Stellungnahme

zum Safe Harbor Review und den Vorschlägen der EU-Kommission in der Mitteilung (2013) 847[1] sowie den Vorschlägen der Art. 29 Arbeitsgruppe[2]
15.08.2014

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. vertritt mehr als 1.700 Unternehmen, davon über 1.200 Direktmitglieder mit etwa 140 Milliarden Euro Umsatz und 700.000 Beschäftigten. Hierzu zählen Anbieter von Software & IT-Services, Telekommunikations- und Internetdiensten, Hersteller von Hardware und Consumer Electronics sowie Unternehmen der digitalen Medien. Der BITKOM setzt sich insbesondere für eine Modernisierung des Bildungssystems, eine innovative Wirtschaftspolitik und eine zukunftsorientierte Netzpolitik ein.

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.

Albrechtstraße 10 A
10117 Berlin-Mitte
Tel.: +49.30.27576-0
Fax: +49.30.27576-400
bitkom@bitkom.org
www.bitkom.org

Ansprechpartner
Susanne Dehmel
Bereichsleiterin Datenschutz
Tel.: +49.30.27576-223
Fax: +49.30.27576-51-223
s.dehmel@bitkom.org

Präsident
Prof. Dieter Kempf

Hauptgeschäftsführer
Dr. Bernhard Rohleder

Die EU-Kommission hat im November 2013 in ihrer Mitteilung über die Funktionsweise der Safe-Harbor-Regelung aus Sicht der EU-Bürger und der in der EU niedergelassenen Unternehmen einige konkrete Vorschläge gemacht, die den durch das Programm gewährleisteten Datenschutz verbessern sollen. Ebenso hat die Artikel 29 Arbeitsgruppe im April 2014 in einem Brief an die EU-Kommission detaillierte Anregungen für die Überarbeitung zu Safe Harbor gegeben. Die Diskussion über die weitere Entwicklung von Safe Harbor als eine der Rechtsgrundlagen für Datentransfers von der EU in die USA wird auf beiden Seiten des Atlantiks fortgeführt. Im Folgenden möchten wir aus BITKOM Sicht zu den gemachten Vorschlägen sowie möglichen weiteren Änderungen, die im Zuge einer Weiterentwicklung der Rechtsgrundlagen vorgenommen werden könnten, Stellung nehmen.

Zusammenfassung

.

- Die Safe Harbor Zertifizierung ist neben den EU-Standardvertragsklauseln und Binding Corporate Rules (BCRs) ein gängiges Rechtsinstrument zur legalen Übermittlung von personenbezogenen Daten von der EU in die USA.

- Der Review muss genutzt werden, um bestehende Schwachstellen des Pakets zu beseitigen und es als rechtssichere Grundlage für Datentransfers mit angemessenem Datenschutzniveau auszugestalten.

- Mehr Transparenz für die Beteiligten auf beiden Seiten des Atlantiks kann durch eine klarere Anleitung der sich zertifizierenden Unternehmen und durch leicht auffindbar veröffentlichte und zur Safe Harbor Webseite verlinkte Privacy Policies erreicht werden.

- Rechtsschutz über alternative Streitbeilegungsverfahren muss leicht verfügbar und erschwinglich sein.

[1] http://ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf
[2] http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140410_wp29_to_ec_on_sh_recommendations.pdf

- Für eine effektive Rechtsdurchsetzung sollten die Instrumente der FTC genutzt und ggf. um zusätzliche risikobezogene Kontrollen ergänzt werden.

- Bei den Vorschlägen zu inhaltlichen Änderungen ist jeweils abzuwägen, ob eine Angleichung an Formulierungen der EU-RL tatsächlich hilfreich ist, um das angemessene Datenschutzniveau sicherzustellen oder ob ggf. im US-Recht verankerte vergleichbare Vorgaben von den Unternehmen besser verstanden und umgesetzt werden. Dies gilt z.B. bei den Vorschlägen zum „Notice and Choice Principle". Sichergestellt sein muss dabei, dass der Schutz der personenbezogenen Daten in den USA dem europäischem Niveau entspricht.

- Bei der Frage der Onward Transfers sollte sichergestellt werden, dass in Fallkonstellationen der Auftragsverarbeitung zwischen EU-Auftraggeber und US-Auftragnehmer das durch Safe Harbor sichergestellte Datenschutzniveau ggf. auch beim Subunternehmer durchgesetzt werden kann, damit der europäische Auftraggeber in der Lage ist, seinen gesetzlichen Pflichten nachzukommen.

- Das Access Principle sollte um eine Erläuterung ergänzt werden, welche Auskünfte regelmäßig zu erteilen sind. Das dort verankerte Löschrecht sollte auf Fälle der unrechtmäßigen Verarbeitung ausgeweitet werden.

- Alle dem Stichwort „Accountability" zuzuordnenden bestehenden Verpflichtungen sollten der besseren Übersicht wegen in einem ausdrücklichen „Accountability Principle" zusammengefasst werden.

- Die Forderungen der EU-Kommission nach mehr Transparenz über die Auslegung der bestehenden US-Vorschriften werden unterstützt. Sie sollten bei den Verhandlungen gesondert adressiert und an die US-Regierung gerichtet werden, da sie nicht allein im Rahmen von Safe Harbor, sondern nur durch eine Änderung nationaler Gesetze erreicht werden können. Für die weiteren Vorschläge der Art. 29 Gruppe, soweit sich diese auf Vorschriften des US-Rechts oder auf Handlungen der Unternehmen beziehen, die durch US-Recht vorgegeben bzw. verboten sind, gilt ebenfalls, dass sie sich direkt an die Regierung richten müssen und nicht allein durch Safe Harbor Vorgaben gelöst werden können.

Gliederung

Einleitung: Wie funktioniert Safe Harbor momentan und wie wird es genutzt?

Das Safe Harbor Paket besteht aus 7 Datenschutzprinzipien und 15 sog. „Frequently Asked Questions".

Die Safe-Harbor-Principles sind:
- Informationspflicht (Notice)
- Wahlmöglichkeit (Choice)
- Weitergabe (Onward Transfer)
- Auskunftsrecht (Access)
- Sicherheit (Security)
- Datenintegrität (Data Integrity)
- Durchsetzung (Enforcement)

Die Prinzipien werden durch die FAQ, die als Leitlinien dienen, ergänzt und konkretisiert. Unternehmen die sich nach diesen Vorgaben selbst zertifizieren und in die Liste des US Handelsministeriums eintragen möchten, müssen sicherstellen, dass sie alle Vorgaben erfüllen. Die Vorgaben sehen vor, dass Unternehmen unter anderem eine Datenschutz Policy erstellen und öffentlich bereitstellen sowie einen festen Kontakt im Unternehmen etablieren. Ferner muss eine Beschwerde- bzw. Streitschlichtungsstelle benannt werden, an die sich Betroffene bei vermuteten Verstößen gegen die Safe Harbor Verpflichtungen wenden können. Nur Unternehmen, die der Jurisdiktion der Federal Trade Commission (FTC) oder des Department of Transport unterliegen, können sich im Rahmen des Programms selbst verpflichten. Mit Ausfüllen des Formulars des Handelsministeriums und der Veröffentlichung der eigenen Verpflichtung auf die Safe Harbor Prinzipien verpflichten sie sich verbindlich und können je nach Zuständigkeit durch die FTC[3] oder das U.S. Department of Transportation (DoT) belangt werden, wenn sie den eingegangenen Verpflichtungen nicht nachkommen. Nach eigenen Angaben[4] hatte die FTC in den ersten zehn Jahren des Bestehens von Safe Harbor keine Beschwerden von EU Seite erhalten, aber schließlich selbst 10 Verfahren wegen Verstößen gegen Safe Harbor durchgeführt und 7 Verfahren wegen falscher Behauptung, die Safe Harbor Zertifizierung durchgeführt zu haben. Teilweise mündeten die Verfahren in umfangreiche Auflagen zur Durchführung von Privacy Programmen und auch in Zahlungen Einzelner in zweistelliger Millionenhöhe.

[3] Section 5 of the Federal Trade Commission Act ("FTC Act")
[5] http://aspe.hhs.gov/admnsimp/pl104191.htm

1 Organisatorische Vorschläge

Sowohl aus den Vorschlägen der Kommission und der Art. 29 Arbeitsgruppe als auch aus den Erfahrungsberichten unserer Mitglieder ergibt sich, dass eine bessere praktische Umsetzung durch Safe Harbor u.a. durch einige organisatorische Maßnahmen erreicht werden könnte. Eine transparentere Darstellung und Hilfestellungen für die Unternehmen zum besseren Verständnis und zur Umsetzung bzw. Kontrolle der Vorgaben wären hier hilfreich.

- Eine deutlichere Darstellung in den Unterlagen zu Safe Harbor, auf welche Arten von Daten und für welche Bereiche Safe Harbor anwendbar ist, so dass auch die sich zertifizierenden Unternehmen in ihren Policies genau angeben können (und sollen), welche Arten von Daten bei Ihnen von Safe Harbor und welche Teile einer Unternehmensgruppe von Safe Harbor umfasst sind. (Vorschlag Art. 29 Gruppe, S. 4, 1. Spiegelstrich)

- Der 1. Vorschlag der EU-KOM, dass selbstzertifizierte Unternehmen ihre Datenschutzbestimmungen offenlegen sollten, ist sinnvoll. Die Datenschutz Policy sollte auf der Webseite des Unternehmens öffentlich zugänglich leicht auffindbar sein. Das Veröffentlichen der Datenschutz Policy ist eine der Anforderungen, die klar aus Safe Harbor hervorgehen und ist auch Voraussetzung für ein mögliches Eingreifen der Federal Trade Commission bei Verstößen.

- Möglicherweise wäre es auch hilfreich für die Unternehmen, wenn das Handelsministerium – wie von der Art. 29 Gruppe(S. 4, 2. Spiegelstrich) vorgeschlagen - Guidelines für das Entwerfen von Safe Harbor Privacy Policies und/oder Beispiele von Safe Harbor Privacy Policies veröffentlichen würde.

- Auch der 2. Vorschlag der EU-KOM, dass die Geschäftsbedingungen zum Datenschutz auf der Website selbstzertifizierter Unternehmen stets mit der Safe-Harbor-Website des US-Handelsministeriums verlinkt sein sollten, auf der alle aktuellen Teilnehmer der Safe-Harbor-Regelung aufgeführt sind, erscheint sinnvoll, weil auf diese Weise europäische Betroffene ohne zusätzlichen Suchaufwand sofort feststellen können, ob ein bestimmtes Unternehmen derzeit der Safe-Harbor-Regelung angehört.

- Eine tabellarische Übersicht mit Vergleich und Erklärung der unterschiedlichen Fachbegriffe, die im Safe Harbor Regelwerk und bei der EU-Richtlinie eine Rolle spielen, wäre sowohl für US-Unternehmen, die sich zertifizieren möchten, als auch für europäische Auftraggeber hilfreich, um mögliche Unterschiede zu erkennen (Beispiel: Vergleich von Agent und Auftragsverarbeiter, „persönliche Information“, „privacy program) (siehe auch Vorschlag der Art. 29 Gruppe, S.4, 6. Spiegelstrich).

- Eine Veröffentlichung der jeweiligen individuell vereinbarten vertraglichen Regelungen zum Datenschutz wie von der EU-KOM vorgeschlagen (Vorschlag 3), erscheint dazu nicht zwingend notwendig und könnte für die Unternehmen aus wettbewerblicher Sicht problematisch sein. Weitere Überlegungen zur Sicherstellung des gleichen Datenschutzniveaus beim Unterauftragnehmer finden sich unter 3.3.

- Ob der in Vorschlag 4 der EU-Kommission vorgesehene besondere Warnhinweis oder die von der Art. 29 Gruppe vorgeschlagene gesonderte Liste der momentan nicht die Anforderungen der Zertifizierung erfüllenden Unternehmen tatsächlich notwendig sind, erscheint fraglich. Es muss aber jedenfalls klar und eindeutig aus der Webseite hervorgehen, ob eine aktuell gültige Safe Harbor Zertifizierung existiert.

2 Vorschläge für eine effektive Rechtsdurchsetzung

2.1 Rechtsschutz

Grundsätzlich sollte der in Safe Harbor verankerte Rechtsschutz über alternative Streitschlichtungsverfahren leicht verfügbar und erschwinglich sein. Daher sind die drei Vorschläge der EU-Kommission zum Rechtsschutz (Verlinkung zum DR, Verfügbarkeit und niedrige Kosten, Überprüfung der Transparenz des ADR-Verfahrens) zu unterstützen. Soweit diese Kriterien sichergestellt werden können, sind weitere Vorgaben hierzu (wie teilweise von der Art. 29 Gruppe gefordert) aus unserer Sicht entbehrlich.

2.2 Rechtsdurchsetzung

- Bei dem 1. Vorschlag der EU-KOM, nachdem nach einer Safe-Harbor-Zertifizierung oder Re-zertifizierung bei einem bestimmten Anteil der Unternehmen von Amts wegen überprüft werden soll, ob sie ihre Datenschutzbestimmungen einhalten (wobei diese Kontrolle über formale Erfordernisse hinausgehen sollte), ist nicht ganz klar, ob hiermit eine materiell-rechtliche Prüfung der Datenschutz Policy anhand der Safe Harbor Vorgaben gemeint ist oder eine Art Audit, die die Umsetzung der Policy im Unternehmen umfasst. Dem Wortlaut nach scheint letzteres der Fall zu sein. Relevant ist die Unterscheidung, weil der Aufwand für ein umfassendes Audit wesentlich höher ist als für eine materiell-rechtliche Prüfung der Unterlagen. Bei beidem stellt sich die Frage, wer die Kosten dafür trüge. Denkbar ist, dass bei Registrierung der Unternehmen in jedem Fall eine summarische Prüfung der Datenschutz Policy auf Compliance der Policy mit den Vorgaben von Safe Harbor erfolgt. Ebenso sollte in einigem Abstand zur Zertifizierung geprüft werden, ob die Policy auch öffentlich zugänglich ist.
  Was anlasslose Kontrollen angeht, erscheint ein risikobezogener Ansatz grundsätzlich sinnvoller als stichprobenartige Kontrollen. Dafür müssten jedoch Kriterien für die Risikobewertung erstellt werden, welche eine Gleichbehandlung sicherstellen. Die Aufsichtsbehörden beiderseits des Atlantiks müssten dazu ein gemeinsames Verständnis entwickeln.

- Der 2. Vorschlag der EU-KOM, wonach ein Unternehmen, bei dem im Zuge einer Beschwerde oder Untersuchung ein Verstoß gegen die Datenschutzbestimmungen festgestellt wurde, ein Jahr später erneut überprüft werden soll, sollte mit dem üblichen Vorgehen der FTC bei Verfahren aufgrund von Beschwerden abgeglichen werden. Denn üblicherweise erlässt die FTC im Falle von begründeten Beschwerden sogenannte „Consent Orders“, durch welche die Unternehmen ohnehin auf längere Zeit (mehrere Jahre) der fortlaufenden Kontrolle durch die FTC unterliegen. Doppelte Kontrollen sollten vermieden werden.

- Bezüglich des 3. Vorschlags der EU-KOM , dass bei bestehenden Zweifeln an der Einhaltung der Safe-Harbor-Grundsätze oder bei Beschwerden gegen ein Unternehmen das US-Handelsministerium die zuständige Datenschutzbehörde in der EU davon in Kenntnis setzen sollte, ist unklar, was genau hier gemeint ist bzw. mit dieser Vorgehensweise erreicht werden soll. Auch wie ein praktikables Verfahren hierfür angesichts der möglichen Vielzahl von für EU-Unternehmen zuständigen Behörden aussehen könnte, wird nicht ausgeführt.

- Auch der 4. Vorschlag EU-KOM, Falschbehauptungen in Bezug auf die Teilnahme an der Safe-Harbor-Regelung sollten weiter untersucht werden, wird unterstützt.

3 Vorschläge für inhaltliche Klarstellungen und Änderungen

3.1 Anwendungsbereich

- Es sollte klargestellt werden, ob und inwiefern die Safe Harbor Prinzipien auch von US-Unternehmen anzuwenden sind, die in einem Vertragsverhältnis mit einem europäischen Unternehmen nur als „Agent" tätig sind, also nur Daten im Auftrag verarbeiten.

3.2 Notice and Choice Principles

Die Art. 29 Gruppe macht verschiedene Vorschläge zur Übernahme von Begriffen oder Mechanismen aus der EU-Datenschutz-Richtlinie, die nicht unbedingt notwendig oder geeignet erscheinen, in der praktischen Umsetzung zu einem besseren Datenschutzniveau zu führen. Es sollte bedacht werden, dass eine 1:1 Übernahme der Richtlinienvorgaben nicht unbedingt zu einem besseren tatsächlichen Datenschutzniveau bei den amerikanischen Unternehmen führen muss. Teilweise sind diese nicht vertraut mit der europäischen Datenschutzsystematik – konkrete Vorgaben, die auf die amerikanischen Verhältnisse zugeschnitten sind, sind unter Umständen allgemeinen Abwägungsklauseln vorzuziehen. Es gilt daher, mit den Vorgaben in Safe Harbor ein der Richtlinie entsprechendes – nicht aber notwendig mit genau den gleichen Vorgaben umgesetztes - Datenschutzniveau zu erreichen.

- Den Änderungsvorschlag zu Human Resources FAQ 9, Answer to Q9 (Art. 29 Gruppe, S.7, 6. Spiegelstrich) halten wir nicht für erforderlich, weil der Mehrwert für die konkrete Fallkonstellation nicht ersichtlich ist. Der Änderungsvorschlag zu Human Resources, Art. 29 Gruppe, S. 8, 1. Spiegelstrich, ist nicht ganz verständlich. Falls damit gemeint ist, dass Transfers von Daten für arbeitsrechtliche Entscheidungen nicht ohne „notice" getroffene werden dürfen, stimmen wir nicht zu, weil dies praktisch möglich sein muss.

- Ausnahme von Notice, Choice and Onward Transfer auf öffentlich zugängliche Informationen (FAQ15) – Art. 29 Gruppe, S.8, 2. Spiegelstrich
  Es ist nicht ersichtlich, dass sich diese Ausnahme negativ für die Betroffenen auswirken könnte – sobald öffentliche Informationen mit weiteren kombiniert

werden oder der Exporteur auf Beschränkungen hinsichtlich der Verwendung hinweist, greift die Ausnahme nicht.

- Zusätzliche Anwendung des Prinzips der Verhältnismäßigkeit oder der Angemessenheit auf das Notice und Choice Prinzip – Art. 29 Gruppe, S. 8, Spiegelstriche 3-5: Die Anwendung des Prinzips der Verhältnismäßigkeit und der Angemessenheit zusätzlich zu den bestehenden Notice und Choice Prinzipien wäre zwar grundsätzlich wünschenswert. Tatsächlich halten wir es aber nicht für unbedingt zielführend mit Blick auf die Sicherstellung eines angemessenen Datenschutzniveaus bei der Datenverarbeitung durch amerikanische Unternehmen. Konkrete Vorgaben, in welchen Fällen der Betroffene informiert oder gefragt werden muss, erscheinen in der Praxis zielführender.

- Dies gilt auch hinsichtlich des Hinweises der Art. 29 Gruppe, S. 6, 4. Absatz „Choice" – Es ist richtig, dass die Vorgaben in Safe Harbor sich von denen in der Richtlinie an dieser Stelle unterscheiden. Im Ergebnis halten wir das in der Safe Harbour Entscheidung der Europäischen Kommission vorgegebene Schutzniveau für vergleichbar. Anstelle einer Abwägung zwischen den eigenen legitimen Interessen an einer Nutzung zu einem veränderten Zweck und entgegenstehender überwiegender Interessen des Betroffenen, wird den amerikanischen Unternehmen in bestimmten Fällen eine Unterrichtung mit Widerspruchsmöglichkeit bei Zweckänderungen aufgegeben. Das ist ein pragmatischer Ansatz, der ebenfalls in der Lage sein könnte, die Rechte der Betroffenen hinreichend zu wahren.

3.3 Onward Transfer Principle

Eine Abfrage unter den Mitgliedern des AK Datenschutz des BITKOM hat ergeben, dass viele Unternehmen, die auf der Basis von Safe Harbor Daten an amerikanische Unternehmen übertragen, die momentan bestehende Regelung zur Datenweitergabe an Subunternehmer nicht für ausreichend halten und daher in der Regel zusätzliche Vereinbarungen hierzu abschließen.

Die Safe Harbor Principles enthalten im Onward Transfer Principle die Verpflichtung, bei Weiterleitung von Daten an einen „Agent" sicher zu stellen, dass sich dieser den Safe Harbor Principles unterwirft, falls er nicht ohnehin selbst Safe Harbor zertifiziert ist oder sich im Geltungsbereich der EU-Richtlinie oder einem Drittstaat mit angemessenen Datenschutzniveau befindet. Wie diese Verpflichtung erfolgen soll und welche Vorgaben die entsprechenden Verträge enthalten müssen, ist nicht näher ausgeführt. Dies kann vor allem im Hinblick auf die Durchsetzung des Datenschutzniveaus problematisch sein, wenn der Agent sich in einem Drittstaat ohne angemessenes Datenschutzniveau befindet und nicht der Aufsicht durch die FTC, der europäischen Aufsicht oder einem entsprechenden Durchsetzungsorgan unterliegt. Sind dann keine ausreichenden vertraglichen Kontroll- und Prüfpflichten von Seiten des verantwortlich bleibenden zertifizierten amerikanischen Unternehmens vorhanden, ist unter Umständen kein Durchgriff auf den Subunternehmer gegeben.

Um diesen Bedenken zu begegnen schlagen wir folgende Überlegungen vor:

- Das bestehende Onward Transfer Principle verpflichtet das zertifizierte Unternehmen, bei Onward Transfers an Subunternehmer in Drittstaaten ohne

angemessenes Datenschutzniveau, die Einhaltung der Safe Harbor Principles vertraglich sicher zu stellen.

- Für die rechtssichere Handhabung und vertragliche Umsetzung von Onward Transfers benötigen Unternehmen zusätzlich klarere Informationen darüber, welche Anforderungen an die Kontrolle von Agents und anderen Dritten, die Daten von Safe-Harbor-zertifizierten Unternehmen erhalten, gestellt werden.

- Um den Pflichten der verantwortlichen Stelle in Europa Rechnung zu tragen, sollte klargestellt werden, dass bestehende vertragliche Vorgaben aus dem Verhältnis europäische verantwortliche Stelle und zertifiziertes Unternehmen ggf. im Rahmen von onward transfers zu berücksichtigen sind.

- Ebenso sollte geklärt werden, wer jeweils gegenüber der europäischen verantwortlichen Stelle und dem Betroffen verantwortlich ist bzw. ob und wie die Verantwortung ggf. vertraglich verteilt kann.

- Bei onward transfers zu Agents von selbstzertifizierten Organisationen, die bereits selbst als Agents agieren, sollte darauf hingewiesen werden, dass der Vertrag, der mit einer verantwortlichen Stelle in der EU unterzeichnet wurde (FAQ10 Article 17 contracts9), eine Regelung enthalten kann, die onward transfers nicht oder nur unter bestimmten Voraussetzungen erlaubt (entspricht Vorschlag der Art. 29 Gruppe, S.7, 2. Spiegelstrich). In diesen Fallkonstellationen sollten die als Agents agierenden selbstzertifizierten Stellen auch verpflichtet werden, auf Verlangen dem europäischen Auftraggeber die für Safe Harbor und das Verarbeitungsverhältnis relevanten Vorgaben entscheidenden Vertragsbestandteile zur Kenntnis zu geben.

3.4 Access Principle

- Der Vorschlag der Art. 29 Gruppe (S.6, 4. Spiegelstrich) in Bezug auf das Auskunftsrecht (Access) klar zu stellen, dass der Betroffene Auskunft über alle verarbeiteten Daten, nicht nur über Kontaktinformationen oder andere spezielle Daten erhält, könnte eventuell sinnvoller so umgesetzt werden, dass eine Art Liste mit den Auskünften erstellt wird, die regelmäßig zu erteilen sind, damit die sich zertifizierenden Unternehmen einschätzen können, welchen Umfang die Pflichten haben, die auf sie zukommen.

- Die Forderung der Art. 29 Gruppe (S.6, 5. Spiegelstrich), das Löschrecht im Access Prinzip auch auf Fälle auszuweiten, in denen Daten ohne Einwilligung des Betroffenen oder unter Verstoß gegen die Prinzipien erhoben oder verarbeitet wird, erscheint sinnvoll.

3.5 Security Principle

Eine Änderung des Textes wie von der Art. 29 Gruppe (S. 7, 4. Spiegelstrich) gefordert, wird nicht für notwendig erachtet. Der Begriff „reasonable precautions“ ist für amerikanische Unternehmen wahrscheinlich besser verständlich, da es auch in amerikanischen Gesetzen wie z.B. dem HIPAA[5] verwendet und eher

[5] http://aspe.hhs.gov/admnsimp/pl104191.htm

streng ausgelegt wird.[6] Nach unserem Verständnis reicht dieser Begriff daher aus, um den europäischen „angemessenen Maßnahmen“ vom Schutzniveau her zu entsprechen.

3.6 Accountability

Der Vorschlag der Art. 29 Gruppe, alle bestehenden „accountability“ Pflichten mit einem besonderen Prinzip zusammen zu fassen, das der „Accountability“ gewidmet ist (siehe z.B. die Referenz zu internen Beschwerdemechnismen, externen oder internen compliance reviews, Schulung der Mitarbeiter, Datenschutzbeauftragten oder ähnliche Funktionen im bestehenden FAQ 7), ist zu unterstützen. Diese Änderung könnte helfen, die internen Maßnahmen klarer zu machen, die in den selbstzertifizierten Organisationen eingesetzt werden müssen und darauf hinweisen, dass diese Maßnahmen vor der Safe Harbor Zertifizierung bereits umgesetzt sein müssen.

4 Zugriffsrechte der Behörden

- Die Kommission schlägt hierzu vor: Die Datenschutzbestimmungen selbstzertifizierter Unternehmen sollten Auskunft darüber geben, in welchem Umfang die Behörden nach Maßgabe des US-Rechts Daten erheben und verarbeiten dürfen, die auf der Grundlage der Safe-Harbor-Regelung übermittelt worden sind. Die Unternehmen sollten insbesondere angehalten werden, in ihren Datenschutzbestimmungen anzugeben, in welchen Fällen sie Ausnahmen von den Safe-Harbor-Grundsätzen anwenden, um Anforderungen der nationalen Sicherheit, des öffentlichen Interesses oder der Rechtsdurchsetzung zu genügen.

  Grundsätzlich halten wir ein Mehr an Transparenz über Behördenzugriffe für wichtig und würden es begrüßen, wenn es allen Unternehmen in den USA und in der EU von Regierungsseite ermöglicht würde, transparent über Behördenzugriffe zu informieren. Denn die Unternehmen haben von sich aus ein großes Interesse daran, ihre Nutzer hierzu zu informieren. In diesem Sinne könnte der Vorschlag der Kommission für eine Regelung, nach der die US-Unternehmen in Datenschutzbestimmungen darüber aufklären, dass sie, soweit sie gesetzlich verpflichtet sind, auch Daten an Behörden übermitteln, zu einem Stück mehr Transparenz beitragen. Wir geben allerdings zu bedenken, dass diese Forderung bereits über das hinausgeht, zu dem europäische Unternehmen verpflichtet sind. Das gilt insbesondere, falls der Vorschlag darüber hinaus so gemeint sein sollte, dass die Unternehmen in ihren Datenschutzbestimmungen die genauen Rechtsgrundlagen samt den Anwendungsfällen oder dem Umfang, in dem diese Vorschriften Datenerhebung zulassen, aufführen sollen. Wir würden dies nicht als sinnvoll erachten, weil es weder der Übersichtlichkeit der Datenschutzbestimmungen dient, noch für die Unternehmen im Einzelnen zu leisten ist.

  Vielmehr müssen die Forderungen der EU-Kommission nach mehr Transparenz über die Auslegung der bestehenden US-Vorschriften bei den Verhandlungen gesondert adressiert und direkt mit der Regierung geklärt werden.

[6] Aktuelle Entscheidungen der FTC dazu unter: http://www.business.ftc.gov/legal-resources/29/35

Hierzu müssten die nationalen Regelungen anpasst werden, das Thema kann also nicht isoliert durch Safe Harbor Vorgaben geregelt werden.

Für die weiteren Vorschläge der Art. 29 Gruppe, soweit sich diese auf Vorschriften des US-Rechts oder auf Handlungen der Unternehmen beziehen, die durch US-Recht vorgegeben bzw. verboten sind, gilt ebenfalls, dass sie sich direkt an die Regierung richten müssen. Auch die Frage, wem welche Rechte und Rechtsschutzmöglichkeiten gegen Überwachungsmaßnahmen durch Behörden oder Geheimdienste eingeräumt werden, muss durch die beteiligten Regierungen geklärt und entschieden werden. Zu begrüßen ist in diesem Zusammenhang die Ankündigung der US-Regierung, den Privacy Act so zu ändern, dass er auch für Nicht-US-Bürger gilt und diesen ein Klagerecht bei Datenschutzverstößen infolge von Behördenzugriffen einräumt.[7]

- Das Prinzip der strikten Erforderlichkeit und Verhältnismäßigkeit muss grundsätzlich für alle Behördenzugriffe auf beiden Seiten des Atlantiks gelten. Die Verhandlungspartner sollten sich in ihrem jeweiligen Wirkungsbereich dafür einsetzen, dass nationale Regelungen für die Kompetenzen der Behörden entsprechend ausgestaltet sind oder werden. Um diese Prämisse auch in der Safe Harbor Vereinbarung deutlich zu machen, könnte man ferner das Kriterium der Verhältnismäßigkeit zusätzlich zur Erforderlichkeit in den Wortlaut der Ausnahme der nationalen Sicherheit aufnehmen (2. Vorschlag der EU-Kommission zu Behördenzugriffen).

[7] http://www.justice.gov/opa/pr/2014/June/14-ag-668.html