

An das  
Bayerisches Landesamt für Datenschutzaufsicht  
Promenade 27  
91522 Ansbach  
DEUTSCHLAND

██████████  
██████████  
██████████  
ÖSTERREICH

Wien, am 25. Juni 2013

## **Beschwerde gegen die „Yahoo! Deutschland GmbH“**

Sehr geehrte Damen und Herren,

Ich bin seit ca. 10 Jahren Nutzer von „yahoo.de“, einem Dienst von „Yahoo! Deutschland“. Angesichts der jüngsten Berichterstattung rund um eine mögliche Zusammenarbeit von „Yahoo!“ mit der amerikanischen „National Security Agency“ (NSA) muss ich davon ausgehen, dass auch meine Daten entgegen den europäischen Gesetzen im Rahmen des „PRISM“ Programms verarbeitet wurden. Entsprechend bringe ich diese Beschwerde ein und bitte das Bayerische Landesamt für Datenschutzaufsicht diesen Sachverhalt genauer zu überprüfen und ggf eine Lösung zu finden die mein Grundrecht auf Datenschutz respektiert.

### **Sachverhalt:**

Ich nutze seit ca 10 Jahren den Dienst „yahoo.de“ für meine private Korrespondenz via E-Mail. Die dafür von mir benutzte E-Mail Adresse ist ██████████. Nach den Nutzungsbedingungen des E-Mail Kontos wird dieser Dienst für Nutzer von „yahoo.de“ von der „Yahoo! Deutschland GmbH“ unter der Adresse „Theresienhöhe 12, 80339 München“ erbracht.

Ich gehe davon aus, dass die Daten nicht nur von „Yahoo! Deutschland“, sondern von weiteren Auftragsverarbeitern innerhalb des Yahoo!-Konzerns verarbeitet werden. Das ergibt sich auch aus den Hinweisen auf der Webseite von „Yahoo! Deutschland“:

*„Wir weisen darauf hin, dass viele unserer Dienste technisch durch Server außerhalb der Europäischen Union, vornehmlich in den Vereinigten Staaten von Amerika, erbracht werden. Informationen und personenbezogene Daten, die wir im Zusammenhang mit unseren Diensten erheben oder die Sie durch unsere Dienste übermitteln oder veröffentlichen, werden möglicherweise dorthin übermittelt und gespeichert. (...) Die Daten bleiben aber unbeschadet dessen in unserer Verantwortung. Informationen und personenbezogene Daten werden entweder zu Unternehmen der Yahoo! Konzerngruppe oder zu sorgfältig ausgewählten Partnern übermittelt (...). Um ein angemessenes Datenschutzniveau zu sichern, hat sich unsere Muttergesellschaft Yahoo! Inc., 701 First Avenue, Sunnyvale, CA 94089, Kalifornien, den "Safe Harbour"-Grundsätzen des US Departement of Commerce (...) unterworfen.“* (siehe <http://info.yahoo.com/privacy/de/yahoo/datatransfer/>)

Für die Übermittlung der Daten ins Ausland ist kein zwingender Grund ersichtlich. Während zB von mir an einen Empfänger in den USA gesendete E-Mails logischerweise auch in die USA übermittelt werden müssen, so ist die Speicherung der Kontodaten (zB Posteingang, Postausgang oder Kundendaten) auch innerhalb der EU bzw des EWR möglich. „Yahoo! Deutschland“ dürfte diese Daten daher freiwillig oder aus rein wirtschaftlichen Überlegungen in die USA übermitteln. Zwingende Gründe für die Speicherung in den USA sind nicht ersichtlich.

Der britische Guardian hat nun enthüllt, dass „Yahoo!“ seit 12. März 2008 einen direkten Zugriff durch den amerikanischen NSA zulässt. Nach den Berichten des Guardian gewähren die betroffenen Unternehmen insbesondere einen direkten „Massenzugriff“ auf seine Server. Ein solcher Zugriff wäre gegenüber dem bekannten Einzelabfragen bei begründetem Verdacht ein deutlich massiverer Eingriff in meine Rechte und mit dem Grundrecht auf Datenschutz nicht vereinbar.

Die bisher veröffentlichten Unterlagen der NSA deuten auch auf eine Art „freiwillige“ Zusammenarbeit hin, da sich nur einige Kommunikationsanbieter wiederfinden. Dienst wie „twitter“ sind zB nicht angeführt. Auch sind neue Unternehmen nur sukzessive hinzugekommen, was auf eine freiwillige Kooperation schließen lässt.

Es besteht begründeter Verdacht, dass die oben zusammengefassten Angaben des Guardian korrekt sind. Während die betroffenen Unternehmen die Existenz eines direkten Zugriffs auf die Server durch den NSA abstreiten und praktisch gleichlautend auf die bisher bekannten Einzelzugriffe verweisen, haben die Spitzen der US-Regierung keine solche Aussagen getätigt. Wären die Angaben falsch oder inkorrekt, wäre eine klare Zurückweisung durch die US-Regierung zu erwarten gewesen.

In den Stellungnahmen von Präsident Obama (<http://on.wsj.com/14FU8eB>) und dem Geheimdienstdirektor James Clapper (<http://tinyurl.com/ltzz5g>, <http://tinyurl.com/mmos4fd> und <http://tinyurl.com/mwgu9d6>) wurde ein direkter Zugriff auf die Server und der im Raum stehende Massenzugriff nicht eindeutig zurückgewiesen. In den Stellungnahmen von James Clapper werden zwar die Zugriffsrechte nach § 1881a U.S.C. genauer erklärt, eine Klarstellung, dass keine Massenauswertung erfolgt, konnte ich darin jedoch nicht finden. Wäre die Enthüllung des Guardian im Kern fehlerhaft oder die entsprechenden Unterlagen gefälscht, so wäre eine klare und unmissverständliche Zurückweisung der Berichte logisch.

Die betroffenen Unternehmen sind nach amerikanischem Recht verpflichtet keine Auskunft zu diesem Programm zu erteilen bzw auch falsche Informationen zu erteilen (engl „gag order“). Das bedeutet, dass bei einer korrekten Berichterstattung des Guardian „Yahoo!“ das Programm trotzdem leugnen muss. Angesichts der Rechtslage in den USA sind die vorliegenden Stellungnahmen daher für sich kein Grund die Berichterstattung des Guardian als falsch zu klassifizieren. „Yahoo!“ hat bisher weder unter Wahrheitspflicht eine Aussage getroffen, noch einen Beweis für die Non-Existenz der beschriebenen Zusammenarbeit geliefert.

Die Behauptung der betroffenen Unternehmen, dass Behörden nicht „direkt“ auf die Server zugreifen können, erinnern stark an die Faktenlage im Fall von „SWIFT“. Hier wurde eine „Black Box“ zwischengeschaltet, welche im Effekt eine Massenabfrage ermöglichte und daher effektiv einem direkten Zugriff auf die Server gleich kam.

- ➔ **Zusammenfassend gehe ich daher davon aus, dass „Yahoo! Deutschland“ meine Daten in den USA durch andere Teile des „Yahoo!-Konzerns“ verarbeiten lässt.**
- ➔ **Es besteht begründeter Verdacht, dass diese Daten durch „Yahoo! Deutschland“ und/oder dem Yahoo!-Konzern über Einzelanfragen hinaus der NSA überlassen werden.**
- ➔ **Die Aussagen von „Yahoo!“ sind im Lichte der US-Gesetzgebung wenig glaubhaft, da der Yahoo!-Konzern potentiell einer Verschwiegenheitspflicht unterliegt („gag order“).**
- ➔ **Ich ersuche Sie daher den Sachverhalt weiter zu ergünden. Vor allem scheinen die Untersuchungsrechte des Landesamts nach § 38 BDSG der Wahrheitsfindung dienlich sein.**

## Rechtliche Ausführungen:

*Hinweis: Da ich leider mit dem BDSG nicht vertraut bin (und dieses systematisch erheblich von der RL 95/46/EG abweicht) war es mir ev. nicht immer möglich die genaue Stelle des BDSG zu benennen. Ich bitte Sie daher im Zweifel auch auf die benannten europäisch einheitlichen Prinzipien und die benannten Stellen in der RL 95/46/EG zu achten.*

### Verantwortlicher:

Nach dem obigen Sachverhalt ist davon auszugehen, dass die „Yahoo! Deutschland GmbH“ die verantwortliche Stelle nach § 1 Abs 2 Z3 BDSG für meine personenbezogenen Daten im Rahmen des E-Mail Dienstes ist. Damit ist „yahoo.de“ für die von mir verwendeten Dienste vom BDSG umfasst.

### Zweckbindung:

Im WP 128 der Artikel 29 Gruppe wurde bei der massenhaften Weitergabe von kommerziellen Daten der „SWIFT“ an US Behörden für Ermittlungszwecke vor allem auch auf die Zweckbindung abgestellt. Auch bei einer massenhaften Weitergabe von Nutzerdaten für Ermittlungszwecke durch „Yahoo! Deutschland“ muss daher davon ausgegangen werden, dass hier ein Verstoß gegen den Grundsatz der Zweckbindung nach § 28 BDSG bzw Art 6 Abs 1 lit b der RL 95/46/EG vorliegt.

Wie bereits im WP 128 der Artikel 29 Gruppe festgestellt wurde, hat der EuGH Art 6 der RL 95/46/EG im Lichte von Art 8 EMRK ausgelegt und ist zum Schluss gekommen, dass eine Weitergabe und Zweckänderung in das Grundrecht auf Privatsphäre nach Art 8 EMRK eingreift und daher nur im Rahmen eines „in einer demokratischen Gesellschaft notwendigen“ Eingriffs erlaubt ist (siehe Entscheidungen C-465/00, C-138/01 und C-139/01 des EuGH vom 20. 5. 2003).

### Verhältnismäßigkeit:

Im WP 128 der Artikel 29 Gruppe wurde festgestellt: *„Die Artikel-29-Gruppe weist darauf hin, dass (...) sogar für die Zwecke der behaupteten Terrorismusermittlungen nur spezifische und individualisierte Daten übermitteln sollte, und nur von Einzelfall zu Einzelfall und in vollständiger Übereinstimmung mit den Datenschutzgrundsätzen. Da dies nicht der Fall ist, ist die derzeit gehandhabte Praxis nicht verhältnismäßig und verletzt somit Artikel 6 Absatz 1 Buchstaben c) der Datenschutzrichtlinie.“*

Aufgrund der analogen Faktenlage bei einer Weitergabe durch „Yahoo! Deutschland“ bzw dem Yahoo!-Konzern an die NSA ist auch in diesem Fall von einem unverhältnismäßigen Eingriff in das Grundrecht auf Datenschutz und somit von einem Bruch des BDSG und Art 6 Abs 1 der RL 95/46/EG auszugehen.

Auslegung analog zum WP 128: Im Fall der belgischen „SWIFT“ stellte die Artikel 29 Gruppe im WP 128 auch auf die Freiwilligkeit der Datenverarbeitung in den USA ab: *„Durch die Entscheidung über die Spiegelung aller Datenverarbeitungstätigkeiten in einem Rechenzentrum in den USA brachte sich SWIFT im Ergebnis selbst in eine vorhersehbare Situation, in der sie den nach US-Recht angeordneten Auflagen unterliegt, und in der die Verarbeitung von personenbezogenen Daten derart organisiert wurde, dass eine Umgehung der bereits bestehenden Strukturen und internationalen Übereinkommen vorzuliegen scheint.“*

Auch im gegenwärtigen Fall stellt sich die Frage, ob sich „Yahoo! Deutschland“ auf Pflichten nach amerikanischen Recht berufen kann, wenn sich „Yahoo! Deutschland“ selbstverschuldet in eine Lage gebracht hat in der sie ggf mit der NSA zusammenarbeiten muss. Meines Erachtens ist die Situation hier ebenso wie bei SWIFT zu bewerten.

### Datenübermittlung in die USA:

Weiter ist davon auszugehen, dass meine personenbezogenen Daten zumindest teilweise in den USA verarbeitet werden. Damit liegt jedenfalls eine Übermittlung von Daten in ein Drittland ohne angemessenes Schutzniveau nach § 4b Abs 2 BDSG vor. Eine solche Übermittlung ist nach Art 25 der RL 95/46/EG nur möglich, soweit mein Grundrecht auf Datenschutz sowohl faktisch wie rechtlich in den USA angemessen geschützt wird.

Zustimmung: Denkbar wäre eine Übermittlung unter den Bedingungen von § 4c BDSG. Im gegenständlichen Fall sind die Ausnahmen nach § 4c BDSG jedoch nicht gegeben. Vor allem haben die Nutzer von „Yahoo! Deutschland“ wohl keine eindeutige und informierte Einwilligung im Wissen der Sachlage gegeben (§ 4c Abs 1 Z1 BDSG), da eine massenhafte Weitergabe an US-Behörden bis dato von „Yahoo! Deutschland“ nicht kommuniziert wurde, sondern im Gegenteil sogar abgestritten wird.

Weitere Grundlagen für die Datenübermittlung nach § 4c BDSG sind mir nicht bekannt und können daher in dieser Anzeige auch nicht angeführt werden. Daher ist im Weiteren nur eine Rechtmäßigkeit nach der „Safe Harbor“-Entscheidung zu prüfen.

#### **Safe Harbor:**

Die amerikanische „Yahoo! Inc.“ (Konzernmutter von „Yahoo! Deutschland“) ist dem „Safe Harbor“ beigetreten (siehe <http://safeharbor.export.gov/companyinfo.aspx?id=17009>) und hat sich damit selbst verpflichtet gewisse Grundsätze (zB bezüglich der Datenweitergabe) einzuhalten. Nach den vorliegenden Information erfolgt eine Übermittlung durch „Yahoo! Deutschland“ nur nach dem „Safe Harbor“.

Die Teilnahme am „Safe Harbor“ verpflichtet zur beschränkten Weitergabe von Daten an Dritte. Insbesondere sind die Zustimmung und die Information des Betroffenen bei der Weitergabe der Daten notwendig. Beides ist bei einer möglichen Weitergabe meiner Daten an den NSA nicht erfolgt. Bezüglich der Daten, welche in meinem Konto über Dritte gespeichert werden, ist eine Zustimmung und Information praktisch unmöglich.

Ausnahme für „nationale Sicherheit“: Nach dem vierten Absatz des Anhangs 1 der „Safe Harbor“-Entscheidung können die Geltung der Grundsätze des „Safe Harbor“ für die „nationale Sicherheit“ begrenzt werden.

Ich bitte Sie daher zu prüfen ob der Yahoo!-Konzern aus zwingenden Gründen der „nationalen Sicherheit“ Daten von europäischen Nutzern mit dem NSA teilt oder aber nur freiwillig weitergibt.

Weiter bitte ich zu prüfen, ob sich eine Weitergabe im Rahmen der Ausnahme des „Safe Harbor“ bewegt oder von dieser Ausnahme nicht mehr umfasst ist und folglich eine Übermittlung der Daten durch „Yahoo! Deutschland“ in die USA rechtswidrig ist. Zur Auslegung bitte ich die Ausführungen unten zu berücksichtigen.

Ausnahme für „Gesetzesrecht“ und „Durchführung von Gesetzen“: Nach dem vierten Absatz des Anhangs 1 der „Safe Harbor“-Entscheidung können die Geltung der Grundsätze des „Safe Harbor“ für die Einhaltung von „Gesetzesrecht“ (und sogar „Richterrecht“) begrenzt werden. Nach den Berichten des Guardian erfolgte der Massenzugriff auf die Server von „Yahoo! Deutschland“ bzw des Yahoo!-Konzerns in den USA auf Grundlage von § 1881a U.S.C. (auch bekannt als 702 FISA).

Ich bitte Sie daher zu prüfen, ob der Yahoo!-Konzern aufgrund von gesetzlichem Zwang Daten mit dem NSA teilt oder aber aufgrund einer freiwilligen Vereinbarung mit amerikanischen Behörden diese Daten weitergibt.

Weiter bitte ich zu prüfen, ob sich eine solche Datenweitergabe im Rahmen der Ausnahme des „Safe Harbor“ bewegt oder von dieser Ausnahme nicht mehr umfasst ist und folglich eine Übermittlung durch „Yahoo! Deutschland“ in die USA rechtswidrig ist. Zur Auslegung bitte ich die Ausführungen unten zu berücksichtigen.

#### **Auslegung der „Safe Harbor“ Entscheidung:**

Nach dem Wortlaut der Entscheidung vom 26. Juli 2000 der Europäischen Kommission zur Anerkennung der Selbstverpflichtung nach dem „Safe Harbor“ (ABl L 2000/215, 7), könnte man die oben genannten Ausnahmen derart auslegen, dass amerikanische Gesetze oder auch Richterrecht ein „blanko Schein“ für die Einschränkung der „Safe Harbor“-Entscheidung der Europäischen Kommission wäre. Auch wäre jede Verarbeitung für die „nationale Sicherheit“ eine weitere „blanko Ausnahme“. Eine genaue Definition und Abgrenzung der „nationalen Sicherheit“ fehlt. Die unter dem Buchstaben „a)“ angeführten Ausnahmen enthalten auch keine Einschränkungen, welche die Verhältnismäßigkeit des Grundrechtseingriffes mit dem Zweck des Eingriffs in Verhältnis bringen würden.

Würde man dieser Auslegung folgen, wäre auch eine massenhafte Weitergabe von Daten an US-Behörden durch einen Auftragsdatenverarbeiter in den USA jederzeit möglich. Die Weitergabe wäre auch ohne

begründeten Verdacht, ohne richterliche Überprüfung und ohne Einhaltung der Grundrechte nach EMRK und GRC möglich. Eine solche Auslegung der „Safe Harbor“-Entscheidung wäre in dieser Form jedoch unmöglich mit den Begrenzungen nach Art 25 der RL 95/46/EG vereinbar, würde gegen den Erwägungsgrund 10 der RL 95/46/EG sprechen und würde auch Art 8 EMRK und Art 8 GRC widersprechen.

Betrachtet man die „Safe Harbor“-Entscheidung jedoch innerhalb des Stufenbaus der Rechtsordnung, so wird klar, dass für eine rechtskonforme Auslegung auch die hierarchisch höher stehenden Grundrechte, das Primärrecht und das Sekundärrecht der Europäischen Union eingebunden werden müssen.

#### **Einschränkende Auslegung im Rahmen der RL 95/46/EG:**

Die „Safe Harbor“-Entscheidung unterliegt jedenfalls der Auslegung im Rahmen der RL 95/46/EG. Eine Entscheidung der Europäischen Kommission kann nicht den Rahmen des zugrundeliegenden Sekundärrechtsakts verlassen, andernfalls wäre diese richtlinienwidrig.

Entsprechend ist bei der Auslegung der obig genannten Ausnahmen darauf Bedacht zu nehmen, dass die Voraussetzungen für ein „Angemessenes Schutzniveau“ nach Art 25 der RL 95/46/EG und WP 12 der Artikel 29 Gruppe nicht unterschritten werden. Andernfalls würde man der Entscheidung der Europäischen Kommission einen richtlinienwidrigen Inhalt unterstellen, dies würde die Ungültigkeit der Entscheidung der Europäischen Kommission zur Folge haben (siehe auch Ausführungen unten).

Die Angemessenheit des Schutzniveaus betrifft nicht nur die Datenverwendung durch das Unternehmen selbst, sondern auch den möglichen und faktischen Zugriff durch Behörden im Drittland. So zB die Ausführungen der Artikel 29 Gruppe im WP 12 in Bezug auf vertragliche Grundlagen: *„Artikel 6 des Vertrags von Amsterdam garantiert die Einhaltung der in der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten enthaltenen Grundrechte. In Drittländern mag es ähnliche Beschränkungen der Möglichkeiten des Staates, die Bereitstellung personenbezogener Daten von Unternehmen (...) zu fordern, nicht immer geben. (...) In einigen Fällen ist ein Vertrag ein zu schwaches Instrument, um angemessene Garantien für den Datenschutz zu bieten, und Übermittlungen in bestimmte Länder sollten nicht genehmigt werden.“*

Insbesondere ist zu prüfen, ob eine Ausnahme für die „nationale Sicherheit“ der USA und „Gesetzesrecht“ der USA im Einklang mit der RL 95/46/EG steht. Bisher wurde davon ausgegangen, dass nur die „nationale Sicherheit“ und „Gesetze“ des betreffenden Mitgliedsstaates – nicht jedoch von Drittstaaten – eine Ausnahme erlaubt. Andernfalls wäre festzustellen, in welchem Fall die „nationale Sicherheit“ oder die Gesetze eines Drittstaates anerkennungswürdig sind.

Wenn eine generelle Anerkennung der „nationalen Sicherheit“ oder der „Gesetze“ von Drittstaaten durch RL 95/46/EG gedeckt wäre, würde das auch eine massenweise Weiterleitung an Behörden von zB China, dem Iran oder Nordkorea erlauben. Das wäre wiederum unmöglich mit EU-Recht und Art 8 EMRK vereinbar.

#### **Einschränkende Auslegung im Rahmen von Art 8 EMRK und Art 8 GRC:**

Die Bestimmungen des BDSG und der RL 95/46/EG sind nach allgemeinen Rechtsgrundsätzen, nach Erwägungsgrund 10 der RL 95/46/EG, aber auch nach der Rechtsprechung des EuGH im Lichte von Art 8 EMRK auszulegen (siehe zB §§ 21ff der Entscheidung C-465/00, C-138/01 und C-139/01 des EuGH vom 20. 5. 2003). Mit dem In-Kraft-Treten des Vertrags von Lissabon ist wohl auch zusätzlich die Grundrechtecharta der Europäischen Union (GRC) bei der Auslegung heranzuziehen.

Ein Eingriff in das Grundrecht auf Privatsphäre darf nach der EMRK nur in einer Weise erfolgen der in einer demokratischen Gesellschaft notwendig ist und muss weiter nach der GRC verhältnismäßig sein. Eine massenhafte Weitergabe von europäischen Nutzerdaten an eine ausländische Behörde ohne begründeten Verdacht und ohne effektiven Rechtsschutz für die Betroffenen würde beiden Grundrechtsakten klar widersprechen. Entsprechend muss die RL 95/46/EG und auf der Richtlinie beruhende die „Safe Harbor“-Entscheidung in einer Weise interpretiert werden, die solchen Massenzugriff unterbindet.

Weiter kann man davon ausgehen, dass die in der Europäischen Union geltenden Grundrechte nach Art 8 EMRK und Art 8 GRC wohl nicht durch eine Verbringung von Daten in Drittländer umgangen werden kann. Analog zum „*Refoulement-Verbot*“ kann angenommen werden, dass durch eine Übermittlungserlaubnis von Daten in ein Drittland ohne effektiven Schutz diese Grundrechte untergeben würden.

Das Problem wird besonders augenscheinlich, wenn man Berichten Glauben schenkt wonach europäische Behörden die Ergebnisse des PRISM-Projekts wiederum von den USA erhalten und in der Europäischen Union nutzen. Im Effekt würde dies zu einer „Auslagerung“ der Spionage aus dem Bereich der EMRK bzw der GRC führen. Meines Erachtens ist daher davon auszugehen, dass die EMRK und die GRC die Union sowie die Mitgliedsstaaten zu einem aktiven Schutz auch gegenüber den Behörden von Drittstaaten verpflichtet.

➔ ***Ich bitte Sie daher die richtlinien- und grundrechtskonforme Auslegung des „Safe Harbor“ genauer zu überprüfen und ggf eine Vorabentscheidung durch den EuGH einzuleiten.***

#### **Rechtswidrigkeit der Entscheidung über das Schutzniveau des „Safe Harbor“?**

Ist es Ihnen nicht möglich die „Safe Harbor“-Entscheidung derart auszulegen, dass der Rahmen der RL 95/46/EG, der EMRK und der GRC eingehalten wird, so ist davon auszugehen, dass die Entscheidung der Europäischen Kommission dem Primärrecht und/oder Sekundärrecht nicht entspricht und damit rechtswidrig ist. Eine Entscheidung der Europäischen Kommission kann unmöglich höherrangiges Recht brechen.

Das „Safe Harbor“ System wurde wiederholt und von vielen Seiten kritisiert, da der Anschein besteht, dass es in der Praxis keinen angemessenen Schutz nach den Kriterien des Art 25 der RL 95/46/EG bietet. Dabei wurde bisher hauptsächlich auf die Datenverarbeitung durch Unternehmen abgestellt oder auf die oft als unzureichend empfundene Durchsetzungsmöglichkeiten. Wie bereits oben ausgeführt, stellt aber Art 25 der RL 95/46/EG auf einen deutlich weiteren Bereich bei der „Angemessenheit des Schutzniveaus“ ab. Dieser umfasst auch den staatlichen Zugriff auf Daten in einem Drittstaat und geht daher über die bisher diskutierte Frage der Angemessenheit des „Safe Harbor“ im Rahmen der unternehmerischen Tätigkeiten weit hinaus.

Die ursprüngliche Entscheidung der Europäischen Kommission über die Angemessenheit einer Selbstverpflichtung nach dem „Safe Harbor“ ist daher besonders auch durch die seit 2000 deutlich geänderte Rechtslage in den USA belastet. So wurden nach den Terroranschlägen vom 11. September 2001 viele neue Befugnisse und faktische Vorgehensweisen in den USA eingeführt, die nicht den europäischen Vorstellungen von Rechtsstaatlichkeit und Grundrechtsschutz genügen.

EU-Bürger genießen in den USA generell keine verfassungsmäßigen Grundrechte, da in den USA bis heute das Konzept von „Bürgerrechten“ vorherrscht (welche nur US-Bürgern und Personen, die sich in den USA aufhalten zustehen). So ist eine „Massenbeschlagnahme“ von Daten von EU-Bürgern vom Schutzbereich der US-Verfassung nicht nur nicht erfasst, sondern unter § 1881a U.S.C. sogar ausdrücklich erlaubt. Es besteht kein effektiver Rechtsschutz, da eine Beschwerde zB nur vom betroffenen Betreiber und nicht vom betroffenen Bürger ergriffen werden kann. Weiter tagt zB der zuständige „FISA-Court“ unter Ausschluss der Öffentlichkeit und hat bis zum heutigen Tag noch fast keinen Antrag der US-Behörden auf Datenzugriff abgelehnt. Auch andere Gesetze, wie der „Patriot Act“, geben weitere (nur schwer mit den EU-Grundrechten zu vereinbarenden) Möglichkeiten auf Datenzugriff. Eine genauere Ausführung der Rechtslage würde den Rahmen dieses Antrags leider sprengen.

Es besteht daher durchaus die berechtigte Befürchtung, dass die Angemessenheitsentscheidung der Europäischen Kommission durch die umfangreichen Veränderungen in den USA nachträglich richtlinien- und grundrechtswidrig geworden ist. Diese Befürchtung wird auch von den oben ausgeführten Auslegungsprinzipien im Rahmen der RL 95/46/EG, Art 8 der EMRK und der GRC bestärkt.

➔ ***Ich bitte Sie daher die Frage der eventuellen Rechtskonformität der „Safe Harbor“-Entscheidung genauer zu überprüfen und ggf eine Vorabentscheidung durch den EuGH einzuleiten.***

### **Beweislast bei der Übermittlung von Daten in ein Drittland:**

Nach §§ 4c Abs 5 und 4c Abs 2 BDSG und Art 26 Abs 2 der RL 95/46/EG liegt die Beweislast für die sichere Datenverarbeitung in einem Drittland beim für die Verarbeitung Verantwortlichen. Das bedeutet, dass es angesichts des erschütterten Vertrauens an „Yahoo! Deutschland“ liegt, sicherzustellen und auch nachzuweisen, dass die in den USA verarbeiteten Daten faktisch und rechtlich einen entsprechenden Schutz genießen. Dies muss auch im Rahmen des „Safe Harbor“ gelten (siehe zB den Beschluss des „Düsseldorfer Kreises“ vom 28./29. April 2010).

Sollte sich „Yahoo! Deutschland“ beispielsweise auf die Verschwiegenheitspflichten nach amerikanischem Recht („gag order“) berufen, so wäre die logische Konsequenz, dass eine Übermittlung der Daten einzustellen ist, da „Yahoo! Deutschland“ nicht in der Lage wäre nach § 4c Abs 2 BDSG und Art 26 Abs 2 der RL 95/46/EG „ausreichend Sicherheiten“ bzw „ausreichende Garantien“ für die grundrechtskonforme Datenverarbeitung in den USA zu bieten.

- **Zusammenfassend ist ein „Massenzugriff“ ohne spezifischen Verdachtsmomenten nach der EMRK und der GRC jedenfalls als grundrechtswidriger Eingriff einzustufen.**
- **Dieser Zugriff widerspricht dem Prinzip der Zweckbindung nach § 28 BDSG bzw Art 6 Abs 1 lit b der RL 95/46/EG und wäre daher illegal.**
- **Ein Massenzugriff ist auch mit dem Prinzip der Verhältnismäßigkeit nach dem BDSG und Art 6 Abs 1 der RL 95/46/EG unvereinbar.**
- **Die RL 95/46/EG erlaubt eine Übermittlung von Daten in ein Drittland nur bei einem „angemessen Schutzniveau“ welches zumindest den Grundrechten nach der EMRK und der GRC gleichkommt.**
- **Eine massenhafte Weiterleitung meiner Daten an den NSA macht daher die Übermittlung in die USA durch „Yahoo! Deutschland“ illegal und widerspricht §§ 4b und 4c BDSG bzw Art 25 ff der RL 95/46/EG der EMRK und der GRC.**
- **Nach §§ 4b und 4c BDSG und Art 26 Abs 2 der RL 95/46/EG muss der für die Datenverarbeitung Verantwortliche ausreichende Sicherheiten hinsichtlich des Schutzes meiner Rechte bieten. Es liegt somit an „Yahoo! Deutschland“ die Verdachtslage mit substantiellen Beweisen zu widerlegen. Andernfalls wäre eine Übermittlung in die USA unzulässig.**
  
- **Ich ersuche Sie daher die notwendigen Schritte einzuleiten um eine rechtswidrige Übermittlung meiner Daten in die USA zu unterbinden, sollte sich der oben geschilderte begründete Verdacht der Datenweitergabe an den NSA durch „Yahoo! Deutschland“ nicht widerlegen lassen.**

Vielen Dank für die Bearbeitung meiner Beschwerde. Ich bin für Rückfragen jederzeit unter [REDACTED] erreichbar. Um eine möglichst effiziente Bearbeitung dieser Beschwerde zu ermöglichen, möchte ich Sie abschließen noch darauf hinweisen, dass inhaltlich ähnliche Beschwerden zu anderen Unternehmen jedenfalls auch bei den Datenschutzbehörden von Irland und Luxemburg eingegangen sind oder bald eingehen werden. Ich hoffe mit diesem Hinweis die Bearbeitung zu erleichtern.

Mit freundlichen Grüßen,

[REDACTED]