EUROPEAN DATA PROTECTION SUPERVISOR

Stellungnahme 1/2016

Vorläufige Stellungnahme zum 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

12. Februar 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. 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.

Diese Stellungnahme basiert auf der allgemeinen Verpflichtung, dass von der EU geschlossene internationale Vereinbarungen mit den Bestimmungen des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) übereinstimmen und die Grundrechte, die ein zentraler Grundsatz des Unionsrechts sind, wahren müssen. Die Bewertung erfolgt insbesondere mit Blick auf die Analyse der Übereinstimmung des Inhalts des Datenschutz-Rahmenabkommens mit den Artikeln 7, 8 und 47 der Charta der Grundrechte der Europäischen Union sowie mit Artikel 16 AEUV über den Schutz personenbezogener Daten.

ZUSAMMENFASSUNG

Die Untersuchung und Verfolgung von Straftaten ist ein legitimes politisches Ziel, und die internationale Zusammenarbeit einschließlich des Austauschs von Informationen ist heute wichtiger denn je. Bisher gibt es in der EU keinen verbindlichen einheitlichen Rahmen in diesem Bereich und daher keinen einheitlichen Schutz der Grundrechte und Grundfreiheiten des Einzelnen. Der EDSB weist bereits seit langem darauf hin, dass **die EU nachhaltige Abkommen über den Austausch personenbezogener Daten mit Drittländern zum Zwecke der Strafverfolgung braucht, die vollumfänglich mit den EU-Verträgen und der Charta der Grundrechte übereinstimmen**.

Daher **begrüßen und unterstützen wir aktiv die Bemühungen der Europäischen Kommission für den Abschluss eines ersten „Datenschutz-Rahmenabkommens“** mit den Vereinigten Staaten. Dieses Abkommen über die internationale Strafverfolgung soll erstmalig den Datenschutz als Grundlage für den Informationsaustausch einrichten. Auch wenn es nicht möglich ist, die Terminologie und Definitionen des Unionsrechts in einer Vereinbarung mit einem Drittland vollständig zu replizieren, muss der Schutz des Einzelnen eindeutig und wirksam geregelt sein, um eine vollumfängliche Übereinstimmung mit dem Primärrecht der EU zu gewährleisten.

Der Europäische Gerichtshof hat in den vergangenen Jahren die Grundsätze des Datenschutzes bestätigt, hierin eingeschlossen Gerechtigkeit, Richtigkeit und Relevanz von Daten, unabhängige Kontrolle und individuelle Rechte des Einzelnen. **Diese Grundsätze sind für öffentliche Einrichtungen ebenso relevant wie für Privatunternehmen, unabhängig von formalen Angemessenheitsfeststellungen der EU** im Hinblick auf Datenschutzgarantien von Drittländern. Angesichts der Sensibilität der für die Strafverfolgung erforderlichen Daten werden diese umso wichtiger.

Mit dieser Stellungnahme sollen die EU-Organe in konstruktiver und objektiver Weise beraten werden, da die Kommission diese schwierige Aufgabe abschließt, die weitreichende Auswirkungen hat, nicht nur auf die Zusammenarbeit zwischen der EU und den Vereinigten Staaten in der Strafverfolgung, sondern auch auf zukünftige internationale Abkommen. Das „Datenschutz-Rahmenabkommen“ ist ein vom kürzlich angekündigten „EU-US-Datenschutzschild“ für die Übermittlung personenbezogener Daten im Geschäftsverkehr getrenntes Dokument, muss jedoch mit diesem zusammen betrachtet werden. Zur Analyse der Interaktion dieser beiden Instrumente und der Modernisierung des EU-Datenschutzrahmens sind gegebenenfalls weitere Betrachtungen erforderlich.

Bevor das Abkommen dem Parlament zur Zustimmung vorgelegt wird, weisen wir die Parteien auf das Erfordernis hin, die Entwicklungen seit dem vergangenen September sorgfältig zu beleuchten, als sie ihre Absicht bekundeten, das Abkommen nach Verabschiedung des US-Gesetzes über den gerichtlichen Rechtsbehelf (Judicial Redress Act) zu schließen. Viele der bereits vorgesehenen Schutzmechanismen sind begrüßenswert, sollten jedoch verstärkt werden, auch im Lichte des Urteils *Schrems* von Oktober, mit dem das Safe-Harbor-Abkommen gekippt wurde, und des politisches Abkommens über die Modernisierung des EU-Datenschutzrahmens über Datentransfer sowie die polizeiliche und justizielle Zusammenarbeit von Dezember.

Der EDSB hat drei wesentliche Verbesserungen ermittelt, deren Umsetzung er für das Abkommen empfiehlt, um eine Übereinstimmung mit der Charta und Artikel 16 des Vertrags zu gewährleisten:

- Klarstellung, dass alle Schutzgarantien für alle natürlichen Personen gelten und nicht nur für EU-Bürger;
- Gewährleistung, dass die Bestimmungen zum gerichtlichen Rechtsbehelf im Sinne der Charta wirksam sind;
- Klarstellung, dass die massenhafte Übermittlung sensibler Daten unzulässig ist.

Die Stellungnahme umfasst weitere Empfehlungen für eine Klarstellung der geplanten Sicherheitsgarantien im Rahmen begleitender Erläuterungen. Für weiteren Rat und Dialog zu diesem Thema stehen wir den Organen jederzeit zur Verfügung.

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, 8 und 47,

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,

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 41 Absatz 2 und Artikel 46 Buchstabe d —

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

I. Kontext des paraphierten Abkommens

1. Am 3. Dezember 2010 billigte der Rat die Aufnahme von Gesprächen zwischen der Europäischen Union (EU) und den Vereinigten Staaten von Amerika (USA) über ein Abkommen zum Schutz personenbezogener Daten bei der Übermittlung und Verarbeitung zum Zwecke der Verhütung, Aufdeckung, Untersuchung und Verfolgung von Straftaten einschließlich terroristischer Akte im Rahmen der justiziellen und polizeilichen Zusammenarbeit in Strafsachen (im Folgenden das „Abkommen“)[1].

2. Die Verhandlungen zwischen der Kommission und den USA wurden am 29. März 2011 offiziell aufgenommen[2]. Am 25. Juni 2014 kündigte der US-Generalstaatsanwalt die Einleitung eines Gesetzgebungsverfahrens an, um Unionsbürgern einen gerichtlichen Rechtsbehelf im Zusammenhang mit Persönlichkeitsrechten in den USA zu gewähren[3]. Nach mehreren Verhandlungsrunden, die sich über vier Jahre erstreckten, wurde das Abkommen am 8. September 2015 paraphiert. Nach Aussage der Kommission sollen die Unterzeichnung und der formale Abschluss des Abkommens erst nach Verabschiedung des US Judicial Redress Act erfolgen[4].

3. Das Europäische Parlament muss dem paraphierten Text des Abkommens zustimmen, der Rat muss ihn unterzeichnen. Solange dies nicht geschehen und das Abkommen nicht formal unterzeichnet ist, können die Verhandlungen zu einzelnen Punkten neu aufgenommen werden. In eben diesem Kontext veröffentlicht der EDSB diese Stellungnahme auf der Grundlage des auf der Website der Kommission veröffentlichten Wortlauts des paraphierten Abkommens[5]. Bei vorliegendem Dokument handelt es sich um eine vorläufige Stellungnahme, basierend auf einer ersten Analyse eines komplexen Rechtsdokuments und unbeschadet weiterer Empfehlungen, die auf der Grundlage weiterer verfügbarer Informationen ausgesprochen werden können, hierin eingeschlossen rechtliche Entwicklungen in den USA, wie beispielsweise die Verabschiedung des Judicial Redress Act. Der EDSB hat drei wesentliche Punkte ermittelt, die einer Verbesserung bedürfen, und unterstreicht zudem andere Aspekte, für die wichtige Klarstellungen empfohlen werden. Mit diesen Verbesserungen kann das Abkommen als mit dem Primärrecht der EU konform betrachtet werden.

II. Grundsätze des EU-Rechts zur internationalen Übermittlung von Daten und Achtung der Grundrechte

4. Gemäß Artikel 216 Absatz 2 AEUV gilt, dass von der Union geschlossene internationale Übereinkünfte, wie das Abkommen, „*die Organe der Union und die Mitgliedstaaten*“ binden. Darüber hinaus bilden internationale Übereinkünfte gemäß ständiger Rechtsprechung des Gerichtshofs der Europäischen Union (EuGH) ab ihrem Inkrafttreten „*einen integrierenden Bestandteil [der Gemeinschaftsrechtsordnung]*“[6] und können Vorrang haben vor den Bestimmungen des abgeleiteten Unionsrechts[7].

5. Der EuGH befand im Hinblick auf von der EU geschlossene internationale Übereinkünfte, dass „die Verpflichtungen aufgrund einer internationalen Übereinkunft *nicht die Verfassungsgrundsätze des EG-Vertrags beeinträchtigen können, zu denen auch der Grundsatz zählt, dass alle Handlungen der Gemeinschaft die Menschenrechte achten müssen*, da die Achtung dieser Rechte eine Voraussetzung für ihre Rechtmäßigkeit ist, die der Gerichtshof im Rahmen des umfassenden Systems von Rechtsbehelfen, das dieser Vertrag schafft, überprüfen muss“[8]. Ausgangspunkt der folgenden Analyse ist das Erfordernis, dass internationale Übereinkünfte mit dem EU-System zum Schutz der Grundrechte übereinstimmen müssen.

6. Aus verschiedenen Rechtsinstrumenten in unterschiedlichen Anwendungsbereichen leiten wir ab, dass das EU-Datenschutzrecht, das nun im Lichte von Artikel 8 der Charta und Artikel 16 AEUV gelesen werden muss, grundsätzlich vorsieht, dass die internationale Übermittlung von Daten an ein Drittland nur dann ohne Beachtung weiterer Vorschriften erfolgen kann, wenn das betreffende Land ein angemessenes Schutzniveau gewährleistet[9]. Sichert ein Drittland kein angemessenes Schutzniveau zu, gelten Ausnahmen für *spezifische* Datenübermittlungen, sofern geeignete Schutzmaßnahmen ergriffen werden.

7. Die letzte Verhandlungsrunde zum Abkommen wurde abgeschlossen, bevor zwei bedeutende Entwicklungen in der EU stattfanden: die politische Einigung über die Modernisierung des EU-Datenschutzrahmens einschließlich der Datenschutz-Grundverordnung[10] und der Datenschutzrichtlinie[11] in Strafsachen sowie das Urteil des Gerichtshofs in der Rechtssache *Schrems*[12], mit dem das Safe Harbor-Abkommen gekippt wurde. Auch wenn sich dieses Urteil nicht unmittelbar auf die internationale Übermittlung von Daten in der Strafverfolgung bezieht, empfehlen wir doch seine Berücksichtigung bei der Bewertung der Rolle, die das Abkommen für das EU-Datenschutzrecht spielen wird. Grund hierfür ist, dass die zentralen Erkenntnisse[13] des Gerichtshofs Artikel 7, 8 und 47 der Charta mit Blick auf die Datenübermittlung[14] auslegen oder direkt anwenden und diese ebenso für den Bereich der Strafverfolgung gelten.

8. Der EU-Rechtsrahmen für den Datenschutz in der Strafverfolgung wird derzeit modernisiert. Der derzeitige Rechtsrahmen besteht aus verschiedenen Rechtsquellen, unter anderem:

a) Rahmenbeschluss 2008/977/JI[15] (im Folgenden „Rahmenbeschluss“), der für die internationale Übermittlung von Daten in der Strafverfolgung insoweit gilt, als die übermittelten Daten dem übermittelnden Mitgliedstaat zuerst von den zuständigen Behörden eines anderen Mitgliedstaats zur Verfügung gestellt wurden;

b) Verordnung Nr. 45/2001[16], die für die internationale Übermittlung von Daten gilt, sofern die Daten von einem Organ oder einer Einrichtung der EU übermittelt werden;
c) mehrere abgeleitete Rechtsakte des Unionsrechts – *lex specialis*, die sich auf die Übermittlung von Daten in Einzelfällen zum Zwecke der Strafverfolgung beziehen und gemäß denen die Datenübermittlung entweder vollständig untersagt[17] oder nur unter Beachtung sehr strenger Auflagen[18] oder auf der Grundlage einer Feststellung zulässig ist, dass im empfangenden Drittland ein angemessenes Datenschutzniveau gewährleistet wird[19];
d) einzelne internationale Übereinkünfte auf EU-Ebene und mitgliedstaatlicher Ebene, die als Rechtsgrundlage für die Datenübermittlung dienen[20];
e) nationale Datenschutzgesetze der Mitgliedstaaten über andere Arten der Datenübermittlung in der Strafverfolgung.

Trotz dieser Vielfalt der Rechtsinstrumente wird die Kohärenz durch die horizontale Anwendung der Charta und des AEUV, wie vorstehend genannt, gewährleistet. Zudem ist zu berücksichtigen, dass alle Mitgliedstaaten Konvention Nr. 108 des Europarats[21] unterzeichnet haben, die auf die Strafverfolgung Anwendung findet und derzeit ebenfalls modernisiert wird.

9. Die folgende Bewertung des vorgeschlagenen Abkommens berücksichtigt den aktuellen Stand des vorstehend genannten Unionsrechts mit Blick auf die internationale Übermittlung personenbezogener Daten in der Auslegung des EuGH und ihre Modernisierung.

III. Zweck, Umfang und Wirkung des Abkommens

1. Hohes Schutzniveau

10. Gemäß Artikel 1 Absatz 1 des Abkommens ist der Zweck des Abkommens, „*die Gewährleistung eines hohen Schutzniveaus für personenbezogene Informationen*“ und die „*Verbesserung der Zusammenarbeit zwischen den Vereinigten Staaten und der Europäischen Union zum Zwecke der Verhütung, Untersuchung, Aufdeckung und Verfolgung von Straftaten einschließlich terroristischer Akte*“. Die beiden Vertragsparteien erkennen im ersten Absatz der Präambel an, dass sie sich beide „*verpflichten, ein hohes Schutzniveau für personenbezogene Informationen zu gewährleisten, die in Verbindung mit der Verhütung, Untersuchung, Aufdeckung und Verfolgung von Straftaten einschließlich terroristischer Akte ausgetauscht werden*“. Somit bestätigt das Abkommen den Bedarf an einem hohen Schutzniveau für seine zukünftige Anwendung. Der EDSB begrüßt diese Schlussfolgerung, die dem allgemeinen EU-Datenschutzrecht[22] und der Rechtsprechung des EuGH in der Auslegung und Anwendung des Rechts auf den Schutz personenbezogener Daten gemäß Artikel 8 der Charta[23] entspricht. Der EDSB weist jedoch darauf hin, dass das hohe Schutzniveau sich vollständig in den Bestimmungen des Abkommens und seiner späteren Anwendung widerspiegeln muss, um wirksam zu sein und dem Primärrecht der EU zu entsprechen.

2. Konformitätsvermutung und Genehmigungen

11. Bezüglich der Wirkung des Abkommens sieht Artikel 5 Absatz 3 vor, dass „*mittels Inkraftsetzen von Abschnitt 2*“ über die Umsetzung in nationales Recht „***die Verarbeitung personenbezogener Informationen*** *durch die Vereinigten Staaten oder die Europäische Union und ihre Mitgliedstaaten im Hinblick auf Angelegenheiten, die in den Anwendungsbereich dieses Abkommens fallen,* ***als mit dem jeweiligen Datenschutzrecht***

***konform gelten**, das die internationale Übermittlung personenbezogener Daten beschränkt oder mit Auflagen versieht, **und keiner weiteren Genehmigung entsprechend dem jeweiligen Recht bedarf**“. Artikel 5 Absatz 3 legt offenbar fest, dass in Fällen, in denen die Parteien in ihren nationalen Rechtssystemen die Bestimmungen des Abkommens umgesetzt haben, jede Verarbeitung personenbezogener Daten im sachlichen Anwendungsbereich des Abkommens als mit dem „nationalen“ Datenschutzrecht der übermittelnden Länder über die internationale Datenübermittlung konform gilt.

12. Der Wortlaut dieser Bestimmung ist vergleichbar mit jenem aus dem Abkommen zwischen der Europäischen Union und den USA über Fluggastdatensätze, in dem die Eignung des Systems des US Department of Homeland Security für die Verarbeitung und Verwendung von Fluggastdatensätzen bestätigt wird (Artikel 19, „Angemessenheit“[24]). Das Abkommen bildet jedoch keine Entscheidung zur Angemessenheit[25] und ist kein eigenständiges Rechtsinstrument, da es die Rechtsgrundlage für die Datenübermittlung nur im Einzelfall ergänzt.

13. Dennoch begründet das Abkommen eine allgemeine Konformitätsvermutung. Vorbehaltlich des Vorhandenseins einer Rechtsgrundlage im Einzelfall werden in der Zukunft keine Genehmigungen mehr erforderlich sein. Daher ist es von wesentlicher Bedeutung sicherzustellen, dass diese „Vermutung“ durch alle erforderlichen Schutzmechanismen im Text des Abkommens untermauert wird.

14. In der „Struktur“ von Artikel 5 des Abkommens ist angegeben, dass Artikel 5 Absatz 3 erst wirksam wird, wenn Artikel 5 Absatz 2 vollumfänglich erfüllt wurde. Gemäß Artikel 5 Absatz 2 sind die Parteien verpflichtet, alle Maßnahmen zu ergreifen, die zur Umsetzung des Abkommens, insbesondere der Bestimmungen über Zugang, Berichtigung und administrative und gerichtliche Rechtsbehelfe, erforderlich sind. Darüber hinaus ist eindeutig angegeben, dass „*die im Abkommen vorgesehenen Schutzmechanismen und Rechtsbehelfe natürlichen und juristischen Personen **in der im anwendbaren nationalen Recht der einzelnen Parteien vorgesehenen Weise zur Verfügung stehen***“, was bedeutet, dass das Abkommen zwecks Wirksamkeit („um natürlichen und juristischen Personen zur Verfügung zu stehen“) in das nationale Recht der Parteien umgesetzt werden muss. Weitere Analysen sind erforderlich, um zu prüfen, in welchem Umfang, auch im Lichte der Rechtsprechung in der Rechtssache *Medellin*[26], das Abkommen als im US-Rechtssystem unmittelbar anwendbar gilt und welche wesentlichen Bestimmungen unter Umständen vom US-Kongress umgesetzt werden müssen, um es in bindendes nationales Recht umzuwandeln.

15. Das Abkommen bezieht sich auf Maßnahmen, die in den geltenden Rechtsrahmen der Parteien umgesetzt werden sollen. Allerdings ist offenbar kein spezifischer Mechanismus für die Bewertung des Grads der Umsetzung in das nationale Recht der Parteien zum Zwecke des Inkrafttretens von Artikel 5 Absatz 3 vorgesehen. Der in Artikel 23 vorgesehene Mechanismus der regelmäßigen gemeinsamen Prüfung scheint die allgemeine Zielsetzung zu verfolgen, die Wirksamkeit der „dieses Abkommen umsetzenden Politiken und Verfahren“ zu beurteilen, mit der Verpflichtung der Parteien, die erste gemeinsame Prüfung „spätestens drei Jahre nach dem Inkrafttreten“ des Abkommens durchzuführen. In diesem Kontext stellt sich die wesentliche Frage, „*wann die Übermittlung von Daten hinsichtlich Angelegenheiten, die in den Geltungsbereich des Abkommens fallen, **als konform** mit den Anforderungen des EU-Datenschutzrechts gilt, das die internationale Übermittlung personenbezogener Daten beschränkt oder mit Auflagen versieht, und keiner weiteren Genehmigung bedarf*“?

16. Hinsichtlich der Tatsache, dass Artikel 5 Absatz 3 des Abkommens die Aufgabe der zuständigen Behörden (Kontrollstellen für Datenschutz oder andere Organe in Abhängigkeit vom Rechtssystem des EU-Mitgliedstaats) der Genehmigung von Datenübermittlungen abschafft, möchte der EDSB daran erinnern, dass die Einrichtung unabhängiger Kontrollstellen in den EU-Mitgliedstaaten ein wesentlicher Bestandteil[27] der Wahrung des Schutzes der Betroffenen bei der Verarbeitung personenbezogener Daten[28] ist. Die nationalen Kontrollstellen sind für die Überwachung der Konformität mit EU-Datenschutzrecht gemäß Artikel 8 Absatz 3 der Charta verantwortlich, wobei jede Behörde bevollmächtigt ist, zu prüfen, ob die Übermittlung personenbezogener Daten aus dem eigenen Mitgliedstaat an ein Drittland mit geltendem Datenschutzrecht übereinstimmt, auch wenn das Rechtssystem des betreffenden Drittlands als angemessen[29] befunden wurde oder eine Konformitätsvermutung auf der Grundlage eines Abkommens vorliegt. Daher stellt der EDSB fest, dass das Fehlen weiterer Genehmigungen gemäß Artikel 5 Absatz 3 des Abkommens die Kompetenzen und Vollmachten unabhängiger Kontrollstellen nicht beeinträchtigt, die Rechtsmäßigkeit von Datenübermittlungen und die Konformität mit geltendem Datenschutzrecht zu überwachen, auch auf der Grundlage von Artikel 21 des Abkommens. Somit ist Artikel 5 Absatz 3 derart auszulegen, dass diese Aufgabe der Kontrollstellen im Sinne von Artikel 8 Absatz 3 der Charta zu erfüllen ist. Der EDSB empfiehlt zur eindeutigen Klarstellung, dass diese Schlussfolgerung in die begleitenden Erläuterungen zum Abkommen eingefügt wird.

3. Verbindung zwischen dem Abkommen und im Einzelfall geltenden Rechtsgrundlagen für die Datenübermittlung

17. Aus dem zweiten Abschnitt der Präambel geht hervor, dass das Abkommen zum Ziel hat, „*den Informationsaustausch zu fördern*“, nämlich in den für die Strafverfolgung relevanten Bereichen mittels Einrichtung eines „*Rahmens für den Schutz personenbezogener Daten bei ihrer Übermittlung*“ zwischen den Parteien [Artikel 1 Absatz 2]. Ferner geht aus Artikel 1 Absatz 3 eindeutig hervor, dass das Abkommen „*in sich und für sich selbst genommen keine Rechtsgrundlage für die Übermittlung personenbezogener Informationen darstellt*“ und „*stets eine Rechtsgrundlage für eine derartige Übermittlung erforderlich ist*“. Der vollständige Rechtsrahmen für die Schutzmaßnahmen in Verbindung mit vom Abkommen abgedeckte Datenübermittlungen besteht aus den Bedingungen des Abkommens, ihrer Umsetzung in das nationale Recht der Parteien und der im Einzelfall geltenden Rechtsgrundlage für die Datenübermittlung. Die Verbindung zwischen dem Abkommen und den folgenden Rechtsgrundlagen für die Übermittlung von Daten zwischen den Parteien ist sehr wichtig. Wir lesen Artikel 5 Absatz 1 in dem Sinne, dass alle im Einzelfall geltenden Instrumente, die eine Rechtsgrundlage für die Datenübermittlung bilden, die Anforderungen aus diesem Abkommen erfüllen müssen, die als Mindeststandard für das Schutzniveau bei der Datenübermittlung zu betrachten sind. Zum Zwecke der Rechtssicherheit empfiehlt der EDSB den Parteien eine Bestätigung – zumindest in den begleitenden Erläuterungen zum Abkommen – dahingehend, dass die im Einzelfall geltenden Rechtsgrundlagen für die Datenübermittlung vollumfänglich mit den im Abkommen vorgesehenen Schutzmaßnahmen übereinstimmen müssen und dass im Falle eines Konflikts zwischen der Rechtsgrundlage im Einzelfall und dem Abkommen letzteres Vorrang hat.

4. Weitergabe an staatliche Behörden

18. In Artikel 5 Absatz 2 des Abkommens ist angegeben, dass „*für die Vereinigten Staaten die Verpflichtungen in einer Weise gelten, die mit den Grundzügen des Föderalismus vereinbar sind*“. Diese Bestimmung kann Auswirkungen haben auf die Weitergabe von den

zuständigen Behörden auf nationaler Ebene in den Vereinigten Staaten, die Erstempfänger der Daten sind, an Stellen auf bundesstaatlicher Ebene, die nicht durch das Abkommen gebunden sind. In diesem Sinne definiert Artikel 2 Absatz 5 die „zuständige Behörde“ in den USA als eine „*nationale Strafverfolgungsbehörde, die für die Verhütung, Untersuchung, Aufdeckung und Verfolgung von Straftaten einschließlich terroristischer Akte verantwortlich ist*“, was Behörden auf bundesstaatlicher Ebene nicht einschließt[30]. Im Gegensatz hierzu sind alle Behörden der EU und ihrer Mitgliedstaaten mit vergleichbarer Zuständigkeit durch das Abkommen gebunden, wie in Artikel 2 Absatz 5 definiert.

19. Einige der potenziell negativen Auswirkungen der analysierten Bestimmung von Artikel 5 Absatz 2 können gegebenenfalls durch Artikel 14 Absatz 2 des Abkommens ausgeglichen werden, gemäß dem die Datenübermittlung von der Bundesebene an die bundesstaatliche Ebene ausgesetzt werden kann, wenn auf bundesstaatlicher Ebene „*personenbezogene Informationen unter Berücksichtigung des Zwecks dieses Abkommens nicht wirksam geschützt werden*“. Der EDSB begrüßt diese Bestimmung, empfiehlt jedoch eine Klarstellung – zumindest in den begleitenden Erläuterungen zum Abkommen – dahingehend, dass im Falle eines unzureichenden Schutzes von an die Bundesebene übermittelten Daten die relevanten Maßnahmen von Artikel 14 Absatz 2 bei Bedarf Maßnahmen hinsichtlich bereits weitergegebener Daten einschließen.

5. Ausnahme aus Gründen der nationalen Sicherheit

20. Gemäß Artikel 3 gilt das Abkommen für „*personenbezogene Informationen, die übermittelt werden*“ zwischen zuständigen Behörden der Parteien oder „*anderweitig übermittelt werden gemäß einer Vereinbarung*“ zwischen den USA und der EU oder ihren Mitgliedstaaten „*zum Zwecke der Verhütung, Untersuchung, Aufdeckung und Verfolgung von Straftaten einschließlich terroristischer Akte*“. Der EDSB begrüßt, dass bilaterale Vereinbarungen zwischen den *Mitgliedstaaten* und den USA ebenfalls in den Anwendungsbereich des Abkommens gestellt werden. Wir nehmen auch zur Kenntnis, dass „Datenübermittlungen *oder andere Formen der Zusammenarbeit zwischen den Behörden der Mitgliedstaaten und der Vereinigten Staaten mit Ausnahme der in Artikel 2 Absatz 5 genannten, die für den Schutz der nationalen Sicherheit zuständig sind*“ nicht in den Anwendungsbereich des Abkommens gemäß Artikel 3 Absatz 2 fallen.

21. Angesichts der breiten Definition der „*zuständigen Behörde*“ gemäß Artikel 2 Absatz 5, die sich im Hinblick auf US-Behörden auf eine „*nationale Strafverfolgungsbehörde, die für die Verhütung, Untersuchung, Aufdeckung und Verfolgung von Straftaten einschließlich terroristischer Akte verantwortlich ist*“, bezieht, in Verbindung mit den Bestimmungen von Artikel 6 Absatz 2, die sicherstellen, dass die weitere Verarbeitung übermittelter personenbezogener Daten „*durch andere Strafverfolgungs-, Regulierungs- oder Verwaltungsbehörden mit den sonstigen Bestimmungen dieses Abkommens übereinstimmen muss*“, folgern wir jedoch, dass nationale, für den Schutz der nationalen Sicherheit zuständige Behörden bei der Verarbeitung von Daten, die zu den im Abkommen definierten Zwecken übermittelt wurden, den Bestimmungen des Abkommens unterliegen. Zur eindeutigen Klarstellung kann diese Schlussfolgerung, sofern zutreffend, in die begleitenden Erläuterungen zum Abkommen eingefügt werden. Schließlich stellt der EDSB fest, dass die breite Definition der „zuständigen Behörde“ auch die Staatsanwaltschaft und Justizbehörden einschließt, sofern sie die vorstehend genannten Aufgaben in Verbindung mit Straftaten erfüllen.

6. Datenübermittlung von privaten Parteien an zuständige Behörden

22. Der EDSB stellt fest, dass sich das Abkommen zwar vornehmlich auf die Übermittlung von Daten zwischen zuständigen Behörden der Parteien bezieht, aber auch auf die Übermittlung von Daten zwischen privaten Parteien und zuständigen Behörden anwendbar sein kann, solange es ein Abkommen zwischen den USA und der EU oder ihren Mitgliedstaaten gibt. Diesbezüglich gilt das Abkommen gemäß Artikel 3 Absatz 1 für personenbezogene Daten, die zwischen zuständigen Behörden im Bereich der Strafverfolgung übermittelt werden „*oder anderweitig gemäß einer Vereinbarung zwischen den [USA] und der [EU] oder ihren Mitgliedstaaten übermittelt werden*". Daher schlussfolgern wir, dass sich das Abkommen auch auf die Datenübermittlung von relevanten Privatunternehmen wie Fluggesellschaften (z. B. Übermittlung von PNR-Daten) oder Dienstleistungsunternehmen, die öffentlich verfügbare elektronische Kommunikationsdienstleistungen anbieten, an zuständige Behörden der Parteien beziehen kann, allerdings nur, wenn diese Übermittlung auf der Grundlage einer internationalen Übereinkunft erfolgt.

7. Anwendung der Schutzmaßnahmen auf natürliche Personen

23. Artikel 3 („Geltungsbereich") enthält keinen spezifischen Verweis auf den *Personenkreis*, der vom Abkommen erfasst ist. Stattdessen wird ein breiter *sachlicher Anwendungsbereich* durch den Verweis angegeben, dass das Abkommen auf (alle) zwischen den Parteien in der Strafverfolgung „*übermittelten personenbezogenen Informationen*" anwendbar ist. Dieser allgemeine Verweis auf personenbezogene Daten scheint zu implizieren, dass die personenbezogenen Daten von natürlichen Personen ebenfalls durch die im Abkommen festgeschriebenen Schutzmaßnahmen geschützt sind. Diese Auslegung wird gestützt durch spezifische Verweise auf einen breiten Personenkreis in Artikel 16 „Zugang", Artikel 17 „Berichtigung" und Artikel 18 „Administrativer Rechtsbehelf" (da eine Bezugnahme auf „jedwede natürliche Person" erfolgt). Allerdings kann ein Widerspruch zur allgemeinen Bestimmung über die„Nicht-Diskriminierung" in Artikel 4 bestehen. Gemäß diesem Artikel muss jede Partei die Pflichten aus dem Abkommen erfüllen, um „*personenbezogene Informationen der eigenen Staatsbürger und der Staatsbürger der anderen Partei*" ohne willkürliche Diskriminierung zu schützen. Darüber hinaus bezieht sich Artikel 19 „Gerichtlicher Rechtsbehelf" allein auf „Staatsbürger" der Parteien.

24. Eine Umsetzung unter Ausschluss von Personen, die nicht Unionsbürger sind, vom durch das Abkommen erfassten Personenkreis würde bedeuten, dass das Abkommen nicht das in Artikel 7, 8 und 47 der Charta geforderte Schutzniveau gewährleistet, gemäß denen die Grundrechte auf Achtung der Privatsphäre, Schutz personenbezogener Daten und einen wirksamen Rechtsbehelf für „jeden" in der EU unabhängig von Nationalität oder Status gelten. Daher empfiehlt der EDSB eine wichtige Klarstellung – zumindest in den begleitenden Erläuterungen zum Abkommen – dahingehend, dass der vom Abkommen erfasste Personenkreis mit der Charta übereinstimmt.

IV. Analyse der wesentlichen Bestimmungen des Abkommens

1. Begriffsbestimmungen

25. Das EU-Datenschutzrecht umfasst etablierte Definitionen für Begriffe wie „personenbezogene Daten" und „Verarbeitung [personenbezogener Daten]". Auch wenn die im Text des Abkommens gewählte Terminologie in Teilen vom EU-Datenschutzrecht

abweicht – da das Abkommen von „personenbezogenen Informationen“ und nicht von „personenbezogenen Daten“ spricht, begrüßt der EDSB die breite Definition von „personenbezogenen Daten“ von Artikel 2 Absatz 1, die der entsprechenden Definition „personenbezogener Daten“ aus der Richtlinie 95/46/EG und Verordnung Nr. 45/2001 folgt. Die Definition in Artikel 2 Absatz 1 des Abkommens bezieht sich jedoch nicht auf „jedwede Informationen“, sondern lediglich auf „Informationen“. Daher können beispielsweise Zweifel dahingehend aufkommen, ob Metadaten, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen, als personenbezogene Informationen gemäß dem Abkommen gelten.

26. Hinsichtlich der Definition einer „Verarbeitung personenbezogener Informationen“ von Artikel 2 Absatz 2 des Abkommens sind einige wesentliche Unterschiede im Vergleich zur Definition der „Verarbeitung personenbezogener Daten“ aus der Richtlinie 95/46/EG und Verordnung Nr. 45/2001 festzustellen. Gemäß Definition im Abkommen bedeutet die „Verarbeitung personenbezogener Informationen“ „*jeden Vorgang oder jede Kombination von Vorgängen, die eine Erfassung, Wartung, Nutzung, Änderung, Organisation oder Strukturierung, Offenlegung oder Verbreitung oder Verfügbarmachung umfasst*“. Im Gegensatz zu den relevanten EU-Instrumenten schließt diese Definition Vorgänge aus dem Geltungsbereich des Abkommens aus, die eine „*Aufzeichnung, Speicherung, Abfrage, einen Abruf, eine Anpassung oder Kombination, Sperrung, Löschung oder Vernichtung*“ beinhalten. Andererseits bezieht sich Artikel 2 Absatz 1 des Abkommens im Gegensatz zur Definition im EU-Datenschutzrecht auf die „*Wartung*“ und „*Verfügbarmachung*“. Diese beiden Begriffe scheinen die im EU-Datenschutzrecht aufgelisteten Vorgänge nicht abzudecken.

27. Daher wird eine Klarstellung empfohlen, um die Anwendung der im Abkommen vorgesehenen Schutzmaßnahmen bei Schlüsselvorgängen zu gewährleisten, beispielsweise wenn eine zuständige Behörde Daten aufzeichnet oder empfangene Informationen lediglich speichert, ohne sie anderweitig zu nutzen. Klargestellt werden sollte, dass der „Abruf“, ein in der Begriffsbestimmung ebenfalls fehlender Begriff, im Begriff „Verwendung“ eingeschlossen ist, da in der Praxis Missbrauch oft durch unrechtmäßigen Abruf personenbezogener Daten entsteht.

28. Der EDSB empfiehlt daher eine Definition der Verarbeitungsvorgänge, die mit den grundlegenden Anforderungen des Unionsrechts übereinstimmen, um die vorstehend genannten Schlüsselvorgänge einzuschließen, beispielsweise die Aufzeichnung und Speicherung von Daten. Sollten die Parteien die Definitionen der Begriffe „personenbezogene Informationen“ und „Verarbeitungsvorgang“ nicht vollständig mit jenen aus dem Unionsrecht in Einklang bringen, empfiehlt der EDSB eine Klarstellung in den begleitenden Erläuterungen zum Abkommen dahingehend, dass die Anwendung der beiden Begriffe im Wesentlichen nicht von ihrer Bedeutung gemäß Unionsrecht abweicht.

2. Zweckbeschränkung und Weitergabe

29. Der EDSB begrüßt die im letzten Abschnitt der Präambel ausgeführte Anerkennung der Grundsätze der Verhältnismäßigkeit und Notwendigkeit. Vor diesem Hintergrund beschränkt Artikel 6 Absatz 1 des Abkommens die Übermittlung personenbezogener Informationen auf „*spezifische, gemäß der Rechtsgrundlage für die Übermittlung zulässige Zwecke (...)*“, und Artikel 6 Absatz 5 sieht ergänzend vor, dass sie zu verarbeiten sind „*in einer Weise, die in Relation zu den Zwecken einer solchen Verarbeitung unmittelbar relevant und nicht*

unangemessen oder übermäßig großzügig ist“. Darüber hinaus ist gemäß Artikel 6 Absatz 2 eine weitere Verarbeitung untersagt, sofern diese mit dem Zweck der Übermittlung nicht vereinbar ist.

30. Hinsichtlich der Weitergabe an einen Staat, der nicht Partei des Abkommens ist, ist gemäß Artikel 7 Absatz 1 und 2 die Zustimmung der zuständigen Behörde erforderlich, die die personenbezogenen Daten ursprünglich übermittelt hat, wobei zu diesem Zweck „*alle relevanten Faktoren*“ der Bestimmung ordnungsgemäß zu berücksichtigen sind. Dieses Schutzniveau wird weiter gestärkt durch die Möglichkeit, die Übermittlung personenbezogener Daten an Behörden von Gebietseinheiten der Parteien gemäß Artikel 14 Absatz 2 des Abkommens auszusetzen, sofern die Bestimmungen zur Zweckbeschränkung und Weitergabe nicht eingehalten werden. Der EDSB begrüßt diese Bestimmungen.

31. In Artikel 7 Absatz 3 ist ferner vorgesehen, dass in Fällen, in denen die Parteien eine Übereinkunft zu Datenübermittlungen schließen, die sich nicht nur auf Einzelfälle bezieht, die „besonderen Bedingungen“ des Abkommens zur Genehmigung von Datenübermittlungen zu beachten sind. Wir stellen fest, dass solche Übermittlungen in der Praxis auch die massenhafte Übermittlung von Daten umfassen können. Entsprechende Bedingungen sind in Artikel 7 Absatz 3 nicht festgelegt. Die massenhafte Verarbeitung von Daten stellt aufgrund der betroffenen Anzahl an Personen und der Menge personenbezogener Daten eine schwerwiegende Verletzung des Rechts auf Privatsphäre und auf den Schutz personenbezogener Daten dar[31]. Wir würden die Aufnahme einer als Hinweis dienenden Liste der vorstehend genannten „besonderen Bedingungen“ in die begleitenden Erläuterungen begrüßen.

3. Informationssicherheit

32. Der EDSB begrüßt die Bestimmungen von Artikel 9 zur Informationssicherheit. Hinsichtlich der Meldung von Informationssicherheitsvorfällen erlaubt Artikel 10 Absatz 2 Buchstabe b jedoch eine Nichtmeldung von Datenschutzverletzungen, wenn eine Meldung „*die nationale Sicherheit gefährden könnte*“, wobei die Wirkung dieser Bestimmung auf der Grundlage einer möglichen Folge („*könnte*“) für die nationale Sicherheit unklar ist. Der EDSB hinterfragt auch die grundsätzliche Notwendigkeit einer Nichtmeldung und gibt zu bedenken, dass eine verzögerte Meldung oder eine Beschränkung der Meldung auf einen bestimmten Empfängerkreis aus Sicherheitsgründen ausreichen könnte. Spezifische Bestimmungen über eine verzögerte Meldung bei der übermittelnden zuständigen Behörde sind im Text nicht zu finden. Der EDSB empfiehlt, in begleitenden Erläuterungen auf die Absicht der Parteien hinzuweisen, diese Bestimmungen anzuwenden, um einerseits Nichtmeldungen auf ein Minimum zu beschränken und andererseits übermäßig verzögerte Meldungen zu vermeiden, aufgrund derer eine zuständige Behörde über einen langen Zeitraum nicht über Datenschutzverletzungen hinsichtlich der von ihr übermittelten Daten informiert wäre.

4. Datenaufbewahrung

33. Gemäß Artikel 12 Absatz 1 sind die Parteien aufgefordert, „*sicherzustellen, dass personenbezogene Informationen nicht länger als nötig und angemessen aufbewahrt werden*“. Im Lichte der im Abkommen aufgeführten Zweckbeschränkung sollte folgende Regelung hinzugefügt werden: „*zu den spezifischen Zwecken, zu denen sie übermittelt wurden*“.

34. Darüber hinaus sollte Artikel 12 Absatz 2, der sich auf die Datenaufbewahrung im Falle massenhafter Übermittlungen bezieht, auch auf die Kriterien Bezug nehmen, die zu berücksichtigen sind, um die Aufbewahrungsdauer gemäß Artikel 12 Absatz 1 unter Berücksichtigung der Grundsätze der Verhältnismäßigkeit und Notwendigkeit zu bestimmen.

5. Massenhafte Übermittlung sensibler Daten

35. Angesichts der Tatsache, dass der Begriff „sensible Daten" von den Parteien unterschiedlich verwendet wird[32], sind die in Artikel 13 Absatz 1 aufgeführten besonderen Datenkategorien zu begrüßen, da der Text die Bedeutung sensibler Daten zum Zwecke des Abkommens klarstellt und an die EU-Definition anpasst[33].

36. Der EDSB ist jedoch besorgt, dass Artikel 13 Absatz 2 die Möglichkeit einer massenhaften Übermittlung sensibler Daten einräumt, da der Abschluss einer Übereinkunft zwischen den USA und der EU oder einem Mitgliedstaat zugelassen wird, um eine „*Übermittlung personenbezogener Informationen, die sich nicht auf Einzelfälle, Ermittlungen oder Strafverfolgung beziehen*", zu ermöglichen. Auch wenn in Artikel 13 Absatz 2 gefordert wird, dass die Art der Informationen zu berücksichtigen ist, wird es doch den jeweiligen Übereinkünften überlassen, die auszutauschenden Datenkategorien zu definieren. In diesem Kontext verweist der EDSB auf seine vorherigen Stellungnahmen zur Verwendung von Fluggastdatensätzen, in denen er sich für den vollständigen Ausschluss sensibler Daten von massenhaften Übermittlungen ausspricht[34]. Der EDSB stellte insbesondere die Verarbeitung sensibler Daten durch das Department of Homeland Security infrage und empfahl, im fraglichen Abkommen ausdrücklich vorzusehen, dass Fluggesellschaften sensible Daten nicht an das Department übermitteln[35].

37. Daher empfiehlt der EDSB, die massenhafte Übermittlung sensibler Daten vom Geltungsbereich des Abkommens auszunehmen.

6. Rechte der betroffenen Person

38. Der EDSB begrüßt, dass das Abkommen verschiedene Rechte der betroffenen Person vorsieht: das Recht auf Auskunft (Artikel 20), das Recht auf Zugang (Artikel 16), das Recht auf Berichtigung, das auch Löschung und Sperrung einschließt (Artikel 17), das Recht auf administrative und gerichtliche Rechtsbehelfe (Artikel 18 und 19) und das Recht, keinen automatisierten Entscheidungen unterworfen zu sein (Artikel 15). Der EDSB möchte daran erinnern, dass die Rechte der betroffenen Person und insbesondere die Rechte auf Zugang und Berichtigung als wesentliche Elemente des Rechts auf den Schutz personenbezogener Daten in Artikel 8 Absatz 2 der Charta festgeschrieben sind.

39. Im Abkommen sind erhebliche Ausnahmen von der Ausübung des Zugangs- und Auskunftsrechts vorgesehen. Hinsichtlich des Zugangsrechts sieht Artikel 16 Absatz 2 eine Zugangsbeschränkung bei Vorliegen zusätzlicher Kriterien vor, beispielsweise zwecks Vermeidung der Behinderung „*offizieller oder rechtlicher Anfragen, Ermittlungen und Verfahren*", Schutz von „*für die Strafverfolgung sensiblen Informationen*", Vermeidung der Behinderung einer „*Verhütung, Untersuchung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung*" neben der „*öffentlichen und nationalen Sicherheit*". Eine weitere Ausnahme besagt, dass der Zugang beschränkt werden kann, um die „*gesetzlich vorgesehenen Interessen im Hinblick auf die Informationsfreiheit und den öffentlichen*

Zugang zu Dokumenten zu schützen“[36]. Schwer vorstellbar ist eine Situation, in der zum Zwecke dieses Abkommens übermittelte personenbezogene Daten von der zuständigen Behörde nicht als „*für die Strafverfolgung sensible Informationen*“ befunden werden, solange keine besonderen Kriterien dahingehend vorliegen[37], was unter dem Begriff „für die Strafverfolgung sensible Informationen“ genau zu verstehen ist.

40. Der EDSB empfiehlt eine Überarbeitung der Ausnahmenliste, um sicherzustellen, dass die betroffene Person *de facto* überhaupt die Möglichkeit hat, auf ihre eigenen Daten zuzugreifen, auch wenn nur in beschränktem Umfang oder durch eine dritte Vertrauensperson in Fällen, in denen der Zugang verweigert wird, um für die Strafverfolgung sensible Informationen zu schützen. In diesem Sinne wird Artikel 16 Absatz 4 begrüßt, da dort ein indirekter Zugang vorgesehen ist. Allerdings ist seine Anwendung nur auf gemäß geltendem nationalem Recht zulässige“ Fälle beschränkt.

41. Darüber hinaus erlaubt Artikel 16 Absatz 1 den Zugang zu Daten „*gemäß dem anwendbaren Rechtsrahmen des Staates, in dem Rechtsschutz beantragt wird*“. Wären die derzeit in den USA geltenden rechtlichen Zugangsvorschriften auf gemäß dem Abkommen übermittelte Daten anwendbar, wären die Bestimmungen von Artikel 8 Absatz 2 der Charta dem ersten Anschein nach nicht erfüllt. Auch wenn der US Privacy Act aus dem Jahr 1974 natürlichen Personen ein Recht auf Zugang zu ihren personenbezogenen Daten einräumt[38], wird dieses Recht doch durch verschiedene Ausnahmeregelungen erheblich beschnitten[39]. Erstens sieht eine Ausnahmeregelung vor, dass sich dieses Recht nicht auf Informationen bezieht, die *„in begründeter Erwartung einer Zivilklage oder eines Zivilverfahrens zusammengestellt wurden“*[40]. Zweitens wird durch allgemeine Ausnahmen die Pflicht auf Zugangsgewährung untergraben, wenn eine Behörde, deren Hauptaufgabe im Bereich der Strafverfolgung liegt, unter Berufung auf diese Ausnahme eine Vorschrift erlässt[41]. Drittens sehen bestimmte Ausnahmen unter anderem vor, dass eine Behörde eine Vorschrift erlassen kann, mit der sie selbst von der Pflicht befreit wird, Zugang zu einem Speichersystem zu gewähren, das als vertraulich eingestufte Informationen enthält, bei denen es sich um „Material im Bereich der Landesverteidigung oder Außenpolitik handelt oder um Untersuchungsmaterial, das zum Zwecke der Strafverfolgung zusammengestellt wurde“[42]. Diese Ausnahmen beschneiden die Ausübung des Zugangsrechts erheblich, wenn es entsprechend den derzeit in den USA geltenden gesetzlichen Bestimmungen ausgeübt werden sollte.

42. Ein wirksames Recht auf Auskunft ist wichtig. In diesem Zusammenhang stellte der EuGH fest, dass, „*dieses Erfordernis einer Unterrichtung der von der Verarbeitung ihrer personenbezogenen Daten betroffenen Personen umso wichtiger*“ ist, „*als es die Voraussetzung dafür schafft, dass sie ihr [...] Auskunfts- und Berichtigungsrecht in Bezug auf die verarbeiteten Daten [...] ausüben können*“[43]. Die Bestimmung zur „Transparenz“ (Artikel 20) hat sehr eingeschränkte Wirkung aufgrund der Tatsache, dass die Informationsmitteilungen zu veröffentlichen sind „*in einer Form und zu einer Zeit, die in dem für die die Mitteilung ausgebende Behörde anwendbaren Recht festgeschrieben sind*“, was in der Praxis bedeuten könnte, dass selbst allgemeine Informationsmitteilungen erst lange nach Durchführung einer bestimmten Übermittlung oder Verarbeitung veröffentlicht werden könnten. Darüber hinaus gelten alle Beschränkungen des Zugangsrechts gleichermaßen auch für die Transparenzpflicht.

43. Als Ergebnis dieser vorläufigen Analyse vertritt der EDSB die Auffassung, dass die Parteien des Abkommens mehr dafür tun sollten, sicherzustellen, dass Beschränkungen der

Ausübung des Zugangsrechts selektiv auf das limitiert werden, was unerlässlich ist, um die genannten öffentlichen Interessen zu wahren und die Transparenzpflicht zu stärken.

44. Der EDSB begrüßt, dass automatisierte Entscheidungen gemäß Artikel 15 „*nicht allein auf der automatisierten Verarbeitung personenbezogener Informationen ohne menschliche Beteiligung basieren dürfen*". Dies ist im Bereich der Strafverfolgung besonders wichtig, da hier die Folgen einer Erstellung von Profilen natürlicher Personen schwerwiegender sein können. Die Schwelle, ab der Artikel 15 zur Anwendung kommt, ist jedoch recht hoch, da gefordert wird, dass die Entscheidungen „*wesentliche nachteilige Maßnahmen*" bewirken müssen, um nicht allein auf automatisierten Verarbeitungen zu basieren, wohingegen gemäß Unionsrecht eine derartige Entscheidung untersagt ist, „*die eine nachteilige Rechtsfolge für die betroffene Person hat oder sie erheblich beeinträchtigt*"[44].

7. Gerichtliche und administrative Rechtsbehelfe

45. Im unterschiedlichen Kontext einer Angemessenheitsfeststellung (Safe Harbor-Entscheidung) stellte der EuGH fest[45], dass das Fehlen eines wirksamen gerichtlichen Rechtsbehelfs im Falle der Übermittlung personenbezogener Daten an ein Drittland dem Wesensgehalt von Artikel 47 der Charta widerspricht, der das Recht auf wirksamen gerichtlichen Rechtsschutz vorsieht. In diesem Zusammenhang befand der EuGH, dass „*eine Regelung, die keine Möglichkeit für den Bürger vorsieht, mittels eines Rechtsbehelfs Zugang zu den ihn betreffenden personenbezogenen Daten zu erlangen oder ihre Berichtigung oder Löschung zu erwirken, den Wesensgehalt des in Art. 47 der Charta verankerten Grundrechts auf wirksamen gerichtlichen Rechtsschutz*" verletzt und stellte fest: „*Nach Art. 47 Abs. 1 der Charta hat nämlich jede Person, deren durch das Recht der Union garantierte Rechte oder Freiheiten verletzt worden sind, das Recht, nach Maßgabe der in diesem Artikel vorgesehenen Bedingungen bei einem Gericht* ***einen wirksamen Rechtsbehelf*** *einzulegen*"[46].

46. Gemäß Artikel 19 Absatz 1 und 2 des Abkommens sind die Parteien verpflichtet, in ihren jeweils geltenden Rechtsrahmen ihren *Bürgern* die Möglichkeit einzuräumen, eine Verweigerung den Rechts auf Zugang zu oder Berichtigung von Daten oder die mutwillig unrechtmäßige Offenlegung von Informationen gerichtlich überprüfen zu lassen. Während Artikel 19 Absatz 1 und 2 Rechtsbehelfe für Unionsbürger in Verbindung mit einigen der wesentlichen Bestimmungen des Abkommens einräumen, haben *natürliche Personen, die nicht Unionsbürger* und anderweitig über die Charta geschützt sind (z. B. Asylbewerber, in der EU ansässige Personen) auf der Grundlage dieser beiden Absätze nicht die Möglichkeit, Rechtsbehelfe einzulegen, um Zugang zu sie betreffenden personenbezogenen Daten zu erlangen oder deren Berichtigung zu erwirken. Darüber hinaus steht weder Unionsbürgern noch Nicht-Unionsbürgern ein Rechtsbehelf zur Verfügung, um die *Löschung* von Daten zu erwirken. Artikel 19 Absatz 3 sieht vor, dass diese Einschränkungen „*unbeschadet jeder anderen gerichtlichen Überprüfung einer Verarbeitung der eine natürliche Person betreffenden personenbezogenen Daten gelten, die gemäß dem Recht des Staates verfügbar ist, in dem der Rechtsbehelf eingelegt wird*". Der EDSB ist in dieser vorläufigen Stellungnahme nicht in der Lage, die Wirksamkeit alternativer Rechtsbehelfe, die gegebenenfalls in sektoralen Rechtsvorschriften, insbesondere in den USA und auf Staatenebene, vorgesehen sind, und die Frage, in welchem Umfang sie einen organischen und umfassenden Rechtsbehelf für alle betroffenen Einzelpersonen darstellen könnten, zu bewerten. Daher bestehen erhebliche Bedenken bezüglich der Übereinstimmung von Artikel 19 mit der Charta. Die **Wirksamkeit** der Rechtsbehelfe, die auch in Artikel 47 der

Charta gefordert wird, muss beurteilt werden, nachdem die Bestimmungen des Abkommens in das nationale Recht der USA umgesetzt wurden[47].

47. Bezüglich des administrativen Rechtsbehelfs stellt der EDSB fest, dass sich Artikel 18 auf den von der zuständigen Behörde, und nicht auf den von einer Kontrollstelle eingeräumten administrativen Rechtsbehelf bezieht, wie in Artikel 2 des Abkommens definiert. Artikel 18 Absatz 1 sieht vor, dass diese Art des administrativen Rechtsbehelfs für angebliche Verletzungen des Rechts auf Zugang, Berichtigung und Löschung gilt. Der EuGH hat betont, dass es für natürliche Personen wesentlich ist, Beschwerden bei unabhängigen Kontrollstellen vorbringen[48] und somit einen administrativen Rechtsbehelf einlegen zu können. Der EDSB liest die Bestimmung zur wirksamen Kontrolle (Artikel 21) und jene zum administrativen Rechtsbehelf (Artikel 18) dahingehend, dass die Möglichkeit für natürliche Personen, nach einer Verletzung von Artikel 16 und 17 des Abkommens (Recht auf Zugang, Berichtigung und Löschung) Beschwerde bei einer Kontrollstelle einzulegen, nicht beschränkt wird.

8. Wirksame Kontrolle

48. Der EDSB begrüßt die Bestimmungen zur Rechenschaftspflicht von Artikel 14, wie in Absatz 19 dieser Stellungnahme erwähnt. Allerdings sollten diese Bestimmungen um eine unabhängige externe Kontrolle ergänzt werden.

49. Diesbezüglich verweist der EDSB darauf, dass Artikel 8 Absatz 3 der Charta vorsieht, dass die Einhaltung der Datenschutzvorschriften von einer unabhängigen Stelle überwacht werden muss[49], was laut EuGH eine Stelle bedeutet, die in ihren Entscheidungen jeglicher Einflussnahme von außen, sei sie unmittelbar oder mittelbar, entzogen ist. Eine solche Kontrollstelle muss nicht nur von den überwachten Parteien unabhängig sein, sondern darf auch nicht Teil des Staates sein, da dieser selbst betroffene Partei sein kann.[50]

50. Der EDSB begrüßt das in Artikel 21 Absatz 1 Buchstabe a festgeschriebene Erfordernis, dass die Kontrollstellen „*unabhängige Aufsichtsfunktionen und -vollmachten ausüben*“ müssen. Auch im Lichte der aktuellen Debatte um wirksame Vollmachten für einige US-Kontrollstellen zur **Durchsetzung** des Datenschutzrechts und des Schutzes der Privatsphäre[51], wie in Artikel 21 Absatz 3 aufgeführt, erachten wir es für wesentlich, dass die Parteien dem Abkommen bilateral unterzeichnete begleitende Erläuterungen beifügen, in denen insbesondere folgende Angaben enthalten sind:

- die Kontrollstellen, die in dieser Sache zuständig sind, und der den Parteien zur Verfügung stehende Mechanismus, um sich gegenseitig über zukünftige Änderungen zu informieren;
- die ihnen tatsächlich zuerkannten Vollmachten;
- Name und Kontaktdaten der Kontaktperson, die bei der Ermittlung der zuständigen Kontrollstelle unterstützend tätig werden kann (siehe Artikel 22 Absatz 2). [52]

9. Gemeinsame Prüfung und Aussetzung

51. Der EDSB begrüßt Artikel 23 zur gemeinsamen Prüfung des Abkommens. Artikel 23 Absatz 3 vermeidet eine „doppelte Durchführung“ gemeinsamer Prüfungen, was Einfluss auf bereits in bestehenden Übereinkünften vorgesehene gemeinsame Prüfungen hat: Allerdings wird der EU-Kommission empfohlen, klarzustellen, welcher Einfluss sich auf die Umsetzung

spezifischer Übereinkünfte ergeben könnte, beispielsweise auf die Abkommen zur Verwendung und Übermittlung von Fluggastdatensätzen[53] oder Zahlungsverkehrsdaten[54].

52. Der EDSB begrüßt auch die Tatsache, dass Artikel 26 eine Aussetzung des Abkommens im Falle einer wesentlichen Verletzung seiner Bestimmungen vorsieht. Zu diesem Zweck unterstreicht der EDSB die herausragende Rolle einer unabhängigen Kontrolle der Anwendung des Abkommens, damit Verletzungen überhaupt erkannt und ermittelt werden können.

V. Schlussfolgerungen

53. Der EDSB begrüßt die Absicht, ein rechtsverbindliches Instrument zu verabschieden, mit dem ein hohes Schutzniveau für personenbezogene Daten sichergestellt werden soll, die zwischen der EU und den USA zum Zwecke der Verhütung, Aufdeckung, Untersuchung und Verfolgung von Straftaten, einschließlich terroristischer Akte, übermittelt werden.

54. Die meisten wesentlichen Bestimmungen des Abkommens entsprechen vollumfänglich oder in Teilen den wesentlichen Garantien des Rechts auf den Schutz personenbezogener Daten in der EU (beispielsweise Rechte der betroffenen Person, unabhängige Kontrolle und Recht auf gerichtliche Überprüfung).

55. Auch wenn das Abkommen aus technischer Sicht keine Angemessenheitsfeststellung darstellt, schafft es doch eine allgemeine Konformitätsvermutung für Übermittlungen auf der Grundlage einer im Einzelfall geltenden Rechtsgrundlage im Rahmen des Abkommens. Daher ist es von wesentlicher Bedeutung, sicherzustellen, dass diese „Vermutung“ durch alle erforderlichen Schutzmechanismen im Text des Abkommens untermauert wird, um eine Verletzung der Charta, insbesondere der Artikel 7, 8 und 47, zu vermeiden.

56. Der EDSB hat drei wesentliche Verbesserungen ermittelt, deren Umsetzung er für das Abkommen empfiehlt, um eine Übereinstimmung mit der Charta und Artikel 16 AEUV zu gewährleisten:

1) Klarstellung, dass alle Schutzgarantien für alle natürlichen Personen gelten und nicht nur für EU-Bürger;

2) Gewährleistung, dass die Bestimmungen zum gerichtlichen Rechtsbehelf im Sinne der Charta wirksam sind;

3) Klarstellung, dass die massenhafte Übermittlung sensibler Daten unzulässig ist.

57. Darüber hinaus empfiehlt der EDSB zum Zwecke der Rechtssicherheit, die folgenden Verbesserungen oder Klarstellungen in den Text des Abkommens oder in begleitende Erläuterungen zum Abkommen oder in die Umsetzungsphase des Abkommens aufzunehmen, wie in dieser Stellungnahme ausgeführt:

1) dass Artikel 5 Absatz 3 derart auszulegen ist, dass die Aufgabe der Kontrollstellen im Sinne von Artikel 8 Absatz 3 der Charta gewahrt bleibt;
2) dass die im Einzelfall geltenden Rechtsgrundlagen für die Datenübermittlung (Artikel 5 Absatz 1) vollumfänglich mit den im Abkommen vorgesehenen

Schutzmaßnahmen übereinstimmen müssen, und im Falle eines Konflikts zwischen der Rechtsgrundlage im Einzelfall und dem Abkommen letzteres Vorrang hat;

3) dass im Falle eines unzureichenden Schutzes von an die Bundesebene übermittelten Daten die relevanten Maßnahmen von Artikel 14 Absatz 2 bei Bedarf Maßnahmen hinsichtlich bereits weitergegebener Daten einschließen;
4) dass die Definitionen der Begriffe „personenbezogene Informationen“ und „Verarbeitungsvorgang“ (Artikel 2) mit den etablierten Definitionen aus dem Unionsrecht in Einklang zu bringen sind. Bei einer nicht vollständigen Übereinstimmung dieser Definitionen wird eine Klarstellung in den begleitenden Erläuterungen zum Abkommen dahingehend empfohlen, dass die Anwendung der beiden Begriffe im Wesentlichen nicht von ihrer Bedeutung gemäß Unionsrecht abweicht;
5) dass eine als Hinweis dienende Liste der „besonderen Bedingungen“ für die massenhafte Übermittlung von Daten (Artikel 7 Absatz 3) in die begleitenden Erläuterungen aufgenommen werden könnte;
6) dass die Parteien die Bestimmungen zur Meldung von Datenschutzverletzungen (Artikel 10) anzuwenden beabsichtigen, um einerseits Nichtmeldungen auf ein Minimum zu beschränken und andererseits übermäßig verzögerte Meldungen zu vermeiden;
7) dass im Lichte der im Abkommen aufgeführten Zweckbeschränkung die Bestimmung zur Datenaufbewahrung von Artikel 12 Absatz 1 um den Zusatz „*zu den spezifischen Zwecken, zu denen sie übermittelt wurden*“ ergänzt wird;
8) dass die Parteien des Abkommens mehr dafür tun werden, sicherzustellen, dass Beschränkungen der Ausübung des Zugangsrechts auf das limitiert werden, was unerlässlich ist, um die genannten öffentlichen Interessen zu wahren, und die Transparenzpflicht zu stärken;
9) dass detaillierte begleitende Erläuterungen dem Abkommen beigefügt werden und insbesondere folgende Angaben enthalten (Artikel 21):
    - die Kontrollstellen, die in dieser Sache zuständig sind, und der den Parteien zur Verfügung stehende Mechanismus, um sich gegenseitig über zukünftige Änderungen zu informieren;
    - die ihnen tatsächlich zuerkannten Vollmachten;
    - Name und Kontaktdaten der Kontaktperson, die bei der Ermittlung der zuständigen Kontrollstelle unterstützend tätig werden kann (siehe Artikel 22 Absatz 2).

58. Abschließend möchte der EDSB auf das Erfordernis hinweisen, dass jede Auslegung, Anwendung und Umsetzung des Abkommens im Falle mangelnder Klarheit oder eines augenscheinlichen Konflikts von Bestimmungen derart erfolgen sollte, dass die Konformität mit den Verfassungsgrundsätzen der EU, insbesondere mit Artikel 16 AEUV und den Artikeln 7 und 8 der Charta, gewahrt wird, und dies unabhängig von den begrüßenswerten Verbesserungen, die sich aus den in dieser Stellungnahme enthaltenen Empfehlungen ableiten lassen.

Geschehen zu Brüssel am 12. Februar 2016

Giovanni BUTTARELLI

Europäischer Datenschutzbeauftragter

Anmerkungen

[1] Siehe MEMO 10/1661 der Europäischen Kommission, veröffentlicht am 3. Dezember 2010, abrufbar unter: http://europa.eu/rapid/press-release_IP-10-1661_de.htm.
[2] Siehe MEMO 11/203 der Europäischen Kommission, veröffentlicht am 29. März 2011, abrufbar unter: http://europa.eu/rapid/press-release_MEMO-11-203_en.htm.
[3] Siehe Pressemitteilung 14-668 des Generalstaatsanwalts der USA, veröffentlicht am 25. Juni 2014, abrufbar unter: http://www.justice.gov/opa/pr/attorney-general-holder-pledges-support-legislation-provide-eu-citizens-judicial-redress.
[4] Siehe MEMO 15/5612 der Europäischen Kommission, veröffentlicht am 8. September 2015, abrufbar unter: http://europa.eu/rapid/press-release_MEMO-15-5612_en.htm.
[5] Text abrufbar unter: http://ec.europa.eu/justice/data-protection/files/dp-umbrella-agreement_en.pdf.
[6] Siehe Rechtssache 181/73, *R. & V. Haegeman gegen Belgischer Staat*, ECLI:EU:C:1974:41, Rdnr. 5 (im Abschnitt „Entscheidungsgründe").
[7] Rechtssache C-308/06, *Intertanko u.a.*, ECLI:EU:C:2008:312, Rdnr. 42.
[8] Verbundene Rechtssachen C-402/05 P und C-415/05 P, *Kadi gegen den Rat der Europäischen Union*, ECLI:EU:C:2008:461, Rdnr. 285.
[9] Siehe hierzu einschlägige Bestimmungen:
- für den Bereich des Binnenmarkts: Artikel 25 und 26 der Richtlinie 95/46/EG,
- für den Bereich der Strafverfolgung, allein im Hinblick auf Daten, die in der Folge einer grenzüberschreitenden Datenübermittlung verarbeitet werden: Artikel 13 des Rahmenbeschlusses 2008/977/JI des Rates über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, ABl. L 350/60,
- für die Übermittlung von Daten von Europol an Drittländer: Artikel 23 Absatz 6 Buchstabe b des Beschlusses des Rates 2009/371/JI vom 6. April 2009 zur Errichtung des Europäischen Polizeiamts (Europol), Abl. L 121/37,
- für die Übermittlung von Daten durch Organe und Einrichtungen der EU: Verordnung Nr. 45/2001, Artikel 9.
Es gibt keine verfügbare Übersicht über nationale datenschutzrechtliche Bestimmungen im Bereich der Strafverfolgung. Siehe auch Studie für den LIBE-Ausschuss „*A Comparison between US and EU Data Protection Legislation for Law Enforcement*" (Autor: F. Boehm), PE 536.459, veröffentlicht im September 2015 (im Folgenden „Boehm-Studie"), S. 30-35.
[10] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) COM(2012)11 [erste Lesung] (im Folgenden „vorgeschlagene DSGV").
[11] Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr COM(2012)10 [erste Lesung] (im Folgenden „vorgeschlagene Datenschutzrichtlinie in Strafsachen").
[12] Rechtssache C-362/14, *Schrems*, ECLI:EU:C:2015:650 (im Folgenden „*Schrems*").
[13] Siehe *Schrems*, Rdnrn. 38, 40, 47, 53, 54, 58, 64, 66, 72, 91, 94, 95.
[14] Genauer bestätigte der Gerichtshof jüngst, dass die im abgeleiteten Unionsrecht festgeschriebenen Anforderungen an die Gewährleistung einer rechtmäßigen internationalen Übermittlung personenbezogener Daten, insbesondere die Möglichkeit der Kommission, Entscheidungen zur Angemessenheit zu treffen „*hinsichtlich des Schutzes der Privatsphäre sowie der Freiheiten und Grundrechte von Personen*" [Richtlinie 95/46, Artikel 25 Absatz 6], auf Artikel 8 Absatz 1 der EU-Charta der Grundrechte („Charta") zurückgehen und darin die ausdrückliche Pflicht zum „Schutz personenbezogener Daten" verankert ist. Siehe diesbezüglich *Schrems*, Rdnr. 72: „*Somit setzt Art. 25 Abs. 6 der Richtlinie 95/46* (Hinweis – Bedingungen dafür, dass die Europäische Kommission das Schutzniveau eines Drittlandes als angemessen erachtet) *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*". Darüber hinaus fordert der Gerichtshof, dass die Gewährleistung eines „angemessenen Schutzniveaus" so zu verstehen ist, 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*" [*Schrems*, Rdnr. 73]. Die Voraussetzung des Vorhandenseins eines grundsätzlich gleichwertigen Schutzniveaus ist sowohl in der künftigen Datenschutz-Grundverordnung [Erwägungsgrund 81 der Präambel] als auch in der Datenschutzrichtlinie in Strafsachen [Erwägungsgrund 47 der Präambel] festgeschrieben.

[15] Rahmenbeschluss 2008/977/JI des Rates über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, ABl. L 350/60.
[16] 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.
[17] Artikel 54 des Beschlusses 2007/533/JI des Rates vom 12. Juni 2007 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II), Abl. L 205/63.
[18] Artikel 31 der Verordnung Nr. 767/2008/EG vom 9. Juli 2008 über das Visa-Informationssystem (VIS) und den Datenaustausch zwischen den Mitgliedstaaten über Visa für einen kurzfristigen Aufenthalt, Abl. L 218/60.
[19] Artikel 23 Absatz 6 Buchstabe b des Beschlusses des Rates 2009/371/JI.
[20] Siehe beispielsweise das Abkommen zwischen den Vereinigten Staaten von Amerika und der Europäischen Union zur Verwendung von Fluggastdatensätzen und deren Übermittlung an das United States Department of Homeland Security, Abl. L 215/5; Beschluss 2009/820/GASP des Rates vom 23. Oktober 2009 über den Abschluss im Namen der Europäischen Union des Abkommens über Auslieferung zwischen der Europäischen Union und den Vereinigten Staaten von Amerika und des Abkommens über Rechtshilfe zwischen der Europäischen Union und den Vereinigten Staaten von Amerika, ABl. L 291/40; siehe auch verschiedene bilaterale Rechtshilfeabkommen zwischen Mitgliedstaaten und Drittländern.
[21] Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, 28. Januar 1981, Nr. 108.
[22] Erwägungsgrund 10 der Richtlinie 95/46/EG und Erwägungsgrund 10 des Rahmenbeschlusses 2008/977/JI des Rates sehen ausdrücklich vor, dass grundsätzlich der Rechtsrahmen für den Datenschutz dieser beiden Rechtsvorschriften darauf abzielen „*muss (...) ein hohes Schutzniveau sicherzustellen*".
[23] Siehe beispielsweise verbundene Rechtssachen C-293/12 und C-594/12, *Digital Rights Ireland* (C-293/12) und *Seitlinger* (C-594/12), ECLI:EU:C:2014:238 (im Folgenden „*DRI*"), Rdnr. 67 und *Schrems*, Rdnrn. 39 und 72.
[24] „*Im Hinblick auf dieses Abkommen und seine Anwendung wird davon ausgegangen, dass das DHS die PNR-Daten im Sinne der einschlägigen Datenschutzvorschriften der EU bei der Verarbeitung und Verwendung angemessen schützt. Wenn Fluggesellschaften dem DHS nach Maßgabe dieses Abkommens PNR-Daten übermittelt haben, gelten die einschlägigen rechtlichen Anforderungen in der EU bezüglich der Übermittlung solcher Daten aus der EU an die Vereinigten Staaten als erfüllt.*"
[25] Der EDSB erinnert darin, dass der Gerichtshof der EU in seiner Rechtsprechung unter Anwendung von Artikel 8 Absatz 1 der Charta unterstrichen hat, dass der Begriff eines „angemessenen Schutzniveaus" so zu verstehen ist, 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 garantierten Niveau der Sache nach gleichwertig ist"* [Schrems, Rdnr. 73]. Das Gericht stellte zudem fest, dass „*bei der Prüfung des von einem Drittland gebotenen Schutzniveaus"* die Verpflichtung besteht, *„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*" (*Schrems*, Rdnr. 75) und dass sie auch „*alle Umstände zu berücksichtigen hat, die bei einer Übermittlung personenbezogener Daten in ein Drittland eine Rolle spielen*" (*Schrems*, Rdnr. 75). Darüber hinaus war einer der zentralen Gründe dafür, dass der EuGH die Safe Harbor-Entscheidung aus dem Jahr 2000 gekippt hat, die Tatsache, dass sie keine begründeten Erkenntnisse dahingehend enthielt, dass das fragliche Rechtssystem ein angemessenes Schutzniveau „gewährleistet" (*Schrems*, Rdnrn. 96 bis 98).
[26] Siehe Urteil des US Supreme Court in der Rechtssache *Medellin gegen Texas*, 552 US (2008), Rdnrn. 505 und 505 Nr. 2: *„Unmittelbar anwendbar bedeutet, dass das Abkommen bei seiner Ratifizierung automatisch nationale Wirkung als Bundesgesetz erhält";* „*Insgesamt* ***können Abkommen zwar internationale Verpflichtungen enthalten... sind aber kein nationales Recht, es sei denn, der Kongress hat entweder Durchführungsbestimmungen erlassen oder das Abkommen selbst umfasst die Absicht, dass es unmittelbar anwendbar ist, und wird zu diesen Bedingungen ratifiziert***". Siehe „International Law and Agreements: Their Effect upon U.S. law", herausgegeben vom Congressional Research Service, 18. Februar 2015, abrufbar unter: www.crs.gov.
[27] *DRI*, Rdnr. 68.
[28] Erwägungsgrund 33 des Rahmenbeschlusses weist erneut darauf hin, dass es sich um „*ein wesentliches Element des Schutzes personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit zwischen den Mitgliedstaaten verarbeitet werden*" handelt. Siehe auch Rechtssache C-518/07, *Kommission gegen Deutschland*, EU:C:2010:125, Rdnr. 25; Rechtssache C-288/12, *Kommission gegen Ungarn*, EU:C:2014:237, Rdnr. 48 und *Schrems*, Rdnr. 41.
[29] *Schrems*, Rdnr. 47, der sich eigens auf Artikel 8 Absatz 3 der Charta bezieht hinsichtlich der Befugnis nationaler Kontrollstellen, die Rechtmäßigkeit der Übermittlung personenbezogener Daten zu prüfen.

[30] Hinweise zu den Auswirkungen derartiger Datenübermittlungen finden sich in der für den LIBE-Ausschuss angefertigten Studie „*The US legal system on data protection in the field of law enforcement. Safeguards, rights and remedies for EU citizens*“ (Autor: F. Bignami), PE 519.215, veröffentlicht im Mai 2015 (im Folgenden „Bignami-Studie“), S. 6 und 7.
[31] *Schrems*, Rdnrn. 93 und 94; siehe auch Bignami-Studie, S. 6.
[32] Siehe hierzu Bignami-Studie, S. 12.
[33] Artikel 8 Absatz 1 der Richtlinie 95/46/EG umfasst eine Aufzählung besonderer Kategorien „*personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie von Daten über Gesundheit oder Sexualleben*“.
[34] Siehe beispielsweise Stellungnahme des EDSB zum Abkommen zwischen der Europäischen Union und Kanada über Fluggastdatensätze, 30.9.2013, Absatz 47; Stellungnahme des EDSB zur Mitteilung der Kommission über das sektorübergreifende Konzept für die Übermittlung von Fluggastdatensätzen (PNR) an Drittländer, 19.10.2010, Absatz 26; Stellungnahme des EDSB zu einem Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Verwendung von Fluggastdatensätzen zu Zwecken der Verhütung, Aufdeckung, Aufklärung und strafrechtlichen Verfolgung von terroristischen Straftaten und schwerer Kriminalität, 25.3.2011, Absatz 6; Stellungnahme des EDSB zum Abkommen zwischen der Europäischen Union und Australien über Fluggastdatensätze, 15.7.2011, Absatz 26; siehe auch Stellungnahme 4/2003 der Artikel 29-Datenschutzgruppe zum Niveau des Schutzes für in die Vereinigten Staaten übermittelte Passagierdaten, angenommen am 23. Juni 2003, S. 7.
[35] Stellungnahme des EDSB zu einem Vorschlag für einen Beschluss des Rates über den Abschluss eines Abkommens zwischen den Vereinigten Staaten von Amerika und der Europäischen Union zur Verwendung von Fluggastdatensätzen und deren Übermittlung an das United States Department of Homeland Security, 9.12.2011, Rdnrn. 15 und 16.
[36] Zum Vergleich: Artikel 9 der Konvention Nr. 108 des Europarats erlaubt Ausnahmen vom Zugangsrecht, auch in der Strafverfolgung, wenn sie durch das Recht vorgesehen und in einer demokratischen Gesellschaft notwendig sind „*(a) zum Schutz der Sicherheit des Staates, der öffentlichen Sicherheit sowie der Währungsinteressen des Staates oder zur Bekämpfung von Straftaten; (b) zum Schutz des Betroffenen oder der Rechte und Freiheiten Dritter.*“
[37] Analog hierzu, wie in *DRI*, Rdnrn. 60 bis 62, gefordert.
[38] 5 U.S.C. §552a(d)(1).
[39] Siehe Bignami-Studie allgemein und Boehm-Studie, S. 53 und 54.
[40] 5 U.S.C. §552a(d)(5); siehe auch Bignami-Studie, S. 12.
[41] 5 U.S.C. §552a(j).
[42] 5 U.S.C. §552a(k).
[43] Rechtssache C-201/14 *Bara gegen CNAS*, ECLI:EU:C:2015:638, Rdnr. 33.
[44] Artikel 7 des Beschlusses 2008/977/JI des Rates und Artikel 19 der vorgeschlagenen Datenschutzrichtlinie in Strafsachen.
[45] *Schrems*, Rdnr. 95.
[46] *Schrems*, Rdnr. 95.
[47] Das Gesetz wurde am 10. Februar 2016 von Kongress verabschiedet, bedarf für ein wirksames Inkrafttreten jedoch weiterer Verfahren. Der Gesetzentwurf wurde von US-Beobachtern dahingehend kritisiert, dass er unzureichenden Rechtsschutz für EU-Bürger biete und in jedem Fall einen wesentlich geringeren Rechtsschutz als das US-Bürgern gemäß Privacy Act 1974 zuerkannte Schutzniveau. Siehe hierzu Bignami-Studie, S. 13, und Schreiben von EPIC an das Committee on the Judiciary des US-Repräsentantenhauses vom 16. September 2015, abrufbar unter: https://epic.org/foia/umbrellaagreement/EPIC-Statement-to-HJC-on-HR1428.pdf.
[48] *Schrems*, Rdnrn. 56 und 58.
[49] Rechtssache C-614/10, *Kommission gegen Österreich*, ECLI:EU:C:2012:631, Rdnr. 36; Rechtssache C-288/12, *Kommission gegen Ungarn*, Rdnr. 47; *Schrems*, Rdnr. 40.
[50] Rechtssache C-518/07, *Kommission gegen Deutschland*, Rdnrn. 18-19, 25 und 30.
[51] Siehe Bignami-Studie, S. 34, und Boehm-Studie, S. 54 und 72.
[52] *Kommission gegen Österreich*, Rdnr. 36; *Kommission gegen Ungarn*; *Kommission gegen Deutschland* und *Schrems*.
[53] Beschluss 2012/472/EU des Rates vom 26. April 2012 über den Abschluss des Abkommens zwischen der Europäischen Union und den Vereinigten Staaten von Amerika zur Verwendung von Fluggastdatensätzen und deren Übermittlung an das United States Department of Homeland Security, Abl. L 215.
[54] Beschluss 2010/412/EU des Rates vom 13. Juli 2010 über den Abschluss 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 für die Zwecke des Programms zum Aufspüren der Finanzierung des Terrorismus, Abl. L 195.