ berufen könnten, können abermals nicht darüber hinwegtäuschen, dass diese Rechtsgrundlagen im Lichte der Artikel 7, 8 und 47 der GRC und der Entscheidung des EuGH in C-362/14 keine „Massenüberwachung“ rechtfertigen können. Eine Umgehung des Primärrechts ist schon rein logisch ausgeschlossen.

Auch die Ausnahmen in Artikel 26(1)(b) bis (e) der RL 95/46/EG, die durchgängig eine Weitergabe der Daten in den Drittstaat „*erfordern*“, sind nicht anwendbar. Dies insbesondere da „Facebook Ireland Ltd“ und die „Facebook Germany GmbH“ meine Daten an „Facebook Inc“ lediglich „outsourcen“ und diese Daten an sich auch direkt innerhalb des EWR verarbeitet werden könnten. Die Übermittlung in die USA ist daher sicherlich von großer wirtschaftlicher und praktischer Bedeutung, aber eben nicht „*erforderlich*“ iSd Artikels 26(1) der RL 95/46/EG.

Das bedeutet nicht, dass nicht *einzelne* Übermittlungen, wenn Daten zwingend in die USA übermittelt werden müssen, unter diesem Artikel rechtmäßig sein können. Für eine generelle Übermittlung diverser Daten an „Facebook Inc“ besteht jedoch keine rechtliche Basis.

Schlussendlich scheint es klar, dass Artikel 26(1)(f) der RL 95/46/EG in diesem Fall nicht anwendbar ist.

4. Andere Vorgaben der RL 95/46/EG

Zusätzlich zur Frage der Übermittlung in ein Drittland (nach Artikel 25 und 2 der RL 95/46/EG) müssen „Facebook Ireland Ltd“ und die „Facebook Germany GmbH“ auch den anderen Vorgaben der RL 95/46/EG, bzw der nationalen Umsetzung dieser Vorgaben, folgen. Dies ergibt sich auch aus den relevanten Entscheidungen der EU-Kommission, wie sich zB aus Artikel 4 der Entscheidung 2010/87/EU ergibt:

„Unbeschadet ihrer Befugnisse, tätig zu werden, um die Einhaltung nationaler Vorschriften gemäß den Kapiteln II, III, V und VI der Richtlinie 95/46/EG zu gewährleisten“.

Dass eine derartige Datenweitergabe gegen diese Prinzipien verstößt hat die Artikel-29-Arbeitsgruppe bereits im gleich gelagerten Fall zu „SWIFT“ (siehe WP 128 vom 22. November 2013) festgehalten.

Insbesondere verstößt die Weitergabe wohl gegen die Prinzipien der Verarbeitung nach „Treu und Glauben“, der Zweckbindung und der Verhältnismäßigkeit in Artikel 6 der RL 95/46/EG. Weiter ist keine Rechtfertigung nach Artikel 7 der RL 95/46/EG zu erblicken, welche eine derartige Weitergabe angesichts der Fakten erlauben würde. Beide Artikel sind ebenfalls im Lichte der klaren Entscheidung des EuGH in C-362/14 zu Art 7, 8 und 47 der GRC zu interpretieren, soweit diese Artikel einen Interpretationsspielraum zulassen.

D. ANTRÄGE

1. Prüfung von „Facebook Inc“

Nach Klausel 8, Absatz 2 des Vertrags zwischen „Facebook Ireland Ltd“ und „Facebook Inc“ hat sich „Facebook Inc“ vertraglich verpflichtet sich einer Überprüfung durch Ihre Behörde „*im gleichen Maße und unter denselben Bedingungen*“ wie eine Überprüfung von „Facebook Ireland Ltd“ bzw ggf auch der Niederlassung in Hamburg zu unterwerfen. Falls Ihnen bezüglich der Fakten in diesem Fall eine derartige Überprüfung nötig erscheint würde ich daher eine solche Überprüfung im Rahmen der rechtlichen Möglichkeiten beantragen.

2. Untersagung der Datenweitergabe

Basierend auf den Fakten und rechtlichen Ausführungen oben – und allen anderen rechtlichen und faktischen Gründen - beantrage ich, dass ihre Behörde der „Facebook Ireland Ltd“ und der „Facebook Germany GmbH“ die Weitergabe meiner Daten an “Facebook Inc” untersagt.

Ebenso beantrage ich, dass Ihre Behörde „Facebook Inc“ die entsprechende Verarbeitung und den Empfang meiner Daten untersagt bzw dem entsprechenden rechtlichen Schritt vornimmt.

Nachdem mir die tiefgreifenden Konsequenzen einer solchen Entscheidung natürlich bewusst sind, würde ich eine entsprechende Übergangsfrist befürworten, die es der „Facebook Germany GmbH“, „Facebook Ireland Ltd“ und dem Facebook-Konzern erlauben die entsprechenden organisatorischen und technischen Maßnahmen zu setzen um einer derartigen Entscheidung zu entsprechen.

Diese Frist ist wohl im Lichte des Verstoßes gegen den *Wesensgehalt* der Grundrechte nach Artikel 7, 8 und 47 der GRC und dem weiterhin stattfindenden Rechtsbruch gegenüber Millionen Nutzern, der Tatsache dass „Facebook Ireland Ltd“ und die „Facebook Germany GmbH“ nun mehr als zwei Jahre seit den Snowden-Veröffentlichungen Zeit zur Lösung dieses bekannten Problems hatte und andererseits den technischen und praktischen Möglichkeiten festzusetzen.

E. ZUM VERFAHREN

Je nach dem weiteren Vorgehen und den einzuholenden Reaktionen der „Facebook Germany GmbH“ und von „Facebook Ireland Ltd“ und ggf anderen Teilen des Facebook-Konzerns behalte ich mir weitere faktische und rechtliche Ausführungen vor. Diese Beschwerde beschränkt sich auf das wichtigste relevante Vorbringen und bildet nicht bereits die Reaktion auf jedes denkmögliche Vorbringen der Gegenseite ab.

Ich bitte Sie im Rahmen dieses Verfahrens alle Schritte der Behörde zu dokumentieren und mir im Rahmen der Akteneinsicht und dem normalen Verfahrensgang alle Dokumente und Akten des Verfahrens sowie alle Vorbringen der Gegenseite entsprechend zu übermitteln.

Durch den internationalen Charakter dieser Beschwerde würde ich auch eine Kooperation mit den Datenschutzbehörden von Irland und Belgien und insbesondere in Hinblick auf „Facebook Ireland Ltd“ ggf auch eine Rechtshilfe nach Artikel 28 Abs 6 der RL 95/46/EG anregen.

Es ist durchaus möglich, dass auf politischer Ebene im Laufe dieses Verfahrens eine neue Alternative zum bisherigen „Safe Harbor“ System gefunden wird. Ich gehe jedoch angesichts der Entscheidung des EuGH in C-362/14 davon aus, dass eine solche Lösung, die hier im Kern grundrechtlichen, Vorbringen nach Art 7, 8 und 47 GRC nicht tangieren wird.

Ich hoffe Ihre Arbeit mit dieser Beschwerde die Arbeit bestmöglich unterstützt zu haben.

Mit freundlichen Grüßen,

Mag. Maximilian Schrems