



Brüssel, den 27.11.2013
COM(2013) 846 final

**MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT UND
DEN RAT**

Wiederherstellung des Vertrauens beim Datenaustausch zwischen der EU und den USA

1. EINLEITUNG: DATENTRANSFER ZWISCHEN DER EU UND DEN USA IM WANDEL

Die Europäische Union und die USA sind strategische Partner, und diese Partnerschaft ist für die Förderung unserer gemeinsamen Werte, unserer Sicherheit und unserer gemeinsamen Führungsrolle in internationalen Angelegenheiten von entscheidender Bedeutung.

Das Vertrauen in diese Partnerschaft hat allerdings Schaden genommen und muss wiederhergestellt werden. Die EU, ihre Mitgliedstaaten und die EU-Bürger haben ihre tiefe Beunruhigung über das Bekanntwerden umfassender Datenerhebungsprogramme der Geheimdienste der USA insbesondere im Zusammenhang mit dem Schutz personenbezogener Daten zum Ausdruck gebracht.¹ Die massenhafte Überwachung privater Kommunikation, sei es von Bürgern, Unternehmen oder Politikern, kann nicht hingenommen werden.

Die Übermittlung personenbezogener Daten stellt einen wichtigen und notwendigen Aspekt der transatlantischen Beziehungen dar. Sie ist integraler Bestandteil der transatlantischen Handelsbeziehungen, auch für neu entstehende digitale Geschäftsbereiche wie soziale Medien oder Cloud-Computing, für die große Datenmengen von der EU in die USA fließen. Darüber hinaus ist sie eine wesentliche Voraussetzung für die Zusammenarbeit der EU und der USA im Bereich der Strafverfolgung sowie für die Zusammenarbeit der Mitgliedstaaten und der USA im Bereich der nationalen Sicherheit. Die USA und die EU haben zur Gewährleistung eines reibungslosen Datenflusses bei gleichzeitiger Sicherung eines hohen Datenschutzniveaus gemäß EU-Recht eine Reihe von Abkommen und Vereinbarungen geschlossen.

Das Thema Handelsbeziehungen ist Gegenstand der Entscheidung 2000/520/EG² (im Folgenden als „Safe-Harbor-Entscheidung“ bezeichnet). Die Entscheidung bietet die Rechtsgrundlage für die Übermittlung personenbezogener Daten aus der EU an in den USA niedergelassene Unternehmen, die die Datenschutz-Grundsätze („Safe Harbor“) beachten.

Der Austausch personenbezogener Daten zwischen der EU und den USA zum Zweck der Strafverfolgung, einschließlich der Prävention und Bekämpfung von Terrorismus und anderer schwerwiegender Formen der Kriminalität, ist in einer Reihe von Abkommen auf EU-Ebene geregelt. Dazu zählen das Abkommen über Rechtshilfe³, das Abkommen über die Verwendung von Fluggastdatensätzen und deren Übermittlung⁴, das Abkommen über die Verarbeitung von Zahlungsverkehrsdaten und deren Übermittlung für die Zwecke des Programms zum Aufspüren der Finanzierung des Terrorismus⁵ und das Abkommen zwischen Europol und den USA. Mit diesen Abkommen werden wichtige die Sicherheit betreffende

¹ Im Sinne dieser Mitteilung ist die Bezugnahme auf EU-Bürger zugleich eine Bezugnahme auf betroffene Personen von Drittstaaten, die in den Anwendungsbereich der EU-Datenschutzvorschriften fallen.

² Entscheidung 2000/520/EG der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des „sicheren Hafens“ und der diesbezüglichen „Häufig gestellten Fragen“ (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA, ABl. L 215 vom 25.8.2000, S. 7.

³ 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.

⁴ Beschluss 2012/472/EU des Rates vom 26. April 2012 über den Abschluss des Abkommens zwischen den Vereinigten Staaten von Amerika und der Europäischen Union über die Verwendung von Fluggastdatensätzen und deren Übermittlung an das United States Department of Homeland Security, ABl. L 215 vom 11.8.2012, S. 4.

⁵ Beschluss 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 vom 27.7.2010, S. 3.

Fragen und die gemeinsamen Sicherheitsinteressen der EU und der USA abgedeckt, wobei zugleich für ein hohes Schutzniveau bei den personenbezogenen Daten gesorgt ist. Darüber hinaus stehen die EU und die USA gegenwärtig in Verhandlungen über ein Rahmenabkommen zum Datenschutz im Bereich der polizeilichen und strafrechtlichen Zusammenarbeit („Rahmenabkommen“).⁶ Das Abkommen zielt darauf ab, ein hohes Datenschutzniveau für die Bürger zu gewährleisten, deren Daten übermittelt werden, und auf diese Weise die Zusammenarbeit EU-USA bei der Bekämpfung von Kriminalität und Terrorismus auf der Grundlage gemeinsamer Werte und vereinbarter Standards weiter zu verbessern.

Diese Instrumente kommen in einem Umfeld zum Einsatz, in dem der Umgang mit personenbezogenen Daten einen immer größeren Stellenwert erhält.

Die Entwicklung der digitalen Wirtschaft hat zu einem exponentiellen Anstieg der Quantität, Qualität, Vielfalt und Art der Tätigkeiten im Bereich der Datenverarbeitung geführt. Im Alltag nehmen die Bürger immer häufiger elektronische Kommunikationsdienste in Anspruch. Der Wert personenbezogener Daten hat zugenommen: Im Jahr 2011 wurden die Daten von EU-Bürgern auf einen Wert von 315 Mrd. EUR geschätzt, und es ist von einem jährlichen Anstieg auf nahezu 1 Bio. EUR bis 2020 auszugehen.⁷ Der Markt für die Analyse sehr großer Datensätze steigt jährlich weltweit um 40%.⁸ Gleichzeitig ist mit der technologischen Entwicklung beispielsweise im Bereich des Cloud-Computings der internationale Datentransfer in den Mittelpunkt der Aufmerksamkeit gerückt, weil grenzüberschreitende Datenströme aus der alltäglichen Realität nicht mehr wegzudenken sind.⁹

Mit der zunehmenden Nutzung elektronischer Kommunikations- und Datenverarbeitungsdienste, darunter des Cloud-Computings, haben auch Umfang und Bedeutung der transatlantischen Datenübermittlungen zugenommen. Dadurch haben Aspekte wie die zentrale Stellung von US-Unternehmen in der digitalen Wirtschaft¹⁰, die Abwicklung eines Großteils der elektronischen Kommunikation über den transatlantischen Datenverkehr und das Volumen der elektronischen Datenströme zwischen der EU und den USA zusätzlich an Bedeutung gewonnen.

Gleichzeitig werfen die modernen Verfahren der Verarbeitung personenbezogener Daten jedoch neue und wichtige Fragen auf. Dies gilt sowohl für neue Methoden der Verarbeitung großer Mengen an Verbraucherdaten zu kommerziellen Zwecken durch Privatunternehmen als auch für die immer besseren Möglichkeiten einer breit angelegten Überwachung der Kommunikationsdaten durch die Geheimdienste.

Groß angelegte Datenerhebungsprogramme der US-Geheimdienste wie PRISM beeinträchtigen die Grundrechte der Europäer, insbesondere ihr Recht auf Privatsphäre und Schutz der personenbezogenen Daten. Diese Programme deuten zudem darauf hin, dass eine Verbindung zwischen der staatlichen Überwachung und der Datenverarbeitung durch Privatunternehmen, in erster Linie US-Internetfirmen, besteht. Infolgedessen sind mit ihnen unter Umständen auch wirtschaftliche Auswirkungen verbunden. Wenn Bürger wegen der

⁶ Der Rat hat am 3. Dezember 2010 einen Beschluss angenommen, in dem die Kommission zur Aushandlung des Abkommens ermächtigt wird. Siehe IP/10/1661 vom 3. Dezember 2010.

⁷ Siehe Boston Consulting Group, „The Value of our Digital Identity“, November 2012.

⁸ Siehe McKinsey, „Big data: The next frontier for innovation, competition, and productivity“, 2011.

⁹ Mitteilung zur Freisetzung des Cloud-Computing-Potenzials in Europa, COM(2012) 529 final.

¹⁰ Beispielsweise belief sich die Gesamtzahl der Unique Visitors bei Hotmail, Google Gmail und Yahoo! Mail aus europäischen Ländern im Juni 2012 auf mehr als 227 Millionen und lag damit über der aller anderen Anbieter. Die Gesamtzahl der europäischen Unique Visitors, die im März 2012 Facebook und Facebook Mobile aufgerufen haben, betrug 196,5 Millionen. Damit war Facebook das größte soziale Netzwerk in Europa. Google ist mit einem Anteil von 90,2 % der weltweiten Internetnutzer die führende Internetsuchmaschine. Der mobile Nachrichtendienst aus den USA, What's App, wurde im Juni 2013 von 91 % der deutschen iPhone-Nutzer verwendet.

massenhaften Verarbeitung ihrer personenbezogenen Daten durch Privatunternehmen oder der Tatsache, dass ihre Daten bei der Nutzung von Internetdiensten durch Geheimdienste überwacht werden, besorgt sind, so könnte dies ihrem Vertrauen in die digitale Wirtschaft schaden und sich dementsprechend auch negativ auf das Wachstum auswirken.

Angesichts dieser Entwicklungen muss der Umgang mit den Datenströmen EU-USA neu gestaltet werden. In der vorliegenden Mitteilung werden die damit verbundenen Aufgaben erörtert. Ferner wird das weitere Vorgehen auf der Grundlage der im Bericht der EU-Ko-Vorsitzenden der Ad-hoc-Arbeitsgruppe EU-USA und in der Mitteilung zur Safe-Harbor-Regelung enthaltenen Ergebnisse erläutert.

Es sollen wirksame Maßnahmen aufgezeigt werden, um das Vertrauen wiederherzustellen, die Zusammenarbeit zwischen der EU und den USA in diesen Bereichen zu intensivieren und die transatlantischen Beziehungen generell zu stärken.

Die Mitteilung beruht auf der Annahme, dass der Standard für den Schutz personenbezogener Daten in einem eigenen Zusammenhang zu betrachten ist und sich nicht auf andere Aspekte der Beziehungen zwischen der EU und den USA auswirken darf, darunter die laufenden Verhandlungen über eine transatlantische Handels- und Investitionspartnerschaft. Aus diesem Grund wird die Frage der Datenschutzstandards nicht Gegenstand der Verhandlungen über die transatlantische Handels- und Investitionspartnerschaft sein, in deren Rahmen die Datenschutzbestimmungen uneingeschränkt eingehalten werden.

In diesem Zusammenhang sei daran erinnert, dass die EU im Rahmen ihrer Zuständigkeiten zwar Maßnahmen ergreifen kann, um insbesondere die Einhaltung der EU-Rechtsvorschriften¹¹ zu gewährleisten, die Wahrung der nationalen Sicherheit jedoch ausschließlich den Mitgliedstaaten obliegt¹².

2. AUSWIRKUNGEN AUF DIE INSTRUMENTE ZUR DATENÜBERTRAGUNG

Als erster Punkt ist anzuführen, dass sich die Safe-Harbor-Regelung bei Daten, die zu kommerziellen Zwecken übermittelt werden, als wichtiges Instrument für Datenübermittlungen zwischen der EU und den USA erwiesen hat. Zeitgleich mit dem Anwachsen der Bedeutung der personenbezogenen Daten in den transatlantischen Handelsbeziehungen hat auch die handelspolitische Bedeutung dieser Regelung zugenommen. In den vergangenen 13 Jahren ist das Safe-Harbor-System auf mehr als 3000 beteiligte Unternehmen ausgeweitet worden, von denen sich mehr als die Hälfte innerhalb der letzten fünf Jahre zur Teilnahme bereiterklärt hat. Nichtsdestotrotz nehmen die Bedenken mit Blick auf das Schutzniveau für in die USA übertragene personenbezogene Daten von EU-Bürgern immer weiter zu. Aufgrund des freiwilligen und deklaratorischen Charakters des Systems wird das Augenmerk verstärkt auf dessen Transparenz und Durchsetzung gelegt. Während die Mehrheit der US-Unternehmen die Grundsätze befolgt, ist dies bei einigen Unternehmen, die dem System beigetreten sind, nicht der Fall. Dies führt dazu, dass Unternehmen, die den Grundsätzen des „sicheren Hafens“ zwar beigetreten sind, diese aber nicht einhalten, in den Genuss von Wettbewerbsvorteilen gegenüber europäischen Unternehmen kommen, die auf denselben Märkten tätig sind.

Darüber hinaus stellt sich die Frage, ob angesichts der Tatsache, dass im Rahmen des „sicheren Hafens“ Einschränkungen der Datenschutzbestimmungen möglich sind, wenn sie sich aus Gründen der nationalen Sicherheit¹³ als notwendig erweisen, die umfassende

¹¹ Siehe Urteil des Gerichtshofs der Europäischen Union in der Rechtssache C-300/11, ZZ gegen Secretary of State for the Home Department.

¹² Artikel 4 Absatz 2 EUV.

¹³ Siehe beispielsweise Safe-Harbor-Entscheidung, Anhang I.

Erfassung und Verarbeitung personenbezogener Informationen im Rahmen von US-Überwachungsprogrammen zum Schutz nationaler Sicherheitsinteressen notwendig und angemessen ist. Die Ergebnisse der Ad-hoc-Arbeitsgruppe EU-USA deuten ferner darauf hin, dass EU-Bürgern in diesen Programmen nicht dieselben Rechte und Verfahrensgarantien wie US-Staatsbürgern eingeräumt werden.

Angesichts der Reichweite dieser Überwachungsprogramme und der Ungleichbehandlung der EU-Bürger stellt sich die Frage nach dem Schutzniveau, das durch die Safe-Harbor-Regelung geboten wird. Die im Rahmen des „sicheren Hafens“ an die USA übermittelten personenbezogenen Daten von EU-Bürgern können durch die US-Behörden in einer Weise eingesehen und weiterverarbeitet werden, die mit dem eigentlichen Zweck ihrer Erfassung in der EU und mit den Gründen für ihre Übermittlung in die USA unvereinbar ist. Die Mehrzahl der US-Internetfirmen, bei denen sich ein unmittelbarer Zusammenhang zu den Programmen herstellen lässt, ist den Safe-Harbor-Grundsätzen beigetreten.

Was zweitens den Datenaustausch zu Zwecken der Strafverfolgung angeht, so haben sich die bestehenden Abkommen (PNR, TFTP) als ausgesprochen wertvolle Instrumente im Umgang mit gemeinsamen Sicherheitsbedrohungen durch schwere grenzüberschreitende Kriminalität und Terrorismus erwiesen und umfassen gleichzeitig Garantien für ein hohes Datenschutzniveau¹⁴. Diese Garantien gelten auch für EU-Bürger, wobei in den Abkommen Mechanismen zur Überprüfung der Anwendung und zum Umgang mit diesbezüglichen Problemen vorgesehen sind. Mit dem TFTP-Abkommen wird ferner ein Aufsichtssystem eingeführt, bei dem unabhängige Prüfer aus der EU darüber wachen, wie die unter das Abkommen fallenden Daten von den USA durchsucht werden.

Angesichts der Bedenken, die in der EU über die US-Überwachungsprogramme laut geworden sind, hat sich die Europäische Kommission diese Instrumente zunutze gemacht, um die Anwendung der Abkommen zu prüfen. Zum PNR-Abkommen wurde eine gemeinsame Überprüfung der Anwendung des Abkommens vorgenommen, an der Datenschutzsachverständige aus der EU und den USA beteiligt waren.¹⁵ Diese Überprüfung ergab keinerlei Hinweise darauf, dass sich die US-Überwachungsprogramme auf die im Rahmen des PNR-Abkommens erfassten Passagierdaten erstrecken oder auswirken. Im Falle des TFTP-Abkommens hat die Kommission offizielle Konsultationen aufgenommen, nachdem Vorwürfe laut geworden waren, dass US-Geheimdienste entgegen dem Abkommen direkt auf personenbezogene Daten in der EU zugreifen. Diese Konsultationen ließen keinerlei Hinweise auf Verletzung des TFTP-Abkommens erkennen, und die USA haben im Anschluss schriftlich zugesichert, dass keine direkte Datensammlung, mit der gegen das Abkommen verstoßen worden wäre, erfolgt sei.

Da im Rahmen von US-Überwachungsprogrammen personenbezogene Informationen in großem Stil erfasst und verarbeitet werden, erweist sich jedoch eine gründliche Überprüfung der Anwendung des PNR- und des TFTP-Abkommens auch in Zukunft als notwendig. Die EU und die USA haben sich demzufolge darauf verständigt, an der Vorbereitung der nächsten gemeinsamen Überprüfung des TFTP-Abkommens, die im Frühjahr 2014 stattfinden wird, zu arbeiten. Im Rahmen dieser und künftiger gemeinsamer Überprüfungen soll für mehr Transparenz mit Blick auf die Funktionsweise des Aufsichtssystems und seinen Beitrag zum Schutz der Daten von EU-Bürgern gesorgt werden. Parallel dazu sind Maßnahmen angedacht,

¹⁴ Siehe den Gemeinsamen Bericht der Kommission und des US-Finanzministeriums über den Nutzen der bereitgestellten TFTP-Daten gemäß Artikel 6 Absatz 6 des Abkommens zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über die Verarbeitung von Zahlungsverkehrsdaten und deren Übermittlung aus der Europäischen Union an die Vereinigten Staaten von Amerika für die Zwecke des Programms zum Aufspüren der Finanzierung des Terrorismus.

¹⁵ Siehe Bericht der Kommission „Gemeinsame Überprüfung der Anwendung des Abkommens zwischen der EU und den USA über die Verwendung von Fluggastdatensätzen und deren Übermittlung an das US Department of Homeland Security“.

um zu gewährleisten, dass im Rahmen des Aufsichtssystems auch weiterhin genau beobachtet wird, in welcher Form die Daten, die an die USA im Rahmen des Abkommens übertragen werden, verarbeitet und vor allem auch zwischen den US-Behörden ausgetauscht werden.

Drittens zeigt sich mit dem Anstieg des Volumens der verarbeiteten personenbezogenen Daten auch die Bedeutung der geltenden rechtlichen und administrativen Garantien. Die Ad-hoc-Arbeitsgruppe EU-USA wollte unter anderem festlegen, welche Vorkehrungen getroffen werden müssen, um die Einschränkungen der Grundrechte der EU-Bürger durch die Verarbeitung möglichst gering zu halten. Garantien sind darüber hinaus auch zum Schutz der Unternehmen erforderlich. Auf der Grundlage bestimmter US-Gesetze wie des Patriot Act können US-Behörden direkt an Unternehmen herantreten und Zugriff auf in der EU gespeicherte Daten verlangen. Europäische Unternehmen und in der EU niedergelassene US-Unternehmen können dementsprechend zur Datenübermittlung in die USA unter Verletzung von Rechtsvorschriften der EU und der Mitgliedstaaten verpflichtet werden und geraten auf diese Weise in das Spannungsfeld zweier im Widerspruch zueinander stehender rechtlicher Verpflichtungen. Die Rechtsunsicherheit, die mit derartigen direkten Ersuchen verbunden ist, kann die Entwicklung neuer digitaler Dienste verzögern, beispielsweise des Cloud-Computings, das für den Einzelnen und Unternehmen gleichermaßen effiziente und kostengünstige Lösungen bieten kann.

3. GEWÄHRLEISTUNG DER WIRKSAMKEIT DES DATENSCHUTZES

Die Übertragung personenbezogener Daten zwischen der EU und den USA ist ein wichtiger Bestandteil der transatlantischen Handelsbeziehungen. Der Austausch von Informationen ist ebenfalls eine wichtige Komponente der Zusammenarbeit zwischen der EU und den USA im Sicherheitsbereich und von entscheidender Bedeutung für das gemeinsame Ziel der Prävention und Bekämpfung von schwerer Kriminalität und Terrorismus. Allerdings haben die jüngsten Enthüllungen über Datenerhebungsprogramme der US-Geheimdienste dem Vertrauen geschadet, auf das sich eine solche Zusammenarbeit stützt. Insbesondere wurde das Vertrauen in den Umgang mit den personenbezogenen Daten beeinträchtigt. Zur Wiederherstellung des Vertrauens in die Datenübermittlungen sollten die im Folgenden genannten Schritte unternommen werden, da dies der digitalen Wirtschaft, der Sicherheit sowohl in der EU als auch in den USA und dem transatlantischen Verhältnis insgesamt zugute kommen würde.

3.1 Die Reform der EU-Datenschutzvorschriften

Die von der Kommission im Januar 2012 angeregte Reform der EU-Datenschutzvorschriften¹⁶ ist die zentrale Antwort in Sachen Schutz personenbezogener Daten. Fünf Aspekte des vorgeschlagenen Datenschutz-Reformpakets sind von besonderer Bedeutung.

Erstens wird mit Blick auf den räumlichen Anwendungsbereich in der vorgeschlagenen Verordnung deutlich gemacht, dass nicht in der Union niedergelassene Unternehmen an das EU-Datenschutzrecht gebunden sind, wenn sie europäischen Verbrauchern Waren und Dienstleistungen anbieten oder ihr Verhalten beobachten wollen. Anders ausgedrückt, das

¹⁶ COM(2012) 10 final: 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, Brüssel, 25.1.2012, und COM(2012) 11 final: 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).

Grundrecht auf Datenschutz gilt unabhängig vom Sitz eines Unternehmens oder seines Verarbeitungsbetriebs.¹⁷

Was zweitens den internationalen Datentransfer anbelangt, so werden in der vorgeschlagenen Verordnung die Voraussetzungen für die Datenübermittlung in ein Drittland festgelegt. Transfers sind nur zulässig, wenn diese Bedingungen, mit denen das Recht natürlicher Personen auf ein hohes Schutzniveau gewährleistet werden kann, erfüllt sind.¹⁸

Drittens sehen die vorgeschlagenen Bestimmungen im Bereich der Durchsetzung verhältnismäßige und abschreckende Sanktionen vor (bis zu 2 % des weltweiten Jahresumsatzes eines Unternehmens), um die Einhaltung der EU-Rechtsvorschriften durch die Unternehmen sicherzustellen.¹⁹ Durch die Androhung spürbarer Sanktionen fühlen sich Unternehmen stärker an die Einhaltung der EU-Rechtsvorschriften gebunden.

Viertens umfasst die vorgeschlagene Verordnung eindeutige Bestimmungen zu den Verpflichtungen und zur Haftung von Datenverarbeitern wie Cloud-Anbietern, auch im Bereich der Sicherheit.²⁰ Wie die Enthüllungen über die Datenerhebungsprogramme von US-Geheimdiensten gezeigt haben, ist dies ein entscheidender Punkt, da diese Programme in der Cloud gespeicherte Daten betreffen. Darüber hinaus können sich Unternehmen, die Speicherplatz in der Cloud anbieten und zur Herausgabe personenbezogener Daten an ausländische Behörden aufgefordert werden, nicht mit dem Verweis darauf, dass sie zwar Datenverarbeiter, aber nicht für die Datenverarbeitung verantwortlich sind, ihrer Verantwortung entziehen.

Fünftens sieht das Paket die Festlegung umfassender Bestimmungen zum Schutz von im Bereich der Strafverfolgung verarbeiteten personenbezogenen Daten vor.

Es wird mit einer raschen Annahme des Pakets im Verlauf des Jahres 2014 gerechnet.²¹

3.2 Das Safe-Harbor-System sicherer machen

Das Safe-Harbor-System ist ein wichtiger Bestandteil der Handelsbeziehungen zwischen der EU und den USA, auf das sich Unternehmen beiderseits des Atlantiks stützen.

Im Kommissionsbericht über die Funktionsweise des Systems konnten einige Schwachstellen ermittelt werden. Aufgrund mangelnder Transparenz und Durchsetzung halten sich einige dem System beigetretene Unternehmen in der Praxis nicht an dessen Grundsätze. Dies wirkt sich nachteilig auf die Grundrechte der EU-Bürger aus. Ferner entstehen auf diese Weise Nachteile für europäische Unternehmen gegenüber ihren Mitbewerbern aus den USA, die

¹⁷ Die Kommission nimmt zur Kenntnis, dass das Europäische Parlament diesen zentralen Grundsatz, der in Artikel 3 der vorgeschlagenen Verordnung verankert ist, bei seiner Abstimmung über die Berichte der MdEP Jan-Philipp Albrecht und Dimitrios Droutsas über die Reform der Datenschutzvorschriften am 21. Oktober 2013 im Ausschuss für bürgerliche Freiheiten, Justiz, und Inneres (LIBE) bestätigt und bekräftigt hat.

¹⁸ Die Kommission nimmt zur Kenntnis, dass der LIBE-Ausschuss des Europäischen Parlaments bei seiner Abstimmung am 21. Oktober 2013 vorgeschlagen hat, eine Bestimmung in die künftige Verordnung aufzunehmen, wonach Anträge ausländischer Behörden auf Zugang zu in der EU erfassten personenbezogenen Daten zunächst durch eine nationale Datenschutzbehörde zu genehmigen sind, sofern ein solcher Antrag nicht auf Grundlage eines Rechtshilfeabkommens oder eines anderen internationalen Abkommens gestellt wird.

¹⁹ Die Kommission nimmt zur Kenntnis, dass der LIBE-Ausschuss bei seiner Abstimmung am 21. Oktober 2013 vorgeschlagen hat, dem Kommissionsvorschlag noch mehr Substanz zu verleihen und hierzu eine Erhöhung der Geldbußen auf bis zu 5 % des weltweiten Jahresumsatzes eines Unternehmens festzulegen.

²⁰ Die Kommission nimmt zur Kenntnis, dass der LIBE-Ausschuss bei seiner Abstimmung am 21. Oktober 2013 die Stärkung der Verpflichtungen und der Haftung der Datenverarbeiter insbesondere mit Blick auf Artikel 26 der vorgeschlagenen Verordnung gebilligt hat.

²¹ In den Schlussfolgerungen des Europäischen Rates vom Oktober 2013 heißt es: „Das Vertrauen der Bürger und Unternehmen in die digitale Wirtschaft muss gefördert werden. Die rasche Verabschiedung eines soliden allgemeinen Rahmens für den Datenschutz in der EU und der Cybersicherheitsrichtlinie ist für die Vollendung des digitalen Binnenmarkts bis 2015 von entscheidender Bedeutung“.

sich zwar am System beteiligen, in der Praxis dessen Grundsätze jedoch ignorieren. Diese Schwachstelle wirkt sich auch auf die Mehrheit der US-Unternehmen aus, die das System ordnungsgemäß anwenden. Das System des sicheren Hafens dient ferner als Kanal für die Übertragung personenbezogener Daten von EU-Bürgern von der EU in die USA durch Unternehmen, die zur Freigabe von Daten an US-Geheimdienste im Rahmen der Datenerhebungsprogramme dieser Dienste aufgefordert werden. Sollten diese Mängel nicht ausgeräumt werden, wären damit Wettbewerbsnachteile für EU-Unternehmen sowie negative Auswirkungen auf das Grundrecht der EU-Bürger auf Datenschutz verbunden.

Die Unzulänglichkeiten des Safe-Harbor-Systems wurden auch bei der Reaktion der europäischen Datenschutzbehörden auf die jüngsten Überwachungsenthüllungen deutlich. Gemäß Artikel 3 der Safe-Harbor-Entscheidung können diese Behörden unter gewissen Voraussetzungen die Datenübermittlung an eine Organisation aussetzen, die den Grundsätzen beigetreten ist.²² Deutsche Datenschutzbeauftragte haben entschieden, keine neuen Genehmigungen mehr für Datenübertragungen in Drittländer (beispielsweise für die Nutzung bestimmter Cloud-Dienste) zu erteilen. Sie wollen ferner prüfen, ob Datenübertragungen im Rahmen des Safe-Harbor-Systems ausgesetzt werden sollten.²³ Maßnahmen dieser Art bergen, wenn sie einzelstaatlich ergriffen werden, die Gefahr, dass sie die einheitliche Anwendung der Regelung durchbrechen, d. h. dass Safe Harbor seine Funktion als Hauptmechanismus zur Übertragung personenbezogener Daten zwischen der EU und den USA einbüßt.

Die Kommission ist gemäß Richtlinie 95/46/EG zur Aussetzung oder Aufhebung der Safe-Harbor-Entscheidung befugt, wenn mit dem System kein angemessenes Schutzniveau mehr gewährleistet werden kann. Ferner sieht Artikel 3 der Entscheidung vor, dass die Kommission zur Aufhebung, Aussetzung oder Beschränkung des Geltungsbereichs der Entscheidung befugt ist, während sie nach Maßgabe von Artikel 4 die Entscheidung im Licht der Erfahrungen mit ihrer Anwendung jederzeit anpassen kann.

Vor diesem Hintergrund sind mehrere strategische Optionen denkbar:

- Beibehaltung des Status quo
- Stärkung des Safe-Harbor-Systems und gründliche Prüfung seiner Funktionsweise
- Aussetzung oder Aufhebung der Safe-Harbor-Entscheidung

Angesichts der festgestellten Schwachstellen kann das Safe-Harbor-System nicht wie bisher fortgeführt werden. Seine Aufhebung würde allerdings den Interessen der beteiligten Unternehmen in der EU und in den USA schaden. Die Kommission ist daher der Auffassung, dass das Safe-Harbor-System eher gestärkt werden sollte.

Die Verbesserungen sollten sowohl auf die strukturellen Mängel bei der Transparenz und der Durchsetzung als auch auf die wichtigsten Grundsätze des Safe-Harbor-Systems und die Ausnahmeregelungen aus Gründen der nationalen Sicherheit ausgerichtet sein.

Damit das System des sicheren Hafens seinen Zweck erfüllen kann, müssen die US-Behörden gründlicher und systematischer überwachen und prüfen, ob die der Regelung beigetretenen Unternehmen die Safe-Harbor-Grundsätze zum Datenschutz beachten. Die Transparenz der

²² Eine Aussetzung kann gemäß Artikel 3 der Safe-Harbor-Entscheidung insbesondere dann erfolgen, wenn eine hohe Wahrscheinlichkeit besteht, dass die Grundsätze verletzt werden; wenn Grund zu der Annahme besteht, dass die jeweilige Durchsetzungsinstanz nicht rechtzeitig angemessene Maßnahmen ergreift bzw. ergreifen wird, um den Fall zu lösen; wenn die fortgesetzte Datenübermittlung für die betroffenen Personen das unmittelbar bevorstehende Risiko eines schweren Schadens schaffen würde, und wenn die zuständigen Behörden in den Mitgliedstaaten die Organisation unter den gegebenen Umständen in angemessener Weise unterrichtet und ihr Gelegenheit zur Stellungnahme gegeben haben.

²³ Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, Pressemitteilung vom 24. Juli 2013.

Datenschutzgrundsätze, nach denen sich die beigetretenen Unternehmen richten, muss verbessert werden. Ferner müssen EU-Bürger Zugang zu erschwinglichen Streitbelegungsmechanismen haben.

Die Kommission wird mit den US-Behörden unverzüglich Gespräche über die festgestellten Mängel aufnehmen. Bis zum Sommer 2014 sollen Abhilfemaßnahmen erarbeitet werden, die anschließend möglichst umgehend umgesetzt werden. Die Kommission wird auf der Grundlage dieser Erkenntnisse eine umfassende Bilanz der Funktionsweise des Safe-Harbor-Systems ziehen. Im Rahmen des allgemeinen Überprüfungsprozesses sollen offene Konsultationen und eine Aussprache im Europäischen Parlament und im Rat sowie Gespräche mit den US-Behörden geführt werden.

Darüber hinaus ist dringend dafür Sorge zu tragen, dass in der Safe-Harbor-Entscheidung über den sicheren Hafen vorgesehene Ausnahmeregelungen aus Gründen der nationalen Sicherheit nur in dringend notwendigen und angemessenen Fällen zur Anwendung kommen.

3.3 Stärkung der Datenschutzgarantien im Bereich der strafrechtlichen Zusammenarbeit

Die EU und die USA verhandeln gegenwärtig über ein Datenschutz-Rahmenabkommen über die Übermittlung und Verarbeitung personenbezogener Informationen im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen. Mit dem Abschluss eines solchen Abkommens, mit dem ein hohes Schutzniveau für personenbezogene Daten verbunden wäre, würde ein wichtiger Beitrag zur Stärkung des Vertrauens beiderseits des Atlantiks geleistet. Durch die Ausweitung des Schutzes der Daten von EU-Bürgern würde die transatlantische Zusammenarbeit im Bereich der Prävention und Bekämpfung von Kriminalität und Terrorismus gestärkt.

Gemäß dem Beschluss über die Ermächtigung der Kommission zur Aushandlung des Rahmenabkommens sollen die Verhandlungen darauf ausgerichtet sein, ein hohes Schutzniveau zu gewährleisten, das dem Besitzstand der EU im Bereich des Datenschutzes entspricht. Diese Vorgabe soll sich in den vereinbarten Bestimmungen und Garantien widerspiegeln, die unter anderem die Zweckbegrenzung, die Bedingungen und die Dauer der Datenspeicherung betreffen. Die Kommission soll sich im Rahmen der Verhandlungen auch um Verpflichtungen zu durchsetzbaren Rechten einschließlich Rechtsmittelverfahren für EU-Bürger, die nicht in den USA ansässig sind, bemühen.²⁴ Eine enge Zusammenarbeit der EU und der USA zur Bewältigung gemeinsamer Sicherheitsherausforderungen soll begleitet sein von dem Bemühen, Bürgern beiderseits des Atlantiks dieselben Rechte zu garantieren, wenn dieselben Daten zu denselben Zwecken verarbeitet werden. Ferner sind Ausnahmeregelungen aus Gründen der nationalen Sicherheit genau zu erläutern. Hierzu sollen gemeinsam Garantien und Beschränkungen festgelegt werden.

Diese Verhandlungen bieten die Gelegenheit festzulegen, dass auf personenbezogene Daten, die sich im Besitz von Privatunternehmen in der EU befinden, von den US-Strafverfolgungsbehörden nicht außerhalb der offiziellen Kooperationskanäle wie Rechtshilfeabkommen oder sektorbezogene Abkommen zwischen der EU und den USA, laut denen Datenübermittlungen dieser Art gestattet sind, zugegriffen wird bzw. dass diese Daten

²⁴ Siehe den entsprechenden Abschnitt der gemeinsamen Presseerklärung zum Justiz- und Innenministertreffen EU-USA am 18. November 2013 in Washington: „Wir sind daher angesichts der Dringlichkeit darum bemüht, die Verhandlungen über ein richtungweisendes und umfassendes Rahmenabkommen zum Datenschutz im Bereich der Strafverfolgung rasch voranzubringen. Mit dem Abkommen könnte durch die Gewährleistung eines hohen Schutzniveaus für die personenbezogenen Daten von EU- und US-Bürgern die Grundlage für die erleichterte Übertragung von Daten im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen geschaffen werden. Wir sind um Klärung der auf beiden Seiten ausstehenden Fragen auch mit Blick auf den Rechtsschutz bemüht (eine zentrale Frage für die EU). Ziel ist es, die Verhandlungen über das geplante Abkommen bis zum Sommer 2014 zum Abschluss zu bringen.“

nicht außerhalb dieses Rahmens übertragen werden. Der Zugang über andere Wege ist nur in klar festgelegten und gerichtlich überprüfbaren Ausnahmefällen gestattet. Von den USA werden in diesem Zusammenhang Verpflichtungserklärungen erwartet.²⁵

Mit einem Rahmenabkommen, das sich auf diese Vorgaben stützt, soll eine allgemeine Grundlage für ein hohes Schutzniveau personenbezogener Daten bei der Übertragung in die USA zum Zweck der Prävention oder Bekämpfung von Kriminalität und Terrorismus gegeben sein. Sektorbezogene Abkommen sollen, sofern sich dies aufgrund der Art der Datenübertragung als notwendig erweist, zusätzliche Bestimmungen und Garantien nach dem Vorbild des PNR- und des TFTP-Abkommens zwischen der EU und den USA umfassen, mit denen strenge Bedingungen für den Datentransfer und Garantien für EU-Bürger festgelegt werden.

3.4 Berücksichtigung europäischer Belange im Rahmen des laufenden US-Reformprozesses

US-Präsident Obama hat eine Überprüfung der Tätigkeiten der nationalen Sicherheitsbehörden auch mit Blick auf den geltenden Rechtsrahmen angekündigt. Dieser Prozess bietet eine wichtige Gelegenheit, auf die Bedenken der EU angesichts der jüngsten Enthüllungen zu Datenerhebungsprogrammen der US-Geheimdienste zu reagieren. Zu den wichtigsten Neuerungen würden die Ausweitung der für US-Bürger und Gebietsansässige geltenden Garantien auf nicht in den USA ansässige EU-Bürger, mehr Transparenz bei den Tätigkeiten der Nachrichtendienste und eine Stärkung der Aufsicht gehören. Mit derartigen Änderungen könnten das Vertrauen in den Datenaustausch EU-USA wiederhergestellt und die Nutzung von Internetdiensten durch Europäer gefördert werden.

Im Zusammenhang mit der Ausweitung der für US-Bürger und Gebietsansässige geltenden Garantien auf EU-Bürger bedarf es einer Prüfung der Rechtsstandards für die US-Überwachungsprogramme, bei denen US- und EU-Bürger nicht gleichbehandelt werden, auch in Bezug auf deren Notwendigkeit und Angemessenheit und unter Berücksichtigung der engen transatlantischen Partnerschaft, die sich auf gemeinsame Werte, Rechte und Freiheiten stützt. Auf diese Weise ließe sich das Maß, in dem Europäer von den Datenerhebungsprogrammen der US-Geheimdienste betroffen sind, verringern.

Mit Blick auf den Rechtsrahmen für die Datenerhebungsprogramme der US-Geheimdienste und seine Auslegung durch die US-Gerichte sowie auf die quantitative Dimension dieser Programme ist die Transparenz zu verbessern. Von derartigen Veränderungen würden die EU-Bürger ebenfalls profitieren.

Die Aufsicht über die Datenerhebungsprogramme der US-Geheimdienste ließe sich durch eine Stärkung der Rolle des Gerichts zur Überwachung der Auslandsgeheimdienste (US Foreign Intelligence Surveillance Court) sowie durch die Einführung von Rechtsmitteln für natürliche Personen verbessern. Mit den genannten Mechanismen könnte die Verarbeitung von für nationale Sicherheitsbelange unbedeutenden personenbezogenen Daten von Europäern eingeschränkt werden.

²⁵ Siehe den entsprechenden Abschnitt der gemeinsamen Presseerklärung zum Justiz- und Innenministertreffen EU-USA am 18. November 2013 in Washington: „Ferner möchten wir den Stellenwert des Rechtshilfeabkommens zwischen der EU und den USA hervorheben. Wir sind auch weiterhin darum bemüht, seine umfassende und zielgerichtete Nutzung zur Beweisermittlung in Strafverfahren sicherzustellen. Es ist auch über die Notwendigkeit der Festlegung gesprochen worden, dass die Strafverfolgungsbehörden auf personenbezogene Daten, die sich im Besitz von Privatunternehmen im Hoheitsgebiet der anderen Vertragspartei befinden, nicht außerhalb der rechtlich zulässigen Kanäle zugreifen. Wir haben uns zudem darauf verständigt, die Funktionsweise des Rechtshilfeabkommens, wie im Abkommen vorgesehen, zu überprüfen und im Bedarfsfall Konsultationen aufzunehmen.“

3.5 Förderung von Datenschutznormen auf internationaler Ebene

Die Schwierigkeiten, die sich im Zusammenhang mit modernen Datenschutzverfahren ergeben, sind nicht allein auf den Datentransfer zwischen der EU und den USA beschränkt. Ein höheres Schutzniveau für personenbezogene Daten ist für jede natürliche Person zu gewährleisten. Es sollten Anstrengungen unternommen werden, die EU-Rechtsvorschriften für die Erfassung, Verarbeitung und Weitergabe von Daten international zu fördern.

In jüngster Zeit wurde eine Reihe von Initiativen für einen verbesserten Schutz der Privatsphäre, insbesondere im Internet, angeregt.²⁶ Die EU sollte sich dafür einsetzen, dass bei eventuell eingeleiteten Initiativen, die in diese Richtung zielen, dem Schutz der Grundrechte, der Meinungsfreiheit, der personenbezogenen Daten und der Privatsphäre gemäß den EU-Rechtsvorschriften und der Cybersicherheitsstrategie der EU umfassend Rechnung getragen wird, und dass die Freiheit, Offenheit und Sicherheit des Cyberspace nicht ausgehöhlt werden. Dazu gehört auch das Modell einer demokratischen und effizienten Verwaltung mit einer Vielfalt an Akteuren.

Mit der gegenwärtigen Reform der Datenschutzvorschriften beiderseits des Atlantiks bietet sich der EU und den USA auch die einzigartige Gelegenheit, international Maßstäbe zu setzen. Hinsichtlich des Datenaustauschs über den Atlantik und darüber hinaus wäre eine Stärkung des nationalen Rechtsrahmens in den USA einschließlich der Annahme des von Präsident Obama im Februar 2012 als Teil einer umfassenden Strategie für einen verbesserten Schutz der Privatsphäre von Verbrauchern angekündigten Rechtekanons für den Verbraucherdatenschutz (Consumer Privacy Bill of Rights) mit eindeutigen Vorteilen verbunden. Das Bestehen eines Katalogs strenger und durchsetzbarer Datenschutzvorschriften, die in der EU und in den USA verankert sind, würde eine solide Grundlage für den grenzüberschreitenden Datenverkehr bilden.

Im Sinne der Förderung von Datenschutzstandards auf internationaler Ebene sollte der Beitritt zum Übereinkommen des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Übereinkommen 108), das auch Ländern offensteht, die nicht Mitglied des Europarates sind,²⁷ ebenfalls unterstützt werden. Sicherheiten und Garantien, die in internationalen Gremien beschlossen wurden, müssen ein hohes Schutzniveau gewährleisten, das mit den Anforderungen des EU-Rechts kompatibel ist.

4. FAZIT UND EMPFEHLUNGEN

Die in der vorliegenden Mitteilung benannten Fragen erfordern Maßnahmen sowohl vonseiten der USA als auch von der EU und ihren Mitgliedstaaten.

Die Bedenken, die im Zusammenhang mit dem transatlantischen Datenaustausch aufgeworfen wurden, sind für die EU und ihre Mitgliedstaaten in erster Linie ein Weckruf, der sie daran erinnert, die Reform der EU-Datenschutzvorschriften zügig und zielgerichtet voranzubringen. Mehr denn je zeigt sich das Erfordernis eines starken Rechtsrahmens mit eindeutigen Vorschriften, die sich auch bei grenzüberschreitenden Datentransfers durchsetzen lassen. Die EU-Organe und -Einrichtungen müssen sich daher weiterhin um die Annahme der Reform der EU-Datenschutzvorschriften bis zum Frühjahr 2014 bemühen, um einen wirksamen und umfassenden Schutz personenbezogener Daten sicherzustellen.

Angesichts des Ausmaßes der transatlantischen Datenströme müssen die Instrumente für diesen Austausch in angemessener Weise an die Anforderungen und Möglichkeiten des digitalen Zeitalters sowie technologische Neuentwicklungen wie das Cloud-Computing

²⁶ Siehe in diesem Zusammenhang den Entwurf einer Resolution zum Schutz der Privatsphäre online und offline, den Deutschland und Brasilien der UN-Generalversammlung vorgelegt haben.

²⁷ Die USA sind bereits Vertragspartner eines weiteren Übereinkommens des Europarates, d. h. des Übereinkommens über Datennetzkriminalität aus dem Jahre 2001 (auch als „Budapester Konvention“ bezeichnet).

angepasst werden. Mit Hilfe bestehender und künftiger Vereinbarungen und Übereinkommen ist der Fortbestand eines hohen Schutzniveaus bei Transfers über den Atlantik sicherzustellen. Ein robustes System des sicheren Hafens liegt sowohl im Interesse der EU-Bürger als auch im Interesse der US-Bürger und US-Unternehmen. Eine Stärkung dieses Systems kann kurzfristig durch eine bessere Überwachung und Anwendung und davon ausgehend durch eine umfassende Überarbeitung seiner Funktionsweise erfolgen. Damit die ursprünglichen Zielsetzungen der Safe-Harbor-Entscheidung – nämlich Kontinuität beim Datenschutz, Rechtssicherheit und freier Datenverkehr zwischen der EU und den USA – erfüllt werden können, sind Verbesserungen erforderlich.

Im Mittelpunkt dieser Verbesserungen steht die Notwendigkeit, dafür zu sorgen, dass die Einhaltung der Safe-Harbor-Grundsätze von den US-Behörden besser überwacht und kontrolliert wird.

Darüber hinaus ist dringend dafür Sorge zu tragen, dass in der Safe-Harbor-Entscheidung vorgesehene Ausnahmeregelungen aus Gründen der nationalen Sicherheit nur in dringend notwendigen und angemessenen Fällen zur Anwendung kommen.

Im Bereich der Strafverfolgung müssen die gegenwärtigen Verhandlungen über ein Rahmenabkommen ein hohes Schutzniveau für die Bürger auf beiden Seiten des Atlantiks zum Ergebnis haben. Mit einem solchen Abkommen würde das Vertrauen der Europäer in Datenübermittlungen zwischen der EU und den USA gestärkt und die Grundlage für einen weiteren Ausbau der Sicherheitszusammenarbeit und –partnerschaft von EU und USA geschaffen. Im Rahmen der Verhandlungen muss es darum gehen, Verpflichtungen dahingehend zu erwirken, dass Verfahrensgarantien einschließlich Rechtsbehelfe für Europäer angeboten werden, die nicht in den USA ansässig sind.

Der Regierung der USA sollte die Verpflichtung abverlangt werden, dass die US-Strafverfolgungsbehörden auf im Besitz von Privatunternehmen in der EU befindliche personenbezogene Daten nicht außerhalb der offiziellen Kooperationskanäle wie Rechtshilfeabkommen oder sektorbezogene Abkommen zwischen der EU und den USA (PNR- und TFTP-Abkommen), die diese Übermittlungen unter strengen Auflagen zulassen, zugreifen, ausgenommen klar festgelegte und gerichtlich überprüfbare Ausnahmefälle.

Ferner müssen die USA die Garantien für US-Bürger und Gebietsansässige auf EU-Bürger ausweiten, die nicht in den USA ansässig sind, die Notwendigkeit und Angemessenheit der Programme sicherstellen und sich um eine bessere Transparenz und Aufsicht innerhalb des für die US-Sicherheitsbehörden geltenden Rechtsrahmens bemühen.

Die in der vorliegenden Mitteilung aufgeführten Probleme werden auf beiden Seiten des Atlantiks ein konstruktives Engagement erforderlich machen. Die EU und die USA können als strategische Partner die gegenwärtigen Spannungen im transatlantischen Verhältnis gemeinsam überwinden und das Vertrauen in die Datenübermittlungen zwischen der EU und den USA wiederherstellen. Gemeinsame politische und rechtliche Verpflichtungen mit Blick auf eine künftige Zusammenarbeit in diesen Bereichen werden das transatlantische Verhältnis insgesamt stärken.