EUROPÄISCHE
KOMMISSION

Brüssel, den 29.2.2016
COM(2016) 117 final

MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT

Transatlantischer Datenaustausch: Wiederherstellung des Vertrauens durch starke Schutzvorkehrungen

1. Einleitung: Der Austausch personenbezogener Daten und die Beziehungen zwischen der EU und den USA

Eine solide transatlantische Partnerschaft zwischen der Europäischen Union und den Vereinigten Staaten ist heute wichtiger als je zuvor. Wir teilen gemeinsame Werte, verfolgen gemeinsame politische und wirtschaftliche Ziele und arbeiten bei der Bekämpfung gemeinsamer Bedrohungen unserer Sicherheit eng zusammen. Die anhaltende Stärke unserer Verbundenheit kommt im Ausmaß unserer Handelsbeziehungen sowie in unserer engen Zusammenarbeit auf der Weltbühne zum Ausdruck.

Der Transfer und der Austausch personenbezogener Daten sind ein zentraler Bestandteil der engen Verbindungen zwischen der Europäischen Union (EU) und den Vereinigten Staaten (USA) - im kommerziellen Bereich ebenso wie bei der Durchsetzung von Rechtsvorschriften. Dieser Datenaustausch erfordert ein hohes Maß an Datenschutz und entsprechende Schutzvorkehrungen.

Im Juni 2013 haben Berichte über groß angelegte Datenerhebungsprogramme der US-Geheimdienste auf EU-Ebene und auf Ebene der Mitgliedstaaten ernsthafte Besorgnis hinsichtlich der Auswirkungen hervorgerufen, die eine groß angelegte Verarbeitung personenbezogener Daten durch öffentliche Stellen und private Unternehmen in den Vereinigten Staaten auf die Grundrechte der Europäer haben könnte.

Am 27. November 2013 veröffentlichte die Kommission eine Mitteilung über die Wiederherstellung des Vertrauens beim Datenaustausch zwischen der EU und den USA[1] mit einem Aktionsplan zur Wiederherstellung des Vertrauens in die Übermittlung von Daten zum Nutzen der digitalen Wirtschaft, des Schutzes der Rechte der europäischen Bürger und der umfassenderen transatlantischen Beziehungen. Um dieses Ziel zu erreichen, wurden folgende Schlüsselmaßnahmen vorgeschlagen:

(i) Annahme des Datenschutz-Reformpakets, das die Kommission im Jahr 2012 vorgeschlagen hatte[2];

(ii) Erhöhung der Sicherheit der Safe-Harbour-Regelung auf der Grundlage der 13 Empfehlungen, die in der Safe-Harbour-Mitteilung[3] dargelegt sind, und

---

[1] Mitteilung der Kommission an das Europäische Parlament und den Rat über die Wiederherstellung des Vertrauens beim Datenaustausch zwischen der EU und den USA, COM(2013) 846 final vom 27.11.2013 (im Folgenden die „Mitteilung von 2013“ oder die „Mitteilung“), abrufbar unter: http://ec.europa.eu/justice/data-protection/files/com_2013_846_en.pdf.

[2] 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 final vom 25.1.2012 und 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 final vom 25.1.2012, abrufbar unter: http://ec.europa.eu/justice/data-protection/reform/index_de.htm

(iii) Stärkung der Datenschutzgarantien im Bereich der strafrechtlichen Zusammenarbeit, insbesondere durch den Abschluss der Verhandlungen über das Datenschutz-Rahmenabkommen zwischen der EU und den USA. Letzteres umfasste auch das Ziel, Zusagen der USA zu durchsetzbaren Rechten für Privatpersonen zu erhalten, einschließlich Möglichkeiten, Datenschutzrechte vor den US-Gerichten geltend zu machen, insbesondere durch den Erlass des „Judicial Redress Act", mit dem bestimmte im U.S. Privacy Act aus dem Jahr 1974 verankerte Rechte, die zum damaligen Zeitpunkt nur US-Bürgern und Gebietsansässigen in den U.S.A. gewährt wurden, auf EU-Bürger erweitert werden.

Diese Ziele wurden in den Politischen Leitlinien[4] der Juncker-Kommission erneut bekräftigt: „*Dem Grundrecht auf Datenschutz kommt im digitalen Zeitalter besondere Bedeutung zu. Neben dem zügigen Abschluss der Gesetzgebungsarbeiten an gemeinsamen Datenschutzregeln innerhalb der Europäischen Union müssen wir auch in unseren Außenbeziehungen auf dieses Recht pochen. Angesichts der jüngst offenbarten Massenüberwachung müssen uns enge Partner wie die Vereinigten Staaten erst wieder davon überzeugen, dass die aktuelle Safe-Harbour-Vereinbarung wirklich sicher ist, wenn sie weiter Bestand haben soll. Die Vereinigten Staaten müssen auch garantieren, dass alle EU-Bürgerinnen und -Bürger das Recht haben, ihre Datenschutzrechte bei US-Gerichten einzuklagen, und zwar unabhängig davon, ob sie auf amerikanischem Boden wohnen. Dies ist unerlässlich, damit in den transatlantischen Beziehungen wieder Vertrauen entstehen kann.*"

Seitdem setzt sich die Kommission für die Verwirklichung dieser Ziele ein. Sie intensivierte die Verhandlungen über das Rahmenabkommen, das am 8. September 2015 von den Vertragsparteien paraphiert wurde. Die interinstitutionellen Beratungen zum Datenschutzreformpaket wurden verstärkt und führten am 15. Dezember 2015 zu einer politischen Einigung zwischen dem Rat und dem Europäischen Parlament. Im Januar 2014 nahm die Kommission Gespräche mit den USA über den Austausch kommerzieller Daten auf, deren Ziel die Stärkung der „Safe-Harbour-Regelung" war. Die Ungültigerklärung der Safe-Harbor-Entscheidung durch den Gerichtshof im *Schrems*-Urteil vom 6. Oktober 2015[5] bestätigte die Notwendigkeit einer neuen Rahmenregelung und gab weitere Anhaltspunkte für die Voraussetzungen, die eine solche zu erfüllen haben würde. Nach dem Urteil gab die Kommission am 6. November 2015 Leitlinien für Unternehmen heraus, in denen sie alternative Instrumente aufgezeigte, die die Übermittlung personenbezogener Daten an die Vereinigten Staaten nach wie vor ermöglichen[6]. Am 2. Februar 2016 wurde eine politische

---

[3] 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, COM(2013) 847 final vom 27.11.2013, S.18-19 (im Folgenden die „Safe-Harbour-Mitteilung"), abrufbar unter: http://ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf.

[4] Ein neuer Start für Europa: Meine Agenda für Jobs, Wachstum, Fairness und demokratischen Wandel - Politische Leitlinien für die nächste Europäische Kommission.

[5] Urteil vom 6. Oktober 2015 in der Rechtssache C-362/14, Maximilian Schrems/Data Protection Commissioner, EU:C:2015:650.

[6] Siehe Mitteilung der Kommission an das Europäische Parlament und den Rat zu der Übermittlung personenbezogener Daten aus der EU in die Vereinigten Staaten von Amerika auf der Grundlage der Richtlinie 95/46/EG nach dem Urteil des Gerichtshofs in der Rechtssache C-362/14 (*Schrems*), COM(2015) 566 final vom

Einigung über eine neue Rahmenregelung für die transatlantische Datenübermittlung, den EU-US-Datenschutzschild[7], erzielt, der an die Stelle der vorherigen Vereinbarung tritt.

Diese Erfolge werden den transatlantischen Beziehungen zugutekommen und dürften zur Wiederherstellung des Vertrauens der Europäer in die digitale Wirtschaft und zur Stärkung ihrer Grundrechte beitragen. Sie werden auch dazu beitragen, dass die EU und ihre Mitgliedstaaten über einen solideren Rechtsrahmen für den Datenschutz verfügen, der zu einer engeren Integration des Binnenmarktes, insbesondere des digitalen Binnenmarkts, führen und die EU in die Lage versetzen wird, sich verstärkt für die Förderung und Entwicklung internationaler Standards für den Schutz der Privatsphäre und den Schutz personenbezogener Daten einzusetzen.

Zeitgleich wurden wichtige Initiativen eingeleitet, die bedeutende Änderungen der Rechtsordnung der Vereinigten Staaten zur Folge hatten. Am 17. Januar 2014 kündigte Präsident Obama[8] Reformen der „U.S. signals intelligence activities“ (signalerfassende Aufklärung) an, die in der Folge ihren Niederschlag in der „Presidential Policy Directive 28“ (PPD-28)[9] fanden. Im Zuge dieser Reformen wurden bestimmte Rechte zum Schutz der Privatsphäre auf Nichtamerikaner ausgeweitet und ein neuer Ansatz bei der Datenerhebung - weg von der Sammelerhebung hin zur gezielten Datenerhebung - eingeführt. Die Kommission begrüßte den neuen Ansatz als einen wichtigen Schritt in die richtige Richtung[10]. Dieser Reformprozess bildete auch die Grundlage für die Beratungen mit den USA über den EU-US-Datenschutzschild. Seitdem wurden weitere Änderungen eingeführt. Unter anderem verabschiedeten die USA. im Juni 2015 den „USA Freedom Act“[11], durch den bestimmte US-Überwachungsprogramme geändert, die gerichtliche Aufsicht gestärkt und mehr Transparenz für die Öffentlichkeit in Bezug auf die Nutzung dieser Programme hergestellt wurde. Am 10. Februar 2016 nahm schließlich der Kongress der Vereinigten Staaten den „Judicial Redress Act“ an, den Präsident Obama am 24. Februar 2016 unterzeichnete[12].

Vor diesem Hintergrund wird in der vorliegenden Mitteilung Bilanz gezogen und untersucht, in welchem Umfang die in der Mitteilung von 2013 formulierten Ziele verwirklicht wurden. Außerdem wird aufgezeigt, in welchen Bereichen nach wie vor Anstrengungen erforderlich sind, um das Vertrauen in die transatlantische Datenübermittlung zu festigen und in vollem Umfang wieder herzustellen.

6.11.2015. Siehe dazu auch die Stellungnahme der Artikel-29- Datenschutzgruppe über die Folgen des *Schrems*-Urteils vom 3. Februar 2016, abrufbar unter: http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160203_statement_consequences_schrems_judgement_en.pdf

[7] Siehe http://europa.eu/rapid/press-release_IP-16-216_de.htm

[8] https://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence

[9] https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities

[10] http://europa.eu/rapid/press-release_MEMO-14-30_en.htm

[11] USA Freedom Act von 2015, Pub. L., No. 114-23, § 401, 129 Stat. 268.

[12] H.R.1428 – Judicial Redress Act“) von 2015 - tritt 90 Tage nach seinem Erlass in Kraft.

2. EU-Datenschutzreform

2.1 Hintergrund

Um die Möglichkeiten einer zunehmend digital vernetzten Welt nutzen und den damit verbundenen Herausforderungen begegnen zu können, legte die Europäische Kommission im Januar 2012 ihr Datenschutz-Reformpaket (im Folgenden „Reform“) vor. Ziel der Reform ist es, mehr Vertrauen in die digitale Wirtschaft zu schaffen, und zwar unabhängig davon, ob personenbezogene Daten innerhalb eines Mitgliedstaats, in der EU oder in Drittstaaten wie den Vereinigten Staaten verarbeitet werden. Zu diesem Zweck sollen die EU-Datenschutzvorschriften verschärft und Einzelpersonen mehr Kontrolle über ihre personenbezogenen Daten gegeben werden.

Das Reformpaket umfasst zwei Rechtsakte: eine allgemeine Datenschutzverordnung[13] (im Folgenden „Verordnung“) zur Festlegung eines gemeinsamen Rahmens der EU für den Datenschutz und eine Richtlinie zum Schutz personenbezogener Daten im Bereich der polizeilichen und justiziellen Zusammenarbeit (im Folgenden „Polizei-Richtlinie“)[14]. Mit dem Vorschlag für eine in den Mitgliedstaaten unmittelbar anwendbare Verordnung verfolgte die Kommission das Ziel, einen gemeinsamen Datenschutzstandard für alle zu schaffen und so zwischen den Mitgliedstaaten bestehende Unterschiede in Bezug auf das Schutzniveau zu beseitigen. Mit der Polizei-Richtlinie werden erstmals gemeinsame Vorschriften auf EU-Ebene eingeführt, wobei den in Justiz und Strafverfolgung bestehenden Traditionen der Mitgliedstaaten Rechnung getragen wurde.

Am 15. Dezember 2015 erzielten das Europäische Parlament und der Rat eine politische Einigung über das Reformpaket. Damit ist eine der wichtigsten Maßnahmen, die in der Mitteilung von 2013 dargelegt war, erfüllt.

2.2 Was hat sich geändert?

Mit der Verordnung werden die in der Datenschutzrichtlinie aus dem Jahr 1995 festgeschriebenen Datenschutzgrundsätze[15] aktualisiert, modernisiert und in einigen Fällen auch verschärft, um die Rechte zum Schutz der Privatsphäre sicherzustellen. Im Mittelpunkt der Verordnung stehen die Stärkung der Rechte des Einzelnen, die Vertiefung des EU-Binnenmarkts, die Sicherstellung einer besseren Durchsetzung der einschlägigen Vorschriften, die Straffung internationaler Transfers personenbezogener Daten sowie die Festlegung internationaler Datenschutzstandards. Die Vorschriften sollen sicherstellen, dass die personenbezogenen Daten der EU-Bürgerinnen und EU-Bürger geschützt sind – und zwar unabhängig davon, wohin sie übermittelt, verarbeitet oder gespeichert werden, d. h. auch außerhalb der EU, wie dies in der digitalen Welt häufig der Fall sein kann. Eine Reihe von Merkmalen der Reform sind besonders hervorzuheben:

---

[13] COM(2012) 11 final vom 25.1.2012: vgl. Fußnote 2.
[14] COM(2012) 10 final vom 25.1.2012: vgl. Fußnote 2.
[15] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. L 281 vom 23.11.1995, S. 31 (im Folgenden die „Datenschutz-Richtlinie").

Erstens: Der **räumliche Anwendungsbereich**: In der Verordnung ist eindeutig festgelegt, dass sie auch für Unternehmen mit Sitz in einem Drittland gilt, wenn diese Waren und Dienstleistungen in der EU anbieten oder das Verhalten von Privatpersonen in der EU verfolgen. Unternehmen mit Sitz außerhalb der EU haben dieselben Regeln anzuwenden wie Unternehmen mit Sitz in der EU. Damit wird der umfassende Schutz der Rechte der einzelnen EU-Bürger sichergestellt. Außerdem werden auf diese Weise gleiche Wettbewerbsbedingungen für EU-Unternehmen und Nicht-EU-Unternehmen geschaffen und Wettbewerbsverzerrungen zwischen EU- und Drittstaats-Unternehmen, die in der EU tätig sind oder deren Zielgruppe die Verbraucher in der EU ist, vermieden.

Zweitens: **Nachdrücklichere Durchsetzung** der Datenschutzvorschriften: Die Verordnung sieht die Harmonisierung der Befugnisse der nationalen Datenschutzaufsichtsbehörden vor und führt damit eine wirksame Sanktionsregelung ein. Die nationalen Datenschutzbehörden werden befugt sein, Geldbußen in Höhe von bis zu 20 Mio. EUR oder bis zu 4 % des weltweiten Jahresumsatzes eines Unternehmens zu verhängen. Diese Befugnis, bei Nichteinhaltung der Datenschutzbestimmungen abschreckende Sanktionen zu verhängen, wird in Verbindung mit dem vorstehend erwähnten räumlichen Anwendungsbereich dafür sorgen, dass die in der EU tätigen Unternehmen einen großes Interesse an der Einhaltung der EU-Rechtsvorschriften haben werden. Mit den neuen Vorschriften wird auch eine klarere und strengere Haftungsregelung für die für die Verarbeitung Verantwortlichen und die Auftragsverarbeiter eingeführt.

Drittens: **Harmonisierte Regeln für die strafrechtliche Zusammenarbeit**: Die Polizei-Richtlinie gewährleistet, dass die Polizei- und Justizbehörden in den Mitgliedstaaten bei der Verarbeitung personenbezogener Daten in strafrechtlichen Angelegenheiten allgemeine Datenschutzgrundsätze und Regeln anwenden werden. Dazu gehören u.a. harmonisierte Vorschriften für die internationale Übermittlung personenbezogener Daten im Rahmen der strafrechtlichen Zusammenarbeit[16]. Die neue Richtlinie wird das Schutzniveau des Einzelnen erhöhen und gleichzeitig sicherstellen, dass die Daten von Opfern, Zeugen und Verdächtigen bei strafrechtlichen Ermittlungen oder im Strafverfahren ausreichend geschützt sind. Die Aufsicht wird von unabhängigen nationalen Datenschutzbehörden wahrgenommen; es muss ein wirksamer Rechtsschutz für Einzelpersonen gewährleistet sein. Gleichzeitig werden stärker harmonisierte Rechtsvorschriften den Polizei- und Justizbehörden eine wirkungsvollere Zusammenarbeit sowohl auf Ebene der Mitgliedstaaten als auch zwischen den Mitgliedstaaten und ihren internationalen Partnern bei der Bekämpfung von Kriminalität

[16] Anders als nach dem 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, der nur den grenzüberschreitenden Austausch von Daten zwischen den zuständigen Behörden der Mitgliedstaaten erfasst, wird die Anwendung solcher Vorschriften im Rahmen der Polizei-Richtlinie nicht mehr davon abhängen, ob es im Vorfeld einen Austausch dieser Daten zwischen den Strafverfolgungsbehörden der Mitgliedstaaten gegeben hat.

und Terrorismus ermöglichen. Dies ist ein ganz wesentlicher Bestandteil der Europäischen Sicherheitsagenda[17].

Viertens: **Strengere Vorschriften für sicherere internationale Datentransfers:** Sowohl die Verordnung als auch die Polizei-Richtlinie sehen transparente, detaillierte und umfassende Vorschriften für die Übermittlung von personenbezogenen Daten an Drittstaaten vor. Sie umfassen alle Formen internationaler Transfers, die zu kommerziellen oder zu Strafverfolgungszwecken zwischen privaten oder öffentlichen Stellen oder zwischen privaten Einrichtungen und Behörden stattfinden. Während sich die Vorschriften für die internationale Datenübermittlung gegenüber den Vorschriften der derzeit geltenden Datenschutzrichtlinie strukturell nicht wesentlich geändert haben (d. h. Angemessenheitsbeschlüsse, Standardvertragsklauseln und verbindliche unternehmensinterne Datenschutzvorschriften sowie bestimmte Ausnahmen vom allgemeinen Verbot der Übermittlung personenbezogener Daten in Länder außerhalb der EU), werden sie im Zuge der Reform in mehrfacher Hinsicht inhaltlich präzisiert und vereinfacht und sollen den Verwaltungsaufwand reduzieren. Darüber hinaus werden einige neue Instrumente für den internationalen Datentransfer eingeführt.

Die Verordnung erweitert auch die **Befugnisse der EU-Datenschutzbehörden**, einschließlich in Bezug auf internationale Datentransfers. Im Vergleich zu der derzeit geltenden Datenschutzrichtlinie sind die Bestimmungen über die Unabhängigkeit, Aufgaben und Befugnisse der EU-Datenschutzbehörden näher ausgeführt und erheblich verbessert. Dazu zählt ganz ausdrücklich die Befugnis, die Übermittlung von Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation auszusetzen. Die Polizei-Richtlinie enthält ähnliche Bestimmungen in Bezug auf internationale Datentransfers und die Befugnisse der Datenschutzbehörden gegenüber den Strafverfolgungsbehörden.

Konkret sieht die Verordnung in Bezug auf die Bestimmungen für die **Angemessenheitsbeschlüsse** der Kommission einen präzisen und umfassenden Katalog von Elementen vor, die die Kommission bei der Bewertung des Datenschutzniveaus der Rechtsordnung eines Drittstaats zu berücksichtigen hat. Die Kommission muss eine umfassende Bewertung zahlreicher Vorschriften, darunter - im Einklang mit dem *Schrems*-Urteil - der Vorschriften für den Zugang der Behörden eines Drittlandes zu personenbezogenen Daten, vornehmen. Ein weiteres wichtiges Kriterium bei dieser Bewertung ist, ob Privatpersonen wirksame und durchsetzbare Datenschutzrechte gewährt und ihnen wirksame administrative und gerichtliche Rechtsbehelfe garantiert werden.

Ferner ist in der Verordnung ausdrücklich festgelegt, dass die Kommission in **regelmäßigen** Abständen, mindestens jedoch alle vier Jahre, alle Angemessenheitsbeschlüsse **überprüfen** muss, damit sie ständig über alle Entwicklungen in einem Drittland, die direkte oder sogar negative Auswirkungen auf das Schutzniveau der Rechtsordnung der Union haben können, auf dem Laufenden ist. Diese kontinuierliche Kontrolle der Angemessenheit wird in Form

[17] Vgl. Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen „Die Europäische Sicherheitsagenda“, COM(2015) 185 final vom 28.4.2012.

eines dynamischen Prozesses stattfinden, da hierzu auch ein Dialog mit den Behörden des betreffenden Drittlands zu führen ist.

In Bezug auf die Übermittlung von Daten in Drittländer, für die kein Angemessenheitsbeschluss vorliegt, sieht die Verordnung die gleichen Bedingungen wie für die Verwendung **alternativer Transferinstrumente**, d. h. Standardvertragsklauseln und verbindliche unternehmensinterne Datenschutzvorschriften, vor und fügt außerdem andere Transferinstrumente hinzu, wie genehmigte Verhaltensregeln und Zertifizierungsverfahren. Außerdem wird in der Verordnung präzisiert, in welcher Situation **Ausnahmeregelungen** in Anspruch genommen werden können.

2.3 Das weitere Vorgehen

Die Datenschutzreform ist ein wichtiger Schritt, um die Grundrechte der Bürger im digitalen Zeitalter zu stärken und Geschäftstätigkeiten zu erleichtern, indem die Vorschriften für Unternehmen im digitalen Binnenmarkt vereinfacht werden. Die Verbraucher in der EU werden EU- und Drittlands-Betreibern erneut vertrauen, was der digitalen Wirtschaft in Europa und weltweit zugutekommen wird. Die Reform wird sich positiv auf die Handelsbeziehungen der EU mit den USA, dem größten Handelspartner der EU, auswirken. Sie wird ein klares und stabiles Umfeld für Unternehmen aus der EU und Drittstaaten schaffen. Den amerikanischen Unternehmen wird die Rechtssicherheit zugutekommen, die sich daraus ergibt, dass sie in einem integrierten Wirtschaftsraum operieren, in dem einheitliche Datenschutzvorschriften angewandt werden.

Durch gemeinsame Vorschriften im Bereich der Strafverfolgung wird sichergestellt werden, dass personenbezogene Daten Einzelner besser geschützt sind und dass die betreffenden Personen einen Anspruch auf einen wirksamen gerichtlichen Rechtsbehelf haben. Die erleichterte grenzübergreifende Zusammenarbeit der Polizei- und Justizbehörden der Mitgliedstaaten wird die Strafverfolgung effizienter machen und damit die Voraussetzungen für eine wirksamere Kriminalprävention in der EU schaffen. Gleichzeitig wird dadurch auch eine reibungslosere Zusammenarbeit mit Polizei und Justiz in Drittländern ermöglicht.

Das Europäische Parlament und der Rat werden das Reformpaket voraussichtlich im ersten Halbjahr 2016 förmlich annehmen. Während die Verordnung zwei Jahre nach ihrer Annahme zur Anwendung kommen wird, ist für die Polizei-Richtlinie ein Umsetzungszeitraum von zwei Jahren vorgesehen. Die zweijährige Übergangsfrist sollte von allen beteiligten Akteuren sowohl innerhalb als auch außerhalb der EU zur Vorbereitung auf die neuen Vorschriften genutzt werden. Die Kommission wird ihren Beitrag zum Gelingen leisten und während der Übergangszeit eng mit den Mitgliedstaaten, Datenschutzbehörden und anderen Akteuren zusammenarbeiten, um die einheitliche Anwendung der Vorschriften zu gewährleisten und Rahmenbedingungen zu schaffen, die einer Einhaltung der neuen Vorschriften förderlich sind.

3. DER EU-US-DATENSCHUTZSCHILD: EINE NEUE RAHMENREGELUNG FÜR DEN UMGANG MIT PERSONENBEZOGENEN DATEN IM TRANSATLANTISCHEN DATENVERKEHR

3.1 Hintergrund

Um den Austausch personenbezogener Daten zwischen der EU und den USA im Rahmen von Handelsbeziehungen zu erleichtern und gleichzeitig den Schutz dieser Daten zu gewährleisten, hatte die Kommission im Jahr 2000 die Safe-Harbour-Regelung als Regelung anerkannt, die ein angemessenes Schutzniveau bietet[18]. Personenbezogene Daten konnten nun - obwohl es kein allgemeines Datenschutzgesetz in den Vereinigten Staaten gab - aus EU-Mitgliedstaaten an Unternehmen in den USA übermittelt werden, die sich auf die in der Regelung vorgesehen Grundsätze des Schutzes der Privatsphäre verpflichtet hatten.

Die Kommission zeigte in ihrer Safe-Harbour-Mitteilung aus dem Jahr 2013[19] eine Reihe von Mängeln auf, die im Laufe der Zeit in Bezug auf die Funktionsweise der Regelung zu Tage getreten waren. Dies waren vor allem mangelnde Transparenz seitens der Unternehmen in Bezug auf ihre Beteiligung an der Regelung und die Tatsache, dass die amerikanischen Behörden die Einhaltung der in der Regelung vorgesehen Grundsätze des Schutzes der Privatsphäre durch die beteiligten Unternehmen nicht in ausreichendem Maße durchsetzten. Darüber hinaus gaben die Anfang des Jahres enthüllten Spionagefälle Anlass zu Bedenken in Bezug auf den Umfang und den Anwendungsbereich bestimmter Datenerhebungsprogramme der US-Geheimdienste und des Zugangs amerikanischer Behörden zu personenbezogenen Daten europäischer Bürger, die auf der Grundlage der Safe-Harbour-Regelung übermittelt worden waren. Unter Berücksichtigung dieser und anderer Erkenntnisse[20] kam die Kommission zu dem Schluss, dass die Safe-Harbour-Regelung überarbeitet werden müsse. Vor diesem Hintergrund formulierte die Kommission 13 Empfehlungen[21] zur Verschärfung und Aktualisierung der in die neue Regelung aufzunehmenden Datenschutzgarantien. Diese Empfehlungen betrafen unter anderem: (i) die Stärkung der substanziellen Grundsätze des Datenschutzschilds und die Steigerung der Transparenz der Datenschutzbestimmungen selbstzertifizierter US-Unternehmen, die sich diese Grundsätze zu eigen gemacht haben; (ii) eine bessere und effektive Kontrolle, Überwachung und Durchsetzung der Einhaltung der Datenschutzgrundsätze durch die Unternehmen; (iii) Verfügbarkeit erschwinglicher Streitbeilegungsmechanismen im Falle von Beschwerden von Privatpersonen; (iv) die Notwendigkeit, dafür zu sorgen, dass der Rückgriff auf die in der Safe-Harbour-Entscheidung

[18] Entscheidung 2000/520/EG der Kommission vom 20. Juli 2000. In dieser auf Artikel 25 Absatz 6 der Datenschutz-Richtlinie gestützten Entscheidung hatte die Kommission die vom US-Handelsministerium herausgegebenen Grundsätze des „sicheren Hafens“ und die diesbezüglichen „Häufig gestellten Fragen“ (FAQ) als für die Zwecke der Übermittlung personenbezogener Daten aus der EU als Garantie für einen angemessenen Schutz anerkannt. Die Safe-Harbour-Regelung funktionierte auf der Grundlage von Verpflichtungserklärungen und Selbstzertifizierungen der beteiligten Unternehmen. Diese Regelung war nach US-Recht für die beteiligten Unternehmen verbindlich und durch die Federal Trade Commission durchsetzbar.

[19] Vgl. Fußnote 3.

[20] Wie der exponentielle Anstieg der Datenströme und ihre zentrale Bedeutung für die transatlantische Wirtschaft oder der rasche Anstieg der Zahl der an der Safe-Harbour-Regelung beteiligten Unternehmen. Siehe „Safe-Harbour-Mitteilung “, S. 37.

[21] Safe-Harbour-Mitteilung“, S. 18-19.

vorgesehene Ausnahmeregelung in Bezug auf die nationalen Sicherheits- und Strafverfolgungsbehörden auf das unbedingt erforderliche Maß beschränkt wird und verhältnismäßig ist.

Auf der Grundlage dieser 13 Empfehlungen leitete die Kommission im Januar 2014 ihre Gespräche mit den US-Behörden ein. Die Nichtigerklärung der Safe Harbour-Entscheidung am 6. Oktober 2015 durch den Gerichtshof bestätigte, wie notwendig eine strengere neue Regelung für den transatlantischen Datenaustausch zu Handelszwecken geworden war. Das Urteil des Gerichtshofs stützte sich zwar auf die Empfehlungen der Kommission aus dem Jahr 2013, ging aber weiter und unterstrich die Notwendigkeit von Beschränkungen, Schutzvorkehrungen und gerichtlichen Kontrollmechanismen, um den Schutz der personenbezogenen Daten der EU-Bürger kontinuierlich zu gewährleisten, und zwar auch in den Fällen, in denen Behörden aus Gründen der nationalen Sicherheit, des öffentlichen Interesses oder der Strafverfolgung personenbezogene Daten abfragen oder verarbeiten.

Am 2. Februar 2016 erzielten die EU und die USA nach zwei Jahren intensiver Verhandlungen eine politische Einigung über die neue Rahmenregelung: den EU-US-Datenschutzschild. Diese neue Regelung beinhaltet wichtige neue Schutzbestimmungen und wird ein hohes Schutzniveau in Bezug auf die Grundrechte von EU-Bürgern gewährleisten. Sie wird Unternehmen auf beiden Seiten des Atlantiks, die Geschäfte miteinander abschließen wollen, die nötige Rechtssicherheit bieten. Außerdem wird sie neuen Schwung in die transatlantische Partnerschaft bringen.

Nach Abschluss der Verhandlungen mit den USA wird die Kommission die neue Regelung der Artikel 29-Datenschutzgruppe (der auch Vertreter der EU-Datenschutzbehörden angehören) vorlegen, damit diese eine Stellungnahme zum vorgesehenen Schutzniveau abgibt. Darüber hinaus wird der Angemessenheitsbeschluss vor seiner Annahme im Rahmen des Komitologieverfahrens geprüft werden. Der Europäische Datenschutzbeauftragte wird ebenfalls angehört werden.

3.2 Was hat sich geändert?

Der EU-US-Datenschutzschild ist die konsequente und effektive Antwort auf die 13 Empfehlungen der Kommission und das *Schrems*-Urteil. Er enthält wichtige Verbesserungen gegenüber dem vorherigen Rechtsrahmen in Bezug auf die Zusagen, zu denen sich die US-Unternehmen verpflichten müssen. Ferner enthält er wichtige neue Verpflichtungen und ausführliche Erklärungen zu den einschlägigen amerikanischen Gesetzen und Praktiken der US-Behörden. Anders als die vorherige Regelung umfasst der Datenschutzschild nicht nur Verpflichtungen in Bezug auf den Handelssektor, sondern - in erheblichem Umfang und erstmals in den EU-USA-Beziehungen - auch in Bezug auf den Zugriff auf personenbezogene Daten durch Behörden, einschließlich aus Gründen der nationalen Sicherheit. In Anbetracht der Rechtsprechung des Gerichtshofs ist dies eine wichtige und notwendige Voraussetzung, um nach den Enthüllungen das Vertrauen in die transatlantischen Beziehungen wieder herzustellen.

Die wichtigsten Bestandteilt dieser neuen Regelung können vier Hauptkategorien zugeordnet werden:

Erstens: **Strenge Auflagen für Unternehmen und konsequente Durchsetzung**: Die neue Regelung ist transparenter und sieht wirksame Aufsichtsmechanismen vor, um sicherzustellen, dass die Unternehmen die Regeln, zu deren Einhaltung sie sich rechtsverbindlich verpflichtet haben, auch tatsächlich einhalten. US-Unternehmen, die personenbezogene Daten von Europa auf der Grundlage des EU-US-Datenschutzschilds importieren möchten, müssen strenge Auflagen in Bezug auf ihre Verarbeitung und den Schutz der Rechte des Einzelnen akzeptieren. Dazu gehören verschärfte Bedingungen und strengere Haftungsbestimmungen für am Datenschutzschild beteiligte Unternehmen, die in die USA oder in andere Drittländer (Weiterübermittlung von Daten) Daten an Dritte übertragen (z. B. zur Vergabe von Unteraufträgen), die nicht am Schutzschild beteiligt sind. Was die Aufsicht anbelangt, hat sich das Handelsministerium der Vereinigten Staaten verpflichtet, regelmäßig und gründlich zu kontrollieren, in welchem Umfang die Unternehmen ihre Zusagen erfüllen, und „Trittbrettfahrer", d. h. Unternehmen, die fälschlicherweise behaupten, an dem Datenschutzschild beteiligt zu sein, auszuschalten. Die Zusagen der Unternehmen sind rechtlich verbindlich und nach dem Recht der Vereinigten Staaten durch die Federal Trade Commission durchsetzbar; Unternehmen, die die Vorschriften nicht einhalten, müssen mit strengen Sanktionen rechnen.

Zweitens: **Klare Grenzen und Schutzvorkehrungen beim Datenzugriff durch US-Behörden**: Erstmals in der Geschichte hat die Regierung der USA, vertreten durch das Department of Justice und das Office of the Director of National Intelligence, das als Aufsichtsorgan für die gesamte U.S. Intelligence Community fungiert, der EU in Form von schriftlichen Erklärungen und Zusicherungen versichert, dass der behördliche Zugriff aus Gründen der Strafverfolgung, der nationalen Sicherheit und anderen Gründen von öffentlichem Interesse eindeutigen Beschränkungen, Schutzmaßnahmen und Überwachungsmechanismen unterliegen wird. Die USA werden auch neue Rechtsbehelfsverfahren für betroffene EU-Bürger im Bereich der nationalen Sicherheit einsetzen, beispielsweise eine Ombudsperson, die von den nationalen Sicherheitsbehörden unabhängig sein wird und zu deren Aufgaben es gehören wird, Beschwerden und Anfragen von EU-Bürgern in Bezug auf den Zugriff auf ihre Daten aus Gründen der nationalen Sicherheit zu beantworten und Einzelpersonen zu bestätigen, dass die geltenden Rechtsvorschriften eingehalten wurden oder dass die Nichteinhaltung korrigiert wurde. Dies ist eine bedeutsame Entwicklung, die nicht nur bei der Datenübertragung auf der Grundlage des Datenschutzschilds zur Anwendung kommen wird, sondern bei der Übermittlung *sämtlicher* personenbezogener Daten, die zu kommerziellen Zwecken in die USA übermittelt werden, unabhängig von der Grundlage für die Übertragung dieser Daten.

Drittens: **Wirksamer Schutz der Rechte der EU-Bürgerinnen und -Bürger durch verschiedene Rechtsbehelfe:** Jedem Bürger und jeder Bürgerin in Europa, die glauben, dass ihre Daten im Rahmen der neuen Regelung missbraucht wurden, stehen mehrere zugängliche und erschwingliche Rechtsbehelfe für Einzelpersonen, darunter auch kostenlose Verfahren der alternativen Streitbeilegung, zur Verfügung. Die Unternehmen verpflichten sich,

Beschwerden innerhalb einer bestimmten Frist zu bearbeiten. Darüber hinaus müssen sich alle Unternehmen, die Zugang zu personenbezogenen Daten aus Europa haben, verpflichten, die Entscheidungen der zuständigen EU-Datenschutzbehörde zu befolgen, während andere Unternehmen eine solche Verpflichtung freiwillig eingehen können. Privatpersonen können ihre Beschwerde auch bei der für sie zuständigen Datenschutzbehörde einlegen, die die Beschwerde in einem formalisierten Verfahren an das Handelsministerium und die Federal Trade Commission weiterleiten wird, um die Untersuchung und Streitbeilegung innerhalb eines angemessenen Zeitrahmens zu erleichtern. Gelingt es nicht, einen Streit mit Hilfe einer dieser Möglichkeiten beizulegen, können Privatpersonen als letztes Mittel das Datenschutzschild-Panel in Anspruch nehmen. Das Datenschutzschild-Panel ist ein Schiedsforum, das verbindliche und durchsetzbare Entscheidungen gegen US-Unternehmen auf der Grundlage des Datenschutzschilds erlassen kann. Darüber hinaus können die Datenschutzbehörden der EU die betreffenden Privatpersonen bei der Vorbereitung ihrer Klage unterstützen. Wie oben erwähnt, wird für Beschwerden über einen möglichen Zugang der nationalen Geheimdienste eine neue Ombudsperson eingesetzt werden, womit eine weitere Rechtsbehelfs-Möglichkeit geschaffen wird.

Viertens: **Gemeinsame jährliche Überprüfung**: Auf diese Weise kann die Kommission die Funktionsweise aller Aspekte des Datenschutzschilds, einschließlich der Beschränkungen und Schutzmaßnahmen in Bezug auf den Datenzugriff aus Gründen der nationalen Sicherheit, in regelmäßigen Abständen überprüfen. Die Kommission und das US- Handelsministerium werden für die Überprüfung zuständig sein, an der sie die Datenschutzbehörden der EU, die nationalen Sicherheitsbehörden der USA und die Ombudsperson beteiligen werden. Auf diese Weise werden die USA hinsichtlich ihrer Zusicherungen in die Pflicht genommen. Die Kommission wird aber noch weitergehen: Sie wird alle anderen Informationsquellen wie freiwillige Transparenzberichte von Unternehmen über den Umfang der von Behörden angeforderten Daten heranziehen[22]. Die jährliche Überprüfung geht über die neue Verordnung hinaus, die solche Überprüfungen mindestens alle vier Jahre vorsieht. Damit wollen sowohl die EU als auch die USA ihre Entschlossenheit zeigen, die vollständige Einhaltung dieser Bestimmungen konsequent sicherzustellen.

Diese Überprüfung wird keine formale Übung ohne Konsequenzen sein. In den Fällen, in denen die US-Unternehmen oder -Behörden ihren Verpflichtungen nicht nachgekommen sind, wird die Kommission das Verfahren zur Aussetzung des Datenschutzschilds aktivieren. Wie der Gerichtshof im *Schrems*-Urteil betont hat , darf ein Angemessenheitsbeschluss nicht nur auf dem Papier existieren, vielmehr müssen die US-Unternehmen und -Behörden die Regelung mit Leben füllen und am Leben erhalten, indem sie ihre Verpflichtungen erfüllen. In den Fällen, in denen sie dies nicht tun, ist der aus einem Angemessenheitsbeschluss resultierende besondere Vorteil für Datentransfers nicht länger gerechtfertigt und wird zurückgenommen.

[22] Große amerikanische Internet-Unternehmen erstellen bereits derartige Berichte, um das Vertrauen ihrer Kunden zurückzugewinnen. Gemäß dem USA Freedom Act von 2015 dürfen freiwillige Berichte über angeforderte Daten veröffentlicht werden - zumindest innerhalb bestimmter Grenzen, um die nationalen Sicherheitsinteressen zu schützen.

3.3 Das weitere Vorgehen

Die im Rahmen des Datenschutzschilds eingegangenen Verpflichtungen der USA werden die Grundlage für einen neuen Angemessenheitsbeschluss der Kommission bilden. Die Unternehmen werden aufgefordert, sich bereits jetzt auf die neue Regelung vorzubereiten, damit sie ihr im Anschluss an die Annahme des Beschlusses der Kommission unverzüglich beitreten können. Die US-Regierung wird ihre schriftlichen Erklärungen im US-Bundesregister (Federal Register) veröffentlichen und damit öffentlich bestätigen, dass sie ihre Verpflichtungen einhalten wird.

Der EU-US-Datenschutzschild erfordert die Mitwirkung zahlreicher Akteure:

- der beteiligten US-Unternehmen, die ihre Verpflichtungen im Rahmen der Regelung in dem Wissen erfüllen müssen, dass die Regelung strikt durchgesetzt werden wird, und sie sanktioniert werden, wenn sie ihre Verpflichtungen nicht einhalten. Die Unternehmen werden außerdem aufgefordert, zur Stärkung des Vertrauens ihrer Verbraucher, die Behandlung von Beschwerden im Rahmen des Datenschutzschilds den EU-Datenschutzbehörden anzuvertrauen, da die europäischen Bürgerinnen und Bürger sich am ehesten an diese Behörden wenden werden. Auch das Ausmaß, in dem Unternehmen bereit sind, die im US-Recht vorgesehene Möglichkeit zu nutzen, Transparenzberichte über den von nationalen Sicherheits- und Strafverfolgungsbehörden beantragten Zugriff auf EU-Daten zu veröffentlichen, wird dazu beitragen, das Vertrauen zu stärken, dass dieser Zugriff auf das erforderliche Maß beschränkt und verhältnismäßig ist[23];

- der verschiedenen US-Behörden, die mit der Beaufsichtigung und Durchsetzung der Regelung betraut sind, die für die Einhaltung der Beschränkungen und Schutzvorschriften hinsichtlich des Datenzugriffs zu Strafverfolgungszwecken und aus Gründen der nationalen Sicherheit zuständig sind, oder die dafür sorgen müssen, dass innerhalb eines angemessenen Zeitraums und auf sinnvolle Weise auf Beschwerden von EU-Bürgern über einen möglichen Missbrauch ihrer personenbezogenen Daten reagiert wird;

- der EU-Datenschutzbehörden, denen eine wichtige Rolle zufällt, wenn es darum geht, sicherzustellen, dass Privatpersonen ihre Rechte im Rahmen des Datenschutzschilds wirksam wahrnehmen können, indem sie ihre Beschwerden an die richtige US-Behörde weiterleiten und mit dieser Behörde zusammenarbeiten, indem sie ferner gegebenenfalls die Ombudsperson einschalten, indem sie Beschwerdeführer dabei unterstützen, ihre Beschwerde vor das Datenschutzschild-Panel zu bringen, und indem sie die Aufsicht über die Übermittlung von Personaldaten ausüben;

- der Kommission, die für die Feststellung der Angemessenheit und deren regelmäßige Überprüfung Sorge trägt: Durch die Umwandlung der Angemessenheitsfeststellung im

[23] Derartige Berichterstattungen dürfen nicht gegen die Bestimmungen des USA Freedom Act verstoßen. Vgl. Fußnote 22.

Rahmen des Datenschutzschilds in eine streng überwachte dynamische Regelung stellen diese regelmäßigen Überprüfungen eine deutliche Abkehr von der früheren statischen Situation dar.

Die jährliche gemeinsame Überprüfung und der anschließende Bericht der Kommission – sowie die Möglichkeit, die Regelung im Fall der Nichteinhaltung auszusetzen – werden somit eine zentrale Rolle spielen, um zu gewährleisten, dass der Datenschutzschild sich bewähren wird. Das gemeinsame Ziel unserer transatlantischen Zusammenarbeit sollte es sein, eine ausgeprägte Kultur des Schutzes der Privatsphäre und der Rechte des Einzelnen zu entwickeln, durch die Vertrauen wiederhergestellt und erhalten werden kann.

4. DAS RAHMENABKOMMEN: STÄRKUNG DER DATENSCHUTZGARANTIEN IM BEREICH DER STRAFRECHTLICHEN ZUSAMMENARBEIT

4.1 Hintergrund

Die Fähigkeit der EU, der Mitgliedstaaten und der USA, sich bei gemeinsamen Bedrohungen und Herausforderungen im Bereich der Sicherheit abzustimmen und gemeinsam zu reagieren, macht eine wichtige Dimension unserer transatlantischen Beziehungen aus. Eine zentrale Voraussetzung für diese gemeinsame Reaktion ist der Austausch personenbezogener Daten im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen. Um dieses Ziel zu verwirklichen, wurden im Laufe der Zeit mehrere bilaterale Abkommen zwischen den Mitgliedstaaten und den USA sowie zwischen der EU und den USA[24] geschlossen. Allerdings ist es genauso wichtig, dass diese Abkommen im Bereich der Strafverfolgung wirksame Datenschutzgarantien bieten. Das zweifache Ziel, mit unseren amerikanischen Partnern bei der Bekämpfung von schwerer Kriminalität und Terrorismus erfolgreich zusammenzuarbeiten und gleichzeitig den Schutz der Europäerinnen und Europäer in Einklang mit ihren Grundrechten und den Datenschutzvorschriften der EU bei der Übermittlung von Daten für diese Zwecke zu verbessern, war der Auslöser der im März 2011 eingeleiteten Verhandlungen über ein internationales Datenschutzabkommen im Bereich der Strafverfolgung, das EU-US-Datenschutz-Rahmenabkommen[25].

Die EU und die USA schlossen ihre Verhandlungen im Sommer 2015 ab. Nachdem das Rahmenabkommen von beiden Parteien am 8. September 2015 in Luxemburg unterzeichnet wurde[26], liegt es nun auf beiden Seiten des Atlantiks zur Ratifizierung vor. Die Unterzeichnung des Rahmenabkommens wurde jedoch an die Bedingung geknüpft, dass der „Judicial Redress Act“ vom US-Kongress angenommen wird, um erstmals die Gleichbehandlung von EU-Bürgern und US-Bürgern im Rahmen des US Privacy Act aus dem

[24] Unter anderem das EU-US-Abkommen über die Erfassung von Fluggastdatensätzen (PNR) und das EU-US-Programm zum Aufspüren der Finanzierung des Terrorismus (TFTP).

[25] Ein Abkommen zwischen der EU und den USA über den Schutz personenbezogener Daten bei deren Übermittlung und Verarbeitung zum Zwecke der Verhütung, Untersuchung, Aufdeckung und Verfolgung von Straftaten, einschließlich terroristischer Handlungen, im Rahmen der polizeilichen Zusammenarbeit und der justiziellen Zusammenarbeit in Strafsachen.

[26] http://europa.eu/rapid/press-release_STATEMENT-15-5610_en.htm

Jahr 1974[27] zu gewährleisten. Das Gesetz wurde am 10. Februar 2016 vom Kongress angenommen und am 24. Februar 2016 unterzeichnet und in Kraft gesetzt.

4.2 Was hat sich geändert?

Erstmals in der Geschichte gibt es ein Rahmenabkommen, in dem ein harmonisiertes und umfassendes Paket von Datenschutzgarantien verankert wurde, die für alle transatlantischen Austauschmaßnahmen zwischen den zuständigen Behörden im Bereich der Durchsetzung des Strafrechts gelten. Das Rahmenabkommen ist in der Tat ein Grundrechte-Abkommen, das ein hohes Schutzniveau festlegt, das als Maßstab für den Datenaustausch in bestehenden und künftigen Abkommen gelten wird.

Erstens: **Die im Rahmenabkommen vorgesehenen Schutzbestimmungen und Garantien werden horizontal für jegliche Form von Datenaustausch im Rahmen der transatlantischen Zusammenarbeit bei der Strafverfolgung in Strafsachen gelten.** Dies schließt die Übermittlung von Daten auf der Grundlage von innerstaatlichen Gesetzen, Abkommen zwischen der EU und den USA (z. B. Rechtshilfeabkommen) sowie von spezifischen Abkommen über die Übermittlung personenbezogener Daten durch Einrichtungen des privaten Rechts zu Strafverfolgungszwecken ein. Unmittelbare Folge der vereinbarten Bestimmungen wird die Anhebung des Schutzniveaus für EU-Bürger sein, deren Daten in die USA übermittelt werden. Des Weiteren wird die Rechtssicherheit für die transatlantische Zusammenarbeit bei der Strafverfolgung erhöht, indem sichergestellt wird, dass bestehende Abkommen alle erforderlichen Schutzvorkehrungen enthalten und so etwaigen rechtlichen Anfechtungen standhalten können.

Zweitens: Die vereinbarten Bestimmungen betreffen alle wesentlichen Datenschutzvorschriften der EU hinsichtlich der **Verarbeitungsstandards** (z. B. die Qualität und Integrität der Daten, Datensicherheit, Rechenschaftspflicht und Aufsicht), der **Garantien und Beschränkungen** (z. B. Beschränkungen des Zwecks und der Verwendung, Vorratsdatenspeicherung, Weiterübermittlung von Daten, Verarbeitung sensibler Daten) sowie der **Rechte des Einzelnen** (Zugang, Berichtigung, administrative und gerichtliche Rechtsbehelfe).

Drittens: Das Abkommen wird gewährleisten, dass bei **Verweigerung des Zugangs, Verweigerung der Berichtigung und unrechtmäßiger Offenlegung Rechtsmittel** zur Verfügung stehen. Dies stellt eine große Verbesserung dar und wird einen wichtigen Beitrag zur Wiederherstellung des Vertrauens in den transatlantischen Datentransfer leisten. Dieser für die EU so wichtigen Forderung, auf die während zahlreicher Jahre nicht reagiert worden war, war bereits im „Judicial Redress Act“, der im März 2015 in den US-Kongress

[27] Der Judicial Redress Act garantiert den Bürgern der von der US-Regierung festgelegten „erfassten“ Länder bestimmte Rechte. Dies wird wiederum davon abhängig gemacht, dass folgende Kriterien erfüllt sind: (a) das Land (oder die regionale Organisation) hat ein Abkommen mit den Vereinigten Staaten über den Schutz der Privatsphäre bei der Übermittlung von Informationen zum Zwecke der Verhütung, Untersuchung, Aufdeckung und Verfolgung von Straftaten geschlossen; (b) das Land (oder die regionale Organisation) erlaubt die Übermittlung personenbezogener Daten zu kommerziellen Zwecken zwischen ihm (ihr) und den Vereinigten Staaten; und c) die Vorschriften über die Übermittlung personenbezogener Daten für kommerzielle Zwecke und damit in Zusammenhang stehende Maßnahmen des Landes oder der regionalen Organisation gefährden nicht die nationalen Sicherheitsinteressen der Vereinigten Staaten.

eingebracht und am 10. Februar 2016 verabschiedet wurde, Rechnung getragen worden. Mit diesem Gesetz werden drei Arten des gerichtlichen Rechtsschutzes, die derzeit nur US-Bürgern und Gebietsansässigen im Rahmen des Privacy Act von 1974 gewährt werden, auf EU-Bürger ausgeweitet[28]. Damit kommen die Bürger der EU erstmals in den Genuss von allgemein geltenden Rechten, die im Zusammenhang mit der transatlantische Übertragung von Daten im Bereich der Strafverfolgung geltend gemacht werden können. Damit wurde ein entscheidender Unterschied in der Behandlung zwischen den EU- und USA-Bürgern beseitigt.

Viertens: Das Rahmenabkommen wendet den Grundsatz der **unabhängigen Überwachung** als unverzichtbare Datenschutzforderung, die allerdings in vielen der bestehenden bilateralen Abkommen nicht vorgesehen ist, auf den gesamten Bereich der Strafverfolgung an. Dazu gehören effektive Befugnisse zur Untersuchung und Beilegung von Beschwerden von Einzelpersonen im Zusammenhang mit der Einhaltung der Vereinbarung.

Fünftens: Die Umsetzung des Abkommens wird **in regelmäßigen Abständ**en gemeinsam **überprüft**. Dabei werden insbesondere die Bestimmungen in Bezug auf die Rechte des Einzelnen (Zugang, Berichtigung, administrative und gerichtliche Rechtsbehelfe) überprüft werden.

Das Rahmenabkommen an sich stellt weder eine rechtliche Grundlage für Datentransfers noch einen Angemessenheitsbeschluss dar.

4.3 Das weitere Vorgehen

Das Inkrafttreten des „Judicial Redress Act“[29] wird den Weg für die Unterzeichnung des Rahmenabkommens bereiten. In Kürze wird die Kommission dem Rat einen Vorschlag für einen Beschluss über die Ermächtigung zur Unterzeichnung des Rahmenabkommens vorlegen. Nach der Unterzeichnung muss der Beschluss über den Abschluss des Abkommens vom Rat nach Zustimmung des Europäischen Parlaments angenommen werden. Das Rahmenabkommen wird eine deutliche Verbesserung der derzeitigen Situation herbeiführen, die durch fragmentierte, uneinheitliche und oft schwache Datenschutzvorschriften und eine Vielzahl von multilateralen, bilateralen, nationalen und branchenspezifischen Instrumenten gekennzeichnet ist. Das Rahmenabkommen hat insofern eine retrospektive Funktion, als es die Datenschutzgarantien in den derzeit geltenden Abkommen ersetzen wird, sofern diese nicht das erforderliche Schutzniveau bieten. In diesem Zusammenhang wird es einen beträchtlichen Mehrwert bewirken, indem es im Wesentlichen die „Lücken" der bestehenden Abkommen füllen wird, die niedrigere Datenschutzstandards als die des Rahmenabkommens enthalten. Damit können sowohl die Kontinuität der strafrechtlichen Zusammenarbeit als auch größere Rechtssicherheit bei Datentransfers ermöglicht werden. Im Hinblick auf künftige Abkommen wird das Rahmenabkommen ein Sicherheitsnetz darstellen, unter das das Schutzniveau nicht sinken kann. Dies ist eine sehr wichtige Garantie für die Zukunft und eine deutliche Veränderung gegenüber der jetzigen Situation, wo Garantien, Schutzvorkehrungen

[28] Gemäß dem „Judicial Redress Act“ können auch andere nicht der EU angehörende Länder oder „Organisationen der regionalen Wirtschaftsintegration“ von dem Gesetz „erfasst“ werden, was zur Folge hat, dass die Bürger dieser Länder bzw. Organisationen ebenfalls ein Recht auf gerichtliche Rechtsbehelfe hätten.
[29] Der Judicial Redress Act tritt 90 Tage nach seinem Erlass in Kraft.

und Rechte für jedes neue Abkommen neu ausgehandelt werden müssen. Das Rahmenabkommen kann somit als Modell dienen, das Standardgarantien enthält, die nicht unterschritten werden können. Dies ist nicht nur für die Beziehungen zwischen der EU und den USA ein sehr wichtiger Präzedenzfall, sondern ganz allgemein für jede künftige Datenschutzregelung oder jedes künftige Datenaustauschabkommen auf internationaler Ebene.

Das zeitgleich mit der Reform ausgehandelte „Rahmenabkommen" steht im Einklang mit den Datenschutzvorschriften der EU. Angesichts der Notwendigkeit, unabhängig davon, ob die Verarbeitung personenbezogener Daten auf nationaler Ebene oder grenzüberschreitend innerhalb der EU und mit Drittländern erfolgt, ein hohes und einheitliches Datenschutzniveau zu gewährleisten, kommt der Wechselwirkung zwischen dem Rahmenabkommen und der Polizei-Richtlinie besondere Bedeutung zu. In diesem Zusammenhang wird das Rahmenabkommen dazu beitragen, die allgemeinen Anforderungen der Reform im transatlantischen Kontext mit Leben zu füllen.

Der Abschluss der Verhandlungen über das Rahmenabkommen, das gemeinsame Standards in einem komplexen Bereich der Gesetzgebung und Politik festlegt, ist ein bedeutender Erfolg. Das künftige Rahmenabkommen wird zur Wiederherstellung und Stärkung des Vertrauens beitragen, die Rechtmäßigkeit der Datenübermittlung gewährleisten und die Zusammenarbeit in diesem Bereich zwischen der EU und den USA erleichtern.

In der Zukunft müssen gemeinsame Herausforderungen im Bereich der polizeilichen und justiziellen Zusammenarbeit gemeinsam bewältigt werden. Eine wichtige, noch nicht geklärte Frage betrifft den direkten Zugriff der Strafverfolgungsbehörden auf personenbezogene Daten, die im Besitz von privaten Unternehmen mit Sitz außerhalb der EU sind. Dieser Zugang sollte grundsätzlich im Rahmen formaler Kooperationswege (z. B. Rechtshilfeabkommen oder andere sektorbezogene Vereinbarungen) geregelt sein. Wenn private Unternehmen aufgefordert werden, Zugriff auf elektronische Beweismittel nach den Rechtsvorschriften eines Landes für den Rechtsvorschriften eines anderen Landes unterliegende personenbezogene Daten zu gewähren, ist diese Situation derzeit für sie mit Rechtsunsicherheit verbunden und könnte sich auf ihre Fähigkeit, in verschiedenen Rechtssystemen zu operieren, auswirken. Parallel zur anstehenden Überprüfung des Rechtshilfeabkommens zwischen der EU und den USA in Strafsachen[30] würde die EU weitere Gespräche mit den USA in dieser Angelegenheit, einschließlich der Entwicklung gemeinsamer und wirksamer Vorschriften zur Sammlung elektronischer Beweismittel, begrüßen.

[30] 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 vom 7.11.2009, S.40.

5. Fazit

Der erfolgreiche Abschluss der in der Mitteilung von 2013 dargelegten Leitaktionen zeigt, dass die EU in der Lage ist, Probleme pragmatisch und fokussiert anzugehen, ohne ihre fest verankerten Werte und Traditionen in Bezug auf die Grundrechte zu opfern. Dies ist auch ein Beweis dafür, dass die EU und die USA in der Lage sind, ihre Differenzen auszuräumen und schwierige Entscheidungen zu treffen, um eine strategische Beziehung, die alle Zeiten überstanden hat, weiterzuführen. Allerdings ist jetzt, wo wir ein neues Kapitel in unseren bilateralen Beziehungen aufschlagen, die Zeit der Wachsamkeit noch nicht vorbei, da wir nach wie vor gemeinsame Bedrohungen und Herausforderungen in einer unberechenbaren Welt bewältigen müssen.

Sobald der Datenschutzschild und das Rahmenabkommen in Kraft sind, ist es an beiden Seiten, dafür Sorge zu tragen, dass diese beiden wichtigen Regelungen für die Datenübermittlung effektiv und nachhaltig funktionieren. Ihr Erfolg hängt weitgehend von der wirksamen Durchsetzung und der Einhaltung der Rechte von Privatpersonen ab sowie von der kontinuierlichen Bewertung ihrer Funktionsweise; Dies erfordert ein anderes Denken: von einem statischen hin zu einem dynamischeren Prozess

Eine wichtige Rolle spielt in diesem Zusammenhang die laufende Reform der Datenerhebungsprogramme der US-Geheimdienste. Die Kommission wird die für 2017 angekündigten Berichte des Privacy and Civil Liberties Oversight Boards der USA über Programme, die unter Abschnitt 702 des USA Foreign Intelligence Surveillance Act betrieben werden, aufmerksam verfolgen. Dies gilt insbesondere für weitere Reformen in Bezug auf Transparenz, Aufsicht und Ausweitung der Garantien für Nicht-US-Bürger.

In Anbetracht der Bedeutung, die die grenzüberschreitenden Datenströme für den transatlantischen Handel haben, wird die EU weitere Fortschritte bei der Gesetzgebung der USA im Bereich des Schutzes der Privatsphäre genau verfolgen. Jetzt, da Europa über ein einheitliches, kohärentes und solides Regelwerk verfügt, hoffen wir, dass auch die USA ihre Bemühungen um ein umfassendes Regelwerk zum Schutz der Privatsphäre und zum Datenschutz fortsetzen werden. Durch einen solchen ganzheitlichen Ansatz könnte zwischen den beiden Systemen auf längere Sicht Konvergenz erzielt werden. Die Kommission wird jährlich ein Gipfeltreffen zum Thema Schutz der Privatsphäre veranstalten, zu dem sie einschlägige NRO und andere Interessenträger und Akteure von beiden Seiten des Atlantiks einladen wird.

Die Partnerschaft zwischen der EU und den USA kann zu einer treibenden Kraft bei der Entwicklung und Förderung internationaler Rechtsstandards für den Schutz der Privatsphäre und personenbezogener Daten werden. Initiativen auf Ebene der Vereinten Nationen, einschließlich der Arbeit des Sonderberichterstatters für das Recht auf Privatsphäre, können in diesem Zusammenhang ebenfalls eine wichtige Rolle spielen. Angesichts der wachsenden Bedeutung dieser Themen weltweit sollten die EU und die USA in den kommenden Jahren die Gelegenheit nutzen, ihre gemeinsamen Werte wie der Schutz der individuellen Freiheitsrechte in der globalisierten digitalen Welt voranzubringen.