# Privacy Shield – kein grundrechtskonformer Ersatz für Safe Harbor

Dokumentation und Bewertung

**Stand: 23.02.2016**

## Inhalt




**Dr. Thilo Weichert**
Waisenhofstraße 41, 24103 Kiel
0431 9719742
weichert@netzwerk-datenschutzexpertise.de

**Karin Schuler**
Kronprinzenstr. 76, 53173 Bonn
0228/24 20 733
schuler@netzwerk-datenschutzexpertise.de

www.netzwerk-datenschutzexpertise.de

Mit Urteil vom 06.10.2015 hat der Europäische Gerichtshof (EuGH) die Safe-Harbor-Entscheidung der EU-Kommission aus dem Jahre 2010 aufgehoben, mit der US-Unternehmen über eine inhaltlich nicht überprüfte Selbstzertifizierung Daten aus Europa importieren konnten (C-362/14, künftig zitiert als Safe-Harbor-Urteil).[1] Die Aufnahme in die resultierende Safe-Harbor-Liste wurde antragstellenden Unternehmen in der Regel innerhalb eines Tages nach Antragstellung ohne effektiven Nachweis eines angemessenen Datenschutzniveaus – weder im Unternehmen noch in den USA- erteilt.

Eine sinngemäße Anwendung der durch den EuGH formulierten Anforderungen bzw. Mängel legt den Schluss nahe, dass auch die durch die EU-Kommission verabschiedeten Standardvertragsklauseln keinen Bestand haben können.

Viele europäische Unternehmen transferieren jedoch im Rahmen ihrer betrieblichen Prozesse personenbezogene Daten in die USA und sind daher auf eine tragfähige, mit europäischem Recht vereinbare Lösung angewiesen. Es bestand die Hoffnung, dass das Urteil des EuGH die Verhandlungen zwischen EU und USA über eine (bessere) Nachfolgeregelung für Safe Harbor befördern würde.

Das Gegenteil ist der Fall, wie das Netzwerk Datenschutzexpertise in der vorliegenden Dokumentation darlegt.

## 1 Reaktionen auf das Safe-Harbor-Urteil

Die Datenschutzbehörden in der Artikel-29-Arbeitsgruppe hatten der EU-Kommission eine Frist für Verhandlungen mit den USA bis Ende Januar 2016 gesetzt, um eine rechtskonforme Lösung für die Übermittlung personenbezogener Daten von Europa in die USA zu finden.

In ihrem Statement vom 16.10.2015 hatte die Artikel-29-Arbeitsgruppe erklärt: „Falls bis Ende Januar 2016 noch keine angemessene Lösung in Zusammenarbeit mit den US-Behörden gefunden wurde und je nachdem, wie die Einschätzung der Datenschutzgruppe zu den Übermittlungsinstrumenten aussieht, sind die EU-Datenschutzbehörden verpflichtet, alle notwendigen und angemessenen Maßnahmen zu ergreifen, einschließlich koordinierter Durchsetzungsmaßnahmen."

## 2 Statement der EU-Kommission vor dem EU-Parlament

Am 01.02.2016, also kurz nach Ablauf der Frist, erklärte die EU-Kommissarin Vera Jourová gegenüber dem Innen- und Rechtsausschuss des EU-Parlaments, dass zwischen der EU und den USA eine Lösung gefunden worden sei:

„Am 6. November letzten Jahres setzte sich die Kommission das Ziel, einen robusten Rechtsrahmen innerhalb von 3 Monate zu etablieren. Wir stellten klar, dass der neue Rahmen umfassend den Anforderungen der Gerichtsentscheidung entsprechen müsse. Wir brauchen eine Vereinbarung, die sich von der aufgehobenen alten zu Safe Harbor vollständig unterscheidet. Wir werden eine dauernde Überprüfung und eine Überprüfung der neuen Vereinbarung sicherstellen. Es kann keine Entscheidung ein-für-alle-Mal wie vor 16 Jahren geben.

[1] https://www.bfdi.bund.de/SharedDocs/Publikationen/EU/Art29Gruppe/SafeHarbor_EuGHUrteilOktober2015.pdf?__blob=publicationFile&v=2

Die letzten Monate haben wir intensiv mit den USA zusammengearbeitet, um die nötigen Zusagen und Klarstellungen zu erhalten, mit denen eine neue, den rechtlichen Anforderungen entsprechende Vereinbarung umgesetzt werden kann.

Die Entscheidung über die Angemessenheit ist eine einseitige Entscheidung. Um diese zu erreichen, benötigen wir starke Zusagen von den USA.

Wir haben unseren amerikanischen Partnern klargemacht, dass eine neue Angemessenheitsentscheidung im Fall einer erneuten gerichtlichen Überprüfung bestehen muss. Dies liegt im Interesse des Grundrechtsstandards, aber auch der Gewährleistung von der Rechtssicherheit für die Wirtschaft.

Die Verhandlungen dauern – auch auf politischer Ebene – an. Letztes Wochenende gab es sehr intensive Gespräche. Im Kollegium der Kommissionsmitglieder wird die Sache morgen erörtert werden, so dass ich noch nicht ins Detail gehen kann. Lassen Sie mich Ihnen aber einen Überblick über die zentralen Themen und den Sachstand geben:

Meine Bemerkungen konzentrieren sich auf vier zentrale Aussagen des Urteils:

- die Notwendigkeit von Begrenzungen und Vorkehrungen beim Datenzugriff durch staatliche Stellen,
- die unabhängige Kontrolle und die individuelle Beschwerdemöglichkeit im Bereich der nationalen Sicherheit,
- die Klärung individueller Beschwerden über die Datenverarbeitung von Unternehmen und
- die Notwendigkeit verbindlicher Zusagen auf US-Seite.
- Lassen Sie mich mit den Begrenzungen und Vorkehrungen beim Datenzugriff durch staatliche Stellen beginnen:
-

Wie Sie wissen, stellte das Schrems-Urteil klar, dass ein solcher Zugriff auf das streng Notwendige begrenzt werden muss. Lassen Sie mich zunächst daran erinnern, dass sich der US-Rechtsrahmen seit den Snowden-Enthüllungen weiterentwickelt hat. Es gab wichtige Reformen unter Präsident Obama, mit denen mehr Transparenz und eine strengere Aufsicht eingeführt wurden. Bei unseren Verhandlungen erhalten wir nun schriftliche Zusicherungen von den USA, dass der Zugriff staatlicher Stellen auf von Europa übermittelte personenbezogene Daten auf das Notwendige und Verhältnismäßige beschränkt werden wird. Diese Zusicherungen müssen bestätigen, dass es keine unterschiedslose Massenüberwachung gibt und die Schutzmechanismen auch auf Nicht-US-Bürger anwendbar sind. Lassen Sie mich klarstellen, dass wir die Entwicklungen in diesem Bereich auch in der Zukunft weiter beobachten müssen. Wir brauchen Vertrauen, doch wir haben auch die Pflicht zur Kontrolle. Wir werden eine gemeinsame jährliche Überprüfung einführen, die sämtliche Aspekte, einschließlich den Datenzugriff durch staatliche Stellen, betrachtet.

Zum zweiten Bereich: die unabhängige Kontrolle und die individuelle Beschwerdemöglichkeit. Wenn wir es mit nationaler Geheimdiensttätigkeit zu tun haben, sind die Möglichkeiten rechtlicher Kontrolle eingeschränkt.

Über eine funktional unabhängige Stelle müssen wir gewährleisten, dass diese individuelle Beschwerden von Europäern beantwortet, wenn diese befürchten, dass ihre personenbezogene Daten unrechtmäßig von US-Behörden im Bereich der nationalen Sicherheit verwendet wurden. Die Stelle erhält Zugang zu Informationen der nationalen Sicherheitsbehörden. Denkbar ist eine Ombudsperson mit realen Handlungsmöglichkeiten, die auf individuelle Beschwerden hin Antworten gibt.

Ich will nun zur Klärung individueller Beschwerden über die Datenverarbeitung von Unternehmen im Fall von Datenschutzverstößen kommen.

Wir arbeiten an einer Vereinbarung, die – auf dem einen oder anderen Weg – eine Klärung jeder individuellen Beschwerde herbeiführt:

- Idealerweise wird, wie die Erfahrung zeigt, die Beschwerde durch das Unternehmen selbst geklärt.
- Gelingt dies nicht, so kann der Bürger eine alternative gebührenfreie Streitbeilegung in Anspruch nehmen.
- Der Bürger kann auch zur Datenschutzbehörde gehen, die Beschwerden an das US-Handelsministerium bzw. an die Federal Trade Commission weiterleitet.
- Es kann dessen ungeachtet ungeklärte Beschwerden geben, die nicht von der Federal Trade Commission aufgegriffen werden. (Die FTC greift strategische Themen auf und bearbeitet weniger individuelle Beschwerden.)
- Deshalb arbeiten wir an einem Mechanismus des „letzten Auswegs“ um sicherzustellen, dass alle Beschwerden mit einer bindenden und durchsetzbaren Entscheidung beendet werden.
- Dies ist für eine neue Vereinbarung wesentlich, da der Anspruch auf gerichtlichen Rechtsschutz in unserer Grundrechtecharta garantiert wird.

Lassen Sie mich betonen, dass die europäischen Datenschutzbehörden in einer neuen Vereinbarung eine aktive Rolle haben müssen. Sie sind gemäß der Charta die Hüter des individuellen Schutzes personenbezogener Daten. Sie müssen die Möglichkeit haben Beschwerden weiterzugeben – unabhängig davon, ob sich diese auf kommerzielle Aspekte beziehen oder auf die nationale Sicherheit – und die Rechte der Europäer hochhalten, deren Daten in die EU übermittelt werden (gemeint sind wohl die USA, T. W.).

Schließlich benötigen wir von den USA förmliche und bindende Verpflichtungen. Dies wird kein internationales Abkommen sein, sondern ein Austausch von Briefen, die von höchster politischer Ebene unterzeichnet und im Federal Register als Verpflichtung veröffentlicht werden.

Zusammengefasst: Wir haben hart daran gearbeitet, von den USA Zusagen zu erhalten um sicherzustellen, dass die neue Vereinbarung den Anforderungen des Gerichtsurteils genügt.“[2]

[2] Übersetzung Thilo Weichert, Originaltext in Englisch auf http://europa.eu/rapid/press-release_SPEECH-16-208_en.htm

# 3 Presseerklärung der EU-Kommission zum EU-US-Datenschutzschild („Privacy Shield“)

Am darauffolgenden Tag, also am 02.02.2016, veröffentlichte die EU-Kommission eine Presseerklärung, die im Folgenden auszugsweise dokumentiert wird:

**„Kommission und Vereinigte Staaten einigen sich auf neuen Rahmen für die transatlantische Datenübermittlung: den EU-US-Datenschutzschild**

Das Kollegium der Kommissionsmitglieder hat die politische Einigung heute gebilligt und Vizepräsident Ansip und Kommissarin Jourová den Auftrag erteilt, die notwendigen Schritte zur Einführung der neuen Regelung in die Wege zu leiten. Der neue Rahmen gewährleistet den Schutz der Grundrechte der europäischen Bürgerinnen und Bürger bei der Übermittlung von Daten in die USA und schafft Rechtssicherheit für die Unternehmen. ...

Die neue Regelung umfasst folgende Elemente:

- **Strenge Auflagen für Unternehmen, die personenbezogene Daten europäischer Bürgerinnen und Bürger verarbeiten, sowie konsequente Durchsetzung:**

US-amerikanische Unternehmen, die personenbezogene Daten aus Europa importieren wollen, müssen sich dazu verpflichten, sich an strenge Auflagen bezüglich der Art der Verarbeitung personenbezogener Daten und des Schutzes der Rechte einzelner Personen zu halten. Das US-Handelsministerium wird dafür sorgen, dass die Unternehmen diese Selbstverpflichtungen auch veröffentlichen, damit sie nach US-Recht von der Federal Trade Commission durchgesetzt werden können. Darüber hinaus müssen sich alle Unternehmen, die mit Personaldaten aus Europa arbeiten, dazu verpflichten, Entscheidungen der europäischen Datenschutzbehörden nachzukommen.

- **Klare Schutzvorkehrungen und Transparenzpflichten bei Zugriff durch US-Regierung:**

Zum ersten Mal haben die USA der EU schriftlich zugesichert, dass der Zugriff von Behörden auf solche Daten aus Gründen der Rechtsdurchsetzung oder der nationalen Sicherheit nur unter Einhaltung klarer Beschränkungen, Schutzvorkehrungen und Aufsichtsmechanismen gestattet sein wird. Ein solcher Zugriff muss die Ausnahme bleiben und darf nur erfolgen, soweit er notwendig und verhältnismäßig ist. Die USA haben eine willkürliche Massenüberwachung der im Rahmen der neuen Regelung in die USA übermittelten personenbezogenen Daten ausgeschlossen. Um zu gewährleisten, dass die Regelung auch funktioniert, wird es eine jährliche gemeinsame Überprüfung geben, bei der auch die Frage des Zugriffs durch nationale Behörden thematisiert wird. Die Europäische Kommission und das US-amerikanische Handelsministerium werden diese Überprüfung gemeinsam durchführen und Sachverständige der US-Nachrichtendienste und der Europäischen Datenschutzbehörden hinzuziehen.

- **Wirksamer Schutz der Rechte der EU-Bürgerinnen und -Bürger durch verschiedene Rechtsbehelfe:**

Ist eine Person der Auffassung, dass ihre Daten gemäß der neuen Regelung missbraucht wurden, stehen ihr mehrere Möglichkeiten offen: Unternehmen müssen Beschwerden innerhalb bestimmter Fristen beantworten. Die europäischen Datenschutzbehörden können Beschwerden an das Handelsministerium und die Federal Trade Commission weiterleiten. Darüber hinaus steht ein

kostenloses Verfahren zur alternativen Streitbeilegung zu Verfügung. Für Beschwerden, die den möglichen Zugriff nationaler Nachrichtendienste betreffen, wird eine neue Ombudsstelle eingerichtet.

**Nächste Schritte**

Das Kollegium hat Vizepräsident Ansip und Kommissarin Jourová heute beauftragt, in den kommenden Wochen einen „Angemessenheitsbeschluss" zu entwerfen, den das Kollegium nach Stellungnahme der gemäß Artikel 29 eingesetzten Datenschutzgruppe und nach Anhörung eines Ausschusses, der sich aus Vertretern der Mitgliedstaaten zusammensetzt, annehmen kann. In der Zwischenzeit treffen die USA die notwendigen Vorkehrungen zur Einrichtung des neuen Rahmens, der neuen Überwachungsmechanismen und der neuen Ombudsstelle."[3]

In einer Erklärung vom 02.02.2016 bestätigte das **US-Wirtschaftsministerium** die Verkündigungen der EU-Kommission, ohne aber präziser zu werden. Interessant ist dessen Aussage zur Kontrolle der geheimdienstlichen Datennutzung:

„Im Zusammenhang mit der Fertigstellung des neuen EU-US-Datenschutzschilds beschreiben die US-Geheimdienste der Europäischen Kommission schriftlich die verfassungsrechtlichen, gesetzlichen und politischen Sicherungen, die auf ihre Maßnahmen anzuwenden sind und die unter der Aufsicht von allen drei Sektoren der US-Regierung stehen.

Das Datenschutzschild eröffnet erstmals für EU-Bürgerinnen und -Bürger einen spezifischen Kanal, um Fragen zu stellen zur telekommunikativen Überwachung, soweit diese vom Datenschutzschild betroffen ist. Als Teil dieses Verfahrens sichern die US zu, in diesen Angelegenheiten geeignete Fragen im Einklang mit unseren nationalen Sicherheitsverpflichtungen zu beantworten."[4]

## 4 Die Antwort der Artikel-29-Arbeitsgruppe

Wer nun vermutete, dass die Artikel-29-Arbeitsgruppe (29 Workingparty = WP29) die Ausführungen der Kommission als zu unkonkret und zu wenig weitgehend zurückweist, wurde enttäuscht. Am 03.02.2016 veröffentlichte sie vielmehr die **Erklärung der Artikel-29-Arbeitsgruppe zu den Konsequenzen des Schrems-Urteils**:

„Die WP29 begrüßt den Umstand des Abschlusses von Verhandlungen zwischen der EU und den USA über die Einführung eines „EU-US-Datenschutzschilds" (EU-U.S.-Privacy Shield), womit die Frist eingehalten wird, die die WP29 in ihrer Erklärung vom 16. Oktober festlegte. Sie freut sich darauf, die relevanten Dokumente zu erhalten, um den Inhalt und die rechtliche Verbindlichkeit genau zur Kenntnis nehmen und um bewerten zu können, ob sie den weitgehenden Bedenken in Bezug auf die internationale Datenübermittlung im Schrems-Urteil genügen. […]

Auch wenn die WP29 anerkennt, dass die USA 2014 und 2015 sich bemüht hat, den Datenschutz für Nicht-US-Bürger zu verbessern, hat sie in Bezug auf den bestehenden US-Rechtsrahmen weiterhin Bedenken hinsichtlich der vier wichtigen Gewährleistungen, insbesondere im Hinblick auf den Anwendungsbereich und den Rechtsschutz.

[3] Quelle: http://europa.eu/rapid/press-release_IP-16-216_de.htm
[4] Übersetzung Thilo Weichert, Original in Englisch unter https://www.commerce.gov/news/fact-sheets/2016/02/eu-us-privacy-shield

Nach der Pressekonferenz der Europäischen Kommission über das EU-US-Datenschutzschild am 2. Februar 2016 ist die WP29 bereit, das Verhandlungsergebnis im Lichte der oben beschriebenen wesentlichen Garantien zu analysieren. Besondere Berücksichtigung wird finden, ob mit der Einführung des EU-US-Datenschutzschilds die Bedenken in Bezug auf den US-Rechtsrahmen abgemildert werden können. […]

Die WP29 fordert die Kommission auf, sämtliche Dokumente zu dem neuen Übereinkommen bis Ende Februar zu übermitteln. Die WP29 wird dann in der Lage sein, ihre Bewertung aller personenbezogenen Datenübermittlungen in die USA in einer außerplanmäßigen Sitzung abzuschließen, die in den kommenden Wochen vorbereitet wird. Danach wird die WP29 beurteilen, ob die Übermittlungsmechanismen wie die Standardvertragsklauseln und die Binding Corporate Rules weiterhin für Datenübermittlungen in die USA verwendet werden können. Derweil geht die WP29 davon aus, dass dies bei den bestehenden Übermittlungsmechanismen weiterhin der Fall ist."[5]

## 5 Reaktionen von Bürgerrechtsorganisationen, Politik und Wirtschaft

Die Reaktionen auf die Ankündigungen zum Datenschutzschild von Bürgerrechtsorganisationen waren durchgehend kritisch[6]. Werner Hülsmann von der Deutschen Vereinigung für Datenschutz (DVD) erklärte: „Solange die schriftliche Zusicherung Washingtons, den Zugang der Sicherheitsbehörden zu Daten von EU-Bürgern klar zu beschränken und besser zu kontrollieren, nicht in ein Gesetz und ein bilaterales Abkommen gegossen werde, ist sie gerade im letzten Jahr der Amtszeit der gegenwärtigen US-Regierung nichts wert." Es bringe nichts, „bindende Zusagen" nur über den Austausch von Briefen machen zu wollen.[7]

Laut der Initiative European Digital Rights (EDRi) hat die Kommission dem Kaiser nur neue Kleider übergestreift. Diese könnten nicht verbergen, dass nicht nur in dem skizzierten, noch völlig unreifen und löchrigen Schutzschild schwere Fehler vorhanden seien, sondern auch in damit zusammenhängenden zusätzlichen Rechtsinstrumenten. EDRi verweist insbesondere auf den Entwurf für den Judical Redress Act, der EU-Bürgerinnen und -Bürgern eigentlich ein Klagerecht in den USA in Datenschutzfragen eröffnen soll (s. u. den Verweis auf die Stellungnahme von Peter Schaar unter 7). Ferner habe der US-Gesetzgeber mit dem Cybersecurity Act Fakten geschaffen, der Unternehmen einen Freibrief zum Datentransfer an nationale Geheimdienste ausstelle.[8]

Konstantin von Notz, Vizefraktionschef der Grünen im Bundestag, sprach von einer „reinen Mogelpackung" und „bloßer Ankündigungspolitik". Die linke EU-Abgeordnete Cornelia Ernst warf der Kommission vor, den Knall der Snowden-Enthüllungen nicht gehört zu haben. Brüssel habe „sich wieder einmal von den USA über den Tisch ziehen lassen". Die Piraten sehen die Kommission

[5] Übersetzung Thilo Weichert, Originalquelle: http://www.cnil.fr/english/news-and-events/news/article/statement-of-the-article-29-working-party-on-the-consequences-of-the-schrems-judgment/

[6] Krempl, "Privacy Shield": Bürgerrechtler schießen scharf gegen geplanten Datenschutzschild, http://www.heise.de/newsticker/meldung/Privacy-Shield-Buergerrechtler-schiessen-scharf-gegen-geplanten-Datenschutzschild-3093494.html

[7] https://www.datenschutzverein.de/wp-content/uploads/2016/02/2016-02-03-DVD_zu_EU-US-Privacy_shield.pdf

[8] McNamee, What´s behind the shield? Unspinning the „privacy shield" spin, https://edri.org/privacyshield-unspinning-the-spin/

angesichts der unverbindlichen Versprechungen gar „als Wiederholungstäter bei der Verletzung unserer Grundrechte“.

Auch der ehemalige Bundesdatenschutzbeauftrage Peter Schaar äußerte sich kritisch in einem Interview „Ist das „Privacy Shield“ endlich ein sicherer Hafen?“, http://www.heise.de/newsticker/meldung/Peter-Schaar-Ist-das-Privacy-Shield-endlich-ein-sicherer-Hafen-3091735.html

Der Digitalverband Bitkom begrüßte dagegen die Einigung als „wichtigen Schritt zu mehr Rechtssicherheit beim Datenaustausch mit den USA“. Die US-Regierung müsse nun zu ihrem Wort stehen, die Übereinkunft sich „in der Praxis bewähren“. Laut der American Chamber of Commerce in Deutschland haben die USA und die EU mit den überarbeiteten Transferabkommen „politische Handlungsfähigkeit auf einem zentralen wirtschaftspolitischen Feld bewiesen“. Mittelfristig müsse es aber zu einer Reform der transatlantischen Rechtshilfeabkommen kommen, um „gemeinsame Standards für grenzüberschreitend Zugriffsmöglichkeiten zu entwickeln“. Der eco-Verband der deutschen Internetwirtschaft meinte, entscheidend sei jetzt „eine verbindliche und tragfähige Regelung für die Zukunft, die den Unternehmen Rechtssicherheit garantiert“. Und der Bundesverband Digitale Wirtschaft (BVDW) sieht noch „wesentliche Fragen offen, die für eine rechtssichere Anwendung der neuen Regeln in der Praxis umgehend gelöst werden müssen“.

## 6 Inhaltliche Anforderungen an einen Datentransfer in Drittstaaten

Unglücklicherweise krankt die gesamte Diskussion bis heute an einem entscheidenden Mangel: die Inhalte des großartig angekündigten Privacy Shields sind nicht bekannt und so bleibt nur, sich in der Auseinandersetzung an den undemokratischen Modalitäten des bisherigen Vertragsentwicklungsverfahrens abzuarbeiten.

Besser wäre es natürlich, die Kommission würde es nicht bei vollmundigen aber substanzlosen Erfolgsmeldungen belassen sondern die Inhalte ihrer Vertragsentwürfe bekanntgeben – wie es gute demokratische Tradition wäre. Sie kann wohl selbst von ihrem Verhandlungsergebnis nicht sonderlich überzeugt sein. Wie sonst wäre es zu erklären, dass man sich hinter angeblichen Geheimhaltungserfordernissen verstecken muss? Dieses zutiefst antidemokratische Vorgehen scheint nach den Erfahrungen mit TTIP nun ein weiteres Mal Schule zu machen.

Was aber sind die Inhalte, über die man sich eigentlich stattdessen auseinandersetzen müsste?

Der EuGH hat im **Safe-Harbor-Urteil** sehr präzise die Anforderungen an einen grundrechtskonformen Datentransfer in Staaten außerhalb der EU beschrieben:

„(72) Somit setzt Art. 25 Abs. 6 der Richtlinie 95/46 die in Art. 8 Abs. 1 der Charta ausdrücklich vorgesehene Pflicht zum Schutz personenbezogener Daten um und soll, wie der Generalanwalt in Nr. 139 seiner Schlussanträge ausgeführt hat, den Fortbestand des hohen Niveaus dieses Schutzes im Fall der Übermittlung personenbezogener Daten in ein Drittland gewährleisten.

(73) Zwar impliziert das Wort „angemessen“ in Art. 25 Abs. 6 der Richtlinie 95/46, dass nicht verlangt werden kann, dass ein Drittland ein dem in der Unionsrechtsordnung garantiertes identisches Schutzniveau gewährleistet. Wie der Generalanwalt in Nr. 141 seiner Schlussanträge ausgeführt hat,

ist der Ausdruck „angemessenes Schutzniveau“ jedoch so zu verstehen, dass verlangt wird, dass das Drittland aufgrund seiner innerstaatlichen Rechtsvorschriften oder internationaler Verpflichtungen tatsächlich ein Schutzniveau der Freiheiten und Grundrechte gewährleistet, das dem in der Union aufgrund der Richtlinie 95/46 im Licht der Charta garantierten Niveau der Sache nach gleichwertig ist. Ohne ein solches Erfordernis würde nämlich das in der vorstehenden Randnummer erwähnte Ziel missachtet. Außerdem könnte das durch die Richtlinie 95/46 im Licht der Charta garantierte hohe Schutzniveau leicht umgangen werden, indem personenbezogene Daten aus der Union in Drittländer übermittelt würden, um dort verarbeitet zu werden.

(74) Aus dem ausdrücklichen Wortlaut von Art. 25 Abs. 6 der Richtlinie 95/46 geht hervor, dass es die Rechtsordnung des Drittlands, auf das sich die Entscheidung der Kommission bezieht, ist, die ein angemessenes Schutzniveau gewährleisten muss. Auch wenn sich die Mittel, auf die das Drittland insoweit zurückgreift, um ein solches Schutzniveau zu gewährleisten, von denen unterscheiden können, die in der Union herangezogen werden, um die Wahrung der Anforderungen, die sich aus der Richtlinie im Licht der Charta ergeben, zu gewährleisten, müssen sich diese Mittel gleichwohl in der Praxis als wirksam erweisen, um einen Schutz zu gewährleisten, der dem in der Union garantierten der Sache nach gleichwertig ist.

(75) Unter diesen Umständen ist die Kommission bei der Prüfung des von einem Drittland gebotenen Schutzniveaus verpflichtet, den Inhalt der in diesem Land geltenden, aus seinen innerstaatlichen Rechtsvorschriften oder internationalen Verpflichtungen resultierenden Regeln sowie die zur Gewährleistung der Einhaltung dieser Regeln dienende Praxis zu beurteilen, wobei sie nach Art. 25 Abs. 2 der Richtlinie 95/46 alle Umstände zu berücksichtigen hat, die bei einer Übermittlung personenbezogener Daten in ein Drittland eine Rolle spielen.“

In Randnummer 83 des Safe-Harbor-Urteils stellt der EuGH dann fest, dass die Kommissions-Entscheidung zu Safe-Harbor „keine hinreichenden Feststellungen zu den Maßnahmen (enthält), mit denen die Vereinigten Staaten von Amerika aufgrund ihrer innerstaatlichen Rechtsvorschriften oder internationalen Verpflichtungen im Sinne von Art. 25 Abs. 6 der Richtlinie ein angemessenes Schutzniveau gewährleisten“. Derartige Feststellungen hält der EuGH für erforderlich.

In Art. 41 Abs. 2 Entwurf für eine **EU-DSGVO** (in der Endfassung voraussichtlich Art. 45), worüber am 15.12.2015 im Trilog zwischen dem Parlament, dem Rat und der Kommission der EU Einigkeit hergestellt wurde, werden die künftigen Anforderungen an eine Angemessenheitsentscheidung festgelegt:

„Bei der Prüfung der Angemessenheit des gebotenen Schutzes berücksichtigt die Kommission insbesondere

(a) die Rechtsstaatlichkeit, die Achtung der Menschenrechte und Grundfreiheiten, die in dem betreffenden Drittland bzw. der betreffenden internationalen Organisation geltenden Vorschriften sowohl allgemeiner als auch sektoraler Art, einschließlich solcher, die die öffentliche Sicherheit, die Verteidigung, die nationale Sicherheit, das Strafrecht sowie den Zugang von Behörden zu personenbezogenen Daten betreffen, als auch die Umsetzung dieser Rechtsvorschriften, Datenschutzbestimmungen, Berufsregeln und Sicherheitsvorschriften einschließlich der Vorschriften für die Weitergabe personenbezogener Daten an ein anderes Drittland bzw. eine andere internationale Organisation sowie die Rechtsprechung, wirksame und durchsetzbare Rechte der

betroffenen Person und wirksame administrative und gerichtliche Rechtsbehelfe für betroffene Personen, deren personenbezogene Daten übermittelt werden;

(b) die Existenz und die Wirksamkeit einer oder mehrerer unabhängiger Aufsichtsbehörden in dem betreffenden Drittland oder denen eine internationale Organisation untersteht und die für die Einhaltung und Durchsetzung der Datenschutzvorschriften, einschließlich angemessener Sanktionsbefugnisse, für die Unterstützung und Beratung der betroffenen Personen bei der Ausübung ihrer Rechte und für die Zusammenarbeit mit den Aufsichtsbehörden der Mitgliedstaaten zuständig sind; und

(c) die von dem betreffenden Drittland bzw. der betreffenden internationalen Organisation eingegangenen internationalen Verpflichtungen oder andere Verpflichtungen, die sich aus rechtlich verbindlichen Konventionen oder Instrumenten sowie aus der Teilnahme des Drittlands an multilateralen oder regionalen Systemen insbesondere in Bezug auf den Schutz personenbezogener Daten ergeben."

## 7 Bewertung des Netzwerks Datenschutzexpertise

Das Netzwerk Datenschutzexpertise kritisiert angesichts der klaren Vorgaben des EuGH die Haltung der EU-Kommission wie auch die Artikel-29-Arbeitsgruppe.

Die aktuellen Veröffentlichungen der EU-Kommission zum EU-US-Privacy-Shield sind inhaltlich unkonkret und im Hinblick auf den vom EuGH eingeforderten Rechtsschutz teils nicht überprüfbar, teils schlichtweg ungenügend.

Die Verlautbarung, eine Einigkeit zwischen der EU und den USA sei erreicht worden, ist offenbar nicht verifizierbar, vermutlich inhaltlich falsch. Sie dürfte in zeitlicher Nähe zu der von der Artikel-29-Arbeitsgruppen gesetzten Frist das Ziel verfolgen, eine positives Signal zu senden. Es ist zu bedauern, dass sich die Artikel-29-Arbeitsgruppe auf diese Verzögerungsstrategie eingelassen hat. Es werden weitere Fristen verstreichen, ohne dass den Bürgerinnen und Bürgern in Europa verbindliche Rechtsschutzmöglichkeiten eröffnet werden.

Die Aussage der Artikel-29-Arbeitsgruppe, sie werde die Bewertung der anderen Übermittlungsmechanismen wie Standard-Vertragsklauseln und BCRs weiter hinauszögern, ist nicht verständlich. Diese Mechanismen genügen offensichtlich derzeit nicht den Anforderungen des EuGH an Datenübermittlungen ins Drittausland ohne angemessenes Datenschutzniveau. Das Netzwerk Datenschutzexpertise fordert die europäischen Datenschutzaufsichtsbehörden auf, gegen nicht-EuGH-konforme Standardverträge und BCRs vorzugehen, nachdem die von die von ihnen selbst gesetzte Frist verstrichen ist. Der EuGH hat betont, dass jede Datenschutzaufsichtsbehörde unabhängig ist (Safe-Harbor-Urteil, Rn. 41 ff.). Dies bedeutet, dass die neu eingeräumten Fristen der Artikel-29-Arbeitsgruppe für einzelne Aufsichtsbehörden nicht verbindlich sein können.

Die Ankündigungen der EU-Kommission zum Rechtsschutz vor Massenüberwachung im Interesse der nationalen Sicherheit als Bestandteil des Privacy-Shields genügen nicht den EuGH-Anforderungen. Der EuGH hat unmissverständlich klargestellt, dass sowohl eine betroffene Person als auch eine Datenschutzbehörde ein Klagerecht haben müssen, was für die Betroffenen in Art. 47 der Europäischen Grundrechte-Charta (EuGRCh) gewährleistet wird (Safe-Harbor-Urteil, Rn. 64, 65). Dieses

Recht wird nicht durch Anforderungen der nationalen Sicherheit eingeschränkt, schon gar nicht durch Sicherheitsinteressen der USA. Dieses Klagerecht darf auch nicht auf die Beschwerdeentgegennahme durch eine Ombudsstelle und einen Anspruch auf Antwort reduziert werden, so wie dies von der EU-Kommission angekündigt wurde. Vielmehr muss eine unabhängige richterliche Kontrolle gewährleistet sein. Zwar könne, so das Gericht, ein Zugriff auf europäische Daten erlaubt sein, wenn dies „zum Schutz der nationalen Sicherheit absolut notwendig und verhältnismäßig“ sei (Safe-Harbor-Urteil Rn. 90, 92 f.), allerdings nur unter bestimmten Bedingungen. Insbesondere müssen die Anforderungen an eine ordnungsgemäße richterliche Prüfung im Hinblick auf Unabhängigkeit, Prüftiefe, Transparenz und Verbindlichkeit der Entscheidung auch in Verfahren erfüllt werden, in denen derartige Eingriffe durch andere Institutionen als Gerichte bewilligt werden sollen. Dies ist bei der angekündigten Ombudsstelle erkennbar nicht der Fall.

Weiterhin fordert der EuGH, dass die Daten nach einem behördlichen Zugriff in Bezug auf deren „Nutzung auf bestimmte, strikt begrenzte Zwecke zu beschränken“ ist (Safe-Harbor-Urteil Rn. 93). Hiervon ist in den Verlautbarungen der EU-Kommission keine Rede.

Die Rechtsbehelfe der Betroffenen müssen zudem „wirksam“ sein (Safe-Harbor-Urteil Rn. 93). Dass diese Anforderung nicht erfüllt wird, ist eindeutig erkennbar. Bei der Ombudsstelle werden Antworten angekündigt, keine verbindlichen Entscheidungen. Hinsichtlich der Datenschutzkontrolle bei US-Unternehmen werden formelle, prozedurale und faktische Hindernisse erwähnt, welche die Betroffenen an der Wahrnehmung ihrer Rechte hindern. Das mehrstufige Vorgehen vor US-Institutionen (Beschwerde bei Unternehmen, dann unentgeltliche Konfliktlösung, dann FTC-Anrufung evtl. unter Einschaltung europäischer Datenschutzbehörden, dann Klagemöglichkeit in den USA) entspricht weitgehend dem alten, als unwirksam erkannten Safe-Harbor-Verfahren.

Fehlt eine Möglichkeit, mittels eines Rechtsbehelfs Zugang zu den ihn betreffenden personenbezogenen Daten zu erlangen oder ihre Berichtigung oder Löschung zu erwirken, so wird gegen Art. 47 EuGRCh verstoßen (Safe-Harbor-Urteil Rn. 95). Dieses Recht wird – soweit bisher erkennbar – weder im Hinblick auf den Zugriff staatlicher Behörden noch im Hinblick auf private US-Unternehmen eingeräumt. Die in den USA geplante, bisher noch in der Gesetzgebung befindlichen Regelungen eines Judical Redress Acts (JRA) genügen den Rechtsschutzanforderungen des EuGH nicht.

Zu berücksichtigen ist schließlich, dass anders als die bisherige Safe-Harbor-Entscheidung der Kommission aus dem Jahr 2000 das Datenschutzschild nicht nur für Unternehmen gelten würde, die zuvor einen – wie auch immer gearteten – Zertifizierungsvorgang durchlaufen haben, sondern ohne weitere Beschränkung für alle Stellen in den USA. Als Empfänger von europäischen Daten kämen damit Unternehmen in Betracht, denen die Pflicht, sich an europäischen Datenschutzregeln zu orientieren, noch nicht einmal ansatzweise bewusst ist.

Gemäß der Erklärung der EU-Kommission soll die Verpflichtung der USA durch einen Austausch von Briefen auf der höchsten politischen Ebene erfolgen. Ein verbindliches Abkommen wird ausdrücklich nicht angestrebt. Einem derartigen exekutiven Austausch dürfte nach US-Verfassungsrecht keine legislative Funktion zukommen, welche die Rechtsprechung bindet. Er ist auch nach europäischem Recht nicht zur Legitimation von Eingriffen in die Grundrechte der Art. 7, und 8 EuGRCh geeignet.

Das Netzwerk Datenschutzexpertise plädiert für justitiable Einzelabsprachen zwischen betroffenen Unternehmen und hat zu diesem Zweck einen Export-Import-Vertrag für Datenübermittlungen in

unsichere Staaten vorgelegt, der Betroffenen in Europa Rechtsschutz gewährt. Nach den aktuellen Veröffentlichungen der EU-Kommission drängt das Netzwerk die Datenschutzbehörden, sich diesem Vorschlag zu widmen und ihn an die EU-Kommission heranzutragen. Standardvertragsklauseln und BCRs sollten umgehend auf den Prüfstand gestellt werden und durch valide rechtliche Instrumente ersetzt werden.

Den bisher veröffentlichten Aussagen zum Privacy Shield zufolge entspricht die Übereinkunft nicht den vom EuGH für einen Datenaustausch vorgegebenen Maßstäben. Es ist daher davon auszugehen, dass ein Datenaustausch mit den USA auf Grundlage des Privacy Shields ohne spezielle vertragliche Abmachungen weiterhin nicht rechtskonform ist.