EUROPÄISCHE
KOMMISSION

Brüssel, den 27.11.2013
COM(2013) 847 final

MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT

über die Funktionsweise der Safe-Harbor-Regelung aus Sicht der EU-Bürger und der in der EU niedergelassenen Unternehmen

MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT

über die Funktionsweise der Safe-Harbor-Regelung aus Sicht der EU-Bürger und der in der EU niedergelassenen Unternehmen

1. EINLEITUNG

Für die Übermittlung personenbezogener Daten aus den EU-Mitgliedstaaten an Drittstaaten ist die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr („Datenschutzrichtlinie“) maßgebend,[1] sofern die Übermittlung in den Anwendungsbereich der Richtlinie fällt.[2]

Nach Maßgabe der Richtlinie kann die Kommission feststellen, dass ein Drittstaat aufgrund seiner nationalen Rechtsvorschriften oder internationalen Verpflichtungen, die er zum Schutz der Rechte von Privatpersonen eingegangen ist, ein angemessenes Schutzniveau gewährleistet und somit die besonderen Beschränkungen für die Datenübermittlung an dieses Land nicht gelten. Diese Beschlüsse werden gemeinhin als **„Angemessenheitsbeschlüsse“** bezeichnet.

Am 26. Juli 2000 erließ die Kommission die Entscheidung 2000/520/EG[3] **(„Safe-Harbor-Entscheidung“**), mit der anerkannt wurde, dass die vom US-Handelsministerium herausgegebenen „Grundsätze des ‚sicheren Hafens‘ zum Datenschutz“ („Grundsätze“) und „Häufig gestellten Fragen“ („FAQ“) ein angemessenes Schutzniveau für die Übermittlung personenbezogener Daten aus der Europäischen Union gewährleisten. Der Safe-Harbor-Entscheidung gingen eine Stellungnahme der Artikel-29-Datenschutzgruppe und eine Stellungnahme des Ausschusses nach Artikel 31 voraus, der die Mitgliedstaaten mit qualifizierter Mehrheit zugestimmt hatten. Zudem hatte das Europäische Parlament die Safe-Harbor-Entscheidung vor ihrem Erlass im Einklang mit dem Beschluss des Rates 1999/468/EG geprüft.

Die Safe-Harbor-Entscheidung erlaubt somit die freie Übermittlung[4] personenbezogener Informationen aus EU-Mitgliedstaaten[5] an Unternehmen in den USA, die den Safe-Harbor-Grundsätzen zugestimmt haben, auch dann, wenn die Datenübermittlung – aufgrund der erheblichen Abweichungen bei den Datenschutzregelungen auf beiden Seiten des Atlantiks – ansonsten nicht den EU-Normen zur Sicherstellung eines angemessenen Datenschutzniveaus genügen würde.

Die Funktionsweise der Safe-Harbor-Vereinbarung basiert auf den Verpflichtungserklärungen und Selbstzertifizierungen der beteiligten Unternehmen. Die Beteiligung ist zwar freiwillig,

---

1 Die Artikel 25 und 26 der Datenschutzrichtlinie geben den rechtlichen Rahmen für die Übermittlung personenbezogener Daten aus der EU an Drittländer außerhalb des EWR vor.

2 Artikel 13 des Rahmenbeschlusses 2008/977/JI des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, umfasst weitere Vorschriften für den Fall, dass es sich um personenbezogene Daten handelt, die ein Mitgliedstaat an einen anderen übermittelt oder diesem zur Verfügung gestellt hat und letzterer beabsichtigt, diese Daten zur Verhütung, Ermittlung, Feststellung oder Verfolgung von Straftaten oder zur Vollstreckung strafrechtlicher Sanktionen an einen Drittstaat oder eine internationale Einrichtung weiterzuleiten.

3 Entscheidung 2000/520/EG der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des „sicheren Hafens“ und der diesbezüglichen „Häufig gestellten Fragen“ (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA (ABl. L 215 vom 28. August 2000, S. 7).

4 Dies schließt nicht aus, dass die Datenverarbeitung weiteren Anforderungen unterliegt, die durch nationale Rechtsvorschriften zur Umsetzung der EU-Datenschutzrichtlinie begründet sind.

5 Aufgrund der Ausweitung der Richtlinie 95/46/EG auf das EWR-Abkommen (Entscheidung 38/1999 vom 25. Juni 1999, ABl. L 296 vom 23.11.2000, S. 41) gilt dies gleichermaßen für Datentransfers aus Drittstaaten in den EWR.

jedoch sind die Unternehmen danach an die geltenden Vorschriften gebunden. Die wichtigsten Grundsätze einer solchen Vereinbarung sind:

a) Transparenz der Datenschutzbestimmungen der beteiligten Unternehmen,

b) Übernahme der Safe-Harbor-Grundsätze in die Datenschutzbestimmungen der Unternehmen und

c) Durchsetzung der Grundsätze, einschließlich durch staatliche Instanzen.

Diese Grundlage des Safe Harbor muss angesichts folgender **neuer Umstände** überprüft werden:

a) Der Datenverkehr, der das rasche Wachstum der digitalen Wirtschaft früher nur peripher beeinflusst hat, nun aber eine zentrale Rolle spielt, hat exponentiell zugenommen. Darüber hinaus hat sich die Datenerhebung, -verarbeitung und -nutzung signifikant weiterentwickelt.

b) Datentransfers sind, insbesondere für die transatlantische Wirtschaft, von größter Bedeutung.[6]

c) Die Zahl der Unternehmen in den USA, die sich an der Safe-Harbor-Regelung beteiligen, ist rasant gewachsen und hat sich seit 2004 verachtfacht (von 400 im Jahr 2004 auf 3246 im Jahr 2013).

d) Die kürzlich bekannt gewordenen Informationen zu den Überwachungsprogrammen der USA werfen neue Fragen über das Schutzniveau auf, das mit der Safe-Harbor-Vereinbarung gewährleistet werden soll.

Diese neue Sachlage ist Anlass für eine Bestandsaufnahme der Safe-Harbor-Regelung auf der Grundlage der von der Kommission zusammengetragenen **Fakten**, der Arbeit der „EU-US Privacy Contact Group" aus dem Jahr 2009, der Studie eines unabhängigen Auftragnehmers aus dem Jahr 2008[7] sowie der Informationen der Ad-hoc-Arbeitsgruppe EU-USA („Arbeitsgruppe"), die infolge der Enthüllungen über die US-Überwachungsprogramme eingerichtet wurde *(siehe parallel erstelltes Dokument)*. Die vorliegende Mitteilung stützt sich auf zwei **Bewertungsberichte der Kommission**, die in der Anfangsphase der Safe-Harbor-Vereinbarung in den Jahren 2002[8] bzw. 2004[9] erstellt wurden.

2. AUFBAU UND FUNKTIONSWEISE DER SAFE-HARBOR-REGELUNG

2.1. Aufbau der Safe-Harbor-Regelung

Ein US-amerikanisches Unternehmen, das dem Safe Harbor beitreten möchte, muss a) in seinen öffentlich zugänglichen Datenschutzbestimmungen angeben, dass es die Safe-Harbor-

6 Studien zufolge würden sich die Aussetzung von verbindlichen unternehmensinternen Vorschriften, Mustervertragsklauseln und der Safe-Harbor-Regelung sowie die daraus folgende Unterbrechung grenzüberschreitender Daten- und Dienstleistungsströme negativ auf das BIP der EU auswirken (-0,8 % bis -1,3 %); ferner würden die EU-Dienstleistungsexporte in die USA aufgrund der eingebüßten Wettbewerbsfähigkeit um 6,7 % sinken. Siehe: „The Economic Importance of Getting Data Protection Right" – eine Studie des European Centre for International Political Economy für die US-Handelskammer, März 2013.

7 Folgenabschätzung des *Centre de Recherche Informatique et Droit* (CRID) der Universität Namur im Auftrag der Europäischen Kommission, 2008.

8 Arbeitsdokument der Kommissionsdienststellen „über die Umsetzung der Entscheidung 520/2000/EG der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des „sicheren Hafens" und der diesbezüglichen „Häufig gestellten Fragen" (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA", SEK(2002) 196 vom 13.12.2002.

9 Arbeitsdokument der Kommissionsdienststellen „The implementation of Commission Decision 520/2000/EC on the adequate protection of personal data provided by the Safe Harbour Privacy Principles and related FAQs issued by the US Department of Commerce", SEC(2004) 1323 vom 20.10.2004.

Grundsätze anerkennt und diese tatsächlich einhält, und b) sich einer Selbstzertifizierung unterziehen, d. h. dem US-Handelsministerium gegenüber erklären, dass es nach diesen Grundsätzen handelt. Die Selbstzertifizierung ist jedes Jahr erneut zu übermitteln. Die Grundsätze in Anhang I der Safe-Harbor-Entscheidung umfassen Bestimmungen über den umfassenden Schutz sowohl der personenbezogenen Daten (Datenintegrität, Sicherheit, Wahlmöglichkeit und Weitergabe) als auch der Verfahrensrechte der betroffenen Personen (Informationspflicht, Auskunftsrecht und Durchsetzung).

Für die Durchsetzung der Regelung in den USA sind in erster Linie zwei US-Behörden – das US-Handelsministerium und die Federal Trade Commission – zuständig.

Das **US-Handelsministerium** überprüft alle Safe-Harbor-Selbstzertifizierungen sowie alle von den Unternehmen jährlich übermittelten Rezertifizierungen, um sicherzustellen, dass alle zu beachtenden Aspekte enthalten sind.[10] Das Ministerium aktualisiert die Liste der Unternehmen, die ihre Selbstzertifizierung gemeldet haben, und veröffentlicht diese Liste sowie die entsprechenden Schreiben auf seiner Website. Darüber hinaus überwacht es die Einhaltung der Regelung und löscht diejenigen Unternehmen aus der Liste, die die Grundsätze nicht beachten.

Im Rahmen ihrer Befugnisse im Bereich des Verbraucherschutzes geht die **Federal Trade Commission** (FTC) gemäß Section 5 des Free Trade Commission Act gegen unfaire oder irreführende Praktiken vor. Dazu führt die FTC Untersuchungen durch, wenn Unternehmen fälschlicherweise angegeben haben, dass sie sich am Safe Harbor beteiligen, oder wenn die beteiligten Unternehmen die Grundsätze nicht beachten. Handelt es sich um Luftfahrtunternehmen, so ist das US-Verkehrsministerium für die Durchsetzung zuständig.[11]

Die Safe-Harbor-Entscheidung ist Teil des EU-Rechts und somit von den Behörden der Mitgliedstaaten anzuwenden. Gemäß der Entscheidung haben die nationalen **Datenschutzbehörden** der EU das Recht, in bestimmten Fällen die Datenübermittlung an Unternehmen, die den Safe-Harbor-Grundsätzen beigetreten sind, auszusetzen.[12] Der Kommission ist jedoch kein Fall bekannt, in dem eine nationale Datenschutzbehörde seit Inkrafttreten der Safe-Harbor-Regelung im Jahr 2000 die Datenübermittlung ausgesetzt hat. Unabhängig von ihren Befugnissen im Rahmen der Safe-Harbor-Entscheidung können die nationalen Datenschutzbehörden tätig werden, um – auch im Falle internationaler Datentransfers – die Einhaltung der in der Datenschutzrichtlinie von 1995 festgelegten allgemeinen Datenschutzgrundsätze sicherzustellen.

Wie in der Safe-Harbor-Entscheidung ausgeführt, **ist die Kommission befugt –** im Einklang mit dem Prüfverfahren gemäß der Verordnung (EU) Nr. 182/2011 – die Entscheidung anhand der Erfahrungen mit ihrer Anwendung jederzeit anzupassen, auszusetzen oder ihren Anwendungsbereich zu beschränken. Dies gilt insbesondere im Falle eines systemimmanenten Mangels seitens der USA, z. B. wenn eine Stelle, die die Einhaltung der Safe-Harbor-Grundsätze in den USA gewährleisten soll, dieser Pflicht nicht ordnungsgemäß nachkommt, oder wenn die Safe-Harbor-Grundsätze durch Rechtsvorschriften der USA

---

10 Trägt die Selbst- oder Rezertifizierung eines Unternehmens nicht den Safe-Harbor-Grundsätzen Rechnung, so teilt das Handelsministerium dem Unternehmen die für die Zertifizierung erforderlichen Maßnahmen mit (z. B. Klarstellungen, Überarbeitung der Datenschutzbestimmungen).

11 Gemäß Titel 49 United States Code, Section 41712.

12 In zwei Fällen kann es erforderlich sein, die Datenübermittlung auszusetzen:
a) wenn die staatliche Einrichtung in den USA feststellt, dass das betreffende Unternehmen die Safe-Harbor-Grundsätze verletzt oder
b) wenn eine hohe Wahrscheinlichkeit besteht, dass die Grundsätze verletzt werden; wenn Grund zu der Annahme besteht, dass die jeweilige Durchsetzungsinstanz nicht rechtzeitig angemessene Maßnahmen ergreift bzw. ergreifen wird, um den Fall zu lösen; wenn die fortgesetzte Datenübermittlung für die betroffenen Personen das unmittelbar bevorstehende Risiko eines schweren Schadens schaffen würde, und wenn die zuständigen Behörden in den Mitgliedstaaten die Organisation unter den gegebenen Umständen in angemessener Weise unterrichtet und ihr Gelegenheit zu Stellungnahme gegeben haben.

verdrängt werden. Wie jede andere Entscheidung der Kommission kann sie jedoch auch aus anderen Gründen geändert oder sogar aufgehoben werden.

2.2. Funktionsweise der Safe-Harbor-Regelung

Zu den **3246**[13] **zertifizierten Unternehmen** zählen sowohl kleine als auch große Unternehmen.[14] Die Durchsetzungsbefugnisse der Federal Trade Commission erstrecken sich nicht auf den Finanzdienstleistungs- und Telekommunikationssektor, der von der Safe-Harbor-Regelung ausgenommen ist. Viele der zertifizierten Unternehmen gehören dem Industrie- und Dienstleistungssektor an, beispielsweise bekannte Internetfirmen sowie Unternehmen aus den Bereichen Informations- und Computerdienste, Reise- und Tourismusdienstleistungen, Gesundheits- oder Kreditkartendienstleistungen sowie Pharmaunternehmen.[15] Hierbei handelt es sich hauptsächlich um US-Unternehmen, die im EU-Binnenmarkt ihre Dienste anbieten. Teilweise handelt es sich auch um Niederlassungen von EU-Unternehmen wie Nokia oder Bayer. 51 % dieser Unternehmen verarbeiten Daten von Mitarbeitern in Europa, die zu personaltechnischen Zwecken in die USA übermittelt werden.[16]

Einige Datenschutzbehörden in der EU zeigen sich **zunehmend besorgt** über Datentransfers im Rahmen der geltenden Safe-Harbor-Regelung. Einige von ihnen kritisieren, dass die Grundsätze sehr allgemein formuliert sind und sowohl Selbstregulierung als auch Selbstzertifizierung kaum hinterfragt werden. Ähnliche Bedenken wurden seitens der Industrie geäußert, der zufolge die mangelnde Durchsetzungspolitik zu Wettbewerbsverzerrungen führt.

Die Safe-Harbor-Regelung basiert auf dem Prinzip der Freiwilligkeit, der Selbstzertifizierung der beteiligten Unternehmen und der Durchsetzung der mit der Selbstzertifizierung eingegangenen Verpflichtung durch staatliche Instanzen. Sowohl mangelnde Transparenz als auch eine unzureichende Durchsetzung untergraben die Safe-Harbor-Regelung.

Ist seitens der USA keine ausreichende Transparenz oder Durchsetzung gewährleistet, liegt die Verantwortung bei den europäischen Datenschutzbehörden sowie bei den an der Safe-Harbor-Regelung beteiligten Unternehmen. Am 29. April 2010 erließen die deutschen Aufsichtsbehörden für den Datenschutz einen Beschluss, wonach sich Unternehmen, die Daten von Europa in die USA übermitteln, vergewissern müssen, dass Unternehmen in den USA, die Daten importieren, die Safe-Harbor-Datenschutzgrundsätze beachten. Weiterhin heißt es in der Erklärung: „Mindestens muss das exportierende Unternehmen klären, ob die Safe Harbor-Zertifizierung des Importeurs noch gültig ist.“[17]

---

13 Am 26. September 2013 waren auf der Liste der Safe-Harbor-Unternehmen **3246** Unternehmen mit Zertifizierungsstatus **„current“** („aktuell“) und **935** mit Zertifizierungsstatus **„not current“** („nicht aktuell“) geführt.

14 Safe-Harbor-Unternehmen mit bis zu 250 Mitarbeitern: 60 % (1925 von 3246). Safe-Harbor-Unternehmen mit mindestens 251 Mitarbeitern: **40 %** (1295 von 3246).

15 Das Unternehmen MasterCard, das mit Tausenden Banken arbeitet, ist ein klares Beispiel dafür, dass die Safe-Harbor-Regelung nicht durch andere Rechtsinstrumente für die Übermittlung personenbezogener Daten ersetzt werden darf (z. B. durch verbindliche unternehmensinterne Vorschriften oder vertragliche Vereinbarungen).

16 Safe-Harbor-Unternehmen, deren Safe-Harbor-Zertifizierung sich auf Personaldaten erstreckt (und die somit erklärt haben, dass sie mit den EU-Datenschutzbehörden zusammenarbeiten werden und deren Auflagen erfüllen): **51 %** (1671 von 3246).

17 Siehe Beschluss des Düsseldorfer Kreises vom 28./29. April 2010. Siehe: Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 28./29. April 2010 in Hannover: http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/290410_SafeHarbor.pdf?__blob=publicationFile Der Europäische Datenschutzbeauftragte (EDSB) Peter Hustinx jedoch erklärte am 7. Oktober 2013 vor dem LIBE-Ausschuss des Europäischen Parlaments: „Wir glauben, dass [bei Safe Harbor] wesentliche Verbesserungen erreicht worden und die meisten Probleme nunmehr gelöst sind.“ https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2013/13-10-07_Speech_LIBE_PH_DE.pdf

Nach den Enthüllungen über die US-Überwachungsprogramme gingen die deutschen Datenschutzbehörden einen Schritt weiter und äußerten am 24. Juli 2013 Bedenken, dass „die Grundsätze in den Kommissionsentscheidungen [...] mit hoher Wahrscheinlichkeit verletzt" sind.[18] Einige Datenschutzbehörden (z. B. die Datenschutzbehörde Bremen) haben von bestimmten Unternehmen, die personenbezogene Daten an US-Anbieter übermitteln, Auskunft darüber verlangt, ob und wie der betreffende Anbieter einen Zugriff der Security Agency (NSA) auf die Daten verhindert. Die irische Datenschutzbehörde hat mitgeteilt, dass sie nach der Berichterstattung über die Überwachungsprogramme der US-Nachrichtendienste kürzlich zwei Beschwerden erhalten hat, bei denen es um das Safe-Harbor-Programm ging. Es habe diese jedoch nicht untersucht, da bei der Übermittlung personenbezogener Daten an das betreffende Drittland die irischen Datenschutzvorschriften eingehalten worden seien. Im Zuge einer ähnlichen Beschwerde hat die luxemburgische Datenschutzbehörde festgestellt, dass Microsoft und Skype bei der Übermittlung von Daten in die USA das Luxemburger Datenschutzgesetz eingehalten haben.[19] Allerdings hat der irische High Court einem Antrag auf gerichtliche Überprüfung stattgegeben, um festzustellen, weshalb der irische Datenschutzbeauftragte in Bezug auf die US-Überwachungsprogramme nicht tätig geworden ist. Eine der beiden Beschwerden wurde von der studentischen Vereinigung „Europe v Facebook (EvF)" eingereicht, die derzeit bei den zuständigen Datenschutzbehörden auch eine ähnliche Beschwerde gegen Yahoo Deutschland laufen hat.

Die unterschiedlichen Reaktionen der Datenschutzbehörden auf die Enthüllungen der Überwachungsprogramme zeigen einerseits, dass die Safe-Harbor-Regelung auseinanderzubrechen droht, und werfen andererseits die Frage auf, inwieweit die Regelung durchgesetzt wird.

3. TRANSPARENZ DER DATENSCHUTZBESTIMMUNGEN DER BETEILIGTEN UNTERNEHMEN

Gemäß FAQ 6 im Anhang II der Safe-Harbor-Entscheidung müssen Unternehmen, die an einer Safe-Harbor-Zertifizierung interessiert sind, dem US-Handelsministerium ihre Geschäftsbedingungen zum Datenschutz mitteilen und diese parallel dazu veröffentlichen. Diese Geschäftsbedingungen müssen eine Verpflichtungserklärung zur Einhaltung der Datenschutzgrundsätze enthalten. Die **Veröffentlichungspflicht, der sowohl die Datenschutzbestimmungen** der selbstzertifizierten Unternehmen als auch die Selbstverpflichtungserklärungen unterliegen, ist eine für das Funktionieren der Regelung grundlegende Voraussetzung.

Ein unzureichender Zugang zu den Datenschutzbestimmungen der Unternehmen geht zu Lasten der Privatpersonen, deren Daten erfasst und verarbeitet werden, und stellt möglicherweise eine **Verletzung des Grundsatzes der Informationspflicht** dar. Oftmals kennen die Betroffenen, deren Daten aus der EU übermittelt werden, weder ihre Rechte noch die Pflichten der selbstzertifizierten Unternehmen.

Die Selbstverpflichtungserklärung eines Unternehmens ist für die **Federal Trade Commission die Grundlage, auf der sie ihre Durchsetzungsbefugnisse wahrnehmen** kann, wenn ein Unternehmen aufgrund unfairer oder irreführender Praktiken gegen diese Grundsätze verstößt. Mangelnde Transparenz seitens der Unternehmen in den USA erschwert

[18] Siehe die Pressemitteilung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder mit dem Titel „Geheimdienste gefährden massiv den Datenverkehr zwischen Deutschland und außereuropäischen Staaten": http://www.bfdi.bund.de/EN/Home/homepage_Kurzmeldungen/PMDSK_SafeHarbor.html?nn=408870.

[19] Siehe die Pressemitteilung der Luxemburger Datenschutzbehörde vom 18. November 2013.

jedoch die Überwachung durch die Federal Trade Commission und beeinträchtigt die Wirksamkeit ihrer Durchsetzungsmaßnahmen.

In den vergangenen Jahren kam es häufig vor, dass selbstzertifizierte Unternehmen ihre Datenschutzbestimmungen nicht veröffentlicht und/oder keine öffentliche Erklärung zur Einhaltung der Datenschutzgrundsätze abgegeben haben. Im Safe-Harbor-Bericht aus dem Jahr 2004 wird daher gefordert, das US-Handelsministerium solle **aktiver prüfen, ob diese Auflage erfüllt ist**.

Seit 2004 hat das US-Handelsministerium neue **Informationsinstrumente** entwickelt, um die Unternehmen dabei zu unterstützen, ihren Transparenzverpflichtungen nachzukommen. Relevante Informationen zur Safe-Harbor-Regelung sind auf der einschlägigen Website[20] des Handelsministeriums abrufbar, auf der die Unternehmen auch ihre Datenschutzbestimmungen hochladen können. Dem Handelsministerium zufolge nutzen die Unternehmen diese Funktion und stellen auf der Website des Ministeriums ihre Datenschutzbestimmungen online, wenn sie ihren Beitritt zur Safe-Harbor-Regelung beantragen.[21] Darüber hinaus hat das Handelsministerium in den Jahren 2009-2013 eine Reihe von Leitfäden für Unternehmen veröffentlicht, die dem Safe Harbor beitreten möchten, (z. B. „Guide to Self-Certification" und „Helpful Hints on Self-Certifying Compliance").[22]

Die Transparenzanforderungen werden von den Unternehmen in unterschiedlichem Maße eingehalten. So übermitteln einige Unternehmen dem Handelsministerium im Rahmen ihrer Selbstzertifizierung lediglich eine Beschreibung ihrer Datenschutzbestimmungen, die meisten aber veröffentlichen diese Bestimmungen auf ihrer Website sowie auf der Website des Handelsministeriums. Jedoch sind diese **Bestimmungen nicht immer nutzerfreundlich dargestellt und einfach zu lesen.** Die Links zu den Datenschutzbestimmungen funktionieren nicht immer oder verweisen teils auf falsche Websites.

Gemäß der Entscheidung und ihren Anhängen **umfasst** die Verpflichtung der Unternehmen, ihre Datenschutzbestimmungen zu veröffentlichen, **mehr als die alleinige Mitteilung** der Selbstzertifizierung beim US-Handelsministerium. Gemäß den FAQ sind im Rahmen der Zertifizierung eine Beschreibung der Geschäftsbedingungen für den Datenschutz zu liefern, sowie klare Angaben darüber, wo genau diese Informationen für die Öffentlichkeit zugänglich sind.[23] Hinweise über den Schutz personenbezogener Daten müssen klar verständlich und für die Öffentlichkeit leicht zugänglich sein. Sie müssen einen Link zur Safe-Harbor-Website des US-Handelsministeriums enthalten, auf der alle „aktuellen" Teilnehmer an der Regelung verzeichnet sind, sowie einen Link zur alternativen Streitbeilegung (ADR). In den Jahren 2000-2013 ist eine Reihe der zertifizierten Unternehmen dieser Verpflichtung jedoch nicht nachgekommen. Im Februar 2013 hat das US-Handelsministerium im Rahmen des fachlichen Austauschs mit der Kommission eingeräumt, dass bis zu 10 % der zertifizierten Unternehmen möglicherweise keine Datenschutzbestimmungen und die damit verbundene Verpflichtungserklärung zur Einhaltung der Safe-Harbor-Grundsätze auf ihren Websites veröffentlicht haben.

Jüngsten Statistiken zufolge besteht auch weiterhin das Problem **falscher Angaben zur Safe-Harbor-Teilnahme**. Rund 10 % der Unternehmen, die sich als Safe-Harbor-Teilnehmer

---

20 http://www.export.gov/SafeHarbour/

21 https://SafeHarbour.export.gov/list.aspx

22 Der Leitfaden ist auf der Website des Safe-Harbor-Programms abrufbar: http://export.gov/SafeHarbour/ Nützliche Hinweise: http://export.gov/SafeHarbour/eu/eg_main_018495.asp.

23 Am 12. November 2013 hat das Handelsministerium bestätigt, dass Unternehmen, die öffentliche Websites haben und Verbraucher-/Kunden-/Besucherdaten erfassen, auf ihren jeweiligen Websites Datenschutzbestimmungen veröffentlichen müssen, die den Safe-Harbor-Grundsätzen Rechnung tragen (Dokument: „U.S.-EU Cooperation to Implement the Safe Harbor Framework" vom 12. November 2013).

ausgeben, sind vom Handelsministerium nicht als aktuelle Teilnehmer gelistet.[24] Solche falschen Angaben stammen einerseits von Unternehmen, die noch nie an der Safe-Harbor-Regelung beteiligt waren, andererseits aber auch von teilnehmenden Unternehmen, die dem Handelsministerium ihre jährliche Rezertifizierung nicht übermittelt haben. Letztere Unternehmen werden weiterhin auf der Safe-Harbor-Website gelistet, jedoch mit dem Zertifizierungsstatus „not current“ („nicht aktuell“). Dies bedeutet, dass es sich um frühere Teilnehmer handelt, die aber noch verpflichtet sind, den Schutz der bereits verarbeiteten Daten zu gewährleisten. Im Falle betrügerischer Praktiken oder bei einem Verstoß gegen die Safe-Harbor-Grundsätze kann die Federal Trade Commission tätig werden (siehe Abschnitt 5.1). Fest steht in jedem Fall, dass Unklarheiten in Bezug auf die bestehenden „Falschangaben“ die Glaubwürdigkeit der Regelung beeinträchtigen.

In den Jahren 2012 und 2013 wies die Europäische Kommission das US-Handelsministerium im Rahmen ihrer regelmäßigen Kontakte darauf hin, dass es nicht ausreicht, wenn die Unternehmen dem Handelsministerium lediglich eine Beschreibung ihrer Datenschutzbestimmungen übermitteln, um so den Transparenzanforderungen nachzukommen. Wichtig ist, dass die Datenschutzbestimmungen öffentlich zugänglich gemacht werden. Ferner wurde das Handelsministerium aufgefordert, **seine periodische Kontrolle der Unternehmenswebsites zu verstärken**, die nach dem Überprüfungsverfahren im Rahmen der ersten Selbstzertifizierung oder der jährlichen Rezertifizierung stattfindet. Auch wurde das Ministerium ersucht, Maßnahmen gegen diejenigen Unternehmen zu ergreifen, die gegen die Transparenzanforderungen verstoßen.

In einem ersten Schritt **hat das US-Handelsministerium daraufhin** Safe-Harbor-Unternehmen, die über eine öffentliche Website verfügen, **seit März 2013 zur Auflage gemacht**, ihre Bestimmungen zum Schutz von Kunden-/Nutzerdaten auf ihrer Unternehmenswebsite zu veröffentlichen. Parallel dazu begann das Handelsministerium, alle Unternehmen zu kontaktieren, deren Datenschutzbestimmungen nicht bereits einen Link zur Safe-Harbor-Website des Handelsministeriums enthielten. Sie wurden aufgefordert, ihre Unternehmenswebsite direkt mit der offiziellen Safe-Harbor-Liste und -Website zu verlinken und so den Verbrauchern zugänglich zu machen. So können die betroffenen Personen in Europa ohne zusätzlichen Suchaufwand sofort die Verpflichtungserklärung einsehen, die das jeweilige Unternehmen dem Handelsministerium übermittelt hat. Darüber hinaus begann das Handelsministerium, die Unternehmen darauf hinzuweisen, dass in den veröffentlichten Datenschutzbestimmungen auch die zuständige Stelle für die alternative Streitbeilegung (ADR-Stelle) anzugeben sei.[25]

Dieses Verfahren muss beschleunigt werden, damit sichergestellt ist, dass alle zertifizierten Unternehmen die Safe-Harbor-Auflagen bis März 2014 vollständig erfüllen (d. h. bis zum Ablauf der Frist für die jährliche Rezertifizierung der Unternehmen, gerechnet ab dem Zeitpunkt der Einführung der neuen Auflagen im März 2013).

Dennoch bestehen nach wie vor Zweifel, ob alle selbstzertifizierten Unternehmen die Transparenzanforderungen umfassend erfüllen. Das US-Handelsministerium sollte daher die

---

[24] Im September 2013 verglich das australische Beratungsunternehmen Galexia die „Falschbehauptungen“ über die Safe-Harbor-Teilnahme in den Jahren 2008 und 2013. Dabei wurde festgestellt, dass parallel zu den wachsenden Mitgliederzahlen im Zeitraum 2008 bis 2013 (von 1109 auf 3246) auch die Zahl der Falschangaben stieg (von 206 auf 427): http://www.galexia.com/public/about/news/about_news-id225.html.

[25] Zwischen März und September 2013 hat das US-Handelsministerium
• 101 Unternehmen, *die ihre Safe-Harbor-konformen Datenschutzbestimmungen auf die Safe-Harbor-Website hochgeladen hatten,* aufgefordert, ihre Datenschutzbestimmungen auch auf ihrer Unternehmenswebsite zu veröffentlichen;
• 154 Unternehmen aufgefordert, in ihren Datenschutzbestimmungen einen Link zur Safe-Harbor-Website vorzusehen;
• mehr als 600 Unternehmen aufgefordert, in ihren Datenschutzbestimmungen eine Stelle für die alternative Streitbeilegung anzugeben.

Einhaltung der mit der ersten Selbstzertifizierung eingegangenen Verpflichtungen sowie die jährlichen Rezertifizierungen strenger prüfen und überwachen.

4. ÜBERNAHME DER SAFE-HARBOR-GRUNDSÄTZE IN DIE DATENSCHUTZBESTIMMUNGEN DER UNTERNEHMEN

Selbstzertifizierte Unternehmen müssen die Datenschutzgrundsätze in Anhang I der Entscheidung einhalten, um die Vorteile des Safe Harbor erhalten und behalten zu können.

In ihrem Bericht von 2004 stellte die Kommission fest, dass zahlreiche **Unternehmen die Safe-Harbor-Grundsätze nicht korrekt** in ihre Datenverarbeitungsvorschriften **übernommen hatten**. So wurden die betroffenen Personen nicht immer klar darüber informiert, für welche Zwecke ihre Daten verarbeitet wurden, oder ihnen wurde nicht die Möglichkeit gegeben, zu wählen, ob ihre Daten an Dritte weitergegeben oder für einen mit dem ursprünglichen Erhebungszweck nicht zu vereinbarenden Zweck verwendet werden dürfen. In ihrem Bericht von 2004 stellte die Kommission fest, das US-Handelsministerium solle sich aktiver für die Teilnahme an der Safe-Harbor-Regelung und die Verbreitung der Grundsätze einsetzen.[26]

Diesbezüglich gab es nur begrenzte Fortschritte. Seit dem 1. Januar 2009 müssen alle Unternehmen dem US-Handelsministerium im Rahmen ihrer jährlichen Safe-Harbor-Rezertifizierung ihre Datenschutzbestimmung vorab zu einer – vom Umfang her allerdings begrenzten – Bewertung vorlegen. Es gibt keine **vollständige Bewertung der tatsächlichen Praxis** der selbstzertifizierten Unternehmen, die die Glaubwürdigkeit des Selbstzertifizierungsverfahrens deutlich steigern würde.

Auf die Bitte der Kommission hin, das US-Handelsministerium möge die selbstzertifizierten Unternehmen strikter und systematischer überwachen, **wird neuen Anträgen nun mehr Aufmerksamkeit gewidmet.** Die Anzahl der Anträge, die nicht angenommen, sondern den Unternehmen mit der Bitte um Nachbesserung der Datenschutzbestimmungen zurückgesandt wurden, ist von 2010 bis 2013 deutlich gestiegen: Bei Rezertifizierungen hat sich die Anzahl verdoppelt, bei Neuanträgen verdreifacht.[27] Das US-Handelsministerium hat der Kommission versichert, dass Zertifizierungen bzw. Rezertifizierungen erst dann abgeschlossen werden, wenn die Datenschutzbestimmungen des betreffenden Unternehmens allen Anforderungen genügen, d. h. wenn eine Erklärung vorliegt, dass die relevanten Safe-Harbor-Grundsätze beachtet werden und die Datenschutzbestimmungen öffentlich zugänglich sind. Jedes Unternehmen muss in seinem Eintrag auf der Safe-Harbor-Liste angeben, wo genau die einschlägigen Bestimmungen zu finden sind. Ferner muss das Unternehmen auf seiner Website eine Stelle für die alternative Streitbeilegung angeben und auf der Website des Handelsministeriums einen Link zur Safe-Harbor-Selbstzertifizierung veröffentlichen. Schätzungen zufolge geben jedoch mehr als 30 % der Safe-Harbor-Teilnehmer in den Datenschutzbestimmungen auf ihren Websites keine ADR-Stelle an.[28]

Bei den meisten Einträgen, die vom US-Handelsministerium von der Safe-Harbor-Liste entfernt wurden, geschah dies auf ausdrücklichen Wunsch der betreffenden Unternehmen (z. B. bei Unternehmenszusammenschlüssen oder -übernahmen bzw. bei Unternehmen, die

---

26 Siehe S. 8 des Berichts von 2004, SEC(2004) 1323.

27 Den im September 2013 vom US-Handelsministerium vorgelegten Statistiken zufolge wurden im Jahr 2010 18 % (93) der 512 Erstanträge auf Zertifizierung und 16 % (231) der 1417 Rezertifizierungsanträge geprüft und die Unternehmen aufgefordert, ihre Datenschutzbestimmungen und/oder Safe-Harbor-Anträge nachzubessern. Auf Ersuchen der Kommission, alle Anträge streng, sorgfältig und systematisch zu prüfen, wurden bis Mitte September 2013 56 % (340) der 602 Erstanträge auf Zertifizierung und 27 % (493) der 1809 Rezertifizierungsanträge geprüft und die betreffenden Unternehmen aufgefordert, ihre Datenschutzbestimmungen nachzubessern.

28 Vortrag von Chris Connolly (Galexia) vor dem LIBE-Ausschuss des Europäischen Parlaments am 7. Oktober 2013.

ihr Geschäft neu ausgerichtet oder ihre Geschäftstätigkeit eingestellt haben). Eine geringere Anzahl von Einträgen wurde gelöscht, weil die Website und auch das zugehörige Unternehmen nicht mehr existierten bzw. der Zertifizierungsstatus bereits mehrere Jahre mit „non current" angegeben war.[29] Jedoch wurde offenbar keine dieser Löschungen vom Handelsministerium wegen Nichteinhaltung der Datenschutzgrundsätze veranlasst.

Der Eintrag in die Safe-Harbor-Liste dient der öffentlichen Bekanntmachung und als Nachweis, dass das betreffende Unternehmen sich zur Einhaltung der Safe-Harbor-Grundsätze verpflichtet hat. **Die Verpflichtung zur Einhaltung der Safe-Harbor-Grundsätze ist** in Bezug auf die vom Unternehmen während seiner Teilnahme an der Safe-Harbor-Regelung erhaltenen Daten **zeitlich nicht befristet**. Für das Unternehmen gelten die Grundsätze so lange, wie es die Daten speichert, nutzt oder veröffentlicht, auch wenn es aus irgendeinem Grund aus der Safe-Harbor-Regelung austritt.

In einigen Fällen wurden **Safe-Harbor-Anträge** bei der administrativen Überprüfung des US-Handelsministeriums **abgelehnt** und die Antragsteller folglich nie in die Safe-Harbor-Liste aufgenommen: **2010** wurden nur **6%** (33) der 513 Unternehmen, die einen Antrag auf Erstzertifizierung gestellt hatten, nicht in die Safe-Harbor-Liste aufgenommen, weil sie den Selbstzertifizierungsstandards des Handelsministeriums nicht genügten. **2013** wurden **12%** (75) der 605 Unternehmen, die einen Antrag auf Erstzertifizierung gestellt hatten, aus diesem Grund nicht in die Safe-Harbor-Liste aufgenommen.

Um die Überwachung transparenter zu gestalten, sollte das US-Handelsministerium zumindest auf seiner Website alle Unternehmen aufführen, die aus der Safe-Harbor-Liste gestrichen wurden, und die Gründe angeben, weshalb die Zertifizierung nicht verlängert wurde. Der Vermerk „not current" („Zertifizierungsstatus nicht aktuell") auf der Liste der Safe-Harbor-Teilnehmer des US-Handelsministeriums sollte nicht nur informationshalber veröffentlicht werden, sondern durch einen **deutlichen** – graphischen und schriftlichen – **Warnhinweis** ergänzt werden, dass das betreffende Unternehmen die Safe-Harbor-Anforderungen derzeit nicht erfüllt.

Darüber hinaus haben einige Unternehmen die Safe-Harbor-Grundsätze noch immer nicht vollständig in ihre Datenschutzbestimmungen übernommen. Neben dem Problem der Transparenz (s. o. Abschnitt 3) geht aus den Datenschutzbestimmungen selbstzertifizierter Unternehmen oftmals nicht klar hervor, zu welchem Zweck Daten erhoben werden und ob die Betroffenen die Möglichkeit haben zu wählen, ob ihre personenbezogenen Daten an Dritte weitergegeben werden dürfen oder nicht. Dies wiederum stellt einen Konflikt mit den Datenschutzgrundsätzen der Informationspflicht und der Wahlmöglichkeit dar. Sowohl Informationspflicht als auch Wahlmöglichkeit sind aber eine grundlegende Voraussetzung dafür, dass Privatpersonen die Kontrolle darüber haben, was mit ihren personenbezogenen Informationen geschieht.

Der erste wichtige Schritt zur Gewährleistung der Konformität – die Übernahme der Safe-Harbor-Grundsätze in die Datenschutzbestimmungen der betreffenden Unternehmen – ist nicht ausreichend sichergestellt. Das US-Handelsministerium sollte dieses Problem vordringlich angehen und hinsichtlich der betrieblichen Praxis der Unternehmen und ihres Umgang mit den Kunden eine Methode zur Gewährleistung der Konformität entwickeln. **Wichtig ist hierbei, dass das US-Handelsministerium die Übernahme der Safe-Harbor-Grundsätze in die Datenschutzbestimmungen der Unternehmen aktiv überprüft** und nicht erst auf Beschwerden von Privatpersonen hin tätig wird.

[29] Das US-Handelsministerium hatte 323 Unternehmen aus der Safe-Harbor-Liste gelöscht (Stand: Dezember 2011): 94 Unternehmen, weil sie ihre Geschäftstätigkeit eingestellt hatten, 88 Unternehmen aufgrund von Zusammenschlüssen oder Übernahmen, 95 auf Antrag der Muttergesellschaft, 41 Unternehmen, weil mehrfach keine Rezertifizierung beantragt wurde, und 5 Unternehmen aus sonstigen Gründen.

5. DURCHSETZUNG DER SAFE-HARBOR-GRUNDSÄTZE VON STAATLICHER SEITE

Es stehen eine Reihe von Mechanismen zur Verfügung, um die effektive Anwendung der Safe-Harbor-Regelung durchzusetzen und Personen, deren Daten durch die Missachtung der Datenschutzgrundsätze nicht hinreichend geschützt wurden, Rechtsschutz zu bieten.

Dem Durchsetzungsgrundsatz zufolge müssen die Datenschutzbestimmungen selbstzertifizierter Organisationen wirksame Mechanismen vorsehen, um die Beachtung des Datenschutzes sicherzustellen. Wie in FAQ 11, FAQ 5 und FAQ 6 ausgeführt, kann diese Auflage dadurch erfüllt werden, dass sich diese Organisationen einer **unabhängigen Beschwerdestelle** anschließen, die sich öffentlich für zuständig erklärt hat, individuellen Beschwerden wegen Verstoßes gegen die Safe-Harbor-Grundsätze nachzugehen. Alternativ dazu können sich die Organisationen auch zur Zusammenarbeit mit dem **EU-Datenschutzgremium**[30] verpflichten. Selbstzertifizierte Unternehmen unterliegen zudem nach Section 5 des Federal Trade Commission Act, der unlautere und irreführende Praktiken verbietet, die im Handel erfolgen oder den Handel beeinträchtigen, der Zuständigkeit der Federal Trade Commission.[31]

Im Bericht von 2004 wurde die Durchsetzung der Safe-Harbor-Regelung kritisch beurteilt. Von der Federal Trade Commission wurde gefordert, sie solle Verstöße aktiver verfolgen und besser über Datenschutzrechte aufklären. Beanstandet wurde auch die Unsicherheit in Bezug auf die Befugnis der Federal Trade Commission zur Durchsetzung der Datenschutzgrundsätze bei Personaldaten.

Das EU-Datenschutzgremium, das als Beschwerdestelle für Personaldaten zuständig ist, hat eine diesbezügliche Beschwerde erhalten.[32] Der Umstand, dass es kaum Beschwerden gibt, lässt allerdings nicht den Schluss zu, dass die Regelung in jeder Hinsicht gut funktioniert. Es sollte von Amts wegen geprüft werden, ob die Unternehmen ihre Datenschutzverpflichtungen auch tatsächlich einhalten. Die EU-Datenschutzbehörden sollten ihrerseits tätig werden, um das Datenschutzgremium besser bekannt zu machen.

Es wurde auf Probleme im Zusammenhang mit der Art und Weise hingewiesen, wie Durchsetzungsbefugnisse von ADR-Stellen ausgeübt werden. Einige dieser Stellen verfügen nicht über geeignete Mittel, um Verstöße gegen die Safe-Harbor-Grundsätze abzustellen. Diese Mängel müssen behoben werden.

5.1 Federal Trade Commission

Die Federal Trade Commission kann bei Verstoß gegen die Safe-Harbor-Zusicherungen eines Unternehmens Durchsetzungsmaßnahmen ergreifen. Als die Safe-Harbor-Regelung eingeführt wurde, sagte die Federal Trade Commission zu, alle Fälle, die von den Behörden

30 Das EU-Datenschutzgremium prüft Beschwerden wegen mutmaßlicher Verletzung von Safe-Harbor-Grundsätzen durch ein an der Safe-Harbor-Regelung teilnehmendes US-Unternehmen. Unternehmen, die sich zur Einhaltung der Safe-Harbor-Grundsätze verpflichten, müssen sich entweder einer unabhängigen Beschwerdestelle anschließen oder mit dem EU-Datenschutzgremium zusammenarbeiten, damit Probleme, die sich aus der Missachtung von Safe-Harbor-Grundsätzen ergeben, ausgeräumt werden können. Verarbeitet ein US-Unternehmen allerdings Personaldaten, die im Rahmen eines Beschäftigungsverhältnisses aus der EU übermittelt werden, ist es in jedem Fall zur Zusammenarbeit mit dem EU-Datenschutzgremium verpflichtet. Verpflichtet sich das Unternehmen von sich aus, mit dem europäischen Datenschutzpanel zusammenzuarbeiten, muss es sich auch dazu verpflichten, den Empfehlungen des Gremiums zu folgen, wenn dieses der Ansicht ist, dass das Unternehmen besondere Maßnahmen (einschließlich in Bezug auf Abhilfen und Entschädigungsleistungen) treffen muss, um den Safe-Harbor-Grundsätzen zu entsprechen.

31 Das US-Verkehrsministerium übt nach Titel 49 Section 41712 des United States Code ähnliche Befugnisse in Bezug auf Luftverkehrsunternehmen aus.

32 Beschwert hatte sich ein schweizerischer Staatsbürger, weshalb das EU-Datenschutzgremium die Beschwerde an die Datenschutzbehörde der Schweiz weitergeleitet hatte (die USA haben mit der Schweiz eine separate Safe-Harbor-Regelung geschlossen).

der EU-Mitgliedstaaten an sie verwiesen werden, vorrangig zu überprüfen.[33] Da in den ersten zehn Jahren der Regelung keine Beschwerden eingingen, beschloss die Federal Trade Commission bei allen Ermittlungen, die sie im Bereich des Datenschutzes und der Datensicherheit durchführt, auch auf Verstöße gegen die Safe-Harbor-Grundsätze zu achten. Seit 2009 hat die Federal Trade Commission wegen Verstößen gegen die Safe-Harbor-Grundsätze 10 Durchsetzungsmaßnahmen gegen Unternehmen ergriffen. Infolge dieser Maßnahmen wurden hauptsächlich Vergleichsverfügungen (settlement orders) – mit erheblichen Geldbußen – erlassen, in denen falsche Datenschutzerklärungen verboten und den Unternehmen umfassende Datenschutzprogramme und -audits über einen Zeitraum von 20 Jahren aufgegeben wurden. Die Unternehmen müssen auf Verlangen der Federal Trade Commission unabhängige Bewertungen ihrer Datenschutzprogramme dulden. Diese Bewertungen werden der Federal Trade Commission regelmäßig gemeldet. Unternehmen ist es verboten, ihre Datenschutzpraktiken und ihre Teilnahme an der Safe-Harbor-Regelung oder vergleichbaren Datenschutzregelungen in einer Weise darzustellen, die nicht den Tatsachen entspricht. Beispiele hierfür sind die Ermittlungen der Federal Trade Commission gegen Google, Facebook und Myspace.[34] 2012 willigte Google in eine Geldbuße von 22,5 Mio. USD ein, um einen Streit beizulegen, bei dem Google vorgeworfen worden war, gegen eine mit seiner Zustimmung ergangene Verfügung (consent order) verstoßen zu haben. Die Federal Trade Commission prüft in allen den Datenschutz betreffenden Ermittlungen von Amts wegen, ob gegen Safe-Harbor-Grundsätze verstoßen wurde.

Die Federal Trade Commission hat unlängst ihre Erklärung und Verpflichtung erneut bekräftigt, Beschwerden wegen Verletzung der Safe-Harbor-Grundsätze, die Selbstregulierungsorgane für den Datenschutz und EU-Mitgliedstaaten an sie verweisen, vorrangig zu prüfen.[35] Die Federal Trade Commission hat in den letzten drei Jahren nur wenige Beschwerden der europäischen Datenschutzbehörden erhalten.

Die Zusammenarbeit zwischen Datenschutzbehörden diesseits und jenseits des Atlantiks wurde in den vergangenen Monaten weiter ausgebaut. So schloss die Federal Trade Commission mit dem irischen Datenschutzbeauftragten am 26. Juni 2013 eine Rechtshilfe-Vereinbarung zur Durchsetzung des rechtlichen Schutzes personenbezogener Informationen im privaten Sektor (Memorandum of Understanding on mutual assistance in the enforcement of laws protecting personal information in the private sector). Diese Vereinbarung stellt einen Rahmen für eine intensivere, straffere und effizientere Zusammenarbeit bei der Durchsetzung der Datenschutzbestimmungen bereit.[36]

Im August 2013 kündigte die Federal Trade Commission an, Unternehmen, die Zugriff auf große Datenbanken mit personenbezogenen Informationen haben, noch strenger zu

---

33 Siehe Anhang V der Kommissionsentscheidung 2000/520/EG vom 26. Juli 2000.

34 Zwischen 2009 und 2012 hat die Federal Trade Commission zehn Durchsetzungsmaßnahmen in Bezug auf Safe-Harbor-Verpflichtungen zum Abschluss gebracht: FTC gegen Javian Karnani und Balls of Kryptonite, LLC (2009), World Innovators, Inc. (2009), Expat Edge Partners, LLC (2009), Onyx Graphics, Inc. (2009), Directors Desk LLC (2009), Progressive Gaitways LLC (2009), Collectify LLC (2009), Google Inc. (2011), Facebook, Inc. (2011), Myspace LLC (2012). Vgl. „Federal Trade Commission of Safe Harbour Commitments“: http://export.gov/build/groups/public/@eg_main/@SafeHarbour/documents/webcontent/eg_main_052211.pdf. Vgl. auch „Case Highlights“: http://business.ftc.gov/us-eu-Safe-Harbour-framework. In den meisten Fällen ging es um Unternehmen, die sich der Safe-Harbor-Regelung angeschlossen, ihre jährliche Zertifizierung aber nicht erneuert hatten und sich trotzdem weiterhin als Teilnehmer der Regelung ausgaben.

35 Diese Verpflichtung wurde in einer Sitzung des Federal Trade Commission Commissioner Julie Brill mit den EU-Datenschutzbehörden (Artikel-29-Arbeitsgruppe) in Brüssel vom 17. April 2013 erneut bekräftigt.

36 http://www.dataprotection.ie/viewdoc.asp?Docid=1317&Catid=66&StartDate=1+January+2013&m=n

überprüfen. Sie richtete außerdem eine Website ein für Datenschutzbeschwerden von Verbrauchern gegen US-Unternehmen.[37]

Die Federal Trade Commission sollte darüber hinaus verstärkte Anstrengungen unternehmen, um Falschbehauptungen in Bezug auf die Teilnahme an der Safe-Harbor-Regelung nachzugehen. Ein Unternehmen, das auf seiner Website behauptet, die Safe-Harbor-Grundsätze einzuhalten, aber auf der Liste des US-Handelsministeriums nicht als „aktueller" („current") Teilnehmer der Regelung geführt wird, führt Verbraucher in die Irre und missbraucht ihr Vertrauen. Falschbehauptungen unterminieren die Glaubwürdigkeit der gesamten Regelung und sollten deshalb sofort von den Websites des Unternehmens entfernt werden. Den Unternehmen sollte eine durchsetzbare Verpflichtung auferlegt werden, die Verbraucher nicht zu täuschen. Die Federal Trade Commission sollte sich weiterhin darum bemühen, Falschbehauptungen in Bezug auf die Teilnahme an der Safe-Harbor-Regelung wie im Fall *Karnani* aufzudecken. In diesem Fall hatte die Federal Trade Commission eine Website in Kalifornien gesperrt, auf der fälschlicherweise die Teilnahme an der Safe-Harbor-Regelung behauptet wurde und von der aus auf europäische Verbraucher ausgerichtete betrügerische Internetgeschäfte getätigt wurden.[38]

Am 29. Oktober 2013 gab die Federal Trade Commission bekannt, dass sie in den letzten Monaten zahlreiche Ermittlungen zur Überprüfung der Einhaltung der Safe-Harbor-Grundsätze eingeleitet habe und dass in den kommenden Monaten weitere Durchsetzungsmaßnahmen zu erwarten seien. Die Federal Trade Commission bestätigte zudem, dass sie entschlossen nach Wegen suche, um effizienter vorzugehen, und weiterhin alle substanziellen Hinweise begrüße wie die Beschwerde, die sie vergangenen Monat von einem Verbraucheranwalt aus Europa erhalten habe, der zahlreiche Verstöße gegen die Safe-Harbor-Grundsätze geltend gemacht habe.[39] Die Behörde sagte auch zu, die Einhaltung der Safe-Harbor-Verfügungen in derselben Weise wie alle anderen Verfügungen systematisch zu überprüfen.[40]

Am 12. November 2013 teilte die Federal Trade Commission der Europäischen Kommission mit, dass **„das Versäumnis eines Unternehmens, sich der Safe-Harbor-Regelung anzuschließen oder seine Teilnahme aufrechtzuerhalten, nicht als solches geeignet ist, es von der Durchsetzung der Safe-Harbor-Verpflichtungen durch die FTC auszunehmen, wenn die Datenschutzbestimmungen des Unternehmens einen Schutz im Sinne der Safe-Harbor-Grundsätze versprechen."**[41]

Im November 2013 teilte das US-Handelsministerium der Europäischen Kommission mit, dass „das Ministerium Safe-Harbor-Teilnehmer künftig einen Monat vor Ablauf ihrer Zertifizierung kontaktieren wird, um ihnen zu erklären, was sie tun müssen, wenn sie sich gegen eine Rezertifizierung entscheiden. Auf diese Weise soll dafür gesorgt werden, dass Unternehmen keine falsche Erklärung bezüglich ihrer Teilnahme an der Safe-Harbor-Regelung abgeben". **Das US-Handelsministerium „wird Unternehmen, die auf eine Rezertifizierung verzichten, darauf hinweisen,** dass sie alle Bezugnahmen auf eine Safe-Harbor-Teilnahme, einschließlich des Safe-Harbor-Gütezeichens des Ministeriums, aus den Datenschutzbestimmungen des Unternehmens und seinen Webseiten entfernen müssen, **und**

---

37 Verbraucher können ihre Beschwerde gegen US-Unternehmen über den Federal Trade Commission Complaint Assistant (https://www.ftccomplaintassistant.gov/) bzw. gegen ausländische Firmen über econsumer.gov (http://www.econsumer.gov) erheben.

38 http://www.ftc.gov/os/caselist/0923081/090806karnanicmpt.pdf

39 http://www.ftc.gov/speeches/brill/131029europeaninstituteremarks.pdf und http://www.ftc.gov/speeches/ramirez/131029tacdremarks.pdf

40 Schreiben der Vorsitzenden der Federal Trade Commission Edith Ramirez an Vizepräsidentin Viviane Reding.

41 Schreiben der Vorsitzenden der Federal Trade Commission Edith Ramirez an Vizepräsidentin Viviane Reding.

sie unmissverständlich warnen, dass eine Missachtung seitens des Unternehmens Durchsetzungsmaßnahmen der FTC zur Folge haben kann“.[42]

Um Falschbehauptungen in Bezug auf die Teilnahme an der Safe-Harbor-Regelung entgegenzuwirken, sollten die Datenschutzbestimmungen auf der Website selbstzertifizierter Unternehmen stets mit der Safe-Harbor-Website des US-Handelsministeriums verlinkt sein, auf der alle „aktuellen“ („current“) Teilnehmer der Safe-Harbor-Regelung aufgeführt sind. Auf diese Weise können europäische Betroffene ohne zusätzlichen Suchaufwand sofort feststellen, ob ein bestimmtes Unternehmen der Safe-Harbor-Regelung derzeit angehört. Das US-Handelsministerium hat im März 2013 damit begonnen, die Unternehmen zu diesem Schritt aufzufordern. Die Bemühungen sollten jedoch verstärkt werden.

Die kontinuierliche Kontrolle und konsequente Durchsetzung der Safe-Harbor-Grundsätze durch die Federal Trade Commission – zusätzlich zu den vorgenannten Maßnahmen des US-Handelsministeriums – ist weiterhin ein zentrales Anliegen, um sicherzustellen, dass die Regelung effektiv funktioniert. Notwendig sind unter anderem häufigere **Kontrollen von Amts wegen und Nachprüfungen, ob die Unternehmen die Safe-Harbor-Grundsätze einhalten**. Die Einlegung von Beschwerden bei der Federal Trade Commission wegen Datenschutzverstößen sollte weiter erleichtert werden.

5.2 EU-Datenschutzgremium

Das EU-Datenschutzgremium wurde auf der Grundlage der Safe-Harbor-Entscheidung geschaffen. Es ist für die Prüfung individueller Beschwerden in Bezug auf Personaldaten zuständig sowie für Fälle, an denen zertifizierte Unternehmen beteiligt sind, die sich für diesen Weg der Streitbeilegung im Rahmen der Safe-Harbor-Regelung entschieden haben (53 % aller Unternehmen). Das Gremium setzt sich aus Vertreten der nationalen Datenschutzbehörden der EU zusammen.

Bislang wurde das Gremium mit vier Beschwerden befasst (zwei im Jahr 2010 und zwei im Jahr 2013). Die beiden Beschwerden aus dem Jahr 2010 wurden an die zuständigen nationalen Datenschutzbehörden verwiesen (UK und Schweiz). Die Prüfung der Beschwerden aus dem Jahr 2013 ist noch nicht abgeschlossen. Die geringe Zahl der Beschwerden lässt sich hauptsächlich damit erklären, dass die Befugnisse des Gremiums auf bestimmte Arten von Daten beschränkt sind.

Zum Teil liegt es aber auch daran, dass das Gremium zu wenig bekannt ist. Seit 2004 auf der Website der Kommission besser über dieses Gremium informiert.[43]

US-Unternehmen, die sich bei einem Teil der Datenkategorien oder bei allen Kategorien personenbezogener Daten, die Gegenstand ihrer Selbstzertifizierung sind, für die Zusammenarbeit mit diesem Gremium entschieden haben und seinen Entscheidungen nachkommen wollen, sollten dies klar und sichtbar in ihren Datenschutzverpflichtungen angeben, damit dieser Aspekt vom US-Handelsministerium überprüft und das Gremium stärker genutzt werden kann. Jede europäische Datenschutzbehörde sollte auf ihrer Website spezielle Seiten zur Safe-Harbor-Regelung einstellen, um europäische Unternehmen und Datensubjekte stärker auf diese Regelung aufmerksam zu machen.

---

42 „U.S.-EU Cooperation to Implement the Safe Harbor Framework“, 12. November 2013.

43 Nach dem Bericht von 2004 wurden auf der Website der Kommission (GD Justiz) Informationen über das EU-Datenschutzgremium in Form von Fragen und Antworten veröffentlicht. Auf diese Weise sollte das Gremium besser bekannt gemacht und Bürgern, die sich wegen eines Verstoßes gegen die Safe-Harbor-Grundsätze bei der Verarbeitung ihrer personenbezogenen Daten beschweren wollen, Hilfestellung gegeben werden: http://ec.europa.eu/justice/policies/privacy/docs/adequacy/information_Safe_harbour_en.pdf

Ein Beschwerdeformular ist erhältlich unter: http://ec.europa.eu/justice/policies/privacy/docs/adequacy/ complaint_form_en.pdf.

5.3 Bessere Durchsetzung

Die vorerwähnten Unzulänglichkeiten in puncto Transparenz und Durchsetzung geben unter europäischen Unternehmen wegen der negativen Auswirkungen der Safe-Harbor-Regelung auf die Wettbewerbsfähigkeit europäischer Unternehmen Anlass zu Besorgnis. Ein europäisches Unternehmen, das in Konkurrenz zu einem US-Unternehmen steht, das an der Safe-Harbor-Regelung teilnimmt, die Grundsätze aber in der Praxis nicht anwendet, hat gegenüber dem US-Unternehmen einen Wettbewerbsnachteil.

Die Zuständigkeit der Federal Trade Commission erstreckt sich auf unlautere und irreführende Praktiken, die im Handel erfolgen oder die den Handel beeinträchtigen. Gemäß Section 5 des Federal Trade Commission Act ist jedoch unter anderem der Bereich der **Telekommunikation** ausgenommen. Telekommunikationsunternehmen dürfen der Safe-Harbor-Regelung deshalb nicht beitreten. Aufgrund der zunehmenden Konvergenz der Technologien und Dienste gehören jedoch viele ihrer direkten Konkurrenten im IKT-Sektor der USA der Safe-Harbor-Regelung an. Der Ausschluss der Telekommunikationsunternehmen vom Datenaustausch auf der Grundlage der Safe-Harbor-Regelung ist für einige europäische Telekommunikationsbetreiber Grund zur Sorge. Dem Europäischen Verband der Telekommunikationsbetreiber (ETNO) zufolge steht dies eindeutig im Widerspruch zu dem wichtigsten Anliegen der Telekommunikationsbetreiber, die gleiche Wettbewerbsbedingungen fordern.[44]

6. STÄRKUNG DER SAFE-HARBOR-GRUNDSÄTZE

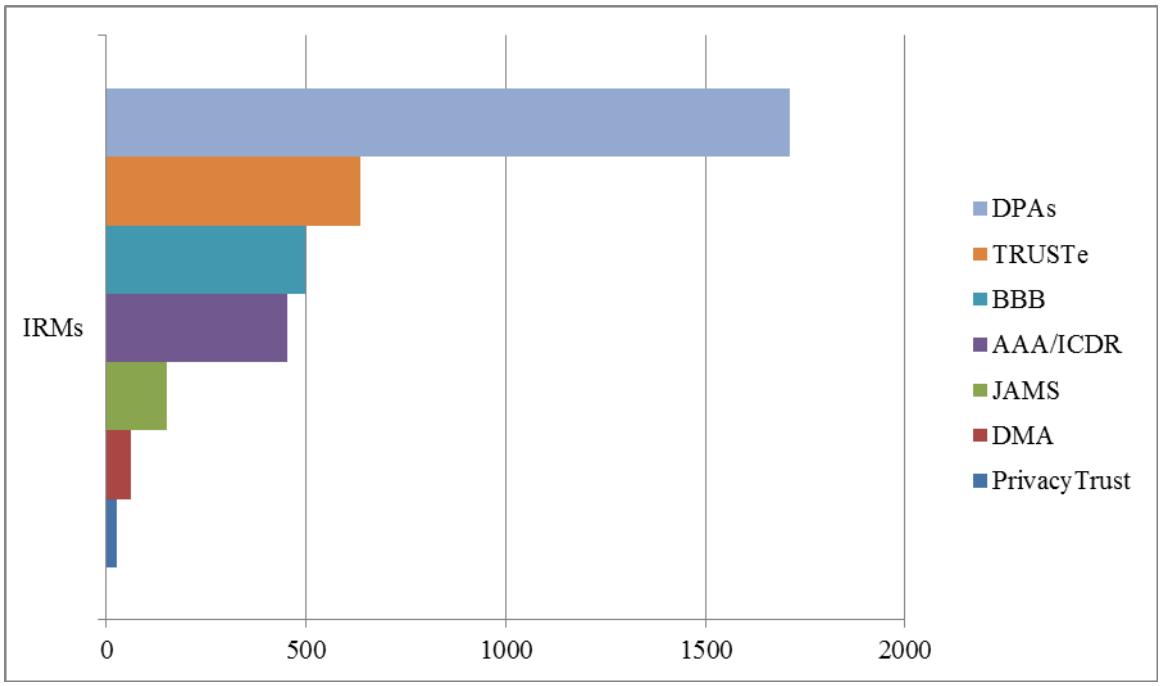
6.1 Alternative Streitbeilegung

Dem Durchsetzungsgrundsatz zufolge muss es **leicht zugängliche und erschwingliche Verfahren** geben, nach denen individuelle Beschwerden und Streitigkeiten behandelt werden. In der Safe-Harbor-Regelung ist zu diesem Zweck ein Verfahren zur alternativen Streitbeilegung (ADR) durch unabhängige Dritte[45] vorgesehen, das zur raschen Konfliktlösung beitragen soll. Die drei wichtigsten Streitbeilegungsinstanzen sind das EU-Datenschutzgremium, BBB (Better Business Bureaus) und TRUSTe.

---

44 In seiner Stellungnahme („ETNO considerations“), die am 4. Oktober 2013 bei den Kommissionsdienststellen einging, ging der Verband zudem ein auf 1) die Definition personenbezogener Daten in der Safe-Harbor-Regelung, 2) die unzureichende Kontrolle der Regelung und 3) den Umstand, dass US-Unternehmen Daten mit weniger Einschränkungen übermitteln können als ihre europäischen Wettbewerber. Dies stelle, so der ETNO, eine eindeutige Diskriminierung europäischer Unternehmen dar und beeinträchtige deren Wettbewerbsfähigkeit. Den Safe-Harbor-Regeln zufolge darf eine Organisation Daten nur dann an Dritte weitergeben, wenn sie die Grundsätze der Informationspflicht und der Wahlmöglichkeit anwendet. Möchte eine Organisation Daten an einen Dritten weitergeben, der in ihrem Auftrag und auf ihre Anweisung tätig ist, kann sie dies tun, sofern der Dritte entweder der Safe-Harbor-Regelung angehört oder der Richtlinie unterliegt, oder ihm auf andere Weise ein angemessenes Schutzniveau attestiert wird oder sich schriftlich in einer Vereinbarung mit der Organisation dazu verpflichtet, zumindest das Maß an Schutz personenbezogener Daten zu gewährleisten, das in den entsprechenden Safe-Harbor-Grundsätzen gefordert wird.

45 Die EU-Richtlinie 2013/11/EU über alternative Streitbeilegung in Verbraucherangelegenheiten macht deutlich, wie wichtig unabhängige, unparteiische, transparente, effektive, schnelle und faire ADR-Verfahren sind.



Seit 2004 wird ADR verstärkt in Anspruch genommen, und das US-Handelsministerium kontrolliert US-amerikanische ADR-Anbieter seither in größerem Maße, um sicherzustellen, dass ihre Informationen über das Beschwerdeverfahren klar, verständlich und zugänglich sind. Inwieweit dieses System als wirksam bezeichnet werden kann, muss sich jedoch erst zeigen, da die Zahl der Fälle derzeit noch zu gering ist.[46]

Zwar ist es dem US-Handelsministerium gelungen, die ADR-Gebühren zu senken, doch verlangen zwei der sieben großen ADR-Anbieter für die Erhebung einer Beschwerde nach wie vor eine Gebühr.[47] Diese ADR-Anbieter werden von 20 % der Safe-Harbor-Unternehmen in Anspruch genommen. Sie haben sich für einen Anbieter entschieden, der Verbrauchern eine Beschwerdegebühr in Rechnung stellt. Dies widerspricht dem Durchsetzungsgrundsatz der Safe-Harbor-Regelung, wonach den Betroffenen „leicht zugängliche, erschwingliche und von unabhängigen Stellen durchgeführte Verfahren“ zur Verfügung stehen müssen. In der Europäischen Union ist die vom EU-Datenschutzgremium gebotene unabhängige Streitbeilegung für alle Betroffenen kostenlos.

Am 12. November 2013 bestätigte das US-Handelsministerium, dass es sich auch weiterhin für den Schutz der Daten von EU-Bürgern einsetzen und gemeinsam mit ADR-Anbietern prüfen wird, ob es möglich ist, die ADR-Gebühren weiter zu senken.

---

46 Einer der großen ADR-Anbieter („TRUSTe“) berichtete beispielsweise, dass er im Jahr 2010 881 Anträge erhalten habe, dass aber nur drei für zulässig und begründet befunden wurden, so dass das betreffende Unternehmen seine Datenschutzbestimmungen und seine Website ändern musste. 2011 gingen 879 Beschwerden ein. Nur in einem Fall musste das betreffende Unternehmen seine Datenschutzbestimmungen ändern. Dem US-Handelsministerium zufolge stammten die weitaus meisten ADR-Beschwerden von Verbrauchern, so zum Beispiel von Internetnutzern, die ihr Passwort vergessen hatten und es nicht bei ihrem Internet-Dienst erfragen konnten. Auf Anfrage der Kommission arbeitete das US-Handelsministerium neue Statistikkriterien aus, die von allen ADR-Stellen zu verwenden sind. Danach wird zwischen bloßen Anfragen und Beschwerden unterschieden, und die Arten von Beschwerden werden klarer voneinander abgegrenzt. Diese neuen Kriterien bedürfen jedoch einer ausführlicheren Erörterung, um sicherzugehen, dass die neuen Statistiken 2014 alle ADR-Anbieter erfassen, vergleichbar sind und relevante Angaben zur Beurteilung der Wirksamkeit der ADR-Verfahren bieten.

47 International Centre for Dispute Resolution / American Arbitration Association (ICDR/AAA) verlangen eine „Antragsgebühr“ von 200 USD und JAMS von 250 USD. Das US-Handelsministerium teilte der Kommission mit, dass es mit AAA, dem teuersten ADR-Anbieter, ein spezielles Programm für Safe Harbor ausgearbeitet habe, das die Kosten für Verbraucher von mehreren Tausend Dollar auf einen Pauschalbetrag von 200 USD verringert.

Was die Sanktionen anbelangt, so verfügen nicht alle ADR-Anbieter über das notwendige Instrumentarium, um einer Missachtung der Datenschutzgrundsätze entgegenzuwirken. Nicht alle ADR-Anbieter sehen überdies als Sanktion die öffentliche Bekanntmachung des Verstoßes vor.

Kommt ein Unternehmen der Abschlussentscheidung eines ADR-Verfahrens nicht nach oder lehnt es die Entscheidung ab, sind die ADR-Anbieter verpflichtet, den betreffenden Fall an die Federal Trade Commission zu verweisen, damit diese den Fall überprüfen und gegebenenfalls Durchsetzungsmaßnahmen ergreifen kann. Bislang wurde der Federal Trade Commission allerdings kein derartiger Fall zur Überprüfung vorgelegt.[48]

Die Anbieter alternativer Streitschlichtungsverfahren veröffentlichen auf ihrer Website eine Liste der Unternehmen, die ihre Dienste in Anspruch nehmen (Dispute Resolution Participants). Auf diese Weise können Verbraucher in einem Streitfall ohne großen Aufwand überprüfen, ob das betreffende Unternehmen bei einem bestimmten ADR-Anbieter gelistet ist. Der ADR-Anbieter BBB führt beispielsweise ein Verzeichnis aller Unternehmen, die seinem ADR-System angeschlossen sind. Daneben gibt es jedoch zahlreiche Unternehmen, die behaupten, einem bestimmten ADR-System beigetreten zu sein, ohne dass sie im Verzeichnis des betreffenden ADR-Anbieters erscheinen.[49]

ADR-Verfahren sollten für die Betroffenen leicht zugänglich und erschwinglich sein und von einer unabhängigen Stelle durchgeführt werden. Ein Betroffener sollte eine Beschwerde ohne übermäßigen Aufwand einlegen können. Alle ADR-Stellen sollten auf ihrer Website Statistiken über die von ihnen bearbeiteten Beschwerden und deren Ausgang veröffentlichen. Sie sollten einer Kontrolle unterliegen, damit sichergestellt ist, dass die Informationen, die sie zum Verfahren und den Beschwerdemodalitäten bereitstellen, klar und verständlich sind, und die alternative Streitbeilegung zu einem wirksamen, vertrauenswürdigen und zielführenden Instrument wird. Es sollte nochmals darauf hingewiesen werden, dass die Bekanntmachung von Verstößen gegen die Safe-Harbor-Grundsätze in den verbindlichen Sanktionenkatalog der ADR-Stellen aufgenommen werden sollte.

6.2 Weitergabe

Im Zuge des exponentiellen Wachstums des Datenverkehrs besteht die Notwendigkeit, auf allen Stufen der Datenverarbeitung sicherzustellen, dass personenbezogene Daten kontinuierlich geschützt sind. Dies gilt insbesondere dann, wenn die Daten von einem Unternehmen, das sich der Safe-Harbor-Regelung angeschlossen hat, an einen **Dritten als Auftragsverarbeiter** übermittelt werden. Eine bessere Durchsetzung der Safe-Harbor-Grundsätze ist daher nicht nur gegenüber Safe-Harbor-Teilnehmern, sondern auch gegenüber Unterauftragnehmern erforderlich.

Möchte ein Unternehmen, das an der Safe-Harbor-Regelung teilnimmt, Daten an einen Dritten weitergeben, der in seinem Auftrag und auf seine Anweisung tätig ist, kann es dies tun, „sofern der Dritte entweder dem 'sicheren Hafen' angehört oder der Richtlinie unterliegt, oder von einer anderen Feststellung angemessenen Schutzniveaus erfasst wird oder sich schriftlich in einer Vereinbarung mit der Organisation dazu verpflichtet, zumindest das Maß an Schutz personenbezogener Daten zu gewährleisten, das in den entsprechenden

48 Siehe FAQ 11.

49 Beispiele: Amazon hat dem US-Handelsministerium mitgeteilt, dass es die ADR-Dienste von BBB nutzt. Im Verzeichnis von BBB ist Amazon jedoch nicht als Teilnehmer des ADR-Systems aufgeführt. Umgekehrt erscheint der Cloud-Anbieter Arsalon Technologies (www.arsalon.net) auf der BBB-Liste der Safe-Harbor-Teilnehmer, obwohl das Unternehmen derzeit nicht am Safe-Harbor-System teilnimmt (Stand: 1 Oktober 2013). BBB, TRUSTe und andere ADR-Anbieter sollten ihre Listen berichtigen und die betreffenden Unternehmen streichen. Von ADR-Anbieter sollte verlangt werden, dass sie nur Unternehmen in ihre Listen aufnehmen, die am Safe Harbor teilnehmen.

Grundsätzen des ‚sicheren Hafens' gefordert wird"[50]. So verlangt das US-Handelsministerium beispielsweise von einem Cloud-Anbieter, dass er auch als Safe-Harbor-Teilnehmer einen Vertrag schließt, wenn er personenbezogene Daten zur Verarbeitung erhält.[51] Diese Bestimmung ist allerdings in Anhang II der Safe-Harbor-Entscheidung nicht klar formuliert.

Da vor allem im Bereich des Cloud-Computing in den vergangenen Jahren deutlich mehr Unterauftragnehmer beschäftigt wurden, sollte ein Safe-Harbor-Unternehmen, wenn es mit einem Unterauftragnehmer einen Vertrag schließt, das US-Handelsministerium davon in Kenntnis setzen und die Datenschutzgarantien veröffentlichen.[52]

Bei den drei vorgenannten Aspekten – alternative Streitbeilegung, bessere Aufsicht und Weitergabe von Daten – besteht Klärungsbedarf.

7. ZUGRIFF AUF IM RAHMEN DER SAFE-HARBOR-REGELUNG ÜBERMITTELTE DATEN

Die Informationen über Umfang und Reichweite der US-Überwachungsprogramme, die im Laufe des Jahres 2013 bekannt geworden sind, haben Zweifel an der Kontinuität des Schutzes der auf der Grundlage der Safe-Harbor-Regelung rechtmäßig in die USA übermittelten personenbezogenen Daten geweckt. So sind alle Unternehmen, die am Programm PRISM beteiligt sind und den US-Behörden den Zugriff auf in den USA gespeicherte und verarbeitete Daten gestatten, der Safe-Harbor-Regelung beigetreten. Safe Harbor ist auf diese Weise zu einem Informationskanal geworden, über den die US-Nachrichtendienste auf personenbezogene Daten zugreifen können, die ursprünglich in der EU verarbeitet worden sind.

Die Safe-Harbor-Entscheidung sieht in Anhang 1 vor, dass die Geltung der Datenschutzgrundsätze durch Gesetz, Regierungsverordnung oder Fallrecht sowie aus Gründen der nationalen Sicherheit, des öffentlichen Interesses und der Rechtsdurchsetzung eingeschränkt werden kann. Grundrechtsbeschränkungen sind nur dann gültig, wenn sie eng ausgelegt werden, in einem der Öffentlichkeit zugänglichen Gesetz niedergelegt sind und in einer demokratischen Gesellschaft angemessen und notwendig sind. In der Safe-Harbor-Entscheidung ist ausdrücklich festgelegt, dass solche Beschränkungen nur zulässig sind, **„insoweit"**, als Erfordernissen der nationalen Sicherheit, des öffentlichen Interesses oder der Rechtsdurchsetzung Rechnung getragen werden muss.[53] Zwar ist in der Safe-Harbor-Entscheidung vorgesehen, dass Daten ausnahmsweise zu Zwecken der nationalen Sicherheit,

---

50 Siehe Kommissionsentscheidung 2000/520/EG, Seite 7 (Weitergabe).

51 Siehe „Clarifications Regarding the U.S.-EU Safe Harbor Framework and Cloud Computing": http://export.gov/static/Safe%20Harbor%20and%20Cloud%20Computing%20Clarification_April%2012%202013_Latest_eg_main_060351.pdf.

52 Diese Bemerkungen beziehen sich auf Cloud-Anbieter, die nicht an der Safe-Harbor-Regelung teilnehmen. Dem Beratungsunternehmen Galexia zufolge ist der Anteil der Safe-Harbor-Teilnehmer (und die Einhaltungsquote) unter Cloud-Anbietern recht hoch. Cloud-Anbieter verfügen in der Regel über ein aus mehreren Komponenten bestehendes Datenschutzsystem, bei dem Direktverträge häufig mit globalen Datenschutzbestimmungen kombiniert werden. Mit einer oder zwei wichtigen Ausnahmen halten Cloud-Anbieter, die Safe-Harbor-Teilnehmer sind, die Kernbestimmungen zur Streitbeilegung und zur Durchsetzung der Safe-Harbor-Grundsätze ein. Es gibt derzeit keine größeren Cloud-Anbieter, die sich fälschlicherweise als Safe-Harbor-Teilnehmer ausgeben. Vortrag von Chris Connolly (Galexia) vor dem LIBE-Ausschuss im Rahmen der Anhörung zum Thema „Elektronische Massenüberwachung von EU-Bürgern".

53 Siehe Anhang 1 der Safe-Harbor-Entscheidung: „Die Geltung dieser Grundsätze kann begrenzt werden a) insoweit, als Erfordernissen der nationalen Sicherheit, des öffentlichen Interesses oder der Durchführung von Gesetzen Rechnung getragen werden muss, b) durch Gesetzesrecht, staatliche Regulierungsvorschriften oder Fallrecht, die unvereinbare Verpflichtungen oder ausdrückliche Ermächtigungen schaffen, vorausgesetzt, die Organisation kann in Wahrnehmung dieser Ermächtigungen nachweisen, dass die Nichteinhaltung der Grundsätze sich auf das Ausmaß beschränkte, das die Einhaltung übergeordneter berechtigter Interessen aufgrund eben dieser Ermächtigung erforderte, oder c) wenn die Richtlinie oder das nationale Recht Ausnahmeregelungen vorsieht, sofern diese Ausnahmeregelungen unter vergleichbaren Voraussetzungen getroffen werden. Im Hinblick auf das Ziel eines wirksameren Schutzes der Privatsphäre sollen die Organisationen die Grundsätze in vollem Umfang und in transparenter Weise anwenden, unter anderem indem sie angeben, in welchen Fällen Abweichungen von den Grundsätzen, die nach b) zulässig sind, bei ihren Datenschutzmaßnahmen regelmäßig Anwendung finden werden. Aus demselben Grund wird, wenn die Wahlmöglichkeit nach den Grundsätzen und/oder nach dem US-Recht besteht, von den Organisationen erwartet, dass sie sich, sofern möglich, für das höhere Schutzniveau entscheiden."

des öffentlichen Interesses oder der Rechtsdurchsetzung verarbeitet werden dürfen, doch war zum Zeitpunkt ihres Erlasses nicht absehbar, dass Nachrichtendienste in großem Maßstab auf Daten zugreifen würden, die im Rahmen von Handelsgeschäften in die USA übermittelt wurden.

Aus Gründen der Transparenz und Rechtssicherheit sollte das US-Handelsministerium die Europäische Kommission zudem von Gesetzen oder Verordnungen (Regulierungsvorschriften) in Kenntnis setzen, die die Beachtung der Safe-Harbor-Grundsätze berühren.[54] Die Ausnahmeregelungen sollten sorgfältig überwacht werden. Sie dürfen nicht dazu benutzt werden, die **Safe-Harbor-Grundsätze** zu unterlaufen.[55] Der breite Zugriff der US-Behörden auf Daten, die von Safe-Harbor-Unternehmen verarbeitet werden, gefährdet die Vertraulichkeit der elektronischen Kommunikation.

7.1 Verhältnismäßigkeit

Nach den Ergebnissen der Ad-hoc-Arbeitsgruppe EU-USA zum Datenschutz lässt das US-amerikanische Recht die umfassende Erhebung und Verarbeitung personenbezogener Daten zu, die von Unternehmen mit Sitz in den USA gespeichert oder in anderer Weise verarbeitet werden. Hierzu können Daten gehören, die auf der Grundlage der Safe-Harbor-Regelung zuvor von der EU in die USA übermittelt wurden. Hier stellt sich die Frage, ob die Safe-Harbor-Grundsätze in der Folge eingehalten werden. Diese groß angelegten Programme können dazu führen, dass auf der Grundlage der Safe-Harbor-Regelung transferierte Daten von US-Behörden über das Maß hinaus, das für den Schutz der nationalen Sicherheit (im Sinne der Ausnahmeklausel in der Safe-Harbor-Entscheidung) unbedingt nötig und angemessen wäre, abgerufen und weiterverarbeitet werden.

7.2 Beschränkungen und Rechtsschutzmöglichkeiten

Wie den Ergebnissen der Ad-hoc-Arbeitsgruppe EU-USA zu entnehmen ist, stehen die nach US-amerikanischem Recht verfügbaren Garantien größtenteils nur US-Bürgern oder Personen mit rechtmäßigem Wohnsitz in den USA zu. Auch gibt es weder für EU- noch für US-Bürger die Möglichkeit, Auskunft über ihre Daten, deren Berichtigung oder Löschung zu erwirken, die im Rahmen der US-Überwachungsprogramme erhoben und weiterverarbeitet werden. Administrative oder gerichtliche Rechtsbehelfe stehen gleichfalls nicht zur Verfügung.

7.3 Transparenz

Unternehmen geben in ihren Datenschutzbestimmungen nicht systematisch an, in welchen Fällen sie von den Safe-Harbor-Grundsätzen abweichen. Privatpersonen und Unternehmen wissen daher nicht, was mit ihren Daten geschieht. Dies ist angesichts der US-Überwachungsprogramme besonders heikel. Europäischen Bürgern, deren Daten auf der Grundlage der Safe-Harbor-Regelung an ein Unternehmen in den USA transferiert werden, wird somit von diesen Unternehmen unter Umständen nicht mitgeteilt, dass US-Behörden auf ihre Daten zugreifen können.[56] Hier stellt sich die Frage nach der Vereinbarkeit mit den Safe-

---

54 Stellungnahme 4/2000 über das Datenschutzniveau, das die Grundsätze des sicheren Hafens bieten, angenommen von der Artikel 29-Datenschutzgruppe am 16. Mai 2000.

55 Stellungnahme 4/2000 über das Datenschutzniveau, das die Grundsätze des sicheren Hafens bieten, angenommen von der Artikel 29-Datenschutzgruppe am 16. Mai 2000.

56 Einige europäische Unternehmen bieten in dieser Hinsicht relativ transparente Informationen. Das Unternehmen Nokia beispielsweise, das Niederlassungen in den USA unterhält und an Safe Harbor teilnimmt, hat in seine Datenschutzbestimmungen folgenden Vermerk aufgenommen: *„Wir können gesetzlich verpflichtet werden, ihre personenbezogenen Daten gegenüber bestimmten Behörden oder Dritten, beispielsweise Strafverfolgungsbehörden in Ländern, in denen wir oder Dritte in unserem Namen tätig sind, offenzulegen.“ („We may be obligated by mandatory law to disclose your personal data to certain authorities*

Harbor-Grundsätzen zur Transparenz. Transparenz sollte so weit gewährleistet sein, wie dies möglich ist, ohne die nationale Sicherheit zu gefährden. Zusätzlich zu der bestehenden Verpflichtung für Unternehmen, in ihren Datenschutzbestimmungen anzugeben, in welchen Fällen die Safe-Harbor-Grundsätze durch Gesetz, Verordnung oder Fallrecht eingeschränkt werden können, sollten Unternehmen angeben, in welchen Fällen sie von den Grundsätzen abweichen, um Anforderungen der nationalen Sicherheit, des öffentlichen Interesses oder der Rechtsdurchsetzung zu genügen.

8. SCHLUSSFOLGERUNGEN UND EMPFEHLUNGEN

Seit dem Jahr 2000, als die Safe-Harbor-Entscheidung erlassen wurde, erfolgt die Übermittlung personenbezogener Daten zwischen der EU und den USA auf der Grundlage dieser Entscheidung. Aufgrund der exponentiellen Zunahme des Datenverkehrs, der Dreh- und Angelpunkt der digitalen Wirtschaft ist, und der signifikanten Entwicklungen bei der Datenerhebung, -verarbeitung und -nutzung kommt dem wirksamen Schutz der Übermittlung personenbezogener Daten eine entsprechend gestiegene Bedeutung zu. Web-Unternehmen wie Google, Facebook, Microsoft, Apple und Yahoo haben mehrere Hundert Millionen Kunden in Europa. Sie übermitteln Mengen an personenbezogenen Daten zur Verarbeitung in die USA, die im Jahr 2000, als die Safe-Harbor-Regelung geschaffen wurde, unvorstellbar waren.

Es bestehen nach wie vor Probleme, die durch mangelnde Transparenz und unzureichende Durchsetzung der Safe-Harbor-Vereinbarung bedingt sind und die jetzt angegangen werden sollten:

a) Transparenz der Datenschutzpraktiken der Safe-Harbor-Teilnehmer

b) effektive Anwendung der Datenschutzgrundsätze durch Unternehmen in den USA

c) Wirksamkeit der Durchsetzung

Ernsthaft in Frage zu stellen ist auch, ob die Datenschutzrechte europäischer Bürger, deren Daten in die USA übermittelt werden, **angesichts des umfassenden Zugriffs der Nachrichtendienste auf Daten, die von Safe-Harbor-Unternehmen in die USA übermittelt werden**, kontinuierlich geschützt sind.

Auf der Grundlage ihrer vorstehenden Ausführungen gibt die Kommission folgende **Empfehlungen** ab:

Transparenz

1. *Selbstzertifizierte Unternehmen sollten ihre Datenschutzbestimmungen offenlegen.* Es reicht nicht aus, wenn Unternehmen dem US-Handelsministerium ihre Geschäftsbedingungen zum Datenschutz vorlegen. Die Datenschutzbestimmungen eines Unternehmens sollten auf seiner Website unmissverständlich und deutlich erkennbar bekanntgemacht werden.

2. *Die Geschäftsbedingungen zum Datenschutz auf der Website selbstzertifizierter Unternehmen sollten stets mit der Safe-Harbor-Website des US-Handelsministeriums verlinkt sein, auf der alle aktuellen Teilnehmer der Safe-Harbor-Regelung aufgeführt sind*. Auf diese Weise können europäische

---

or other third parties, for example, to law enforcement agencies in the countries where we or third parties acting on our behalf operate.")

Betroffene ohne zusätzlichen Suchaufwand sofort feststellen, ob ein bestimmtes Unternehmen derzeit der Safe-Harbor-Regelung angehört. Die Möglichkeit, die Teilnahme an der Regelung nur vorzuspiegeln, würde dadurch begrenzt; gleichzeitig würde sich die Glaubwürdigkeit der Regelung erhöhen. Das US-Handelsministerium hat im März 2013 damit begonnen, die Unternehmen zu diesem Schritt aufzufordern. Die Bemühungen sollten jedoch verstärkt werden.

3. *Selbstzertifizierte Unternehmen sollten Datenschutzbestimmungen in Verträgen, die sie mit Unterauftragnehmern, z. B. mit „Cloud-Computing"-Diensten, schließen, veröffentlichen.* Die Safe-Harbor-Regelung erlaubt die Weiterübermittlung an Dritte, z. B. Anbieter von Cloud-Diensten, die im Auftrag eines selbstzertifizierten Unternehmens tätig sind. Nach unserem Verständnis verlangt das US-Handelsministerium von selbstzertifizierten Unternehmen in diesem Fall, dass es mit dem Dritten einen Vertrag schließt. Wenn ein Safe-Harbor-Unternehmen einen solchen Vertrag schließt, sollte es das US-Handelsministerium davon in Kenntnis setzen und die Datenschutzgarantien veröffentlichen.

4. *Auf der Website des US-Handelsministeriums sollten alle Unternehmen kenntlich gemacht werden, die nicht mehr an der Safe-Harbor-Regelung teilnehmen.* Der Vermerk „Not current" (derzeit nicht der Safe-Harbor-Regelung angeschlossen) in der Liste der Safe-Harbor-Teilnehmer des US-Handelsministeriums sollte durch einen deutlichen Warnhinweis ergänzt werden, dass das betreffende Unternehmen die Safe-Harbor-Anforderungen derzeit nicht erfüllt. Das Unternehmen ist jedoch dennoch verpflichtet, die Safe-Harbor-Anforderungen für Daten zu beachten, die es im Rahmen der Regelung erhalten hat.

Rechtsschutz

1. *Die Datenschutzbestimmungen auf der Unternehmenswebsite sollten mit einem Link zu der zuständigen Stelle für alternative Streitbeilegung (ADR) und/oder zu dem EU-Datenschutzgremium versehen sein*. Europäische Betroffene könnten dann bei einem Problem sofort die ADR-Stelle oder das EU-Gremium kontaktieren. Das US-Handelsministerium hat im März 2013 damit begonnen, die Unternehmen zu diesem Schritt aufzufordern. Die Bemühungen sollten jedoch verstärkt werden.

2. *ADR sollte leicht verfügbar und erschwinglich sein. Einige ADR-Stellen erheben für die Bearbeitung einer Beschwerde im Rahmen der Safe-Harbor-Regelung nach wie vor Gebühren, die für den Einzelnen recht hoch sein können (200-250 USD).* In Europa hingegen ist die Inanspruchnahme des Datenschutzgremiums für Beschwerden im Rahmen der Safe-Harbor-Regelung kostenlos.

3. *Das US-Handelsministerium sollte die ADR-Anbieter systematischer überprüfen, was die Transparenz der Informationen anbelangt, die sie über ihr Verfahren und das Follow-up der Beschwerden bereitstellen, sowie den Zugang zu diesen Informationen*. Die Streitbeilegung wird so zu einem wirksamen, vertrauenswürdigen und zielführenden Instrument. Es sollte nochmals darauf hingewiesen werden, dass die Bekanntmachung von

Verstößen gegen die Safe-Harbor-Grundsätze in den verbindlichen Sanktionenkatalog der ADR-Stellen aufgenommen werden sollte.

Durchsetzung

1. *Nach einer Safe-Harbor-Zertifizierung oder Rezertifizierung sollte bei einem bestimmten Anteil der Unternehmen von Amts wegen überprüft werden, ob sie ihre Datenschutzbestimmungen einhalten (diese Kontrolle sollte über formale Erfordernisse hinausgehen).*

2. *Wurde im Zuge einer Beschwerde oder Untersuchung ein Verstoß gegen die Datenschutzbestimmungen festgestellt, sollte das Unternehmen ein Jahr später erneut überprüft werden.*

3. *Bestehen Zweifel an der Einhaltung der Safe-Harbor-Grundsätze oder liegen Beschwerden gegen ein Unternehmen vor, sollte das US-Handelsministerium die zuständige Datenschutzbehörde in der EU davon in Kenntnis setzen.*

4. *Falschbehauptungen in Bezug auf die Teilnahme an der Safe-Harbor-Regelung sollten weiter untersucht werden.* Ein Unternehmen, das auf seiner Website behauptet, die Safe-Harbor-Grundsätze einzuhalten, aber auf der Liste des US-Handelsministeriums nicht als „aktueller“ („current“) Teilnehmer der Regelung geführt wird, führt Verbraucher in die Irre und missbraucht ihr Vertrauen. Falschbehauptungen beeinträchtigen die Glaubwürdigkeit der gesamten Regelung und sollten deshalb sofort von den Websites des Unternehmens entfernt werden.

Zugriffsrecht der US-Behörden

1. *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.*

2. *Wichtig ist, dass von der in der Safe-Harbor-Entscheidung vorgesehenen Ausnahme der nationalen Sicherheit nur so weit Gebrauch gemacht wird, wie dies unbedingt notwendig oder angemessen ist.*