# Safe Harbor in der „Post-Snowden-Ära“*

Walter Hötzendorfer, Erich Schweighofer

Arbeitsgruppe Rechtsinformatik
Universität Wien
Schottenbastei 10-16/2/5
1010 Wien
walter.hoetzendorfer@univie.ac.at
erich.schweighofer@univie.ac.at

**Abstract:** Die von Edward Snowden enthüllte umfassende Überwachungspraxis der US-Geheimdienste hat die Safe-Harbor-Lösung betreffend die transatlantische Datenübermittlung mehr denn je zum Gegenstand der öffentlichen Debatte gemacht. Nach einer Analyse der Überwachungsmöglichkeiten im Internet und der rechtlichen Grundlagen der Datenübermittlung in die USA beschäftigt sich der Beitrag mit der Rechtmäßigkeit und der Umsetzungspraxis von Safe Harbor – sowohl allgemein als auch im Hinblick auf den ans Licht gekommenen Datenzugriff durch US-Geheimdienste. Schließlich wird erörtert, ob Safe Harbor die derzeitige Aufmerksamkeit zu Recht genießt, ob eine Aufhebung der Safe-Harbor-Entscheidung die Situation überhaupt verbessern könnte und welche Alternativen es zu einer Aufhebung gibt.

## 1 Einleitung

Ein wesentlicher Teil des Datenverkehrs zwischen der EU und den USA beruht auf der sogenannten Safe-Harbor-Entscheidung[1] aus dem Jahr 2000. US-amerikanische Unternehmen, die sich Safe Harbor anschließen, indem sie sich verpflichten, bestimmte Bedingungen einzuhalten, können genehmigungsfrei Daten aus dem europäischen Raum beziehen. Schon bisher wurde Kritik an Safe Harbor und insbesondere an der Einhaltung der Regeln sowie der Ernsthaftigkeit von Kontrollen geäußert. Im Lichte der Enthüllungen Edward Snowdens über die umfassenden Überwachungsaktivitäten der US-Geheimdienste[2] forderte die deutsche Datenschutzkonferenz die Suspendierung der Safe-

* Dieser Beitrag beschäftigt sich nicht generell mit der – überaus wichtigen – Frage „Was machen wir gegen die Überwachung?“, sondern mit der Frage „Was machen wir mit Safe Harbor?“, da im Zuge der Snowden-Enthüllungen politisch wieder Bewegung in diese Frage gekommen ist. Am 27.11.2013 – d.h. nach Fertigstellung dieses Beitrags – gab die Kommission bekannt, Safe Harbor nicht aufheben oder aussetzen, aber durch Verhandlungen mit den USA wesentlich verbessern zu wollen (siehe COM(2013) 846 final und COM(2013) 847 final) – ein Vorgehen, das dem in diesem Beitrag avisierten sehr nahe kommt.

[1] 2000/520/EG: Entscheidung 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.

[2] Eine übersichtliche Zusammenstellung der enthüllten Fakten ist bei Zeit Online zu finden: http://www.zeit.de/digital/datenschutz/2013-07/faq-nsa-skandal/komplettansicht

Harbor-Entscheidung [Dk13]. Dies wird seitens deutscher Unternehmen sehr ernst genommen und führte zu zahlreichen Anfragen, denn die deutschen Datenschutzbehörden der Länder erwägen derzeit, Datenübermittlungen auf der Basis von Safe Harbor tatsächlich nicht mehr zuzulassen.[3] EU-Kommissarin Viviane Reding bezeichnete Safe Harbor als Schlupfloch, das geschlossen werden müsse, und lässt Safe Harbor daher derzeit evaluieren [EC13].

Der österreichische Datenschutzaktivist Max Schrems brachte im Juni 2013 infolge der Snowden-Enthüllungen bei den jeweils zuständigen europäischen Datenschutzbehörden Beschwerden gegen Facebook und Apple (in Irland), gegen Skype und Microsoft (in Luxemburg) sowie gegen Yahoo (in Bayern) ein.[4] Er argumentiert, die Datenübermittlung der europäischen Tochterunternehmen dieser Konzerne an die US-Konzernmütter auf Basis von Safe Harbor sei rechtswidrig, da die Daten durch die Übermittlung der Überwachung durch US-Geheimdienste ausgesetzt würden.

## 2 Private Daten

Diese Beschwerden nur wenige Tage nach den ersten Enthüllungen Snowdens sind eine erste unmittelbare rechtliche Reaktion der Zivilgesellschaft auf diese Enthüllungen und zeigen folgenden Zusammenhang auf: Eine wesentliche Voraussetzung der bekannt gewordenen elektronischen Überwachungsmaßnahmen der Geheimdienste der USA und anderer westlicher Staaten ist die allgegenwärtige Nutzung zahlreicher Services der großen US-Internetkonzerne wie Google, Facebook, Microsoft und Apple, die seit der Jahrtausendwende entwickelt wurden und sich seither in ungeahntem Ausmaß etabliert haben. Zahlreiche Aktivitäten des täglichen Lebens haben sich in hohem Maße auf das Internet verlagert, allen voran die persönliche Kommunikation und der Konsum medialer Berichterstattung. Dadurch hinterlassen Menschen immer mehr digitale Spuren, was zum Teil vermeidbar wäre, zahlreichen Aktivitäten jedoch inhärent und somit in diesen Fällen unvermeidbar ist.[5]

Oftmals werden Überwachungsaktivitäten im Internet mit der Überwachung der elektronischen Kommunikation gleichgesetzt. Diese Sichtweise ist jedoch zu eng. Durch die genannte Entwicklung wird die Überwachung von Personen in dreierlei Hinsicht begünstigt. Erstens werden immer mehr Informationen über Personen – im Sinne von Attributen [SH12] – gespeichert, die zum Teil auch öffentlich abrufbar sind. Zweitens werden immer mehr Daten über Aktivitäten von Personen und insbesondere deren Aufenthaltsorte gespeichert. Drittens sind es natürlich – neben den Attributen und Aktivitätsdaten –

[3] So die Landesbeauftragte für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen, Dr. Imke Sommer, mündlich bei einer Podiumsdiskussion am 20.09.2013 in Brüssel.
[4] Näheres dazu sowie die weitere Entwicklung in dieser Sache kann auf http://www.europe-v-facebook.org nachgelesen werden.
[5] Beispielsweise ist die (Re-)Identifikation der Nutzer kostenloser Nachrichtenseiten mittels Cookies – jedenfalls aus Sicht der Nutzer – in der Regel nicht erforderlich, jedoch weit verbreitet. Dies ist ein Anwendungsfall, bei dem „das Hinterlassen von Spuren“ reduziert werden könnte. Demgegenüber basieren z.B. Social Networks wie Facebook, LinkedIn und Xing gerade auf der umfassenden Speicherung der Aktivitäten, Nachrichten, Fotos und Aufenthaltsorte des Nutzers, die dieser größtenteils bewusst vornimmt. Hier ist eine „anonymere“ Nutzung schwer vorstellbar oder würde die Funktionalität stark einschränken.

die Kommunikationsdaten, die in stetig wachsendem Umfang übertragen und vielfach auch gespeichert werden. Ein immer größerer Teil der zwischenmenschlichen Kommunikation erfolgt via Internet und somit in einer Form, die den – rechtmäßigen wie auch rechtswidrigen – Zugang zu Kommunikationsinhaltsdaten und -metadaten sowie deren automatisierte Weiterverarbeitung sehr erleichtert. Hinzu kommt, dass aus den gespeicherten Daten implizit noch eine Vielzahl weiterer personenbezogener Informationen abgeleitet werden kann, die zum Teil nicht einmal den Betroffenen selbst bekannt bzw. bewusst sind.

Das Vorhandensein immer größerer Mengen personenbezogener Daten ist eine notwendige, jedoch keine hinreichende Bedingung, um Überwachung auf Basis dieser Daten durchführen zu können. Dafür müssen auch die Kapazitäten und Fähigkeiten vorhanden sein, um aus den Daten aussagekräftige Erkenntnisse abzuleiten.[6] Die allermeisten der genannten Daten werden auf der Infrastruktur privater Unternehmen übertragen und auf Servern privater Unternehmen gespeichert. Somit ist eine weitere Bedingung für die Auswertung dieser Daten durch Behörden deren Zugriff auf diese Daten. Dabei ist zu unterscheiden zwischen dem Zugriff auf Daten, während diese im Internet übertragen werden, und dem Zugriff auf Daten, die auf Servern gespeichert sind.[7] Letzterer ist jener Fall, mit dem sich der Beitrag im Folgenden beschäftigt.

## 3 Übermittlung personenbezogener Daten in die USA

Die USA sind aus der Perspektive des europäischen Datenschutzrechts ein „unsicheres Drittland", also ein Land, in dem kein angemessenes Datenschutzniveau besteht.[8] Hintergrund dieser Tatsache sind zwei völlig unterschiedliche Herangehensweisen an das Thema Datenschutz diesseits und jenseits des Atlantiks. Während in Europa Datenschutz als Grundrecht gilt,[9] ist dies in den USA nicht umfassend der Fall. Vielmehr steht dort ein Grundrecht einem umfassenden Datenschutz sogar tendenziell entgegen, und zwar das im ersten Verfassungszusatz normierte Grundrecht der Redefreiheit. In Europa ist

[6] Eine wichtige Erkenntnis aus den Enthüllungen von Edward Snowden ist, dass die Informatik einen Entwicklungsstand erreicht hat, der es ermöglicht, aus diesen Daten brauchbare Erkenntnisse zu ziehen. Dies wird derzeit – nicht nur im Kontext von Überwachung – unter dem Stichwort Big Data diskutiert [MC13].

[7] Der direkte Zugriff auf Daten, die sich auf den Endgeräten der Nutzer befinden, ist hier als dritte Möglichkeit zu nennen. Dieser wird aber schon aufgrund des dafür nötigen hohen individuellen Aufwands vergleichsweise selten vorkommen und ist somit kein Massenphänomen.

[8] Ob in einem Drittland ein angemessenes Datenschutzniveau besteht, bestimmt die Kommission gemäß Art. 25 Abs. 6 DSRL (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, ABl. L 281, 31 vom 23.11.1995). Anzumerken ist, dass ein Vergleich zwischen dem tatsächlichen Datenschutzniveau in den USA und jenem in der EU nicht ausschließlich auf Basis der Rechtslage durchgeführt werden kann, da in Europa im Datenschutz eine große Diskrepanz zwischen Rechtslage und Umsetzungspraxis herrscht. Ein solcher Vergleich ist hier auch nicht intendiert. Die gemeinschaftsrechtliche Qualifikation der USA als „unsicheres Drittland" ist ein Faktum, das hier nicht hinterfragt wird.

[9] Art. 8 GRC (Charta der Grundrechte der Europäischen Union), Art. 8 EMRK (Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten – Europäische Menschenrechtskonvention) und nationale Grundrechte wie z.B. das deutsche Recht auf informationelle Selbstbestimmung und § 1 DSG 2000 (Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 – DSG 2000), BGBl. I Nr. 165/1999 idF BGBl. I Nr. 57/2013) in Österreich.

daher Datenschutz grundsätzlich als Verbotsnorm mit Erlaubnistatbeständen ausgestaltet, wohingegen in den USA betreffend private Auftraggeber nur einzelne sektorspezifische Datenschutzbestimmungen bestehen[10] sowie eine Tradition der Selbstregulierung, die mittels Wettbewerbsrecht sanktioniert wird und auch im Safe-Harbor-System eine wesentliche Rolle spielt [Ge04]. Europäische Auftraggeber dürfen personenbezogene Daten grundsätzlich nicht in ein unsicheres Drittland übermitteln, es sei denn, der Betroffene hat eingewilligt oder die Übermittlung ist für die Erfüllung eines Vertrages erforderlich, den der Auftraggeber mit dem Betroffenen oder in dessen Interesse geschlossenen hat.[11] Die DSRL sieht mit den Standardvertragsklauseln[12] sowie Binding Corporate Rules Auswege aus dieser Situation vor, die auf der Ebene der einzelnen Unternehmen ansetzen. Da dem Datenverkehr zwischen der EU und den USA besondere Bedeutung zukommt, wurde diesbezüglich mit Safe Harbor eine einzigartige pragmatische Lösung geschaffen, die zwar ebenfalls auf der Ebene der einzelnen Unternehmen angesiedelt ist, den Datenverkehr zwischen Europa und den USA aber wesentlich vereinfacht.

Binding Corporate Rules sind ein Instrument für Datenübermittlung innerhalb multinationaler Unternehmen und internationaler Organisationen. Diese können unternehmensweit gültige Regeln für den Umgang mit personenbezogenen Daten definieren. Damit diese die Funktion von Binding Corporate Rules erfüllen, müssen sie von den Datenschutzbehörden aller EU-Mitgliedstaaten akzeptiert werden, in denen das jeweilige Unternehmen tätig ist. Die Artikel-29-Gruppe hat zahlreiche Dokumente ausgearbeitet, welche die Erstellung und Abnahme von Binding Corporate Rules unterstützen.[13] Mit Ausnahme von eBay findet sich keiner der großen US-Internetkonzerne auf der Liste jener Unternehmen, für die Binding Corporate Rules genehmigt wurden.[14]

## 4 Safe Harbor

Die Safe-Harbor-Lösung besteht aus einem Bündel von Dokumenten, die vonseiten der USA im Zuge von Verhandlungen mit der Kommission ausgearbeitet wurden, und einer Entscheidung der Kommission[15] (im Folgenden „(Safe-Harbor-)Entscheidung"), die diesen Dokumenten in Europa rechtliche Wirkung verleiht. Die Dokumente sind der Entscheidung als Anhänge I-VII angefügt. Im Kern besagt die Entscheidung, dass die Übermittlung von Daten an US-Unternehmen, welche sich zur Einhaltung bestimmter Bedingungen verpflichten, zulässig ist [GS12, Rn. 14-16 m.w.N.]. Safe Harbor trans-

[10] Z.B. der Video Privacy Protection Act von 1988, 18 USC § 2710-2711 [Ge04, S. 73 f.].
[11] Art. 26 Abs. 1 a) bis c) DSRL. Die Bestimmung enthält weitere Ausnahmen, die jedoch hier von untergeordneter Relevanz sind.
[12] Art. 26 Abs. 2 DSRL.
[13] Siehe unter http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm.
[14] Die Liste ist unter folgender Adresse zu finden: http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/bcr_cooperation/index_en.htm.
[15] Entscheidung 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, 7 vom 25.08.2000.

formiert dadurch wesentliche Prinzipien des europäischen Datenschutzrechts in das in den USA übliche System der freiwilligen Selbstverpflichtung [Ge04].

Laut Genz ist Safe Harbor kein völkerrechtlicher Vertrag und auch kein Verwaltungsabkommen, insbesondere aufgrund der Unilateralität der Safe-Harbor-Entscheidung, welcher ebenso wie den vonseiten der USA ausgearbeiteten Dokumenten der Charakter einer völkerrechtlichen Willenserklärung oder Willensbekundung fehlt [Ge04, S. 158 ff.]. Man könnte argumentieren, dass bereits ein Briefwechsel, wie er im Vorfeld der Safe-Harbor-Entscheidung zwischen 1998 und 2000 zwischen der Kommission und dem US-Handelsministerium erfolgt ist, eine internationale Übereinkunft i.S.d. Art. 218 AEUV darstellen kann.[16] Da aber die Voraussetzungen des Art. 218 bzw. von dessen Vorgängerbestimmung Art. 300 EGV nicht erfüllt werden, wäre diese Vereinbarung unwirksam [Pi13] oder zumindest mit dem Nichtigkeitsgrund des Art. 46 WVK belastet, weil hier grundlegende Prinzipien des internen Völkervertragsrechts der EU verletzt werden und den USA die Kenntnis dieser Bestimmungen entgegen gehalten werden kann.[17] Allerdings kann mit dem Prinzip des estoppel argumentiert werden [CM07], welches legitime Erwartungen eines Staates schützt, die durch das Verhalten eines anderen Staates geweckt wurden. Aufgrund des Verhandlungsprozesses ist evident, dass keine einseitige Entscheidung, sondern eine bilaterale Lösung angestrebt wurde. Die EU hat damit Praxis geschaffen, auf welche die USA gutgläubig vertrauen können. Allerdings haben die USA durch wesentliche Verletzungen dieses Arrangements den guten Glauben verloren und können daher das estoppel-Prinzip nicht mehr anwenden. Die EU aber kann sich nach wie vor auf estoppel berufen und den USA die Völkerrechtsverletzung vorwerfen. Durch einseitige Aufhebung der Safe Harbor-Entscheidung wäre diese Möglichkeit frustriert.

Die Kommission stützt ihre Entscheidung auf Art. 25 Abs. 6 DSRL.[18] Diese Bestimmung ermächtigt die Kommission, festzustellen, dass ein Drittland aufgrund seiner innerstaatlichen Rechtsvorschriften oder internationaler Verpflichtungen, die es insbesondere infolge von Verhandlungen gemäß Abs. 5 leg. cit. eingegangen ist, ein angemessenes Datenschutzniveau gewährleistet. Keine dieser beiden Bedingungen ist jedoch erfüllt, denn in der Entscheidung wurde ein angemessenes Datenschutzniveau weder aufgrund der Rechtvorschriften der USA noch aufgrund völkerrechtlicher Verpflichtungen der USA festgestellt. Genz folgert jedoch aus dem letzten Halbsatz von Art. 25 Abs. 6 DSRL, dass nicht nur an formale Kriterien, sondern insbesondere an das effektiv erzielte Schutzniveau angeknüpft werden solle [Ge04, S. 165]. Selbst nach dieser Sichtweise ist jedoch die Kompetenz der Kommission zum Erlassen der Safe-Harbor-Entscheidung zweifelhaft, weil – wie noch zu zeigen sein wird – Safe Harbor keinen effektiven Schutz der Privatsphäre sowie der Freiheiten und Grundrechte bietet.

[16] EuGH 09.08.1994, Rs. C-327/91.

[17] Auch das Europäische Parlament hat auf diese Auslegungsvariante hingewiesen: Entschließung des Europäischen Parlaments ABl. C 121, 152 vom 24.04.2001, S. 155.

[18] Rechtliche Grundlage von Entscheidungen war bis zum Vertrag von Lissabon Art. 249 EGV. Das Institut der Entscheidung wurde durch den Vertrag von Lissabon durch das Institut des Beschlusses ersetzt (Art. 288 AEUV).

Inhaltlicher Kern der Entscheidung ist Art. 1 Abs. 1, welcher festlegt, dass die „Grundsätze des ‚sicheren Hafens' zum Datenschutz" (Anhang I der Entscheidung, im Folgenden „Safe-Harbor-Grundsätze"), umgesetzt gemäß der „Häufig gestellten Fragen" (FAQ, Anhang II), ein angemessenes Schutzniveau für personenbezogene Daten gewährleisten, die von der Europäischen Union an in den Vereinigten Staaten niedergelassene Organisationen übermittelt werden. Eine solche Übermittlung ist zulässig, wenn die Organisation, die die Daten erhält, sich öffentlich verpflichtet, die Grundsätze einzuhalten, und in den USA einer staatlichen Einrichtung unterliegt, die zur Behandlung von Beschwerden über die Nichteinhaltung der Grundsätze berechtigt ist (Art. 1 Abs. 2 b)). Die EU erkennt gemäß der Anlage zu Anhang I als solche Einrichtung Die Federal Trade Commission (FTC) sowie das US-Verkehrsministerium an. Zu beachten ist daher, dass die Anwendung von Safe Harbor auf Unternehmen beschränkt ist, die der Aufsicht einer dieser beiden US-Behörden unterliegen. Wie Anhang III zu entnehmen ist, trifft dies für mehrere nennenswerte Branchen nicht zu. Zum Institut der FAQ ist zu erwähnen, dass diese als Ausführungsbestimmungen zu betrachten sind, deren Bedeutung den Grundsätzen nicht nachsteht. Bestimmungen in Form von Fragen und Antworten sind in den USA bei Verfahrens- und Verwaltungsvorschriften nicht unüblich [Ge04]. Bemerkenswert ist, dass für Fragen der Auslegung und Einhaltung der Grundsätze einschließlich der FAQ US-Recht heranzuziehen ist (Abs. 6 der Grundsätze).

Wie bereits deutlich wurde, handelt es sich bei Safe Harbor um eine freiwillige Selbstverpflichtung. Die oben genannten US-Internetkonzerne sind diese Verpflichtung eingegangen und auf der entsprechenden Liste eingetragen.[19] Ein Unternehmen kann diese Verpflichtung eingehen (die Entscheidung verwendet den Begriff sich „qualifizieren"), indem es dies gegenüber dem US-Handelsministerium bekannt gibt (genannt „Selbstzertifizierung", FAQ 6) oder indem es sich einem vom Privatsektor entwickelten Datenschutzprogramm (Gütesiegelprogramm) anschließt, das sich an die Safe-Harbor-Grundsätze hält. Eine Auditierung oder sonstige materielle Überprüfung der Umsetzung der Safe-Harbor-Grundsätze durch Unternehmensexterne ist nicht vorgesehen, es sei denn ein Gütesiegelprogramm sieht dies vor. Eine Durchsetzung erfährt die Selbstverpflichtung jedoch durch die Bestimmungen des Wettbewerbsrechts.

Mit diesem Aspekt befasst sich ausführlich Anhang III: Die Durchsetzung im Safe-Harbor-System beruht darauf, dass die Unterwerfung unter die Safe-Harbor-Grundsätze eine wettbewerbsrelevante öffentliche Erklärung ist. Ein Verstoß gegen die Grundsätze ist ein wettbewerbsrechtlich unlauterer Verstoß gegen diese Erklärung und somit ein Verstoß gegen Abschnitt 5 des Federal Trade Commission Act.[20] Die Federal Trade Commission (FTC) hat die Befugnis, gegen solche Verstöße vorzugehen.[21]

[19] Dies kann unter https://safeharbor.export.gov/list.aspx überprüft werden.
Apple: http://safeharbor.export.gov/companyinfo.aspx?id=17535,
Facebook: http://safeharbor.export.gov/companyinfo.aspx?id=18810,
Google: http://safeharbor.export.gov/companyinfo.aspx?id=16626,
Microsoft: http://safeharbor.export.gov/companyinfo.aspx?id=19225, jeweils abgerufen am 15.10.2013.
[20] 15 USC § 45(a)(1).
[21] 15 USC § 53(b). Ähnliches gilt für das US-Verkehrsministerium in dessen Zuständigkeitsbereich.

## 5 Safe Harbor?

Wenden wir uns nun der Frage zu, wie gut Safe Harbor funktioniert und ob es daher seinen Namen zu Recht trägt oder nicht. Dies erfolgt zunächst durch einen kurzen Blick auf bisher bereits bekannte Umsetzungsschwächen von Safe Harbor und im nächsten Abschnitt schließlich im Lichte der Snowden-Enthüllungen.

Bereits 2004 stellte eine von der Kommission in Auftrag gegebene Studie wesentliche Mängel in der Einhaltung der Grundsätze, in der Selbstzertifizierung und in der Durchsetzung fest, wobei es jedoch zu keinen Beschwerden gekommen war, was auf geringes Bewusstsein bei den Betroffenen zurückgeführt wurde [DAP04]. Ähnlich ernüchternde Ergebnisse lieferte die vielzitierte Studie aus dem Jahr 2008 [Co08]. Sie stellte z.B. fest, dass zahlreiche Organisationen fälschlicherweise angaben, sich Safe Harbor unterworfen zu haben, sowie eine Vielzahl weiterer Fälle von falschen Angaben. Zahlreiche weitere Organisationen erfüllten nicht einmal die einfachsten Voraussetzungen von Safe Harbor. Ebenso wurde festgestellt, dass ein wesentlicher Teil der Unternehmen einen äußerst kostspieligen Streitschlichtungsmechanismus gewählt hatte. Trotz dieser Missstände kam es erst im September 2009 zum ersten Verfahren der FTC gegen ein Unternehmen, das fälschlicherweise behauptet hatte, Safe Harbor zu entsprechen [Ro09]. Connolly berichtete jüngst vor dem LIBE-Ausschuss des Europäischen Parlaments, dass sich die Situation zwar etwas gebessert hätte, die wesentlichen Probleme aber nach wie vor bestünden [Co13].

Aus diesen Ergebnissen kann geschlossen werden, dass die Methode der Selbstzertifizierung in Verbindung mit (europäischen) Rechtsunterworfenen, denen diese Methode i.d.R. ebenso fremd ist wie die Mittel der Durchsetzung – die überdies mit hohem Aufwand und hohen Kosten verbunden sind –, derzeit nicht geeignet ist, die europäischen Datenschutzstandards zu wahren. Während Safe Harbor insgesamt angesichts der unterschiedlichen Zugänge zum Datenschutz diesseits und jenseits des Atlantiks als guter Kompromiss gelten kann, liegen die Probleme insbesondere in der Umsetzung und Kontrolle. Hier sind – unabhängig von den nachfolgenden Ausführungen zur Überwachung – dringend maßgebliche Verbesserungen nötig.

## 6 Safe Harbor in der „Post-Snowden-Ära“

Seitdem bekannt wurde, dass die Rechtsordnung der USA den verdachtsunabhängigen umfassenden Zugriff auf von US-Unternehmen gespeicherte personenbezogene Daten durch US-Geheimdienste vorsieht, ist unabhängig vom Inhalt der Safe-Harbor-Grundsätze zu bezweifeln, dass diese einen angemessenen Schutz gewährleisten. Denn es wurde erkennbar, dass ein Unternehmen schon alleine deswegen keinen angemessen Schutz gewährleisten kann, weil es der Rechtsordnung der USA unterworfen ist und somit dem Zugriff auf die gespeicherten Nutzerdaten durch US-Geheimdienste unterliegt, der mit europäischen Grundrechten unvereinbar ist, insbesondere mit dem

Art 8 Abs 1 EMRK[22] sowie mit Art 7 und 8 GRC. Dies kann in der gebotenen Kürze wie folgt begründet werden:[23]

In *Klass* warnt der EGMR vor der Gefahr, „die Demokratie mit der Begründung, sie zu verteidigen, zu untergraben oder sogar zu zerstören", und hält fest, dass im Namen des Kampfes gegen Spionage und Terrorismus nicht zu jedweder Maßnahme geheimer Überwachung gegriffen werden dürfe, die geeignet erscheint.[24] Jede solche Maßnahme muss verhältnismäßig sein. Die systematische Überwachung eines bedeutenden Teils der Weltbevölkerung ohne einen konkreten Verdacht lässt bereits aufgrund ihrer Dimension und Eingriffstiefe an ihrer Verhältnismäßigkeit zweifeln. Auch kann bezweifelt werden, dass die Überwachungsergebnisse tatsächlich nur zu Zwecken der Terrorbekämpfung und nationalen Sicherheit verwendet werden. Überdies sind die in *Rotaru* durch den EGMR aufgestellten Anforderungen hinsichtlich der gerichtlichen Kontrolle geheimer Überwachungsmaßnahmen[25] und die in *Weber* zusammengefassten Kriterien der Vorhersehbarkeit (im Sinne klarer gesetzlicher Vorgaben)[26] nicht erfüllt. Bereits die Tatsachen, dass sowohl die gesetzlichen Grundlagen der Maßnahmen geheim sind als auch die Rechtsprechung darüber im Geheimen erfolgt, widersprechen beiden Kriterien. Auch die in *Klass* angesprochenen Sicherheitsmaßnahmen gegen Missbrauch[27] sind nicht vorhanden, wie schon allein dadurch deutlich wurde, dass Edward Snowden als Einzelperson an so viele geheime Informationen gelangen konnte.

Somit zeitigt die Safe-Harbor-Entscheidung einen dem EU-Primärrecht widersprechenden Effekt, denn die sie führt dazu, dass personenbezogene Daten, die in den Anwendungsbereich der Grundrechtsordnung der EU fallen, an Unternehmen übermittelt werden, welche der Rechtsordnung der USA unterworfen sind und somit den oben beschriebenen grundrechtswidrigen Überwachungsmaßnahmen. Potenziell gilt dies für jede auf Safe Harbor basierende Übermittlung, wodurch die gesamte Safe-Harbor-Entscheidung betroffen ist.

Auch ein Blick auf den Inhalt der Safe-Harbor-Grundsätze offenbart ein Problem der Safe-Harbor-Entscheidung, das nicht lösbar erscheint. Gemäß dem vierten Absatz der Grundsätze kann deren Geltung für Erfordernisse der nationalen Sicherheit, des öffentlichen Interesses oder der Durchführung von Gesetzen sowie durch nationales Gesetzes- oder Richterrecht beschränkt werden. Diese Ausnahme definiert somit einen Vorrang

---

[22] Siehe insb. EGMR 26.03.1987, 9248/81 *Leander*, EGMR 25.03.1998, 9248/81 *Kopp*, EGMR 16.02.2000, 27798/95 *Amann*, EGMR 04.05.2000, 28341/95, *Rotaru*, EGMR 29.06.2006, 54934/00, *Weber*, EGMR 01.07.2008, 58243/00 *Liberty* etc.

[23] Zum Grundrechtsverstoß durch PRISM und andere Überwachungsprogramme siehe auch die Entschließung des Europäischen Parlaments zu dem Überwachungsprogramm der Nationalen Sicherheitsagentur der Vereinigten Staaten, den Überwachungsbehörden in mehreren Mitgliedstaaten und den entsprechenden Auswirkungen auf die Privatsphäre der EU-Bürger (2013/2682(RSP)) sowie den Text einer Beschwerde vor dem EGMR gegen das Vereinigte Königreich wegen des Erhalts ausländischer Überwachungsdaten und des TEMPORA-Programms (58170/13), abrufbar unter https://www.privacynotprism.org.uk/assets/files /privacynotprism/496577_app_No_58170-13_BBW_ORG_EP_CK_v_UK_Grounds.pdf, abgerufen am 13.10.2013.

[24] EGMR 09. 06. 1978, 5029/71, *Klass* (Rz.49).

[25] EGMR 04.05.2000, 28341/95, *Rotaru* (Rz. 57).

[26] EGMR 29.06.2006, 54934/00, *Weber* (Rz. 93), m.w.N.

[27] EGMR 09. 06. 1978, 5029/71, *Klass* (Rz.59).

des Rechtsordnung der USA[28] gegenüber den Grundsätzen. Auch diese Ausnahme lässt an der Grundrechtskonformität der Safe-Harbor-Entscheidung zweifeln, denn die Entscheidung legt es in die Hände der Rechtsordnung der USA, über die Geltung der Grundsätze zu entscheiden. Somit basiert die Entscheidung auf einer variablen – und wie sich gezeigt hat zum Teil auch geheimen – Grundlage, nämlich der Rechtsordnung der USA. Das durch die Entscheidung anerkannte Datenschutzniveau ist daher nicht genau abschätzbar und der Versuch dessen Angemessenheit ex ante festzustellen muss zumindest als gewagt bezeichnet werden.[29]

## 7 Aufhebung von Safe Harbor?

Die Zuständigkeit, die Safe-Harbor-Entscheidung aufzuheben oder anzupassen, liegt bei der Kommission. Sie hat die Befugnis, gemäß Art. 25 Abs. 4 DSRL festzustellen, dass ein Drittland kein angemessenes Schutzniveau aufweist. In Art. 4 der Entscheidung ist deren Anpassung durch die Kommission vorgesehen. Die Kommission hat diesbezüglich eine Untersuchung in Auftrag gegeben [EC13]. Jeder Mitgliedstaat, das Europäische Parlament oder der Rat haben die Möglichkeit, vor dem EuGH gegen die Safe-Harbor-Entscheidung Nichtigkeitsklage gem. Art. 263 AEUV zu erheben, mit der Begründung, dass diese gegen Unionsrecht verstößt. Dies lässt sich auf obige Argumentation stützen und es ist nicht unwahrscheinlich, dass es zu einer solchen Klage kommt. Somit ist die Entscheidung „von Aufhebung bedroht“ und es ist insgesamt unwahrscheinlich, dass Safe Harbor langfristig unverändert weiterbesteht. Auch die Bestrebungen zum Beschluss einer Datenschutzgrundverordnung – über die derzeit nicht gesagt werden kann, ob, wann und mit welchem Inhalt sie beschlossen wird – stützen dieses Ergebnis.

Kurzfristig können auch die nationalen Datenschutzbehörden autonom und einzelfallbezogenen Datenübermittlungen im Rahmen von Safe Harbor untersagen, wie von der deutschen Datenschutzkonferenz angedeutet [Dk13]. Art. 3 Abs. 1 der Entscheidung gibt ihnen die Möglichkeit die Datenübermittlung im Einzelfall auszusetzen, wenn eine hohe Wahrscheinlichkeit besteht, dass die Grundsätze verletzt werden. Zu beachten ist auch, die genehmigungsfreie Übermittlung gemäß Art. 25 Abs. 1 DSRL nur vorbehaltlich der Beachtung der aufgrund der anderen Bestimmungen dieser Richtlinie erlassenen einzelstaatlichen Vorschriften gilt. Eine solche Vorschrift ist in Österreich die Bestimmung des § 7 Abs. 2 Z. 3 DSG 2000, die Übermittlungen generell nur dann zulässt, wenn „durch Zweck und Inhalt der Übermittlung die schutzwürdigen Geheimhaltungsinteressen des Betroffenen nicht verletzt werden“, und in Deutschland § 4b Abs. 2 BDSG[30], wonach die „Übermittlung unterbleibt, soweit der Betroffene ein schutzwürdiges Interesse an

[28] Wie sich jedenfalls aus der Zusammenschau mit Anhang IV ergibt, ist hier die Rechtsordnung der USA und nicht etwa jene der EU gemeint.
[29] Hinsichtlich der Verantwortung der Auftraggeber argumentiert die irische Datenschutzbehörde hierzu in einer Reaktion auf die bereits erwähnte Beschwerde gegen Apple (abrufbar unter http://www.europe-v-facebook.org/Response_23_7_2013.pdf, abgerufen am 13.10.), Zugriff auf personenbezogene Daten für Zwecke der Strafverfolgung sei im Safe-Harbor-Programm vorhergesehen und ohnehin behandelt worden. Wie soeben ausgeführt trifft dies zu, sagt aber nichts über die Zulässigkeit der Safe-Harbor-Entscheidung aus.
[30] Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), das zuletzt durch Artikel 1 des Gesetzes vom 14. August 2009 (BGBl. I S. 2814) geändert worden ist.

dem Ausschluss der Übermittlung hat.“ Auf Basis dieser Bestimmungen können die nationalen Datenschutzbehörden einzelne Datenübermittlungen untersagen, von denen sie aufgrund der allgemeinen Meldepflicht (§ 17 DSG 2000 bzw. § 4d BDSG) Kenntnis haben. Dies ist nicht zu verwechseln mit der Genehmigung, die bei Anwendung von Safe Harbor – oder der Standardvertragsklauseln – nicht erforderlich ist [Pi13].

## 8 Der Zugriff der US-Behörden

Bevor wir aus diesen rechtlichen Möglichkeiten die Schlussfolgerungen ziehen, soll der Blickwinkel noch etwas erweiterter werden, um zu klären, ob Safe Harbor in der Frage des Schutzes vor unverhältnismäßiger US-Überwachung überhaupt jenen Stellenwert hat, der im derzeit in der politischen Debatte eingeräumt wird. Nicht nur Safe Harbor ermöglicht den US-Behörden Zugriff auf Daten europäischer Nutzer. Dies soll im Folgenden anhand dreier Szenarien verdeutlicht werden. Die meisten großen US-IT-Unternehmen haben europäische Tochterunternehmen. Die Vertragsbeziehungen der europäischen Kunden kommen mit diesen europäischen Tochterunternehmen zustande. Mit anderen Worten, für europäische Nutzer sind Facebook, Microsoft, etc. europäische Unternehmen. Diese europäischen Tochterunternehmen nutzen im Rahmen ihrer Diensterbringung häufig die IT-Infrastruktur ihrer US-Konzernmütter, sodass personenbezogene Daten der europäischen Nutzer auf Server in die USA übermittelt werden (Szenario I). Dazu ist eine rechtliche Grundlage erforderlich, wie sie insbesondere durch Safe Harbor besteht. Mittlerweile haben manche dieser Unternehmen aber auch Server in Europa, z.B. Microsoft [Ba11]. Werden Daten europäischer Nutzer auf diesen Servern gespeichert und kann gewährleistet werden, dass diese Daten „Europa nicht verlassen“ (Szenario II), dann ist dies kein Anwendungsfall von Safe Harbor. In Szenario III schließlich besteht kein Tochterunternehmen in der EU und der europäische Nutzer übermittelt seine Daten direkt an ein US-Unternehmen.

In den Szenarien I und III ist die Zugriffsmöglichkeit durch US-Behörden offensichtlich. Hinsichtlich Szenario II blieb in der Diskussion der letzten Monate über Safe Harbor folgender Aspekt häufig unbeachtet: US-Unternehmen sind nach US-Recht auch dann verpflichtet, US-Behörden Zugang zu den von ihnen gespeicherten Nutzerdaten zu gewähren, wenn diese nicht auf Servern gespeichert sind, die sich auf dem Territorium der USA befinden [Ba11]. Regelmäßig werden die Unternehmen in Szenario II wohl dieser Pflicht nachkommen, auch wenn sie dabei gegen europäisches Datenschutzrecht verstoßen.[31] Somit ist die Übermittlung von Daten europäischer Betroffener auf US-Server nicht das Entscheidende. Die Nutzung von Services von US-Unternehmen unterliegt in jedem Fall den Überwachungsbefugnissen der US-Behörden. Faktisch macht es somit keinen Unterschied, ob und auf welcher rechtlichen Grundlage man diese Daten auf US-Server übermittelt. Wie auch immer die Zukunft von Safe Harbor aussehen wird, solange die Überwachungsbefugnisse der US-Behörden unverändert bleiben, kann man Daten, die von US-Unternehmen verarbeitet werden, dem Zugriff dieser Behörden nicht entzie-

[31] Die nähere Analyse dieser Situation und der Möglichkeiten, sie zu verbessern, würde den Rahmen dieses Beitrags sprengen. Es wäre lohnenswert, dies in einem gesonderten Beitrag zu behandeln.

hen. Der US-Überwachung kann nur entgehen, wer keine Services von US-Unternehmen nutzt, was derzeit im US-dominierten Internet unrealistisch ist.

## 9 Schlussfolgerungen

Wie sich gezeigt hat, weist Safe Harbor nach wie vor große Umsetzungsschwächen auf und ist – wenn nicht schon bisher, dann spätestens seit den Enthüllungen Edward Snowdens – mit europäischen Grundrechten unvereinbar. Zudem bestehen berechtigte Zweifel an der Kompetenz der EU-Kommission zur Erlassung der Safe-Harbor-Entscheidung. Diese Gründe sprechen für die Aufhebung der Safe-Harbor-Entscheidung durch die Kommission, auch weil ansonsten deren Aufhebung durch den EuGH droht.

Dabei ist jedoch zu bedenken, dass ein wesentlicher Teil des Datentransfers zwischen der EU und den USA ohne Safe Harbor keine rechtliche Grundlage mehr hätte und somit ein großer Teil der Nutzung der Dienste der bedeutendsten Unternehmen der IT-Branche durch europäische Nutzer von einem solchen Schritt betroffen wäre. Aus diesem Grund sowie angesichts des Ergebnisses der obigen Analyse zum estoppel-Prinzip erscheint es aus praktischen Erwägungen nicht sinnvoll, Safe Harbor so rasch als möglich außer Kraft zu setzen, selbst wenn dies rechtlich geboten erschiene. Wie gezeigt wurde, ist Safe Harbor zudem nur einer von zahlreichen Aspekten des NSA-Skandals und ein Ende von Safe Harbor kann an der Überwachung europäischer Nutzer von US-Unternehmen durch US-Behörden nichts ändern. Einerseits zeigt Szenario II oben, dass Daten faktisch nicht nur dann dem Zugriff der US-Behörden unterliegen, wenn sie – z.B. auf Basis von Safe Harbor – in die USA übermittelt werden. Andererseits ist Safe Harbor nicht die einzige Rechtsgrundlage für rechtmäßige Datenübermittlung in die USA und jede solche Datenübermittlung führt zur Zugriffsmöglichkeit der US-Behörden. Hinzu kommt, dass nicht nur US-Geheimdienste, sondern auch Geheimdienste europäischer Staaten unverhältnismäßige Überwachungsmaßnahmen durchführen.

Im Hinblick auf die USA ist überwiegend die US-Rechtsordnung (und die dortige Rechtspraxis) entscheidend, um die Überwachungssituation zu verbessern. In dieser Hinsicht könnte sich Safe Harbor doch als geeigneter Ansatzpunkt erweisen, jedoch nicht aus unionsrechtlich-dogmatischer sondern aus völkerrechtlicher Sicht: Es sollte versucht werden, auf Basis der bestehenden Safe-Harbor-Vereinbarung mit den USA eine Nachfolgeregelung zu verhandeln, welche die Befugnisse der US-Behörden klar definiert und begrenzt. Dies erscheint nicht völlig unrealistisch. Auch in den Fällen SWIFT und PNR geschah die Datensammlung durch US-Behörden zunächst verdeckt und im Widerspruch zu europäischen Grundrechten und wurde dann mittels Abkommen durch beiderseitige Zugeständnisse auf eine rechtliche Grundlage gestellt.

## Literaturverzeichnis


[Ba11] Barnitzke, B.: Microsoft: Zugriff auf personenbezogene Daten in EU-Cloud auf Grund US Patriot Act möglich. MMR-Aktuell 2011, 321103.

[CM07] Cottier, T.; Müller, J.P.: Estoppel. In (Wolfrum, R., Hrsg.): Max Planck Encyclopedia of Public International Law. Oxford University Press, Oxford, 2007.

[Co08] Connolly, Ch.: The US Safe Harbor - Fact or Fiction? (2008). Galexia, Pymont, 2008, abrufbar unter http://www.galexia.com/public/research/assets/safe_harbor_fact_or_fiction_2008/safe_harbor_fact_or_fiction.pdf, abgerufen am 13.10.2013.

[Co13] Connolly, Ch.: EU/US Safe Harbor – Effectiveness of the Framework in relation to National Security Surveillance, Speaking Notes, 07. Oktober 2013, abrufbar unter http://www.europarl.europa.eu/document/activities/cont/201310/20131008ATT72504/20131008ATT72504EN.pdf, abgerufen am 14.10.2013.

[DAP04] Dhont, J.; Asinari, M.V.P.; Poullet, Y.: Safe Harbour Decision Implementation Study, at the request of the European Commission, Internal Market DG. Namur, 2004, abrufbar unter http://ec.europa.eu/justice/policies/privacy/docs/studies/safe-harbour-2004_en.pdf, abgerufen am 13.10.2013

[Dk13] Datenschutzkonferenz: Geheimdienste gefährden massiv den Datenverkehr zwischen Deutschland und außereuropäischen Staaten, Pressemitteilung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24. Juli 2013, abrufbar unter http://www.bfdi.bund.de/DE/Home/homepage_Kurzmeldungen2013/PMDerDSK_SafeHarbor.html?nn=408908%29, abgerufen am 13.10.2013.

[EC13] European Commission: Informal Justice Council in Vilnius, MEMO/13/710, 19. Juli 2013. abrufbar unter http://europa.eu/rapid/press-release_MEMO-13-710_en.htm, abgerufen am 13.10.2013.

[Ge04] Genz, A.: Datenschutz in Europa und den USA: Eine rechtsvergleichende Untersuchung unter besonderer Berücksichtigung der Safe-Harbor-Lösung. Deutscher Universitäts-Verlag, Wiesbaden, 2004.

[GS12] Gola, P.; Schomerus, R.: BDSG Bundesdatenschutzgesetz, 11. Auflage. Beck, München 2012.

[MC13] Mayer-Schönberger, V.; Cukier, K.: Big Data: A Revolution That Will Transform How We Live, Work and Think. John Murray, London, 2013.

[Pi13] Pilz, C.: Abkommen, Vertrag, Beschluss – Was ist Safe-Harbor?. Blogeintrag vom 28. Juli 2013, abrufbar unter http://www.delegedata.de/2013/07/abkommen-vertrag-beschluss-was-ist-safe-harbor/, abgerufen am 06.10.2013.

[PS13] Perlroth, N.: Shane, S.: As F.B.I. Pursued Snowden, an E-Mail Service Stood Firm. New York Times, 02. Oktober 2013, abrufbar unter http://www.nytimes.com/2013/10/03/us/snowdens-e-mail-provider-discusses-pressure-from-fbi-to-disclose-data.html?_r=1&, abgerufen am 08.10.2013.

[Ro09] Robertson, S.: Byte - US Prosecution for false web claim of Safe Harbor status. Galexia.com, 11. September 2009, abrufbar unter http://www.galexia.com/public/research/articles/research_articles-byte08.html, abgerufen am 14.10.2013.

[SH12] Schweighofer, E.; Hötzendorfer, W.: Elektronische Identitäten – Öffentliche und private Initiativen. In (von Lucke, J., Geiger, C.P., Kaiser, S., Schweighofer, E., Wimmer, M.A., Hrsg.): Auf dem Weg zu einer offenen, smarten und vernetzten Verwaltungskultur. Gemeinsame Fachtagung Verwaltungsinformatik (FTVI) und Fachtagung Rechtsinformatik (FTRI) 2012, GI-Edition Lecture Notes in Informatics, GI, Bonn 2012; S. 137-148.