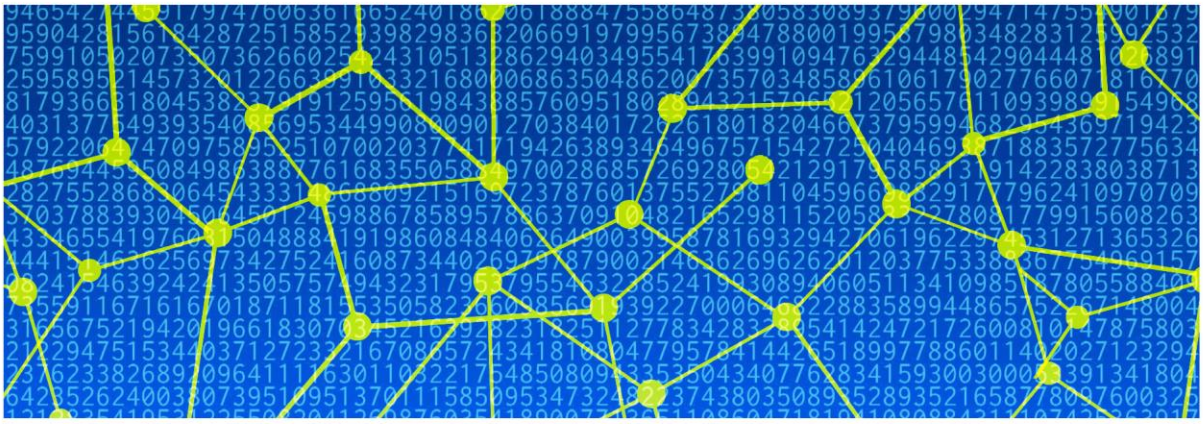

EUROPEAN DATA PROTECTION SUPERVISOR

Stellungnahme 4/2016

Stellungnahme zu „EU-US-Datenschutzschild Entwurf einer Angemessenheits-entscheidung“

EDPS

30. Mai 2016

Der Europäische Datenschutzbeauftragte (EDSB) ist eine unabhängige Einrichtung der EU und hat nach Artikel 41 Absatz 2 der Verordnung (EG) Nr. 45/2001 „im Hinblick auf die Verarbeitung personenbezogener Daten (...) sicherzustellen, dass die Grundrechte und Grundfreiheiten natürlicher Personen, insbesondere ihr Recht auf Privatsphäre, von den Organen und Einrichtungen der Gemeinschaft geachtet werden"; er ist „für die Beratung der Organe und Einrichtungen der Gemeinschaft und der betroffenen Personen in allen die Verarbeitung personenbezogener Daten betreffenden Angelegenheiten" zuständig. Gemäß Artikel 28 Absatz 2 der Verordnung (EG) Nr. 45/2001 ist die Kommission zur Konsultation des EDSB verpflichtet, „wenn [sie] einen Vorschlag für Rechtsvorschriften bezüglich des Schutzes der Rechte und Freiheiten von Personen bei der Verarbeitung personenbezogener Daten annimmt".

Er wurde zusammen mit dem Stellvertretenden Datenschutzbeauftragten im Dezember 2014 ernannt und spezifisch mit einem konstruktiven und proaktiven Vorgehen beauftragt. In der im März 2015 veröffentlichten Fünf-Jahres-Strategie legt der EDSB dar, wie er diesen Auftrag auf verantwortungsvolle Weise zu erfüllen gedenkt.

In dieser Stellungnahme geht es um den Auftrag des EDSB, die EU-Organe bezüglich der Datenschutzimplikationen ihrer Politiken zu beraten und eine verantwortliche Politikgestaltung zu fördern, im Einklang mit Maßnahme 9 der Strategie des EDSB: „Förderung einer verantwortungsvollen und fundierten politischen Entscheidungsfindung".

Zusammenfassung

Datenströme fließen weltweit. Die EU ist gebunden durch die Verträge und die Charta der Grundrechte der Europäischen Union, die alle natürlichen Personen in der EU schützen. Die EU ist verpflichtet, mit allen erforderlichen Maßnahmen zu gewährleisten, dass die Rechte auf Privatsphäre und auf den Schutz personenbezogener Daten bei allen Verarbeitungsvorgängen einschließlich Übermittlungen gewahrt werden.

Seit den 2013 erfolgten Enthüllungen über Überwachungsaktivitäten haben sich die EU und ihr strategischer Partner, die USA, um die Definition neuer, auf einem System von Selbstzertifizierung beruhender Standards für die Übermittlung personenbezogener Daten aus der EU in die USA zu kommerziellen Zwecken bemüht. Wie die nationalen Datenschutzbehörden in der EU erkennt auch der EDSB den Wert eines nachhaltigen Rechtsrahmens für kommerzielle Datenübermittlungen zwischen der EU und den USA, den beiden jeweils größten Handelspartnern weltweit, in einer Zeit globaler, momentaner und unvorhersehbarer Datenströme. Dieser Rahmen muss jedoch umfassender Ausdruck der gemeinsamen demokratischen und auf den Rechten des Einzelnen beruhenden Werte sein, die auf EU-Seite im Vertrag von Lissabon und der Charta der Grundrechte und auf US-amerikanischer Seite in der Verfassung der Vereinigten Staaten verankert sind.

Der Entwurf des Datenschutzschilds mag ein Schritt in die richtige Richtung sein, doch bietet er mit seinem jetzigen Wortlaut unserer Auffassung nach nicht in angemessener Form alle Garantien für den Schutz der EU-Rechte natürlicher Personen in Bezug auf Privatsphäre und Datenschutz, einschließlich gerichtlicher Rechtsbehelfe. Es sind noch erhebliche Verbesserungen erforderlich, sollte die Europäische Kommission eine Angemessenheitsentscheidung annehmen wollen. So sollte die EU insbesondere weitere Zusicherungen bezüglich Notwendigkeit und Verhältnismäßigkeit einholen, anstatt einen routinemäßigen Zugang von US-Behörden auf übermittelte Daten auf der Grundlage von Kriterien zu legitimisieren, die eine Rechtsgrundlage im Empfängerland haben und nicht in der EU, wie dies in den Verträgen, EU-Gerichtsurteilen und den Mitgliedstaaten gemeinsamen verfassungsrechtlichen Traditionen bekräftigt ist.

Darüber hinaus können in einem Zeitalter von hoher „Hyperconnectivity“ und verteilten Netzwerken die Selbstregulierung durch private Organisationen sowie Vertretung und Zusagen durch Amtsträger kurzfristig eine Rolle spielen, während sie langfristig nicht ausreichen würden, die Rechte und Interessen natürlicher Personen zu wahren und in vollem Umfang den Bedürfnissen einer globalisierten digitalen Welt gerecht zu werden, in der sich nunmehr viele Länder Datenschutzrechtsvorschriften festgelegt haben.

Daher wäre eine längerfristige Lösung im transatlantischen Dialog zu begrüßen, auch um in verbindlichem Bundesrecht zu verfügen, dass zumindest die Hauptgrundsätze der Rechte klar und prägnant benannt werden, wie es auch bei anderen Drittländern ist, die in der Frage, ob sie ein angemessenes Schutzniveau bieten, „streng beurteilt“ wurden; was der EuGH in seinem Urteil in der Rechtssache Schrems als den nach EU-Recht geltenden Standards „der Sache nach gleichwertig“ bezeichnet hat, und was nach Ansicht der Artikel 29-Datenschutzgruppe bedeutet, „das Wesen der Grundprinzipien“ des Datenschutzes enthaltend.

Wir nehmen wohlwollend die von den US-Behörden an den Tag gelegte stärkere Transparenz bei der Nutzung der Ausnahme von den Datenschutzschildgrundsätzen in den Bereichen Strafverfolgung, nationale Sicherheit und öffentliches Interesse zur Kenntnis.

In der Safe Harbour-Entscheidung aus dem Jahr 2000 wurde ein Zugriff aus Gründen der nationalen Sicherheit als Ausnahme behandelt, wohingegen die Aufmerksamkeit, die im Entscheidungsentwurf zum Datenschutzschild dem Zugriff, dem Filtern und der Auswertung von für kommerzielle Zwecke übermittelten personenbezogenen Daten durch Strafverfolgungsbehörden und Geheimdienste gewidmet wird, darauf hindeutet, dass die Ausnahme zur Regel geworden ist. Der EDSB entnimmt dem Entwurf der Entscheidung und ihrer Anhänge insbesondere, dass ungeachtet neuerer Tendenzen von der undifferenzierten Überwachung auf allgemeiner Grundlage hin zu gezielteren und ausgewählten Ansätzen der Umfang der Fernmeldeaufklärung und das Volumen von aus der EU übermittelten Daten, die nach der Übermittlung und insbesondere im Transit möglicherweise gesammelt und verwendet werden, nach wie vor sehr groß und damit zu hinterfragen sind.

Auch wenn diese Praktiken darüber hinaus mit Aufklärung in anderen Ländern zu tun haben mag, und auch wenn wir die Transparenz der US-Behörden bezüglich dieser neuen Realität begrüßen, könnte der derzeitige Entscheidungsentwurf diese Vorgehensweise legitimieren. Daher fordern wir die Europäische Kommission auf, ein starkes Signal auszusenden: Mit Blick auf die Verpflichtungen, die sich für die EU aus dem Vertrag von Lissabon ergeben, sollten Zugriff und Nutzung von für kommerzielle Zwecke übermittelten Daten durch Behörden, selbst wenn die Daten nur im Transit sind, nur unter außergewöhnlichen Umständen und nur dann erfolgen, wenn es für genau spezifizierte Zwecke im öffentlichen Interesse unerlässlich ist.

Bezüglich der Bestimmungen über Übermittlungen zu kommerziellen Zwecken sollte von für die Verarbeitung Verantwortlichen nicht erwartet werden, dass sie ständig die Compliance-Modelle wechseln. Überdies wurde der Entscheidungsentwurf auf der Grundlage des bestehenden EU-Rechtsrahmens formuliert, der aber im Mai 2018 von der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung) abgelöst wird, also weniger als ein Jahr nach der vollständigen Umsetzung des Datenschutzschildes durch die für die Verarbeitung Verantwortlichen. Die Datenschutz-Grundverordnung schafft neue und verschärft bestehende Pflichten für Verantwortliche, die über die neun im Datenschutzschild entwickelten Grundsätze hinausgehen. Unabhängig von letzten Änderungen am Entwurf empfehlen wir der Europäischen Kommission, die künftigen Aussichten seit ihrem ersten Bericht umfassend zu bewerten, rechtzeitig gegebenenfalls relevante Schritte im Hinblick auf längerfristige Lösungen als Ersatz für den Datenschutzschild zu ermitteln, mit solideren und stabileren Rechtsrahmen, damit die transatlantischen Beziehungen einen neuen Schub erhalten.

Daher gibt der EDSB spezifische Empfehlungen zum Datenschutzschild ab.

INHALTSVERZEICHNIS

DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 16,

gestützt auf die Charta der Grundrechte der Europäischen Union, insbesondere auf Artikel 7 und 8,

gestützt auf 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 (nachstehend „die Richtlinie"),

gestützt auf den Rahmenbeschluss 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,

gestützt auf die Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr, insbesondere auf Artikel 28 Absatz 2, Artikel 41 Absatz 2 und Artikel 46 Buchstabe d —

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

I. EINLEITUNG

Am 6. Oktober 2015 erklärte der Gerichtshof der Europäischen Union (nachstehend „EuGH")[1] die Entscheidung über die Angemessenheit des Sicheren Hafens[2] für ungültig. Am 2. Februar 2016 erzielte die Europäische Kommission mit den USA eine politische Einigung über einen neuen Rahmen für Übermittlungen personenbezogener Daten, der die Bezeichnung „EU-US-Datenschutzschild" (nachstehend „Datenschutzschild") trägt. Am 29. Februar stellte die Europäische Kommission der Öffentlichkeit den Entwurf einer Entscheidung über die Angemessenheit dieses neuen Rahmens (nachstehend „Entscheidungsentwurf")[3] nebst sieben Anhängen vor, einschließlich der Grundsätze des Datenschutzschildes und schriftlicher Erklärungen und Zusagen von Seiten US-amerikanischer Amtsträger und Behörden. Dem EDSB ging der Entscheidungsentwurf zur Konsultation am 18. März dieses Jahres zu.

Der EDSB hat wiederholt seine Auffassung zu Übermittlungen personenbezogener Daten zwischen der EU und den USA dargelegt[4] und hat sich auch an den Arbeiten an der Stellungnahme der Artikel 29-Datenschutzgruppe (nachstehend: „WP29") zu dem Entscheidungsentwurf als Mitglied dieser Arbeitsgruppe beteiligt[5]. Die WP29 hat schwerwiegende Bedenken geäußert und die Europäische Kommission ersucht, Lösungen zu finden, mit denen sich diese Bedenken ausräumen lassen. Die Mitglieder der WP29 gehen davon aus, dass alle in der Stellungnahme verlangten Klarstellungen erfolgen werden[6]. Am 16. März legten 27 gemeinnützige Organisationen in einem Schreiben an EU- und US-Behörden ihre Kritik an dem Entscheidungsentwurf dar[7]. Am 26. Mai nahm das Europäische Parlament eine Entschließung zur transatlantischen Datenübermittlung[8] an, in der die Kommission aufgefordert wird, den Dialog mit den USA weiterzuführen, um auf weitere

Verbesserungen bei der Datenschutzschild-Regelung angesichts ihrer derzeitigen Mängel zu drängen[9].

Als unabhängiger Berater des EU-Gesetzgebers gemäß der Verordnung (EG) Nr. 45/2001 legt der EDSB nun Empfehlungen an die an dem Verfahren Beteiligten vor, die sich insbesondere an die Kommission wenden. Diese Empfehlungen sollen sowohl prinzipientreu als auch pragmatisch sein, denn sie sollen proaktiv der EU dabei helfen, ihre Ziele mit angemessenen Maßnahmen zu erreichen. Er ergänzt und unterstreicht einige, wenn auch nicht alle Empfehlungen in der Stellungnahme der WP29.

Im Vergleich zur Safe Harbour-Entscheidung weist der Entscheidungsentwurf eine Reihe von Verbesserungen auf, vor allem im Hinblick auf die Grundsätze für die Verarbeitung von Daten für kommerzielle Zwecke. Bezüglich des Zugangs zu den unter dem Datenschutzschild übermittelten Daten für Behörden begrüßen wir, dass zum ersten Mal das Justizministerium, das Außenministerium und das Büro des Direktors der National Intelligence in die Verhandlungen eingebunden waren. Fortschritte im Vergleich zu der älteren Safe Harbour-Entscheidung allein reichen jedoch nicht aus. Korrekter Orientierungspunkt ist nicht eine zuvor für ungültig erklärte Entscheidung, da sich die Angemessenheitsentscheidung auf den derzeitigen EU-Rechtsrahmen stützen muss (insbesondere auf die Richtlinie, Artikel 16 des Vertrags über die Arbeitsweise der Europäischen Union sowie Artikel 7 und 8 der Charta der Grundrechte der Europäischen Union, ausgelegt durch den EuGH). Artikel 45 der Datenschutz-Grundverordnung der EU[10] enthält neue Anforderungen an Datenübermittlungen auf der Grundlage einer Angemessenheitsentscheidung.

Im vergangenen Jahr bekräftigte der EuGH, die Schwelle für die Angemessenheitsbeurteilung sei der Begriff „der Sache nach gleichwertig“, und forderte eine strenge Beurteilung anhand dieses strengen Maßstabs[11]. Angemessenheit verlangt nicht einen Rahmen, der mit dem der EU identisch ist, doch sollten insgesamt betrachtet der Datenschutzschild und die Rechtsordnung der USA alle Kernelemente des EU-Datenschutzrahmens enthalten. Dies erfordert sowohl eine Gesamtbeurteilung der Rechtsordnung als auch eine Prüfung der wichtigsten Elemente des EU-Datenschutzrahmens[12]. Wir gehen davon aus, dass die Beurteilung insgesamt durch Wahrung des Wesens dieser Elemente geschehen sollte. Darüber hinaus müssen aufgrund des Vertrags und der Charta spezifische Elemente wie unabhängige Kontrolle und Beschwerde untersucht werden.

Diesbezüglich ist sich der EDSB der Tatsache bewusst, dass viele Organisationen auf beiden Seiten des Atlantiks auf das Ergebnis der Verhandlungen über diese Angemessenheitsentscheidung warten. Sollte der EuGH jedoch auch die neue Entscheidung für ungültig erklären, brächte dies erhebliche Rechtsunsicherheit für betroffene Personen und hohen Aufwand vor allem für KMU mit sich. Und würde der Entscheidungsentwurf angenommen und dann vom EuGH für ungültig erklärt werden, müsste eine neue Angemessenheitsregelung ausgehandelt werden, dieses Mal nach der Datenschutz-Grundverordnung. Wir empfehlen daher mit Blick auf das bevorstehende Datum der vollständigen Anwendung der Datenschutz-Grundverordnung in zwei Jahren einen zukunftsorientierten Ansatz.

Der Entscheidungsentwurf spielt eine Schlüsselrolle in den Beziehungen zwischen der EU und den USA, zumal gerade zwischen ihnen auch Handels- und Investitionsverhandlungen stattfinden. Außerdem sind viele der in unserer Stellungnahme behandelten Aspekte sowohl

für den Datenschutzschild als auch für andere für Übermittlungen wichtige Instrumente relevant, wie die verbindlichen unternehmensinternen Datenschutzregelungen (Binding Corporate Rules, nachstehend: „BCR“) und Standardvertragsklauseln (Standard Contractual Clauses, nachstehend: „SCC“). Der Entscheidungsentwurf ist aber auch weltweit von Bedeutung, da sich viele Drittländer vor dem Hintergrund der Annahme des neuen EU-Datenschutzrahmens an ihn anlehnen werden.

Daher würden wir eine allgemeine Lösung für Übermittlungen aus der EU in die USA begrüßen, die jedoch ausreichend umfassend und solide sein sollte. Hierzu müssen eindeutige Verbesserungen vorgenommen werden, damit langfristig die Achtung unserer Grundrechte und Grundfreiheiten gewährleistet ist. Nach der Annahme sollte die Entscheidung nach einer ersten Beurteilung durch die Europäische Kommission rechtzeitig überprüft werden, um gegebenenfalls relevante Schritte in Richtung längerfristiger Lösungen als Ersatz für den Datenschutzschild zu überlegen, mit solideren und stabileren Rechtsrahmen, damit die transatlantischen Beziehungen einen neuen Schub erhalten.

Der EDSB entnimmt dem Entwurf der Entscheidung und ihrer Anhänge ferner, dass ungeachtet neuerer Tendenzen von der undifferenzierten Überwachung auf allgemeiner Grundlage hin zu gezielteren und ausgewählten Ansätzen der Umfang der Fernmeldeaufklärung und das Volumen von aus der EU übermittelten Daten, die nach der Übermittlung und insbesondere im Transit möglicherweise gesammelt und verwendet werden, nach wie vor sehr groß und damit zu hinterfragen sind.

Auch wenn diese Praktiken darüber hinaus mit Aufklärung in anderen Ländern zu tun haben mag, und auch wenn wir die Transparenz der US-Behörden bezüglich dieser neuen Realität begrüßen, könnte der derzeitige Entscheidungsentwurf als Legitimation dieser Vorgehensweise ausgelegt werden. Die Frage bedarf einer sorgfältigen demokratischen Prüfung durch die Öffentlichkeit. Daher fordern wir die Europäische Kommission auf, ein starkes Signal auszusenden: Mit Blick auf die Verpflichtungen, die sich für die EU aus dem Vertrag von Lissabon ergeben, sollten Zugriff und Nutzung von für kommerzielle Zwecke übermittelten Daten durch Behörden, selbst wenn die Daten nur im Transit sind, nur unter außergewöhnlichen Umständen und nur dann erfolgen, wenn es für genau spezifizierte Zwecke im öffentlichen Interesse unerlässlich ist.

Des Weiteren halten wir fest, dass wichtige, für das Privatleben natürlicher Personen in der EU relevante Zusicherungen offensichtlich mit einem gewissen Detailgrad nur in internen Schreiben von US-Behörden gemacht werden (beispielsweise Erklärungen zu Aktivitäten der Fernmeldeaufklärung über Transatlantikkabel, wenn überhaupt)[13]. Auch wenn wir die Kompetenz der ehrenwerten Verfasser dieser Schreiben nicht in Frage stellen wollen, und auch wenn wir einsehen, dass diese Erklärungen nach einer Veröffentlichung im Amtsblatt und im *Federal Register* als „schriftliche Zusicherungen“ betrachtet werden, auf deren Grundlage die Beurteilung durch die EU erfolgt, stellen wir doch ganz allgemein fest, dass einigen dieser Erklärungen aufgrund ihrer Bedeutung ein größere Rechtswirkung zukommen müsste.

Neben Gesetzesänderungen und internationalen Abkommen[14] könnten noch weitere praxisnahe Lösungen in Erwägung gezogen werden. Mit unserer Stellungnahme möchten wir diesbezüglich pragmatische Hilfestellung leisten.

II. HAUPTEMPFEHLUNGEN

1. Integration aller wichtigen Datenschutzgrundsätze

Im Entscheidungsentwurf heißt es, der Datenschutzschild insgesamt gewähre ein Schutzniveau, das der Sache nach gleichwertig dem Niveau sei, das durch die wesentlichen Grundprinzipien der Richtlinie gewährleistet sei[15]. Der derzeitige Entwurf spart jedoch einige wesentliche Details dieser Grundsätze aus, insbesondere im Zusammenhang mit **Datenspeicherung** und **automatisierter Verarbeitung**. Andere wesentliche Elemente, wie der Grundsatz der **Zweckbindung**, sollten besser erläutert werden. Auch die **Ausnahmen** von den Anforderungen des Datenschutzschildes sollten genauer benannt werden. Im Entscheidungsentwurf wird nicht vollständig erklärt, wie der Datenschutzschild oder die Rechtsordnung der USA, selbst zusammengenommen, diese Lücken füllen könnten. Wie bereits erwähnt, sollte der Datenschutzschild daher dahingehend geändert werden, dass alle wichtigen Grundsätze des EU-Datenschutzes[16] besser integriert werden, wie noch später in Abschnitt III.1 dieser Stellungnahme ausgeführt werden wird. Außerdem sollten die Bestimmungen zu **Weiterübermittlungen**, das **Recht auf Auskunft** und das **Recht auf Widerspruch** verbessert werden. Der EDSB weist in diesem Zusammenhang auf die Empfehlungen der WP29 hin.

2. Beschränkung der Ausnahmen

Gemäß Anhang II.I.5(a) können die Grundsätze des Datenschutzschildes eingeschränkt werden, sofern es die nationale Sicherheit, die Strafverfolgung oder andere öffentliche Interessen erfordern. Anhang II.I.5(b) erlaubt Einschränkungen der Grundsätze auch, wenn ein Gesetz, eine Verordnung oder die Rechtsprechung zu widerstreitenden Verpflichtungen oder ausdrücklichen Genehmigungen führt, ohne irgendeine Beschränkung des Zwecks eines solchen Zugangs. **Die Zwecke, zu denen Ausnahmen erlaubt sind, und das Erfordernis einer Rechtsgrundlage sollten** sowohl in (a) als auch in (b) **präziser formuliert werden**. Der EDSB stellt fest, dass die Safe Harbour-Entscheidung[17] unter anderem für ungültig erklärt wurde, weil es keine Regeln für die Begrenzung von Eingriffen durch US-Behörden in die Rechte der Personen gab, deren Daten aus der EU übermittelt wurden. Der Gerichtshof forderte ferner klare und präzise Regeln für die Begrenzung der Tragweite und der Anwendung von Eingriffen in Grundrechte[18]. **Aus den gleichen Gründen sollten in Anhang II.I.5(c) genauer die Zwecke angegeben werden, für die Ausnahmen möglich sind, oder sollte der Anhang gestrichen werden.**

Der EDSB begrüßt die Bemühungen um mehr Transparenz in den Informationen des Büros des Direktors der National Intelligence über den Zugang von US-Behörden zu Daten[19]. Der EDSB erkennt ferner eine deutliche Ausrichtung in der Presidential Policy Directive 28 (nachstehend: „PPD 28“) gegen eine massive Datenerhebung. PPD 28 erlaubt allerdings die Weiterverarbeitung von in großen Mengen erhobenen Daten zur „Erleichterung einer gezielten Erhebung“ und für mindestens sechs weitere Zwecke. Des Weiteren heißt es zwar im Entscheidungsentwurf, dass Fernmeldeaufklärung nur dann betrieben werden darf, wenn sie für einen ausländischen Nachrichtendienst oder eine ausländische Spionageabwehr erfolgt, doch ist der Begriff „ausländischer Nachrichtendienst“ sehr weit definiert[20]. Ferner gehen wir davon aus, dass die Bedingungen für den Zugang von US-Behörden zu personenbezogenen Daten, „die übermittelt wurden“[21], sich von denen für den Zugriff auf „zu übermittelnde“[22] personenbezogene Daten unterscheiden. Wir empfehlen eine nuanciertere Formulierung von Erwägungsgrund 55 des Entscheidungsentwurfs, in dem es heißt, die

Beschränkungen des Zugangs und der Verwendung von personenbezogenen Daten, die gemäß dem EU-US-Datenschutzschild für Zwecke der nationalen Sicherheit übermittelt werden, seien „klar“[23].

PPD 28 stellt zwar eine positive Entwicklung dar, doch bleibt abzuwarten, inwieweit **weitere politische und legislative Änderungen**, z. B. im Hinblick auf Executive Order 12333, **zur Erfüllung der Bedingungen für die Angemessenheit beitragen könnten**. Die Überprüfung 2017 von Section 702 FISA, bei der momentan offensichtlich die Regierung keine besonderen Ziele identifizieren oder dem Foreign Intelligence Surveillance Court eine Begründung für die Auswahl bestimmter Ziele gebe muss[24], könnte hier ebenfalls eine gute Möglichkeit bieten.

3. Bessere Mechanismen für Beschwerden und Kontrolle

Wie auch von der WP29 festgestellt, sollte zur Verbesserung des im Bereich der nationalen Sicherheit vorgeschlagenen Beschwerdemechanismus die Rolle der **Ombudsperson** weiter ausgebaut werden, so dass sie **unabhängig** nicht nur von den Nachrichtendiensten, sondern auch von jeder anderen Behörde arbeiten kann[25]. Eine praxisnahe Option hierfür könnte die Möglichkeit sein, unmittelbar dem Kongress zu berichten.

Wir empfehlen der Europäischen Kommission, verstärkt hinzuarbeiten auf **konkrete Zusagen, dass die Informations- und Kooperationsersuchen der Ombudsperson sowie ihre Entscheidungen und Empfehlungen von allen zuständigen Behörden und Stellen tatsächlich befolgt und umgesetzt werden.** Begrüßen würden wir ferner weitere Zusagen von US-Behörden betreffend eine engere **Zusammenarbeit zwischen den verschiedenen Kontrollebenen**. Die entsprechenden Kontrollstellen, insbesondere die betreffenden Inspectors-General, könnten zusagen, der Koordinierung mit der Ombudsperson Vorrang einzuräumen. Bei ihrer fallweisen Prüfung von Beschwerden könnte sie die laufende Bewertung der US-Rechtsgrundlagen für Beaufsichtigung durch das PCLOB und dessen Empfehlungen besser berücksichtigen.

Der EDSB stellt fest, dass die Funktion dieser Stellen darin besteht, die Befolgung US-amerikanischer Gesetze, Vorschriften und Urteile zu beaufsichtigen, was zu unterschiedlichen Schutzniveaus für US-Bürger und Nicht-US-Bürger führt und eine Verarbeitung durch US-Behörden zulässt; dies dürfte kaum den im EU-Datenschutzrahmen vorgesehenen Ausnahmen „in der Sache gleichwertig“ sein[26]. Wir fordern die Europäische Kommission zur Prüfung der Frage auf, ob es machbar ist, **EU-Vertreter a) in die Bewertung der Ergebnisse des Kontrollsystems** für die Verarbeitung durch US-Behörden von personenbezogenen Daten, die aus der EU übermittelt wurden, und **b) in die Meldung bestimmter personenbezogener Daten, die** von US-Behörden **verarbeitet werden sollen**, und dies insbesondere dann, wenn Gefahr besteht, dass Grundrechte nicht gewahrt werden, **einzubeziehen**. Diese Einbeziehung könnte sogar in Form eines Gremiums erfolgen, dem vertrauenswürdige hochrangige Vertreter eines oder mehrerer Parlamentsausschüsse aus der EU und/oder nationaler Kontrollgremien für Nachrichtendienste und/oder Oberster Gerichte und/oder Datenschutzbehörden (nachstehend: „DSB“) der EU oder einzelner Länder angehören.

Die von der Kommission im Zusammenhang mit dem Abkommen zwischen der EU und den USA über die Verarbeitung von Zahlungsverkehrsdaten und deren Übermittlung (nachstehend: „TFTP“) ins Spiel gebrachten Lösungen waren ein Präzedenzfall, vor allem

was die **Genehmigung durch eine Justizbehörde** angeht, bevor bestimmten Ersuchen von US-Behörden stattgegeben werden darf[27]. Zur ursprünglichen TFTP-Regelung gehörte auch die Kontrolle der Weiterverarbeitung der Daten **durch einen EU-Richter**[28]. Derzeit sind auch **Datenschutzbehörden der EU** in die Kontrolle der Bearbeitung von US-Ersuchen eingebunden[29]. Hilfreiche Beispiele lassen sich auch in einigen EU-Mitgliedstaaten finden, in denen die Tätigkeit nationaler Nachrichtendienste der Kontrolle durch Datenschutzbehörden unterliegt[30]. In diesem Zusammenhang könnte die **Meldung der** von US-Behörden **zu verarbeitenden Kategorien personenbezogener Daten** an ein Gremium, dem auch eine unabhängige Behörde aus der EU angehört, insbesondere in Fällen, in denen die Verarbeitung Bedenken im Hinblick auf EU-Standards weckt, dabei helfen, diese Bedenken auszuräumen.

III. WEITERE EMPFEHLUNGEN

1. Bestimmungen zu Übermittlungen zu kommerziellen Zwecken

Umfassende Integration der Grundsätze der Datenminimierung und Datenspeicherung

Der EDSB empfiehlt, Anhang II dahingehend zu ändern, dass klarer **untersagt wird, personenbezogene Daten länger, als** es für die Erreichung der Zwecke, für die sie erhoben und/oder weiterverarbeitet werden, **erforderlich** ist, **in einer Form zu speichern, die die Identifizierung der betroffenen Person ermöglicht**. Diese Verpflichtung gehört zu den wesentlichen Grundsätzen des Datenschutzrechts, weil durch sie gewährleistet wird, dass personenbezogene Daten nicht länger als erforderlich verarbeitet werden; dann müssten zertifizierte Organisationen eine Datenspeicherpolitik festlegen[31].

Anhang II.II.5 des Entscheidungsentwurfs besagt, dass „personenbezogene Daten auf die Daten beschränkt sein müssen, die für die Zwecke der Verarbeitung *von Belang* sind". Der EDSB empfiehlt, im Einklang mit dem Grundsatz der Datenminimierung die Bedingung hinzuzufügen, dass **personenbezogene Daten *den Zwecken entsprechen* müssen, für die sie erhoben und/oder weiterverarbeitet werden, dafür erheblich sein müssen und *nicht darüber hinausgehen* dürfen oder *darauf beschränkt* sein müssen**[32].

Weitere Garantien bezüglich der automatisierten Verarbeitung

In Anhang II sollte ein Grundsatz mit Garantien für den Schutz legitimer Interessen natürlicher Personen für den Fall hinzugefügt werden, dass sie einer Entscheidung unterworfen werden, die für sie rechtliche Folgen nach sich zieht oder sie erheblich beeinträchtigt und die **ausschließlich aufgrund einer automatisierten Verarbeitung** von Daten zum Zwecke der Bewertung einzelner Aspekte ihrer Person ergeht, wie beispielsweise ihrer beruflichen Leistungsfähigkeit, ihrer Kreditwürdigkeit, ihrer Zuverlässigkeit, ihres Verhaltens usw. Solche Garantien könnten unter anderem vorsehen, dass sie von dem für die Verarbeitung Verantwortlichen verlangen können, das Eingreifen eines Menschen zu gestatten, ihren Standpunkt darzulegen und die Entscheidung anzufechten sowie Informationen über die der Verarbeitung zugrundeliegende Logik zu erhalten. Orientierungshilfe könnte Artikel 15 der Rahmenvereinbarung bieten[33].

Klarstellung des Grundsatzes der Zweckbindung

Wie die WP29 festgestellt hat, sind in dem Entscheidungsentwurf immer wieder auftretende Begriffe wie „andere Zwecke", „wesentlich andere" Zwecke oder „eine nicht im Einklang mit (...) stehende Verwendung" nicht klar und können zu Missverständnissen führen[34]. Der

EDSB empfiehlt eine **Straffung der rund um den Begriff „Zweck" verwendeten Konzepte**. Am besten sollte im gesamten Dokument der Ausdruck „(nicht) kompatibler Zweck" verwendet werden. Auf jeden Fall sollte spezifiziert werden, dass „wesentlich andere" Zwecke, für die Daten weiterverarbeitet werden können, mit den Zwecken vereinbar sein sollten, für die die Daten ursprünglich erhoben wurden.

Die Weiterverwendung zu **Marketingzwecken** von personenbezogenen Daten, die ursprünglich für die medizinische oder pharmazeutische Forschung oder in Personalabteilungen verarbeitet wurden, sollte auf keinen Fall als mit dem ursprünglichen Zweck vereinbar betrachtet werden. Daher sollte die Erwähnung einer solchen Möglichkeit in den Zusatzgrundsätzen 9(b)(i) und 14(b)(i) gestrichen werden.

Beschränkung von Ausnahmen

Die zahlreichen Ausnahmen von den Grundsätzen des Datenschutzschildes[35] erschweren möglicherweise Organisationen, betroffenen Personen und Datenschutzbehörden die Beantwortung der Frage, ob bestimmte Arten der Verarbeitung abgedeckt sind. Dies ist besonders wichtig, weil dann kommerzielle Übermittlungen, die nicht unter den Entscheidungsentwurf fallen, durch andere Instrumente (z. B. BCR, SCC) abgedeckt sein müssen. Im Sinn der Rechtssicherheit sollte der Umfang dieser Ausnahmen im Entscheidungsentwurf klar und eindeutig festgelegt werden. Außerdem können einige von ihnen problematisch sein, weil sie möglicherweise **den Kernanforderungen des EU-Datenschutzrechts widersprechen**.

Dies gilt auch für **„journalistisches Material"**[36], das von den Anforderungen der Grundsätze des Datenschutzschildes vollkommen ausgenommen ist. Es besteht allerdings die Verpflichtung, zwischen dem Recht auf Meinungsfreiheit und den Rechten auf Privatsphäre und Schutz personenbezogener Daten abzuwägen, beide nach der Charta und im Einklang mit der Richtlinie, wie sie vom EuGH ausgelegt wurde, insbesondere in den Urteilen in den Rechtssachen Google Spain[37] und Satamedia[38].[39] Wir empfehlen daher, diese allgemeine Befreiung durch spezifische Ausnahmen bei bestimmten Anforderungen[40] nur dort zu ersetzen, wo sie erforderlich sind, um die Rechte auf Privatsphäre und Datenschutz mit den Vorschriften über Meinungsfreiheit in Einklang zu bringen, und wo dieses „journalistische Material" auch für journalistische Zwecke verwendet werden soll.

Bessere Mechanismen für Beschwerden und Kontrolle

Bezüglich der Kontrolle von Übermittlungen zu kommerziellen Zwecken werden wir trotz positiver Veränderungen auch weiterhin **ein Ergebnis empfehlen, bei dem US-Behörden systematisch und wirksam die Einhaltung der Grundsätze des Datenschutzschildes überwachen**. So könnte der Entscheidungsentwurf beispielsweise durch eindringliche Hinweise darauf ergänzt werden, wie Vor-Ort-Begehungen oder Inspektionen in den Räumlichkeiten selbstzertifizierter Unternehmen durchgeführt werden können, bei denen geprüft wird, ob die Grundsätze des Datenschutzschildes eingehalten werden[41]. Bezüglich der „Arbeitsweise des Gremiums der Datenschutzbehörden"[42] sollte sich der Wortlaut präziser dazu äußern, wie die Arbeitsweise dieses Gremiums im Vergleich zu der des nach der Safe Harbour-Entscheidung eingerichteten aussieht. Wir gehen davon aus, dass bewährte Elemente früherer Erfahrungen übernommen werden. Mit Blick auf neuere Entwicklungen in der US-Durchsetzung empfehlen wir ferner eine Klarstellung der Rollen von FCC und FTC gegenüber Anbietern von Breitbandinternetdiensten.

Der Entscheidungsentwurf sollte die Klagemöglichkeiten vor US-Gerichten prüfen, die in der Praxis natürlichen Personen zur Verfügung stehen, deren Daten gemäß dem Datenschutzschild übermittelt wurden. Zwar zeigt die Vielzahl von Wegen, die natürlichen Personen offensteht, die Rechtsbehelf auf Ebene des Bundes oder der Bundesstaaten einlegen möchten, die Bereitschaft, natürlichen Personen wirksame Beschwerdemechanismen zur Verfügung zu stellen, doch steht dem die Komplexität des Systems entgegen. Zur Erleichterung des direkten Zugangs natürlicher Personen zu unabhängigen Rechtsbehelfen und unter Berücksichtigung der Komplexität der vorgeschlagenen Mechanismen empfehlen wir, das System zu verbessern und auf die freiwillige Option für zertifizierte Organisationen insofern aufzubauen, als sie Daten verarbeiten, die im Einklang mit den Datenschutzschild übermittelt wurden, und sich der **Kontrolle durch Datenschutzbehörden unterwerfen** können und damit von deren Sachverstand im Bereich der Verarbeitung personenbezogener Daten profitieren können. In diesem Zusammenhang hat die WP29 ebenfalls empfohlen, in Datenschutzbestimmungen die Möglichkeit für natürliche Personen aus der EU vorzusehen, Schadenersatzklagen in der EU einzureichen[43].

2. Empfehlungen betreffend den Zugang durch US-Behörden

Im Entscheidungsentwurf heißt es, dass alles in allem die vorgesehenen Kontroll- und Beschwerdemechanismen der betroffenen Person Rechtsmittelmöglichkeiten an die Hand geben, um Auskunft über ihre personenbezogenen Daten zu erhalten und deren Berichtigung oder Löschung zu verlangen[44]. Der Entscheidungsentwurf nimmt allerdings keine umfassende Bewertung der Möglichkeiten für natürliche Personen vor, ihre **Rechte auf Auskunft, Berichtigung oder Löschung** von Daten wahrzunehmen, die von Behörden für andere Zwecke als die nationale Sicherheit erhoben oder abgerufen wurden (z. B. Strafverfolgung oder andere Zwecke „im öffentlichen Interesse“)[45]. Dieser Punkt bedarf in dem Entscheidungsentwurf einer Klarstellung. In diesem Zusammenhang stellt der EDSB fest, dass der vor kurzem angenommene *Judicial Redress Act*[46] nur für „Aufzeichnungen“ gilt, die von öffentlichen oder privaten Stellen in den abgedeckten Ländern (also der EU) unmittelbar an US-Behörden[47] übermittelt wurden. Er gilt also nicht für Daten, die zwischen privaten Einrichtungen gemäß dem Datenschutzschild übermittelt und dann von US-Behörden angefordert oder abgerufen werden.

Der EDSB stellt fest, dass in den USA mehrere Ebenen für Kontrolle und Beschwerden bestehen, die aber zusammen genommen offensichtlich nicht alle Stellen abdecken, an denen die Regierung Zugang zu personenbezogenen Daten hat. Darüber hinaus genießen Nicht-US-Bürger nicht immer die gleichen Rechte nach der Verfassung, den Gesetzen und Vorschriften der USA wie US-Bürger. Daher sind diese Kontroll- und Beschwerdemechanismen für den Datenschutzschild nur von begrenzter Relevanz. Für den Zugang für Strafverfolgungs- und andere Zwecke im öffentlichen Interesse sind daher **weitere Garantien für unabhängige Kontrolle und Beschwerde** erforderlich.

3. Beurteilung der Auswirkungen anderer einschlägiger Gesetze und Regeln

Alle Regeln, die auf Daten anzuwenden sind, die gemäß dem Entscheidungsentwurf aus der EU in die USA übermittelt werden, sollten mit Blick auf die Ausnahmen von den Grundsätzen des Datenschutzschildes für Verarbeitungen zu kommerziellen Zwecken oder für Fälle, in denen andere Regeln mit diesem Grundsätzen kollidieren, bewertet werden. In

diese Bewertung sollten auch **US-Gesetze des Bundes und der Bundesstaaten** einbezogen werden, die den **Zugang aus** anderen **Gründen des öffentlichen Interesses** als nationale Sicherheit und Strafverfolgung erlauben, sowie andere Gesetze und Verordnungen mit Auswirkungen auf den Schutz personenbezogener Daten[48]. Einbezogen werden sollten in diese Bewertung ferner einschlägige **internationale Zusagen**, und hier vor allem diejenigen, die für personenbezogene Daten, die ursprünglich für kommerzielle Zwecke verarbeitet wurden, den Zugriff für Behörden oder die Übermittlung durch Behörden vorsehen.

4. Eine aussagekräftige Überprüfung

Wie auch von der WP29 gefordert, sollte die gemeinsame Überprüfung der Anwendung des Datenschutzschildes nicht nur in Form von Sitzungen mit öffentlichen und privaten Stellen erfolgen, sondern auch von **Inspektionen vor Ort**. Die Überprüfung sollte nicht auf den kommerziellen Teil des Entscheidungsentwurfs begrenzt sein, sondern auch den **Zugang für US-Behörden zu den gemäß dem Datenschutzschild übermittelten Daten** umfassen. Dies sollte in dem Entscheidungsentwurf genau geregelt werden. Im Entscheidungsentwurf sollte ferner erwähnt werden, dass die **Schlussfolgerungen und Befunde zumindest der Datenschutzbehörden aus der EU in den Bericht** über die gemeinsame Überprüfung **einfließen**.

5. Wechselwirkung mit der Datenschutz-Grundverordnung

Wie bereits erwähnt, sollte jede Lösung für Übermittlungen zwischen der EU und den USA, die eine gewisse Stabilität bietet, dem neuen Datenschutzrahmen der EU Rechnung tragen. Nur so lässt sich ein kohärentes Niveau an Schutz und Rechtssicherheit bezüglich der wichtigsten Grundsätze des EU-Datenschutzrahmens erzielen, und dies nicht nur kurzfristig, sondern auch auf mittlere und lange Sicht. So sollte sich der Entscheidungsentwurf vor allem mit einigen neuen Elementen in der Datenschutz-Grundverordnung befassen, die es in der jetzigen Richtlinie noch nicht gibt, wie die Grundsätze von **Datenschutz durch Technik**, **Datenschutz durch datenschutzfreundliche Voreinstellungen** oder **Datenübertragbarkeit**. Der EDSB hält fest, dass die Datenschutz-Grundverordnung auch klarere und detailliertere Kriterien für Angemessenheitsentscheidungen enthält, darunter die Existenz und die wirksame Funktionsweise **unabhängiger Aufsichtsbehörden** in dem betreffenden Drittland[49].

Schließlich bedeutet die Datenschutz-Grundverordnung eine Neuerung bezüglich des Anwendungsbereichs des EU-Datenschutzrahmens. Nicht in der EU niedergelassene Verantwortliche oder Auftragsverarbeiter unterliegen so lange den EU-Vorschriften, wie ihre Verarbeitungstätigkeiten dazu dienen, Personen in der EU Waren oder Dienstleistungen anzubieten oder das Verhalten dieser Personen zu beobachten. In diesen Fällen befreit eine Zertifizierung gemäß dem Datenschutzschild zertifizierte Organisationen nicht von der Anwendung des EU-Datenschutzrahmens, wenn sie in dessen neuen Anwendungsbereich fallen. In einem solchen Fall hat der EU-Rechtsrahmen Vorrang vor den Grundsätzen des Datenschutzschildes, und die entsprechenden Organisationen sind gehalten, sich vollumfänglich an die Datenschutz-Grundverordnung zu halten.

IV. SCHLUSSFOLGERUNG

Der EDSB begrüßt die Bemühungen der Parteien um eine Lösung für Übermittlungen personenbezogener Daten aus der EU in die USA für kommerzielle Zwecke in einem System

der Selbstzertifizierung. Es sind allerdings noch deutliche Verbesserungen erforderlich, um einen soliden, langfristig stabilen Rahmen zu erreichen.

Geschehen zu Brüssel am 30. Mai 2016

(gezeichnet)

Giovanni BUTTARELLI

Europäischer Datenschutzbeauftragter

[1] Rechtssache C-362/14, Maximilian Schrems gegen Data Protection Commissioner, 6. Oktober 2015 (nachstehend: *„Schrems"*).

[2] 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 (bekannt gegeben unter Aktenzeichen K(2000) 2441), (ABl. L215 vom 25.8.2000, S. 7).

[3] Durchführungsbeschluss der Kommission vom XXX gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des vom EU-US-Datenschutzschild gewährten Schutzes, abrufbar unter: http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf.

[4] Siehe die Stellungnahme des Europäischen Datenschutzbeauftragten zur Mitteilung der Kommission an das Europäische Parlament und den Rat „Wiederherstellung des Vertrauens beim Datenaustausch zwischen der EU und den USA" und zur Mitteilung der Kommission an das Europäische Parlament und den Rat „Über die Funktionsweise der Safe-Harbour-Regelung aus Sicht der EU-Bürger und der in der EU niedergelassenen Unternehmen", 20. Februar 2014, und den Vortrag des EDSB in der Verhandlung vor dem EuGH in der Rechtssache *Schrems*, abrufbar unter: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Court/2015/15-03-24_EDPS_Pleading_Schrems_vs_Data_Commissioner_EN.pdf).

[5] Artikel 29-Datenschutzgruppe in der Stellungnahme 01/2016 zu der Entscheidung über die Angemessenheit des EU-US-Datenschutzschilds (WP 238), abrufbar unter: http://ec.europa.eu/jus.tice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf.

[6] Siehe ferner das Grundsatzreferat des UK Information Commissioner Christopher Graham auf der IAPP Europe Data Protection Intensive 2016 Conference in London. Rede abrufbar (Video) unter: https://iapp.org/news/video/iapp-europe-data-protection-intensive-2016-christopher-graham-keynote/.

[7] Schreiben an die Artikel 29-Datenschutzgruppe und andere Einrichtungen, unterzeichnet von Access Now und 26 weiteren NRO.

[8] Entschließung des Europäischen Parlaments vom 26. Mai 2016 zur transatlantischen Datenübermittlung (2016/2727(RSP)).

[9] *Ebenda*, Rn. 14.

[10] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).

[11] *Schrems*, Rn. 71, 73, 74 und 96.

[12] Dieser Ansatz war schon Gegenstand einer der ersten Arbeitsunterlagen der WP29 zum Thema Datenübermittlungen (WP 12: Arbeitsunterlage „Übermittlungen personenbezogener Daten in Drittländer: Anwendung von Artikel 25 und 26 der Datenschutzrichtlinie der EU", 24. Juli 1998).

[13] Siehe z. B. Klarstellungen in Anhang VI.1. a) dahingehend, dass PPD28 für Daten gelten würde, die von Transatlantikkabeln durch die U.S. Intelligence Community erhoben würden.

[14] In der Verhandlung vor dem EuGH in der Rechtssache *Schrems* führte der EDSB Folgendes aus: *„Einzige wirksame Lösung ist die Aushandlung eines internationalen Abkommens, das angemessenen Schutz gegen*

undifferenzierte Überwachung und Verpflichtungen in den Bereichen Aufsicht, Transparenz, Beschwerde und Datenschutzrechte bietet", Vortrag des EDSB in der Verhandlung vor dem Gerichtshof vom 24. März 2015 in der Rechtssache C-362/14 (Schrems gegen Data Protection Commissioner).

[15] Entscheidungsentwurf, Erwägungsgrund 49.

[16] Im Urteil *Schrems* befand der Gerichtshof, Artikel 1 der Safe Harbour-Entscheidung der Kommission verstoße gegen die Anforderungen der Richtlinie und sei aus diesem Grund ungültig (siehe Rn. 98). Daher prüfte er nicht den Inhalt der Grundsätze des „sicheren Hafens". Er wies jedoch darauf hin, die Richtlinie solle nicht nur einen wirksamen und umfassenden Schutz der Grundfreiheiten und Grundrechte natürlicher Personen gewährleisten, sondern auch ein hohes Niveau des Schutzes dieser Rechte und Freiheiten. Ziel von Artikel 25 Absatz 6 sei es, den Fortbestand dieses hohen Niveaus des Schutzes im Fall der Übermittlung personenbezogener Daten in ein Drittland zu gewährleisten (siehe Rn. 72). Das „angemessene Schutzniveau" sei als ein Schutzniveau zu verstehen, das dem in der Union aufgrund der Richtlinie im Licht der Charta garantierten Niveau „der Sache nach gleichwertig" ist. Andernfalls würde das vorstehend erwähnte Ziel missachtet und könne das durch die Richtlinie garantierte Schutzniveau durch Übermittlungen in Drittländer leicht umgangen werden (siehe Rn. 73). Auch wenn sich die von dem betreffenden Drittland verwendeten Mittel möglicherweise von denen der EU unterscheiden (z. B. ein System der Selbstzertifizierung (siehe Rn. 80), müssen sie sich gleichwohl als wirksam erweisen, um diesen in der Sache gleichwertigen Schutz zu gewährleisten (Rn. 74). Diese Kontrolle sollte auf jeden Fall angesichts der Bedeutung des Schutzes personenbezogener Daten für das Grundrecht auf Achtung der Privatsphäre und der großen Zahl von Personen, deren Grundrechte verletzt werden können, strikt sein (Rn. 78). Daher seien alle wesentlichen Elemente der Richtlinie zu berücksichtigen.

[17] *Schrems*, Rn. 88.

[18] Im Urteil *Schrems* forderte der EuGH klare und präzise Regeln für die Begrenzung der Tragweite und der Anwendung von Eingriffen in die Grundrechte der Personen, deren Daten von der EU in die USA übermittelt wurden (Rn. 81). Derartige Regeln, die auch Garantien für den Schutz vor Missbrauch enthalten sollten, sind umso bedeutsamer, wenn die Daten automatisch verarbeitet werden und eine erhebliche Gefahr des unberechtigten Zugangs zu ihnen besteht (Rn. 91). Siehe auch Digital Rights Ireland gegen Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Ireland and the Attorney General, und Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl und andere, Gerichtshof der Europäischen Union, 8. April 2014, Verbundene Rechtssachen C-293/12 und C-594/12, Rn. 54-55). Darüber hinaus sollten sich solche Regeln auf ein objektives Kriterium stützen, das es ermöglicht, die Verarbeitung auf bestimmte, strikt begrenzte Zwecke zu beschränken, die den Eingriff zu rechtfertigen vermögen (*Schrems*, Rn. 93).

[19] Entscheidungsentwurf, Anhang VI.

[20] Dazu zählen nicht nur „Informationen über die Fähigkeiten, Absichten oder Aktivitäten ausländischer Regierungen oder von Teilen dieser Regierungen" und „internationale Terroristen", sondern auch Informationen über „ausländische Organisationen" und „ausländische Personen" (Presidential Policy Directive 28: Signals Activities (PPD-28) (17. Januar 2014), Fußnote 2).

[21] Entscheidungsentwurf, Erwägungsgrund 65.

[22] Entscheidungsentwurf, Erwägungsgrund 67.

[23] Entscheidungsentwurf, Erwägungsgrund 55.

[24] PCLOB Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, 2. Juli 2014, S. 106.

[25] Entscheidungsentwurf, Erwägungsgründe 53 und 104.

[26] Die Kommission führt aus: „Angesichts der Reichweite dieser Überwachungsprogramme und der Ungleichbehandlung der EU-Bürger stellt sich die Frage nach dem Schutzniveau, das durch die Safe-Harbour-Regelung geboten wird" (*Mitteilung „Wiederherstellung des Vertrauens beim Datenaustausch zwischen der EU und den USA"* (COM(2013) 846 final, S. 4). Zu den erheblichen Unterschieden zwischen den Garantien, die für US-Bürger bzw. Nicht-US-Bürger gelten, siehe auch *Report on the Findings by the EU Co-chairs of the ad hoc EU-U.S. Working Group on Data Protection* vom 27. November 2013, S. 17.

[27] Siehe die Pressemitteilung der Europäischen Kommission zur Annahme eines Vorschlags für ein Mandat für die Aushandlung eines Abkommens über die Übermittlung von Bankdaten mit der Regierung der Vereinigten Staaten im Rahmen des Programms zum Aufspüren der Finanzierung des Terrorismus, 24. März 2010. Im endgültigen Wortlaut des Abkommens wurde die richterliche Genehmigung durch die Genehmigung durch Europol ersetzt, im Einklang mit Artikel 4 des Abkommens zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über die Verarbeitung von Zahlungsverkehrsdaten und deren Übermittlung aus der Europäischen Union an die Vereinigten Staaten von Amerika für die Zwecke des Programms zum Aufspüren der Finanzierung des Terrorismus (ABl. L 195 vom 27.7.2010, S. 5).

[28] Siehe die „TFTP-Zusicherungen“ zur Verarbeitung personenbezogener Daten aus der EU durch das Finanzministerium der Vereinigten Staaten zu Zwecken der Terrorismusbekämpfung – „SWIFT“ (ABl. C 166 vom 20.7.2007, S. 18), in denen der EU gestattet wurde, eine „renommierte europäische Persönlichkeit“ zu benennen, die überprüft, ob die USA ihre Zusagen einhalten. 2008 ernannte die Europäische Kommission Richter Bruguière als „renommierte Persönlichkeit“ (Pressemitteilung der Europäischen Kommission, *EU prüft „Terrorist Finance Tracking Programme“ der USA*, IP/08/400, 7. März 2008).

[29] Im Rahmen ihrer Aufsichtstätigkeit überwacht die Gemeinsame Kontrollinstanz von Europol, die sich aus Vertretern der einzelnen nationalen Datenschutzbehörden der EU zusammensetzt, die Rolle von Europol bei der Erledigung von US-Ersuchen um personenbezogene Daten im Rahmen des TFTP-Abkommens. Außerdem sind nationale Datenschutzbehörden der EU an der gemeinsamen Überprüfung des Abkommens beteiligt, im Einklang mit Artikel 13 des Abkommens zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über die Verarbeitung von Zahlungsverkehrsdaten und deren Übermittlung aus der Europäischen Union an die Vereinigten Staaten von Amerika für die Zwecke des Programms zum Aufspüren der Finanzierung des Terrorismus (ABl. L 195 vom 27.7.2010, S. 5).

[30] Siehe Garante per la protezione dei dati personali, „Summary of key activities by the Italian DPA in 2013“, Ziffer 1.1, abrufbar unter: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3205017 (in englischer Sprache) und die Pressemitteilung (in italienischer Sprache), „Sicurezza dati personali: Protocollo d'intenti tra l'Autorità Garante e il Direttore Generale del Dis“, 11. November 2013, abrufbar unter: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2746204. Siehe ferner Agentur der Europäischen Union für Grundrechte, „Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU – Mapping Member States' legal frameworks, 2015“, abrufbar unter: http://fra.europa.eu/sites/default/files/fra_uploads/fra-2015-surveillance-intelligence-services_en.pdf.

[31] In Anhang VI ist zwar eine Speicherfrist von fünf Jahren für nachrichtendienstliche Zwecke vorgesehen, doch heißt es dort auch, dass Daten länger als fünf Jahre gespeichert werden können, „wenn diese längere Speicherung im nationalen Interesse der Vereinigten Staaten liegt“. Dieser Grundsatz gilt ferner nicht für Daten, die zu kommerziellen Zwecken übermittelt und verwendet werden.

[32] Siehe Artikel 6 Absatz 1 Buchstabe c der Richtlinie.

[33] Abkommen zwischen den Vereinigten Staaten von Amerika und der Europäischen Union über den Schutz personenbezogener Daten bei deren Übermittlung und Verarbeitung zum Zwecke der Verhütung, Untersuchung, Aufdeckung und Verfolgung von Straftaten. Zur Paraphierung bereiter Entwurf abrufbar unter: http://ec.europa.eu/justice/data-protection/files/dp-umbrella-agreement_de.pdf. Siehe auch die Stellungnahme 1/2016 des EDSB vom 12. Februar 2016 über das Regenschirm-Abkommen, Punkt 44.

[34] Artikel 29-Datenschutzgruppe in der Stellungnahme 01/2016 zu der Entscheidung über die Angemessenheit des EU-US-Datenschutzschilds (WP 238), S. 20.

[35] Zusatzgrundsatz 3 beispielsweise sieht einen Haftungsausschluss gemäß dem Datenschutzschild für Internetdiensteanbieter, Telekommunikationsanbieter und „andere Organisationen“ vor, wenn sie lediglich im Namen einer anderen Organisation Daten übermitteln, routen, switchen oder zwischenspeichern. Erwägungsgrund 47 der Richtlinie 95/46/EG schließt nicht aus, dass es sich bei solchen Unternehmen um Auftragsverarbeiter handeln kann, weshalb sie dann der Richtlinie unterworfen sein können. Im Übrigen ist die Verarbeitung von Daten durch solche Unternehmen bereits durch die Datenschutzrichtlinie für elektronische Kommunikation abgedeckt. Schließlich betrifft die Haftungsausschlussregelung der Richtlinie 2000/31 über den elektronischen Geschäftsverkehr nicht das Datenschutzrecht (Artikel 1 Absatz 5 Buchstabe b). Da Telekommunikationsanbieter offensichtlich vom Anwendungsbereich des Datenschutzschildes ausgenommen sind, führt ihre Aufnahme in diesen Grundsatz zu Verwirrung.

[36] Anhang II, III, 2(b) des Entscheidungsentwurfs.

[37] Rechtssache C-131/12 – Google Spain gegen Agencia Española de Protección de Datos und Mario Costeja González, 13. Mai 2014.

[38] Rechtssache C-73/0716 Tietosuojavaltuutettu gegen Satakunnan Markkinapörssi Oy und Satamedia Oy, 16. Dezember 2008.

39 Siehe auch die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte, insbesondere Von Hannover gegen Deutschland, Nr. 59320/00, Von Hannover gegen Deutschland (Nr. 2) [GK] Nrn. 40660/08 und 60641/08, und Axel Springer AG gegen Deutschland [GK] Nr. 39954/08.

[40] Siehe auch Artikel 9 der Richtlinie.

[41] In *Schrems*, Rn. 81, sagt der EuGH zum System der Selbstzertifizierung: *„[...] beruht die Zuverlässigkeit eines solchen Systems [...] wesentlich auf der Schaffung wirksamer Überwachungs- und Kontrollmechanismen, die es erlauben, in der Praxis etwaige Verstöße gegen Regeln zur Gewährleistung des Schutzes der Grundrechte, insbesondere des Rechts auf Achtung der Privatsphäre sowie des Rechts auf den Schutz personenbezogener Daten, zu ermitteln und zu ahnden“.*

[42] Siehe Zusatzgrundsätze in Anhang II.III.5 (c) des Datenschutzschildes.
[43] Artikel 29-Datenschutzgruppe in der Stellungnahme 01/2016 zur Entscheidung über die Angemessenheit des EU-US-Datenschutzschilds (WP 238), S. 27, und Artikel 29-Datenschutzgruppe, Schreiben an Vizepräsidentin Reding vom 10. April 2014, S. 5, abrufbar unter: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140410_wp29_to_ec_on_sh_recommendations.pdf.
[44] Entscheidungsentwurf, Punkt 50-51.
[45] Entscheidungsentwurf, S. 29.
[46] Judicial Redress Act of 2015, Pub.L. 114-126, H.R. 1428.
[47] Sec. 2h4a of the Judicial Redress Act.
[48] Wie der Health Insurance Portability and Accountability Act of 1996, Pub.L., 110 Stat. 1936 (HIPAA) oder der Children's Online Privacy Protection Act of 1998, Pub.L. 105-277, 112 Stat. 2681-728 (COPPA).
[49] Siehe Artikel 45 Absatz 2 Buchstabe b Datenschutz-Grundverordnung.