EUROPÄISCHE
KOMMISSION

Brüssel, den 29.4.2016
COM(2016) 238 final

2016/0127 (NLE)

Vorschlag für einen

BESCHLUSS DES RATES

über die Unterzeichnung – im Namen der Europäischen Union – des Abkommens zwischen den Vereinigten Staaten von Amerika und der Europäischen Union über den Schutz personenbezogener Daten bei der Verhütung, Untersuchung, Aufdeckung und Verfolgung von Straftaten

BEGRÜNDUNG

1. KONTEXT DES VORSCHLAGS

• Gründe und Ziele des Vorschlags

Im November 2006 wurde aus hohen Beamten der Kommission, des Ratsvorsitzes sowie des Justizministeriums, des Ministeriums für innere Sicherheit und des Außenministeriums der USA eine hochrangige Kontaktgruppe gebildet, um zu sondieren, wie die EU und die USA beim Austausch strafverfolgungsrelevanter Informationen enger und effizienter zusammenarbeiten und dabei gewährleisten könnten, dass der Schutz der personenbezogenen Daten und der Privatsphäre garantiert ist. Die hochrangige Kontaktgruppe gelangte in ihrem Abschlussbericht vom Oktober 2009[1] zu dem Ergebnis, dass die beste Option ein internationales Abkommen wäre, das die EU und die USA verpflichtet, vereinbarte gemeinsame Datenschutzgrundsätze für transatlantische Datenübermittlungen auf dem Gebiet der Strafverfolgung anzuwenden. Ein solches Abkommen hätte den Vorteil, die Grundlagen für einen wirksamen Schutz der Privatsphäre und der personenbezogenen Daten beim Austausch strafverfolgungsrelevanter Informationen zu schaffen, und würde ein Höchstmaß an Rechtssicherheit bieten.

Am 3. Dezember 2010 erließ der Rat einen Beschluss zur Ermächtigung der Kommission zur Aufnahme von Verhandlungen über ein Abkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika 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 (im Folgenden „Rahmenabkommen“).[2]

Am 28. März 2011 leitete die Kommission die Verhandlungen ein. Am 8. September 2015 paraphierten die Vertragsparteien das Abkommen.

Mit dem Rahmenabkommen wird (zum ersten Mal überhaupt) ein umfassender Rahmen von Datenschutzgrundsätzen und -garantien für die Übermittlung personenbezogener Daten[3] zum Zwecke der Strafverfolgung zwischen den USA einerseits und der Europäischen Union oder ihren Mitgliedstaaten andererseits geschaffen. Das doppelte Ziel besteht darin, ein hohes Maß an Datenschutz zu gewährleisten und dadurch die Zusammenarbeit zwischen den Vertragsparteien zu verbessern. Das Rahmenabkommen selbst bildet zwar nicht die

---

1 Berichte der hochrangigen Kontaktgruppe für den Informationsaustausch und den Schutz der Privatsphäre und der personenbezogenen Daten, Brüssel, 23. November 2009, 15851/09, JAI 822 DATAPROTECT 74 USA 102.

2 Zusammen mit der Annahme der EU-Datenschutzreform und des neuen „EU-US-Datenschutzschilds“ für Datenübermittlungen im kommerziellen Bereich ist der Abschluss eines richtungweisenden, umfassenden Rahmenabkommens ein Kernelement der Strategie, die in der Mitteilung der Kommission zur Wiederherstellung des Vertrauens beim Datenaustausch zwischen der EU und den USA (COM(2013) 846 vom 27. November 2013, abrufbar unter: http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52013DC0846&qid=1460535055571&from=DE) dargelegt wurde; bekräftigt wird dies auch in den Politischen Leitlinien von Kommissionspräsident Juncker und in der Mitteilung der Kommission an das Europäische Parlament und den Rat „Transatlantischer Datenaustausch: Wiederherstellung des Vertrauens durch starke Schutzvorkehrungen“ (COM(2016) 117 final vom 29. Februar 2016, abrufbar unter: http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52016DC0117&qid=1460536229059&from=DE).

3 Der Ausdruck „personenbezogene Daten“ hat im Rahmenabkommen dieselbe Bedeutung wie im Unionsrecht.

Rechtsgrundlage für die Übermittlung personenbezogener Daten an die USA, ergänzt aber erforderlichenfalls die Datenschutzgarantien in bestehenden und künftigen Datenübermittlungsübereinkünften oder nationalen Bestimmungen, die zu Datenübermittlungen ermächtigen.

Dies stellt eine ganz erhebliche Verbesserung gegenüber der derzeitigen Rechtslage dar, bei der personenbezogene Daten auf der Grundlage von Rechtsinstrumenten (internationalen Übereinkünften oder internen Rechtsvorschriften) über den Atlantik übermittelt werden, die im Allgemeinen keine oder nur schwache Datenschutzbestimmungen enthalten.

- **Kohärenz mit den bestehenden Vorschriften in diesem Bereich**

Das Rahmenabkommen wird den Schutz aller personenbezogenen Daten betroffener Personen in der EU verbessern, wenn diese Daten zum Zwecke der Strafverfolgung mit den USA ausgetauscht werden. Durch die Schaffung eines umfassenden Rahmens von Datenschutzgarantien wird das Abkommen die bestehenden Übereinkünfte (sowohl die bilateralen Abkommen zwischen Mitgliedstaaten und den USA als auch die Abkommen zwischen der EU und den USA), auf deren Grundlage den USA zum Zwecke der Strafverfolgung personenbezogene Daten übermittelt werden, ergänzen, sofern und soweit sie nicht das erforderliche Maß an Schutz und Garantien bieten.

Darüber hinaus wird das Abkommen ein „Sicherheitsnetz“ für künftige Abkommen zwischen der EU bzw. Mitgliedstaaten und den USA bilden, unter das das Schutzniveau nicht sinken kann. Dies ist eine wichtige Garantie für die Zukunft und eine deutliche Veränderung gegenüber der jetzigen Situation, in der Garantien, Schutzvorkehrungen und Rechte für jedes neue Abkommen neu ausgehandelt werden müssen.

Insgesamt wird das Rahmenabkommen einen erheblichen zusätzlichen Nutzen mit sich bringen, da der Schutz betroffener Personen in der EU im Einklang mit den Vorgaben des Primär- und Sekundärrechts der EU verbessert wird. Zum allerersten Mal wird eine Datenschutzregelung eingeführt, die umfassend und konsequent für alle Datenübermittlungen in einem bestimmten Bereich (nämlich für den transatlantischen Datenaustausch im Bereich der polizeilichen Zusammenarbeit und der justiziellen Zusammenarbeit in Strafsachen) gilt. Zudem untermauert das Rahmenabkommen im transatlantischen Kontext die allgemeinen Anforderungen an internationale Datenübermittlungen, die in der künftigen Richtlinie 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 (im Folgenden „Polizei-Richtlinie“)[4], die am 14. April 2016 erlassen wurde, festgelegt werden. Mit dem Rahmenabkommen wird daher auch ein wichtiger Präzedenzfall für ähnliche Abkommen mit anderen internationalen Partnern geschaffen.

- **Kohärenz mit der Politik der Union in anderen Bereichen**

Das Rahmenabkommen dürfte erhebliche Auswirkungen auf die polizeiliche Zusammenarbeit und die Zusammenarbeit bei der Strafverfolgung mit den Vereinigten Staaten haben. Durch die Schaffung eines umfassenden gemeinsamen Rahmens von Datenschutzvorschriften und -

[4] 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 – 2012/0010 (COD)), abrufbar unter: http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52012PC0010&from=de).

garantien versetzt es die EU oder ihre Mitgliedstaaten einerseits und die Strafverfolgungsbehörden der USA andererseits in die Lage, wirksamer zusammenzuarbeiten. Darüber hinaus gewährleistet das Rahmenabkommen, dass die bestehenden Übereinkünfte mit allen notwendigen Schutzvorkehrungen versehen sind. Dies ermöglicht sowohl die Kontinuität der Zusammenarbeit bei der Strafverfolgung als auch eine größere Rechtssicherheit bei Datenübermittlungen. Ferner erleichtert das Abkommen den Abschluss künftiger Datenübermittlungsübereinkünfte mit den USA auf dem Gebiet der Strafverfolgung, da die Datenschutzgarantien bereits vereinbart sind und somit nicht immer wieder neu ausgehandelt werden. Und schließlich ist die Einführung gemeinsamer Normen in diesem zentralen, aber komplexen Bereich der Zusammenarbeit ein wichtiger Erfolg, der wesentlich zur Wiederherstellung des Vertrauens in den transatlantischen Datenverkehr beitragen kann.

2. RECHTSGRUNDLAGE, SUBSIDIARITÄT UND VERHÄLTNISMÄSSIGKEIT

• Rechtsgrundlage

Rechtsgrundlage für diesen Vorschlag ist Artikel 16 AEUV in Verbindung mit Artikel 218 Absatz 5 AEUV.

• Subsidiarität

Das Rahmenabkommen fällt nach Artikel 3 Absatz 2 AEUV in die ausschließliche Zuständigkeit der Union. Das Subsidiaritätsprinzip findet daher keine Anwendung.

• Verhältnismäßigkeit

Das Rahmenabkommen enthält die nach den Verhandlungsrichtlinien des Rates erforderlichen Datenschutzgarantien. Diese gelten sowohl nach der Charta der Grundrechte als auch nach dem sich weiterentwickelnden Besitzstand der Union als notwendige Elemente zur Gewährleistung des erforderlichen Schutzes, wenn personenbezogene Daten an ein Drittland übermittelt werden. Weder ein wesentlich kleinerer Katalog von Garantien noch ein weniger verbindliches Instrument könnte als ausreichend angesehen werden, um einen solchen Schutz zu erzielen. Der Vorschlag geht daher nicht über das hinaus, was für die Erreichung des politischen Ziels erforderlich ist, einen Rahmen für den Schutz personenbezogener Daten bei deren Übermittlung zwischen den Vereinigten Staaten einerseits und der Europäischen Union oder ihren Mitgliedstaaten andererseits im Rahmen der Strafverfolgung zu schaffen.

• Wahl des Instruments

Die Schaffung eines verbindlichen Rahmens für den Schutz personenbezogener Daten, der die bestehenden Übereinkünfte ergänzt und eine Basis für künftige Übereinkünfte bildet, ist nur durch Abschluss eines internationalen Abkommens zwischen der EU und den Vereinigten Staaten möglich.

Zudem bietet ein internationales Abkommen, wie die hochrangige Kontaktgruppe in ihrem Bericht vom Oktober 2009 betont, ein Höchstmaß an Rechtssicherheit.

3. ERGEBNISSE DER EX-POST-BEWERTUNG, DER KONSULTATION DER INTERESSENTRÄGER UND DER FOLGENABSCHÄTZUNG

• Ex-post-Bewertung/Eignungsprüfungen bestehender Rechtsvorschriften

Entfällt.

- **Konsultation der Interessenträger**

Die Kommission hat dem vom Rat bestellten besonderen Ausschuss regelmäßig mündlich und schriftlich über den Fortgang der Verhandlungen Bericht erstattet. Das Europäische Parlament wurde über seinen Ausschuss für bürgerliche Freiheiten, Justiz und Inneres (LIBE) regelmäßig mündlich und schriftlich unterrichtet.

- **Einholung und Nutzung von Expertenwissen**

Mit der Maßnahme werden die Verhandlungsrichtlinien des Rates vom 3. Dezember 2010 umgesetzt.

- **Folgenabschätzung**

Eine Folgenabschätzung war nicht erforderlich. Das vorgeschlagene Abkommen steht mit den Verhandlungsrichtlinien des Rates im Einklang.

- **Effizienz der Rechtsetzung und Vereinfachung**

Entfällt.

- **Grundrechte**

Die Bestimmungen des Rahmenabkommens dienen dem Schutz des Grundrechts auf Schutz personenbezogener Daten und des Rechts auf einen wirksamen Rechtsbehelf und ein unparteiisches Gericht, die in Artikel 8 bzw. Artikel 47 der Charta der Grundrechte der Europäischen Union verankert sind.

4. AUSWIRKUNGEN AUF DEN HAUSHALT

Das vorgeschlagene Abkommen hat keine Auswirkungen auf den Haushalt.

5. WEITERE ANGABEN

- **Durchführungspläne sowie Monitoring-, Bewertungs- und Berichterstattungsmodalitäten**

Das Rahmenabkommen bedarf zwar der Durchführung durch die Mitgliedstaaten, es sind aber keine größeren Gesetzesänderungen zu erwarten, da die materiellrechtlichen Bestimmungen des Rahmenabkommens weitgehend Vorschriften entsprechen, die für die Behörden der EU und der Mitgliedstaaten bereits nach Unions- und/oder nationalem Recht gelten.

- **Ausführliche Erläuterung einzelner Bestimmungen des Vorschlags**

Im Einklang mit den Verhandlungsrichtlinien des Rates enthält das Rahmenabkommen fünf Kategorien von Bestimmungen: i) horizontale Bestimmungen, ii) Datenschutzgrundsätze und -garantien, iii) subjektive Rechte, iv) Aspekte der Anwendung des Abkommens und der Aufsicht und v) Schlussbestimmungen.

i) Horizontale Bestimmungen

i) Zweck des Abkommens (Artikel 1)

Um den Zweck des Abkommens (die Gewährleistung eines hohen Schutzes personenbezogener Daten und die Verbesserung der Zusammenarbeit auf dem Gebiet der Strafverfolgung) zu erreichen, wird mit dem Abkommen ein Rahmen für den Schutz

personenbezogener Daten bei deren Übermittlung zwischen den USA einerseits und der EU und ihren Mitgliedstaaten andererseits zur Verhütung, Untersuchung, Aufdeckung und Verfolgung von Straftaten einschließlich terroristischer Handlungen festgelegt. Die Bezugnahme auf die Begriffe „Verhütung, Untersuchung, Aufdeckung und Verfolgung von Straftaten“ (im Folgenden zusammenfassend „Strafverfolgung“) gewährleistet, dass das Abkommen mit der Struktur des derzeitigen und künftigen Besitzstands der Union im Bereich des Datenschutzes (insbesondere der Abgrenzung des Anwendungsbereichs der Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr („Datenschutz-Grundverordnung“)[5] und der „Polizei-Richtlinie“) vereinbar ist.

Mit der Klarstellung, dass das Rahmenabkommen selbst nicht als Rechtsgrundlage für Übermittlungen personenbezogener Daten dient und dass dafür stets eine (gesonderte) Rechtsgrundlage erforderlich ist, macht Artikel 1 auch deutlich, dass es sich bei dem Rahmenabkommen um ein echtes Grundrechtsabkommen handelt, mit dem Schutzvorkehrungen und Garantien für solche Übermittlungen festgelegt werden.

ii) Begriffsbestimmungen (Artikel 2)

Die Schlüsselbegriffe des Rahmenabkommens sind in Artikel 2 definiert. Die Bestimmung der Begriffe „personenbezogene Daten“, „Verarbeitung personenbezogener Daten“, „Vertragsparteien“, „Mitgliedstaat“ und „zuständige Behörde“ entsprechen im Wesentlichen der Bestimmung dieser Begriffe in anderen Abkommen zwischen der EU und den USA und/oder im Besitzstand der Union im Bereich des Datenschutzes.

iii) Anwendungsbereich des Abkommens (Artikel 3)

In Artikel 3 des Rahmenabkommens ist dessen Anwendungsbereich festgelegt. Es wird gewährleistet, dass die im Rahmenabkommen vorgesehenen Schutzvorkehrungen und Garantien auf alle Datenübermittlungen im Rahmen der transatlantischen Zusammenarbeit bei der Strafverfolgung in Strafsachen Anwendung finden. Dies gilt unter anderem für Datenübermittlungen auf der Grundlage interner Rechtsvorschriften sowie der Abkommen zwischen der EU und den USA (z. B. Rechtshilfeabkommen zwischen der EU und den USA), der Abkommen zwischen Mitgliedstaaten und den USA (z. B. Rechtshilfeabkommen, Abkommen zur Verbesserung der Zusammenarbeit bei der Verhütung und Bekämpfung schwerer Kriminalität oder Abkommen oder Vereinbarungen zu Screening-Informationen über Terroristen) und besonderer Übereinkünfte, in denen die Übermittlung personenbezogener Daten durch private juristische Personen zum Zwecke der Strafverfolgung vorgesehen ist (z. B. Abkommen zwischen der EU und den USA über Fluggastdatensätze[6] oder Abkommen zum Programm zum Aufspüren der Finanzierung des Terrorismus[7]). Der Anwendungsbereich ist anhand der Datenübermittlungen definiert, d. h., er umfasst

---

5 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 – 2012/0011 (COD)), abrufbar unter: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_de.pdf.

6 Abkommen 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. 5).

7 Abkommen 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. 5).

grundsätzlich alle Datenübermittlungen zwischen der EU und den USA zum Zwecke der Strafverfolgung, unabhängig von der Staatsangehörigkeit oder dem Wohnsitz der betroffenen Person.

Das Rahmenabkommen gilt nicht für Übermittlungen personenbezogener Daten (oder andere Formen der Zusammenarbeit) zwischen den für den Schutz der nationalen Sicherheit zuständigen Behörden der USA und der Mitgliedstaaten.

iv) Diskriminierungsverbot (Artikel 4)

Nach Artikel 4 muss jede Vertragspartei das Rahmenabkommen ohne willkürliche oder ungerechtfertigte Diskriminierung zwischen ihren eigenen Staatsangehörigen und denen der anderen Vertragspartei umsetzen.

Dieser Artikel ergänzt und stärkt andere Bestimmungen des Abkommens (insbesondere die Artikel über Sicherheitsvorkehrungen zugunsten betroffener Personen wie die Rechte auf Zugang, Berichtigung und einen behördlichen Rechtsbehelf; siehe unten), da er gewährleistet, dass EU-Bürger und US-Bürger bei der praktischen Anwendung dieser Bestimmungen durch US-Behörden grundsätzlich gleichbehandelt werden.

v) Wirkung des Abkommens (Artikel 5)

Die bestehenden Abkommen zwischen der EU bzw. Mitgliedstaaten und den USA werden durch das Rahmenabkommen gegebenenfalls, d. h., sofern und soweit sie nicht die notwendigen Datenschutzgarantien enthalten, ergänzt.[8]

Bei wirksamer Umsetzung des Rahmenabkommens (und insbesondere seiner Artikel über die subjektiven Rechte) wird die Vereinbarkeit mit den geltenden Vorschriften für internationale Datenübermittlungen vermutet. Diese – weder automatische noch allgemeine – Vermutung kann, wie alle Vermutungen, widerlegt werden. Es handelt sich nicht um eine automatische Vermutung, weil sie ausdrücklich von der wirksamen Umsetzung des Rahmenabkommens durch die USA abhängig gemacht wird, genauer gesagt – wie Artikel 5 Absatz 2 ausdrücklich klarstellt – von der wirksamen Umsetzung der Artikel über die Rechte betroffener Personen (insbesondere auf Zugang, Berichtigung sowie einen behördlichen und einen gerichtlichen Rechtsbehelf). Es handelt sich auch nicht um eine allgemeine Vermutung, denn da das Rahmenabkommen kein „eigenständiges“ Instrument für Datenübermittlungen ist, gilt diese Vermutung notwendigerweise nur im Einzelfall, d. h., es muss geprüft werden, ob das Rahmenabkommen und die besondere Rechtsgrundlage für die Datenübermittlung zusammen einen mit den EU-Datenschutzvorschriften im Einklang stehenden Schutz bieten. Anders ausgedrückt: Im Unterschied zu einem Angemessenheitsbeschluss bedeutet diese Klausel weder eine „en bloc“-Anerkennung des in den Vereinigten Staaten gebotenen Schutzniveaus als solchem noch eine Generalermächtigung für Datenübermittlungen.

ii) Datenschutzgrundsätze und -garantien

Die unten beschriebenen Artikel enthalten wichtige Grundsätze für die Verarbeitung personenbezogener Daten sowie zentrale Garantien und Beschränkungen.

[8] In der Präambel wird im vierten Erwägungsgrund erklärt, dass das Rahmenabkommen Abkommen, die ein angemessenes Datenschutzniveau gewährleisten, nicht ändert oder Bedingungen unterwirft oder in sonstiger Weise von ihnen abweicht; dies gilt nicht für Artikel 19 über den gerichtlichen Rechtsbehelf, der auch auf diese Abkommen Anwendung findet. Dies ist beim Abkommen über Fluggastdatensätze und beim Abkommen zum Programm zum Aufspüren der Finanzierung des Terrorismus der Fall.

i) Zweck- und Verwendungsbeschränkungen (Artikel 6)

Im Einklang mit der Charta der Grundrechte der EU und dem Besitzstand der Union wendet Artikel 6 den Grundsatz der Zweckbindung auf alle unter das Rahmenabkommen fallenden Übermittlungen personenbezogener Daten an, sowohl, wenn sich die Übermittlung auf einen spezifischen Fall bezieht, als auch, wenn die USA und die EU bzw. ihre Mitgliedstaaten ein Abkommen schließen, das zur Übermittlung großer Mengen personenbezogener Daten ermächtigt. Die Verarbeitung (einschließlich der Übermittlung) darf nur für eindeutige und rechtmäßige Zwecke im Anwendungsbereich des Rahmenabkommens erfolgen, d. h. zur Verhütung, Untersuchung, Aufdeckung und Verfolgung von Straftaten einschließlich terroristischer Handlungen.

Darüber hinaus ist die Weiterverarbeitung personenbezogener Daten durch andere (Strafverfolgungs-, Regulierungs- oder Verwaltungs-)Behörden als die erste empfangende Behörde einer Vertragspartei unter der Voraussetzung zulässig, dass sie mit den Zwecken, für die die Daten ursprünglich übermittelt wurden, nicht unvereinbar ist und dass diese andere Behörde alle übrigen Bestimmungen des Rahmenabkommens einhält.

Die übermittelnde zuständige Behörde kann im Einzelfall auch zusätzliche Bedingungen (z. B. für die Verwendung der Daten) festlegen.

Und schließlich dürfen personenbezogene Daten nur „in einer Weise verarbeitet werden, die in Bezug auf die Zwecke der Verarbeitung unmittelbar relevant und weder exzessiv noch zu weit gefasst ist."

Artikel 6 ist eine zentrale Bestimmung des Abkommens. Er gewährleistet die Geltung der Garantien für den gesamten „Lebenszyklus" eines Datensatzes von der ursprünglichen Übermittlung aus der EU bis zu seiner Verarbeitung durch eine zuständige US-Behörde und umgekehrt sowie seiner möglichen Weitergabe an/Weiterverarbeitung durch eine andere US-Behörde bzw. – im Falle einer Übermittlung aus den USA an eine zuständige Behörde der EU oder (eines) ihrer Mitgliedstaaten – seiner möglichen Weitergabe an/Weiterverarbeitung durch eine andere Behörde der EU oder eines Mitgliedstaats.

ii) Weiterübermittlung (Artikel 7)

Die in Artikel 7 festgelegten Beschränkungen für die Weiterübermittlung bewirken, dass eine US-Behörde, die von der EU oder einem ihrer Mitgliedstaaten empfangene Daten einem nicht durch das Abkommen gebundenen Drittland oder einer internationalen Organisation weiterübermitteln will, zunächst die Zustimmung der Strafverfolgungsbehörde in der EU einholen muss, die die Daten ursprünglich den Vereinigten Staaten übermittelt hat. Diese Vorschrift gilt ebenso für den Fall, dass eine Behörde der EU oder eines ihrer Mitgliedstaaten von den USA empfangene Daten einem Drittland oder einer internationalen Organisation weiterübermitteln will.

Bei der Entscheidung über ihre Zustimmung muss die Behörde, die die Daten ursprünglich übermittelt hat, alle relevanten Faktoren berücksichtigen, unter anderem den Zweck, zu dem die Daten ursprünglich übermittelt wurden, und die Frage, ob das Drittland bzw. die internationale Organisation einen angemessenen Schutz personenbezogener Daten bietet. Sie kann die Datenübermittlung zudem von spezifischen Bedingungen abhängig machen.

Wie die Artikel über die Zweckbindung (Artikel 6, siehe oben), die Speicherfristen (Artikel 12, siehe unten) und sensible Daten (Artikel 13, siehe unten) trägt dieser Artikel der

besonderen Sensibilität der Übermittlung großer Mengen von Daten unverdächtiger Personen (z. B. Fluggastdatensätze aller Fluggäste, die einen Flug gebucht haben, unabhängig von einem konkreten Verdacht) ausdrücklich Rechnung, indem er vorschreibt, dass „sich nicht auf spezifische Fälle“ beziehende personenbezogene Daten nur unter den in dem betreffenden Abkommen festgelegten spezifischen Bedingungen für eine ordnungsgemäß begründete Weiterübermittlung weiterübermittelt werden dürfen.

Auch der besondere Fall der Weiterübermittlung an einen anderen Staat innerhalb der EU (Bsp.: Die französische Polizei gibt Daten, die sie vom amerikanischen FBI erhalten hat, an die deutsche Polizei weiter.) ist in diesem Artikel (Absatz 4) behandelt: Wenn für eine solche Übermittlung eine vorherige Zustimmung erforderlich ist, kann die Behörde, die die Daten ursprünglich übermittelt hat (z. B. das amerikanischen FBI), die Zustimmung nicht aus datenschutzrechtlichen Gründen ablehnen oder Bedingungen festlegen (da alle beteiligten Behörden durch das Rahmenabkommen gebunden sind).

iii) Qualität und Vollständigkeit der Daten (Artikel 8)

Die Vertragsparteien treffen angemessene Maßnahmen, um sicherzustellen, dass die übermittelten personenbezogenen Daten mit der für ihre rechtmäßige Verarbeitung erforderlichen und angemessenen Genauigkeit, Relevanz, Aktualität und Vollständigkeit erhalten bleiben. Falls der empfangenden oder der übermittelnden Behörde erhebliche Zweifel an der Relevanz, Aktualität, Vollständigkeit oder Genauigkeit der erhaltenen oder übermittelten personenbezogenen Daten zur Kenntnis gelangen, teilt sie dies der übermittelnden bzw. der empfangenden Behörde nach Möglichkeit mit.

iv) Informationssicherheit (Artikel 9) und Meldung von Datensicherheitsvorfällen (Artikel 10)

Diese Artikel tragen dazu bei, ein hohes Maß an Sicherheit der zwischen den Vertragsparteien des Rahmenabkommens ausgetauschten personenbezogenen Daten zu gewährleisten.

Erstens treffen die Vertragsparteien nach Artikel 9 geeignete technische und organisatorische Sicherheitsvorkehrungen zum Schutz personenbezogener Daten gegen zufällige oder unrechtmäßige Zerstörung, zufälligen Verlust und unberechtigte Offenlegung, unberechtigte Änderung, unberechtigten Zugang oder sonstige unberechtigte Verarbeitung. Zu diesen Vorkehrungen gehört auch, dass nur Personal mit einer entsprechenden Ermächtigung Zugang zu personenbezogenen Daten gewährt wird.

Zweitens werden nach Artikel 10 bei einem Sicherheitsvorfall, von dem ein erhebliches Schadensrisiko ausgeht, unverzüglich geeignete Schadensbegrenzungsmaßnahmen getroffen, zu denen auch die Benachrichtigung der übermittelnden Behörde und, wenn es den Umständen des Vorfalls angemessen ist, der betroffenen Person gehört. Die Ausnahmen von der Benachrichtigungspflicht sind in der Bestimmung abschließend aufgeführt und entsprechen angemessenen Beschränkungen (z. B. nationale Sicherheit).

v) Führung von Aufzeichnungen (Artikel 11)

Die Vertragsparteien müssen über wirksame Methoden (z. B. Protokolle) zum Nachweis der Rechtmäßigkeit der Verarbeitung und Verwendung personenbezogener Daten verfügen.

Diese Bestimmung stellt eine wichtige Sicherheitsvorkehrung zugunsten betroffener Personen dar, da sie den Strafverfolgungsbehörden die Beweislast dafür auferlegt, dass eine bestimmte Datenverarbeitung im Einklang mit dem geltenden Recht vorgenommen wurde. Die Pflicht

zur Dokumentation der Datenverarbeitung bewirkt insbesondere, dass es im Falle einer unrechtmäßigen Verarbeitung eine „Spur“ gibt. Dies dürfte die Bearbeitung von Beschwerden und die Geltendmachung von Ansprüchen in Bezug auf die Rechtmäßigkeit der Datenverarbeitung erleichtern.

vi) Speicherfrist (Artikel 12)

Für die Verarbeitung von Daten gelten besondere Speicherfristen, um sicherzustellen, dass die Daten nicht länger gespeichert werden, als notwendig und angemessen ist. Bei der Festlegung dieser Speicherfristen muss eine Reihe von Faktoren berücksichtigt werden, insbesondere der Zweck der Verarbeitung oder Verwendung, die Art der Daten und die Auswirkungen auf die Rechte und Interessen der betroffenen Personen.

Für den Fall, dass die Vertragsparteien ein Abkommen über die Übermittlung großer Datenmengen schließen, ist vorgesehen, dass ein solches Abkommen eine besondere Bestimmung über die geltende Speicherfrist enthalten muss. Mit dieser Bestimmung erkennen die Vertragsparteien den Grundsatz an, dass solche Abkommen eine besondere Speicherfrist enthalten müssen, der daher nicht erneut ausgehandelt werden muss.

Die Speicherfristen werden regelmäßig überprüft, um bestimmen zu können, ob veränderte Umstände eine Änderung der geltenden Frist erforderlich machen.

Um Transparenz zu gewährleisten, müssen die Speicherfristen veröffentlicht oder auf andere Weise öffentlich zugänglich gemacht werden.

vii) Besondere Kategorien von Daten (Artikel 13)

Personenbezogene Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder sonstige Überzeugungen, eine Gewerkschaftszugehörigkeit oder die Gesundheit oder das Sexualleben betreffende Informationen hervorgehen, dürfen nur unter Wahrung angemessener Garantien im Einklang mit dem geltendem Recht verarbeitet werden (z. B. Unkenntlichmachung der Daten, nachdem sie zu dem vorgesehenen Zweck verarbeitet wurden, oder obligatorische aufsichtsbehördliche Genehmigung für den Datenzugang).

In Abkommen, die die Übermittlung großer Mengen personenbezogener Daten zulassen, müssen die für die Verarbeitung besonderer Kategorien von Daten maßgeblichen Standards und Bedingungen näher spezifiziert werden.

Die Bestimmungen über besondere Kategorien von Daten stehen mit der Vorgabe des Artikels 6 (Zweck- und Verwendungsbeschränkungen) im Einklang, dass die Verarbeitung unmittelbar relevant sein muss und nicht exzessiv sein darf.

viii) Automatisierte Entscheidungen (Artikel 15)

Eine Verarbeitung personenbezogener Daten, die zu Entscheidungen mit negativen Auswirkungen auf betroffene Personen führen könnte (z. B. im Zusammenhang mit der Erstellung von Täterprofilen), darf nicht allein auf der Grundlage automatisierter Verfahren erfolgen, es sei denn, dies ist nach internem Recht zulässig und es bestehen angemessene Garantien einschließlich der Möglichkeit, das Eingreifen eines Menschen zu erwirken.

ix) Transparenz (Artikel 20)

Betroffene Personen haben Anspruch auf Informationen (im Wege allgemeiner Bekanntmachungen oder individueller Belehrungen und vorbehaltlich „angemessener Beschränkungen“) über den Zweck der Verarbeitung und die mögliche weitere Verwendung ihrer personenbezogenen Daten, über die für die Verarbeitung der Daten maßgeblichen Gesetze oder Vorschriften, über Dritte, denen gegenüber ihre personenbezogenen Daten offengelegt werden könnten, sowie über die zur Verfügung stehenden Möglichkeiten für den Zugang zu den Daten, für ihre Berichtigung oder für einen Rechtsbehelf.

Die Schärfung des Bewusstseins betroffener Personen dafür, warum und von wem ihre Daten verarbeitet werden, trägt dazu bei, dass betroffene Personen ihr Recht auf Zugang, Berichtigung oder einen Rechtsbehelf ausüben können (siehe unten, Artikel 16-19).

iii) Subjektive Rechte

Diese Rechte sind für den Schutz betroffener Personen von besonderer Bedeutung, da sie erstmals in den Genuss von allgemein geltenden Rechten kommen, die im Zusammenhang mit der transatlantische Übermittlung personenbezogener Daten auf dem Gebiet der Strafverfolgung geltend gemacht werden können.

i) Zugang und Berichtigung (Artikel 16 und Artikel 17)

Das Recht auf Zugang ermöglicht es jeder betroffenen Person, Zugang zu ihren personenbezogenen Daten zu beantragen und zu erhalten. Die Gründe für eine Beschränkung des Zugangs sind abschließend aufgeführt und entsprechen angemessenen Beschränkungen (z. B. Schutz der nationalen Sicherheit, Vermeidung der Beeinträchtigung der Untersuchung oder Verfolgung von Straftaten, Schutz der Rechte und Freiheiten anderer). Für den Zugang zu den eigenen Daten dürfen keine übermäßigen Kosten auferlegt werden.

Das Recht auf Berichtigung ermöglicht es jeder betroffenen Person, die Berichtigung oder Bereinigung eigener personenbezogener Daten zu beantragen, sofern diese ungenau sind oder nicht ordnungsgemäß verarbeitet wurden. Dies kann die Ergänzung, Löschung, Sperrung oder sonstige Maßnahmen oder Verfahren zur Beseitigung von Ungenauigkeiten oder von Folgen einer nicht ordnungsgemäßen Verarbeitung einschließen.

Wenn die zuständige Behörde des Empfängerlands aufgrund eines Antrags einer betroffenen Person, einer Benachrichtigung durch den Übermittler der personenbezogenen Daten oder eigener Ermittlungen zu dem Schluss kommt, dass die Daten ungenau sind oder nicht ordnungsgemäß verarbeitet wurden, ergänzt, löscht oder sperrt sie die Daten oder nimmt eine sonstige Berichtigung oder Bereinigung vor.

Sofern dies nach nationalem Recht zulässig ist, können betroffene Personen eine Aufsichtsbehörde (im Falle betroffener Personen in der EU eine nationale Datenschutzbehörde) ermächtigen, den Zugang oder die Berichtigung in ihrem Namen zu beantragen. Die Möglichkeit, Rechte über eine Behörde und innerhalb einer Rechtsordnung, die ihnen vertraut sind, mittelbar auszuüben, dürfte betroffenen Personen ganz konkret bei der Durchsetzung ihrer Rechte helfen.

Wenn der Zugangs- oder Berichtigungsantrag abgelehnt oder ihm mit Einschränkungen stattgegeben wird, teilt die mit dem Antrag befasste Behörde der betroffenen Person (oder ihrem ordnungsgemäß ermächtigten Vertreter) die Gründe für die Ablehnung des Zugangs-

oder Berichtigungsantrags bzw. die Einschränkungen mit. Die Pflicht, der betroffenen Person eine begründete Antwort zu erteilen, dient dazu, ihr die Ausübung ihres Rechts auf einen behördlichen und einen gerichtlichen Rechtsbehelf zu ermöglichen und zu erleichtern, falls der Zugangs- oder Berichtigungsantrag von der betreffenden Strafverfolgungsbehörde abgelehnt oder ihm nur eingeschränkt stattgegeben wird.

ii) Behördlicher Rechtsbehelf (Artikel 18)

Sollte eine betroffene Person mit dem Ergebnis ihres Antrags auf Zugang zu personenbezogenen Daten oder deren Berichtigung nicht einverstanden sein, kann sie einen behördlichen Rechtsbehelf einlegen. Um die wirksame Ausübung dieses Rechts zu erleichtern, kann die betroffene Person wie bei Zugang und Berichtigung eine Aufsichtsbehörde (im Falle betroffener Personen in der EU eine nationale Datenschutzbehörde) oder einen anderen Vertreter dazu ermächtigen, sofern dies nach geltendem internem Recht zulässig ist.

Die Behörde, bei der der Rechtsbehelf eingelegt wird, erteilt der betroffenen Person eine schriftliche Antwort, in der sie gegebenenfalls mitteilt, welche Abhilfemaßnahmen getroffen wurden.

iii) Gerichtlicher Rechtsbehelf (Artikel 19)

Die Bürger der Vertragsparteien können einen gerichtlichen Rechtsbehelf einlegen, wenn i) der Zugang verweigert, ii) die Berichtigung verweigert oder iii) Daten von den Behörden der anderen Vertragspartei unrechtmäßig offengelegt wurden.

In den USA wurde dem im *Judicial Redress Act* Rechnung getragen, der am 24. Februar 2016 von Präsident Obama unterzeichnet wurde. Mit diesem Gesetz werden die drei im amerikanischen *Privacy Act* von 1974 vorgesehenen Gründe für einen gerichtlichen Rechtsbehelf, die bisher nur von US-Bürgern und Einwohnern mit Daueraufenthaltstitel geltend gemacht werden konnten, auf die Bürger der „erfassten Länder“[9] ausgeweitet. In der Präambel des Rahmenabkommens wird im vierten Erwägungsgrund klargestellt, dass diese Ausweitung auch im Falle von Daten gilt, die nach Übereinkünften wie dem Abkommen über Fluggastdatensätze und dem Abkommen zum Programm zum Aufspüren der Finanzierung des Terrorismus ausgetauscht werden. Zusammen mit dem *Judicial Redress Act* wird Artikel 19 somit den Rechtsschutz für EU-Bürger erheblich verbessern.

Obwohl der *Judicial Redress Act* eine Reihe von Beschränkungen enthält (insbesondere gilt er nur für die Daten von Bürgern aus „erfassten Ländern“, deren Daten von EU-Strafverfolgungsbehörden übermittelt wurden, vor allem – aber nicht nur – von EU-Bürgern), wird mit Artikel 19 des Rahmenabkommens eine seit langem erhobene Forderung der EU erfüllt.

---

[9] Ein „erfasstes Land“ (*covered country*) im Sinne des amerikanischen *Judicial Redress Act* ist ein Land, i) das mit den USA ein Abkommen geschlossen hat, in dem ein angemessener Schutz der Privatsphäre bei der Übermittlung von Informationen zum Zwecke der Strafverfolgung vorgesehen ist (oder das effektiv Informationen zum Zwecke der Strafverfolgung übermittelt hat und über einen angemessenen Schutz der Privatsphäre bei der Übermittlung solcher Informationen verfügt); ii) das auf der Grundlage eines Abkommens mit den USA oder auf andere Weise die Übermittlung personenbezogener Daten zu kommerziellen Zwecken zulässt; iii) dessen Politik in Bezug auf die Übermittlung personenbezogener Daten zu kommerziellen Zwecken die nationalen Sicherheitsinteressen der Vereinigten Staaten nicht wesentlich beeinträchtigt. Ob ein Land „erfasst“ ist, entscheidet der Justizminister der USA.

Die Bestimmung steht mit den Politischen Leitlinien von Kommissionspräsident Juncker im Einklang, in denen es heißt: „*Die Vereinigten Staaten müssen … 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.*“ Ferner entspricht sie der Entschließung des Europäischen Parlaments vom 12. März 2014 zu dem Überwachungsprogramm der Nationalen Sicherheitsagentur der Vereinigten Staaten, in der das Parlament die umgehende Wiederaufnahme der Verhandlungen mit den USA zu dem „Rahmenabkommen“ fordert, das „*EU-Bürgern die gleichen Rechte wie US-Bürgern einräumen*“ und „*gültige und durchsetzbare … gerichtliche Rechtsbehelfe für alle EU-Bürger in den USA ohne jegliche Diskriminierung gewährleisten sollte*“[10].

Artikel 19 Absatz 3 stellt klar, dass die Ausweitung der drei obengenannten Gründe für einen gerichtlichen Rechtsbehelf bestehende andere Möglichkeiten für eine gerichtliche Überprüfung in Bezug auf die Verarbeitung von Daten (etwa nach dem *Administrative Procedure Act*, dem *Electronics Communication Privacy Act* oder dem *Freedom of Information Act*) unberührt lässt. Die Inanspruchnahme dieser anderen Rechtsgrundlagen für einen gerichtlichen Rechtsbehelf steht allen von einer Datenübermittlung zum Zwecke der Strafverfolgung betroffenen Personen in der EU unabhängig von ihrer Staatsangehörigkeit und ihrem Wohnsitz offen.

iv) Aspekte der Anwendung des Abkommens und der Aufsicht

i) Rechenschaftspflicht (Artikel 14)

Es müssen Maßnahmen zur Stärkung der Rechenschaftspflicht der Behörden vorhanden sein, die unter das Rahmenabkommen fallende personenbezogene Daten verarbeiten. Insbesondere muss die empfangende Behörde, wenn sie personenbezogene Daten an andere Behörden weitergibt, diesen die nach dem Abkommen geltenden Garantien und mögliche zusätzliche (einschränkende) Bedingungen mitteilen, die nach Artikel 6 Absatz 3 (Zweck- und Verwendungsbeschränkungen) an die Übermittlung geknüpft werden. Schwere Verstöße werden mit geeigneten abschreckenden straf-, zivil- oder verwaltungsrechtlichen Sanktionen geahndet.

Die Maßnahmen zur Stärkung der Rechenschaftspflicht umfassen gegebenenfalls auch die Einstellung der Übermittlung personenbezogener Daten an nicht unter das Rahmenabkommen fallende Stellen der Vertragsparteien, falls diese unter Berücksichtigung des Zwecks des Abkommens (und insbesondere der Zweckbindung und der Bestimmungen über die Weiterübermittlung) keinen wirksamen Schutz personenbezogener Daten gewährleisten. Diese Bestimmung behandelt den Fall, dass personenbezogene Daten von einer EU-Behörde einer US-Bundesbehörde (also einer unter das Abkommen fallenden Behörde) übermittelt und dann einer Strafverfolgungsbehörde auf Bundesstaatsebene weiterübermittelt werden. Nach den verfassungsrechtlichen Vorschriften der USA kann der Bund die Bundestaaten nur in

[10] Siehe Nummer 57 und Buchstabe BJ der Entschließung vom 12. März 2014 zu dem Überwachungsprogramm der Nationalen Sicherheitsagentur der Vereinigten Staaten, die Überwachungsbehörden in mehreren Mitgliedstaaten und die entsprechenden Auswirkungen auf die Grundrechte der EU-Bürger und die transatlantische Zusammenarbeit im Bereich Justiz und Inneres (2013/2188(INI), abrufbar unter: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0230+0+DOC+XML+V0//DE.

begrenztem Umfang auf internationaler Ebene binden.[11] Um die Kontinuität des Schutzes der Daten zu gewährleisten, die US-Bundesbehörden übermittelt und dann an Strafverfolgungsbehörden auf Bundesstaatsebene weitergegeben werden, bestimmt dieser Artikel dennoch Folgendes: i) er bezieht die „sonstigen Behörden" der Vertragsparteien (die nicht unter das Abkommen fallen, z. B. die Behörden der US-Bundesstaaten) in seinen Anwendungsbereich ein, ii) er schreibt vor, dass diesen Behörden die im Rahmenabkommen vorgesehenen Garantien mitzuteilen sind, und iii) er bestimmt, dass die Übermittlung an diese Behörden gegebenenfalls einzustellen ist, falls sie personenbezogene Daten unter Berücksichtigung des Zwecks des Rahmenabkommens und insbesondere seiner Artikel über die Zweckbindung und die Weiterübermittlung nicht wirksam schützen.

Dieser Artikel ist ein wichtiger Baustein für ein wirksames Durchsetzungs- und Aufsichtssystem im Rahmen des Abkommens, da mit ihm sichergestellt werden soll, dass die zuständigen Strafverfolgungsbehörden für die Einhaltung des Rahmenabkommens verantwortlich sind. Betroffenen Personen erleichtert er die Geltendmachung von Ansprüchen, wenn ein Verstoß gegen das Abkommen vorliegt (für den die Behörden haften).

Und schließlich können EU-Behörden den entsprechenden US-Behörden gegenüber Bedenken hinsichtlich der Erfüllung von deren Pflichten aus Artikel 14 (einschließlich der in diesem Zusammenhang getroffenen Maßnahmen) äußern und sachdienliche Informationen anfordern. Der wirksamen Umsetzung dieses Artikels wird auch im Rahmen der gemeinsamen Überprüfungen (siehe unten, Artikel 23) besondere Aufmerksamkeit geschenkt.

ii) Wirksame Aufsicht (Artikel 21)

Die Vertragsparteien müssen über eine oder mehrere Behörden verfügen, die unabhängig Aufsichtsfunktionen und -befugnisse ausüben, die auch Überprüfungs-, Untersuchungs- und Eingriffsmaßnahmen umfassen. Diese Behörden müssen befugt sein, von betroffenen Personen eingereichte Beschwerden, die sich auf Maßnahmen zur Umsetzung des Rahmenabkommens beziehen, entgegenzunehmen und ihnen nachzugehen und bei Rechtsverstößen im Zusammenhang mit dem Abkommen eine strafrechtliche Verfolgung einleiten oder Disziplinarmaßnahmen verhängen zu lassen. Angesichts der Besonderheiten des Systems der USA nehmen dort mehrere Aufsichtsbehörden (darunter die Datenschutzbeauftragten, die Generalinspektoren und das *Privacy and Civil Liberties Oversight Board*) gemeinsam die Aufsichtsaufgaben wahr, die in der EU von den Datenschutzbehörden erfüllt werden.

Dieser Artikel ergänzt die Garantien, die auf der Grundlage der Bestimmungen über Zugang, Berichtigung und den behördlichen Rechtsbehelf zur Verfügung stehen. Insbesondere ermöglicht er es betroffenen Personen, bei unabhängigen Behörden Beschwerde über die Umsetzung des Rahmenabkommens durch die andere Vertragspartei einzulegen.

iii) Zusammenarbeit zwischen den Aufsichtsbehörden (Artikel 22)

Die Aufsichtsbehörden arbeiten zusammen, um eine wirksame Umsetzung des Abkommens und insbesondere des Systems für die mittelbare Ausübung der subjektiven Rechte auf Zugang, Berichtigung und einen behördlichen Rechtsbehelf sicherzustellen (siehe oben, Artikel 16-18).

[11] Da es sich bei den USA um eine Bundesrepublik handelt, sind die Kompetenzen auf den Bund und die einzelnen Bundesstaaten verteilt (siehe in diesem Zusammenhang auch Artikel 5 Absatz 2 des Rahmenabkommens).

Ferner werden nationale Kontaktstellen eingerichtet, die bei der Ermittlung der im Einzelfall zu kontaktierenden Aufsichtsbehörde behilflich sind. Angesichts der Vielzahl verschiedener Aufsichtsbehörden in den USA soll mit der Schaffung einer zentralen „Eingangsstelle“ für Ersuchen um Unterstützung und Zusammenarbeit zu einer effizienten Bearbeitung dieser Ersuchen beigetragen werden.

iv) Gemeinsame Überprüfung (Artikel 23)

Die Vertragsparteien führen regelmäßig eine gemeinsame Überprüfung der Umsetzung und der Wirksamkeit des Rahmenabkommens durch, bei der sie der wirksamen Umsetzung der Artikel über die subjektiven Rechte (auf Zugang, Berichtigung sowie einen behördlichen und einen gerichtlichen Rechtsbehelf) und der Frage der Übermittlung von Daten an nicht unter das Abkommen fallende Gebietseinheiten (d. h. die US-Bundesstaaten) besondere Aufmerksamkeit schenken. Die gemeinsame Überprüfung erfolgt erstmals spätestens drei Jahre nach dem Inkrafttreten des Abkommens und danach in regelmäßigen Abständen.

Den jeweiligen Delegationen gehören auch Vertreter von Datenschutzbehörden und von Strafverfolgungs- bzw. Justizbehörden an, die Ergebnisse der gemeinsamen Überprüfung werden veröffentlicht.

v) Schlussbestimmungen

Das Rahmenabkommen enthält eine Reihe von Schlussbestimmungen, die Folgendes betreffen:

- die Notifikation von Rechtsakten, die die Umsetzung des Abkommens wesentlich beeinflussen, an die andere Vertragspartei. Insbesondere notifizieren die USA der EU Maßnahmen im Zusammenhang mit der Anwendung des *Judicial Redress Act* (Artikel 24);
- Konsultationen bei Streitigkeiten über die Auslegung oder Anwendung des Abkommens (Artikel 25);
- die Möglichkeit einer Aussetzung des Abkommens durch eine Vertragspartei im Falle einer erheblichen Verletzung des Abkommens durch die andere Vertragspartei (Artikel 26);
- den räumlichen Geltungsbereich des Abkommens, um der besonderen Position des Vereinigten Königreichs, Irlands und Dänemarks Rechnung zu tragen (Artikel 27);
- die unbegrenzte Geltungsdauer des Abkommens (die angesichts der Art des Abkommens, das einen Rahmen von Schutzvorkehrungen und Garantien darstellt, und der Möglichkeit, das Abkommen auszusetzen oder zu kündigen, gerechtfertigt ist) (Artikel 28);
- die Möglichkeit für jede Vertragspartei, das Abkommen durch Notifikation an die andere Vertragspartei zu kündigen; personenbezogene Daten, die vor der Kündigung übermittelt wurden, werden jedoch weiterhin im Einklang mit den Vorschriften des Rahmenabkommens verarbeitet (Artikel 29 Absätze 2 und 3);
- das Inkrafttreten des Abkommens am ersten Tag des Monats, der auf den Tag folgt, an dem die Vertragsparteien einander den Abschluss ihrer internen Genehmigungsverfahren notifiziert haben (Artikel 29 Absatz 1);

- die Sprachenklausel (unmittelbar vor der Zeile für die Unterschrift), nach der i) das Abkommen in englischer Sprache unterzeichnet und von der EU in den übrigen 23 Amtssprachen der EU abgefasst wird; ii) der Wortlaut des Abkommens in anderen Amtssprachen der EU nach der Unterzeichnung im Wege eines diplomatischen Notenwechsels mit den USA für verbindlich erklärt werden kann; iii) bei Abweichungen zwischen verschiedenen verbindlichen Sprachfassungen des Abkommens die englische Fassung gilt.

2016/0127 (NLE)

Vorschlag für einen

BESCHLUSS DES RATES

über die Unterzeichnung – im Namen der Europäischen Union – des Abkommens zwischen den Vereinigten Staaten von Amerika und der Europäischen Union über den Schutz personenbezogener Daten bei der Verhütung, Untersuchung, Aufdeckung und Verfolgung von Straftaten

DER RAT DER EUROPÄISCHEN UNION –

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 16 in Verbindung mit Artikel 218 Absatz 5,

auf Vorschlag der Europäischen Kommission,

in Erwägung nachstehender Gründe:

(1) Am 3. Dezember 2010 ermächtigte der Rat die Kommission, mit der Regierung der Vereinigten Staaten von Amerika Verhandlungen über ein Abkommen über den Schutz personenbezogener Daten bei deren Übermittlung und Verarbeitung zum Zwecke der Verhütung, Untersuchung, Aufdeckung und Verfolgung von Straftaten einschließlich terroristischer Handlungen aufzunehmen.

(2) Die Verhandlungen mit der Regierung der Vereinigten Staaten von Amerika sind abgeschlossen; der Wortlaut des Abkommens wurde am 8. September 2015 paraphiert.

(3) Mit dem Abkommen soll ein umfassender Rahmen von Datenschutzgrundsätzen und -garantien für die Übermittlung personenbezogener Daten zum Zwecke der Strafverfolgung zwischen den USA einerseits und der Europäischen Union oder ihren Mitgliedstaaten andererseits geschaffen werden. Ziel ist es, ein hohes Maß an Datenschutz zu gewährleisten und dadurch die Zusammenarbeit zwischen den Vertragsparteien zu verbessern. Das Rahmenabkommen selbst bildet zwar nicht die Rechtsgrundlage für die Übermittlung personenbezogener Daten an die USA, ergänzt aber erforderlichenfalls die Datenschutzgarantien in bestehenden und künftigen Datenübermittlungsübereinkünften oder nationalen Bestimmungen, die zu Datenübermittlungen ermächtigen.

(4) Sämtliche Bestimmungen des Abkommens fallen in die Zuständigkeit der Union. Insbesondere hat die Union die Richtlinie 2016/XXX/EU[12] 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 erlassen.

(5) Die Europäische Union hat die ausschließliche Zuständigkeit, soweit das Abkommen gemeinsame Regeln der Union beeinträchtigen oder deren Tragweite verändern könnte.

[12] 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, mit der der Rahmenbeschluss 2008/977/JI des Rates aufgehoben wird.

(6) Nach Artikel 6a des dem Vertrag über die Europäische Union und dem Vertrag über die Arbeitsweise der Europäischen Union (AEUV) beigefügten Protokolls Nr. 21 über die Position des Vereinigten Königreichs und Irlands hinsichtlich des Raums der Freiheit, der Sicherheit und des Rechts sind die Vorschriften des Abkommens über die Verarbeitung personenbezogener Daten im Rahmen der Ausübung von Tätigkeiten, die in den Anwendungsbereich des Dritten Teils Titel V Kapitel 4 (Justizielle Zusammenarbeit in Strafsachen) und Kapitel 5 (Polizeiliche Zusammenarbeit) des AEUV fallen, für das Vereinigte Königreich und Irland nicht bindend, wenn das Vereinigte Königreich und Irland nicht durch Unionsvorschriften gebunden sind, nach denen das Abkommen eingehalten werden muss.

(7) Nach den Artikeln 1 und 2 des dem Vertrag über die Europäische Union und dem Vertrag über die Arbeitsweise der Europäischen Union beigefügten Protokolls Nr. 22 über die Position Dänemarks beteiligt sich Dänemark nicht an der Annahme dieses Beschlusses und ist weder durch das Abkommen gebunden noch seiner Anwendung unterworfen.

(8) Das Abkommen sollte vorbehaltlich seines späteren Abschlusses unterzeichnet werden –

HAT FOLGENDEN BESCHLUSS ERLASSEN:

Artikel 1

Die Unterzeichnung des Abkommens zwischen den Vereinigten Staaten von Amerika und der Europäischen Union über den Schutz personenbezogener Daten bei der Verhütung, Untersuchung, Aufdeckung und Verfolgung von Straftaten im Namen der Union wird – vorbehaltlich seines Abschlusses – genehmigt.

Der Wortlaut des zu unterzeichnenden Abkommens ist diesem Beschluss beigefügt.

Artikel 2

Das Generalsekretariat des Rates stellt die für die Unterzeichnung des Abkommens – vorbehaltlich seines Abschlusses – erforderliche Bevollmächtigungsurkunde für die von der Kommission benannte Person aus.

Artikel 3

Dieser Beschluss tritt am Tag seines Erlasses in Kraft.

Geschehen zu Brüssel am

Im Namen des Rates
Der Präsident

EUROPÄISCHE
KOMMISSION

Brüssel, den 29.4.2016
COM(2016) 238 final

ANNEX 1

ANHANG

ABKOMMEN ZWISCHEN DEN VEREINIGTEN STAATEN VON AMERIKA UND DER EUROPÄISCHEN UNION ÜBER DEN SCHUTZ PERSONENBEZOGENER DATEN BEI DER VERHÜTUNG, UNTERSUCHUNG, AUFDECKUNG UND VERFOLGUNG VON STRAFTATEN

zum

Vorschlag für einen Beschluss des Rates

über die Unterzeichnung – im Namen der Europäischen Union – des Abkommens zwischen den Vereinigten Staaten von Amerika und der Europäischen Union über den Schutz personenbezogener Daten bei der Verhütung, Untersuchung, Aufdeckung und Verfolgung von Straftaten

ABKOMMEN ZWISCHEN DEN VEREINIGTEN STAATEN VON AMERIKA UND DER EUROPÄISCHEN UNION ÜBER DEN SCHUTZ PERSONENBEZOGENER DATEN BEI DER VERHÜTUNG, UNTERSUCHUNG, AUFDECKUNG UND VERFOLGUNG VON STRAFTATEN

INHALT

Präambel

Artikel 1: Zweck

Artikel 2: Begriffsbestimmungen

Artikel 3: Anwendungsbereich

Artikel 4: Diskriminierungsverbot

Artikel 5: Wirkung des Abkommens

Artikel 6: Zweck- und Verwendungsbeschränkungen

Artikel 7: Übermittlung von Informationen in Drittländer

Artikel 8: Aufrechterhaltung der Qualität und der Vollständigkeit der Daten

Artikel 9: Informationssicherheit

Artikel 10: Meldung von Datensicherheitsvorfällen

Artikel 11: Führung von Aufzeichnungen

Artikel 12: Speicherfrist

Artikel 13: Besondere Kategorien personenbezogener Daten

Artikel 14: Rechenschaftspflicht

Artikel 15: Automatisierte Entscheidungen

Artikel 16: Zugang

Artikel 17: Berichtigung

Artikel 18: Behördlicher Rechtsbehelf

Artikel 19: Gerichtlicher Rechtsbehelf

Artikel 20: Transparenz

Artikel 21: Wirksame Aufsicht

Artikel 22: Zusammenarbeit zwischen den Aufsichtsbehörden

Artikel 23: Gemeinsame Überprüfung

Artikel 24: Notifikation

Artikel 25: Konsultation

Artikel 26: Aussetzung

Artikel 27: Räumlicher Geltungsbereich

Artikel 28: Geltungsdauer

Artikel 29: Inkrafttreten und Kündigung

In der Erwägung, dass die Vereinigten Staaten und die Europäische Union entschlossen sind, einen hohen Schutz der personenbezogenen Daten zu gewährleisten, die im Zusammenhang mit der Verhütung, Untersuchung, Aufdeckung und Verfolgung von Straftaten einschließlich Terrorismus ausgetauscht werden,

in der Absicht, einen dauerhaften Rechtsrahmen zur Erleichterung des Austauschs von für die Verhütung, Untersuchung, Aufdeckung und Verfolgung von Straftaten einschließlich Terrorismus wichtigen Informationen als Mittel zum Schutz ihrer demokratischen Gesellschaften und gemeinsamen Werte zu schaffen,

in der Absicht, insbesondere Standards für den Schutz personenbezogener Daten zu schaffen, die auf der Grundlage bestehender und künftiger Abkommen zwischen den USA und der EU und ihren Mitgliedstaaten im Bereich der Verhütung, Untersuchung, Aufdeckung und Verfolgung von Straftaten einschließlich Terrorismus ausgetauscht werden,

in der Erkenntnis, dass bestimmte zwischen den Vertragsparteien bestehende Abkommen über die Verarbeitung personenbezogener Daten vorsehen, dass diese Abkommen ein angemessenes Datenschutzniveau im Rahmen dieser Abkommen gewährleisten, bekräftigen die Vertragsparteien, dass das vorliegende Abkommen nicht so auszulegen ist, dass diese Abkommen geändert oder Bedingungen unterworfen werden oder in sonstiger Weise von ihnen abgewichen wird, wobei die Vertragsparteien gleichwohl berücksichtigen, dass die in Artikel 19 des vorliegenden Abkommens festgelegten Pflichten in Bezug auf den gerichtlichen Rechtsbehelf für sämtliche im Rahmen des vorliegenden Abkommens erfolgenden Datenübermittlungen und ungeachtet künftiger Überprüfungen oder Änderungen der besagten Abkommen gemäß ihren Modalitäten gelten sollen,

in Anerkennung der Tatsache, dass beide Vertragsparteien der Wahrung der Privatsphäre traditionell große Bedeutung beimessen, was sich unter anderem in den von der hochrangigen Kontaktgruppe EU-USA für den Informationsaustausch und den Schutz der Privatsphäre und personenbezogener Daten ausgearbeiteten Grundsätzen für den Schutz der Privatsphäre und den Schutz personenbezogener Daten bei der Verarbeitung für Strafverfolgungszwecke, in der Charta der Grundrechte der Europäischen Union und den geltenden EU-Rechtsvorschriften, in der Verfassung der Vereinigten Staaten und den geltenden amerikanischen Rechtsvorschriften sowie in den von der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung entwickelten Grundsätzen einer fairen Informationspraxis widerspiegelt, und

in Anbetracht der von den Vertragsparteien in ihren jeweiligen Rechtsrahmen umgesetzten Grundsätze der Verhältnismäßigkeit und Notwendigkeit beziehungsweise Relevanz und Angemessenheit

KOMMEN DIE VEREINIGTEN STAATEN VON AMERIKA UND DIE EUROPÄISCHE UNION WIE FOLGT ÜBEREIN:

Artikel 1: Zweck des Abkommens

1. Zweck dieses Abkommens ist die Gewährleistung eines hohen Schutzes personenbezogener Daten und die Verbesserung der Zusammenarbeit zwischen den Vereinigten Staaten und der Europäischen Union und ihren Mitgliedstaaten bei der Verhütung, Untersuchung, Aufdeckung und Verfolgung von Straftaten einschließlich Terrorismus.

2. Zu diesem Zweck wird in diesem Abkommen der Rahmen für den Schutz personenbezogener Daten bei ihrer Übermittlung zwischen den Vereinigten Staaten einerseits und der Europäischen Union und ihren Mitgliedstaaten andererseits festgelegt.

3. Das Abkommen selbst dient nicht als Rechtsgrundlage für Übermittlungen personenbezogener Daten. Derartige Übermittlungen bedürfen in allen Fällen einer Rechtsgrundlage.

Artikel 2: Begriffsbestimmungen

Im Sinne dieses Abkommens bezeichnet der Ausdruck

1. „personenbezogene Daten" alle Informationen über eine bestimmte oder bestimmbare natürliche Person. Als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind;

2. „Verarbeitung personenbezogener Daten" jeden Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, die Pflege, die Verwendung, die Änderung, die Organisation oder Strukturierung, die Offenlegung oder Verbreitung oder die Löschung;

3. „Vertragsparteien" die Europäische Union und die Vereinigten Staaten von Amerika;

4. „Mitgliedstaat" einen Mitgliedstaat der Europäischen Union;

5. „zuständige Behörde" im Fall der Vereinigten Staaten eine amerikanische nationale Strafverfolgungsbehörde, die für die Verhütung, Untersuchung, Aufdeckung und Verfolgung von Straftaten einschließlich Terrorismus zuständig ist, und im Fall der Europäischen Union eine Behörde der Europäischen Union oder eines Mitgliedstaats, die für die Verhütung, Untersuchung, Aufdeckung und Verfolgung von Straftaten einschließlich Terrorismus zuständig ist.

Artikel 3: Anwendungsbereich

1. Dieses Abkommen gilt für personenbezogene Daten, die zwischen den zuständigen Behörden der einen Vertragspartei und den zuständigen Behörden der anderen Vertragspartei oder gemäß einem zwischen den Vereinigten Staaten und der Europäischen Union oder ihren

Mitgliedstaaten geschlossenen Abkommen über die Verhütung, Aufdeckung, Untersuchung und Verfolgung von Straftaten einschließlich Terrorismus übermittelt werden.

2. Dieses Abkommen berührt nicht etwaige Datenübermittlungen und sonstige Formen der Zusammenarbeit zwischen anderen als den in Artikel 2 Absatz 5 genannten Behörden der Mitgliedstaaten und der Vereinigten Staaten, die für den Schutz der nationalen Sicherheit verantwortlich sind.

Artikel 4: Diskriminierungsverbot

Jede Vertragspartei erfüllt ihre aus diesem Abkommen erwachsenden Pflichten zum Schutz der personenbezogenen Daten ihrer eigenen Staatsangehörigen und der Staatsangehörigen der anderen Vertragspartei unabhängig von deren Staatsangehörigkeit und ohne willkürliche und ungerechtfertigte Diskriminierung.

Artikel 5: Wirkung des Abkommens

1. Dieses Abkommen ergänzt gegebenenfalls die geltenden Bestimmungen über den Schutz personenbezogener Daten in zwischen den Vertragsparteien oder zwischen den Vereinigten Staaten und Mitgliedstaaten geschlossenen internationalen Abkommen, die in den Anwendungsbereich des vorliegenden Abkommens fallende Sachverhalte regeln, ersetzt diese jedoch nicht.

2. Die Vertragsparteien treffen alle erforderlichen Maßnahmen zur Umsetzung dieses Abkommens und insbesondere ihrer darin niedergelegten jeweiligen Pflichten in Bezug auf den Datenzugang, die Datenberichtigung sowie den behördlichen und den gerichtlichen Rechtsbehelf für betroffene Personen. Von den in diesem Abkommen vorgesehenen Schutzmechanismen und Rechtsbehelfen können natürliche und juristische Personen nach Maßgabe der in den geltenden internen Rechtsvorschriften der jeweiligen Vertragspartei vorgesehenen Modalitäten Gebrauch machen. Für die Vereinigten Staaten von Amerika sind deren Pflichten im Einklang mit ihren Grundsätzen des Föderalismus anwendbar.

3. Bei der Umsetzung von Absatz 2 gilt die durch die Vereinigten Staaten oder durch die Europäische Union und ihre Mitgliedstaaten erfolgende Verarbeitung personenbezogener Daten in Bezug auf in den Anwendungsbereich dieses Abkommens fallende Sachverhalte als konform mit den jeweiligen Datenschutzvorschriften, welche Einschränkungen oder Auflagen für die internationale Übermittlung von personenbezogenen Daten vorsehen, und es ist keine zusätzliche Genehmigung nach diesen Rechtsvorschriften erforderlich.

Artikel 6: Zweck- und Verwendungsbeschränkungen

1. Die Übermittlung personenbezogener Daten darf ausschließlich für bestimmte Zwecke erfolgen, die nach der in Artikel 1 genannten Rechtsgrundlage zulässig sind.

2. Die Weiterverarbeitung personenbezogener Daten durch eine Vertragspartei darf nicht unvereinbar mit den Zwecken sein, für die die Daten übermittelt wurden. Sie gilt insbesondere dann als konform, wenn sie gemäß den Bestimmungen geltender internationaler Abkommen und schriftlich niedergelegter internationaler Rahmen für die Verhütung, Aufdeckung,

Untersuchung oder Verfolgung schwerer Straftaten erfolgt. Bei jeder in dieser Form erfolgenden Verarbeitung personenbezogener Daten durch andere nationale Strafverfolgungs-, Regulierungs- oder Verwaltungsbehörden sind zudem die sonstigen Bestimmungen dieses Abkommens einzuhalten.

3. Dieser Artikel berührt nicht die Möglichkeit der übermittelnden zuständigen Behörde, die Datenübermittlung im Einzelfall in dem nach dem geltenden Rechtsrahmen zulässigen Umfang zusätzlichen Bedingungen zu unterwerfen. Derartige Bedingungen dürfen keine allgemeinen Datenschutzbedingungen (d.h. in keinem Zusammenhang mit dem spezifischen Sachverhalt des Falles stehende Bedingungen) einschließen. Wenn die Datenübermittlung an Bedingungen geknüpft wird, muss die die Daten empfangende zuständige Behörde diesen nachkommen. Die die Daten übermittelnde zuständige Behörde kann zudem von der die Daten empfangenden Behörde Auskunft über die Verwendung der übermittelten Daten verlangen.

4. Falls die Vereinigten Staaten einerseits und die Europäische Union oder ein Mitgliedstaat andererseits ein Abkommen über die Übermittlung von sich nicht auf spezifische Fälle, spezifische Untersuchungen oder spezifische Strafverfolgungsmaßnahmen beziehenden Daten schließen, werden in einem solchen Abkommen die spezifischen Zwecke festgelegt, zu denen die betreffenden Daten übermittelt und verarbeitet werden dürfen.

5. Die Vertragsparteien stellen in ihren jeweiligen Rechtsvorschriften sicher, dass personenbezogene Daten in einer Weise verarbeitet werden, die in Bezug auf die Zwecke der Verarbeitung unmittelbar relevant und weder exzessiv noch zu weit gefasst ist.

Artikel 7: Übermittlung von Informationen in Drittländer

1. Hat eine zuständige Behörde einer Vertragspartei personenbezogene Daten zu einem bestimmten Fall an eine zuständige Behörde der anderen Vertragspartei übermittelt, so dürfen diese Daten nur dann an einen nicht durch dieses Abkommen gebundenen Staat oder an eine internationale Einrichtung übermittelt werden, wenn die vorherige Zustimmung der zuständigen Behörde, die die Daten ursprünglich übermittelt hat, vorliegt.

2. Bei der Erteilung ihrer Zustimmung zu einer Übermittlung gemäß Absatz 1 berücksichtigt die zuständige Behörde, die die Daten ursprünglich übermittelt hat, alle relevanten Faktoren einschließlich der Schwere der Straftat, des Zwecks, zu dem die Daten ursprünglich übermittelt wurden, und der Frage, ob der nicht durch dieses Abkommen gebundene Staat oder die betreffende internationale Einrichtung einen angemessenen Schutz personenbezogener Daten gewährleistet. Sie kann die Datenübermittlung zudem von spezifischen Bedingungen abhängig machen.

3. Falls die Vereinigten Staaten einerseits und die Europäische Union oder ein Mitgliedstaat andererseits ein Abkommen über die Übermittlung von sich nicht auf spezifische Fälle, spezifische Untersuchungen oder spezifische Strafverfolgungsmaßnahmen beziehenden Daten schließen, dürfen diese Daten nur unter den in einem solchen Abkommen festgelegten spezifischen Bedingungen für eine ordnungsgemäß begründete Weiterübermittlung weiterübermittelt werden. In einem solchen Abkommen sind zudem geeignete Mechanismen für die gegenseitige Unterrichtung der zuständigen Behörden vorzusehen.

4. Dieser Artikel ist nicht so auszulegen, als berühre er Anforderungen, Pflichten oder Praktiken, denen zufolge die vorherige Zustimmung der zuständigen Behörde, die die Daten

ursprünglich übermittelt hat, einzuholen ist, bevor die Daten an einen durch dieses Abkommen gebundenen Staat oder an eine durch dieses Abkommen gebundene Einrichtung übermittelt werden dürfen, sofern eine solche Übermittlung nicht aufgrund des in dem betreffenden Staat oder in der betreffenden Einrichtung herrschenden Datenschutzniveaus abgelehnt oder von bestimmten Bedingungen abhängig gemacht wird.

Artikel 8: Aufrechterhaltung der Qualität und der Vollständigkeit der Daten

Die Vertragsparteien ergreifen angemessene Maßnahmen, um sicherzustellen, dass personenbezogene Daten mit der für ihre rechtmäßige Verarbeitung notwendigen und angemessenen Genauigkeit, Relevanz, Aktualität und Vollständigkeit aufbewahrt werden. Zu diesem Zweck müssen die zuständigen Behörden über Verfahren verfügen, deren Zweck es ist, die Qualität und Vollständigkeit personenbezogener Daten sicherzustellen, darunter die Folgenden:

a) die in Artikel 17 genannten Maßnahmen;

b) falls der übermittelnden zuständigen Behörde erhebliche Zweifel an der Relevanz, Aktualität, Vollständigkeit oder Genauigkeit derartiger personenbezogener Daten oder einer von ihr übermittelten Bewertung zur Kenntnis gelangen, teilt sie dies der empfangenden zuständigen Behörde nach Möglichkeit mit;

c) falls der empfangenden zuständigen Behörde erhebliche Zweifel an der Relevanz, Aktualität, Vollständigkeit oder Genauigkeit personenbezogener Daten, die sie von einer Regierungsbehörde erhalten hat, oder einer von der übermittelnden zuständigen Behörde vorgenommenen Bewertung der Genauigkeit der Daten oder der Zuverlässigkeit einer Quelle zur Kenntnis gelangen, teilt sie dies der übermittelnden zuständigen Behörde nach Möglichkeit mit.

Artikel 9: Informationssicherheit

Die Vertragsparteien stellen sicher, dass sie über geeignete technische und organisatorische Sicherheitsvorkehrungen verfügen, die personenbezogene Daten gegen Folgendes schützen:

a) zufällige oder unrechtmäßige Zerstörung,

b) zufälliger Verlust und

c) unberechtigte Offenlegung, unberechtigte Änderung, unberechtigter Zugang oder sonstige unberechtigte Verarbeitung.

Diese Vorkehrungen müssen angemessene Garantien in Bezug auf die erforderliche Ermächtigung für den Zugang zu personenbezogenen Daten einschließen.

Artikel 10: Meldung von Datensicherheitsvorfällen

1. Nach Feststellung eines Vorfalls, der den zufälligen Verlust, die zufällige Zerstörung, den unberechtigten Zugang oder die unberechtigte Offenlegung oder Änderung von personenbezogenen Daten nach sich zieht, von denen ein erhebliches Schadensrisiko ausgeht,

prüft die empfangende zuständige Behörde unverzüglich die Wahrscheinlichkeit und das Ausmaß des potenziellen Schadens für betroffene Personen und für die Integrität des Programms der übermittelnden zuständigen Behörde und ergreift unverzüglich geeignete Schadensbegrenzungsmaßnahmen.

2. Die Schadensbegrenzungsmaßnahmen schließen die Benachrichtigung der übermittelnden zuständigen Behörde ein. Diese Benachrichtigung kann

a) geeignete Einschränkungen in Bezug auf die Weiterleitung der Benachrichtigung einschließen;

b) aufgeschoben werden oder entfallen, falls durch sie die nationale Sicherheit gefährdet werden könnte;

c) aufgeschoben werden, falls durch sie die öffentliche Sicherheit gefährdet werden könnte.

3. Wenn es den Umständen des Vorfalls angemessen ist, können die Schadensbegrenzungsmaßnahmen auch die Benachrichtigung der betroffenen Person einschließen, sofern Folgendes durch eine solche Benachrichtigung nicht gefährdet werden kann:

a) die öffentliche oder die nationale Sicherheit;

b) amtliche Ermittlungen, Untersuchungen oder Verfahren;

c) die Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten;

d) Rechte und Freiheiten Dritter, insbesondere der Schutz von Opfern und Zeugen.

4. Die an der Übermittlung der personenbezogenen Daten beteiligten zuständigen Behörden können einander bezüglich des Vorfalls und der Reaktion darauf zu Rate ziehen.

Artikel 11: Führung von Aufzeichnungen

1. Die Vertragsparteien müssen über wirksame Methoden zum Nachweis der Rechtmäßigkeit der Verarbeitung personenbezogener Daten verfügen; diese können die Verwendung von Protokollen und sonstigen Aufzeichnungen einschließen.

2. Die zuständigen Behörden können diese Protokolle oder Aufzeichnungen für die Aufrechterhaltung des ordnungsgemäßen Betriebs der betreffenden Datenbanken und Dateien, für die Wahrung der Datenintegrität und -sicherheit und erforderlichenfalls für Sicherungsverfahren verwenden.

Artikel 12: Speicherfrist

1. Für Aufzeichnungen, die personenbezogene Daten enthalten, sehen die Vertragsparteien in ihren geltenden Rechtsrahmen besondere Speicherfristen vor, durch die sichergestellt wird, dass personenbezogene Daten nicht länger gespeichert werden, als notwendig und angemessen ist. Bei der Festlegung dieser Speicherfristen wird den Zwecken der Verarbeitung, der Art der Daten und der sie verarbeitenden Behörde, den Auswirkungen auf

die Rechte und Interessen der betroffenen Personen und anderen geltenden rechtlichen Erwägungen Rechnung getragen.

2. Falls die Vereinigten Staaten einerseits und die Europäische Union oder ein Mitgliedstaat andererseits ein Abkommen über die Übermittlung personenbezogener Daten schließen, das sich nicht auf spezifische Fälle, spezifische Untersuchungen oder spezifische Strafverfolgungsmaßnahmen bezieht, so schließt dieses eine besondere, einvernehmlich vereinbarte Bestimmung über die Speicherfristen ein.

3. Die Vertragsparteien sehen Verfahren für eine regelmäßige Überprüfung der Speicherfrist vor, um bestimmen zu können, ob veränderte Umstände eine weitere Änderung der geltenden Frist erforderlich machen.

4. Die Vertragsparteien veröffentlichen derartige Speicherfristen oder machen sie auf andere Weise öffentlich zugänglich.

Artikel 13: Besondere Kategorien personenbezogener Daten

1. Personenbezogene Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder sonstige Überzeugungen, eine Gewerkschaftszugehörigkeit oder die Gesundheit oder das Sexualleben betreffende Informationen hervorgehen, dürfen nur unter Wahrung angemessener Garantien im Einklang mit dem geltendem Recht verarbeitet werden. Diese Garantien können insbesondere Folgendes umfassen: eine Beschränkung der Zwecke, zu denen die Daten verarbeitet werden dürfen, indem beispielsweise die Verarbeitung nur von Fall zu Fall zugelassen wird, die Unkenntlichmachung, Löschung oder Sperrung von Daten, nachdem sie zu dem vorgesehenen Zweck verarbeitet wurden, eine Beschränkung des Kreises der Mitarbeiter, die Zugang zu den Daten erhalten, spezielle obligatorische Schulungen für Mitarbeiter, die Zugang zu den Daten erhalten, eine obligatorische aufsichtliche Genehmigung für den Datenzugang oder andere Schutzmaßnahmen. Diese Garantien müssen der Art der Daten, etwaigen besonders sensiblen Informationen und dem Zweck, zu dem die Daten verarbeitet werden, gebührend Rechnung tragen.

2. Falls die Vereinigten Staaten einerseits und die Europäische Union oder ein Mitgliedstaat andererseits ein Abkommen über die Übermittlung personenbezogener Daten schließen, das sich nicht auf spezifische Fälle, spezifische Untersuchungen oder spezifische Strafverfolgungsmaßnahmen bezieht, so werden darin die für die Verarbeitung dieser Daten maßgeblichen Standards und Bedingungen näher spezifiziert und dabei die Art der Daten und der Zweck, zu dem diese verwendet werden, gebührend berücksichtigt.

Artikel 14: Rechenschaftspflicht

1. Die Vertragsparteien müssen über Maßnahmen zur Stärkung der Rechenschaftspflicht für die im Rahmen dieses Abkommens erfolgende Verarbeitung personenbezogener Daten durch ihre zuständigen Behörden und ihre sonstigen Behörden verfügen, an die personenbezogene Daten übermittelt wurden. Diese Maßnahmen schließen die Meldung der geltenden Garantien für im Rahmen dieses Abkommens erfolgende Übermittlungen personenbezogener Daten sowie etwaiger von der übermittelnden zuständigen Behörde gemäß Artikel 6 Absatz 3 festgelegter Bedingungen ein. Schwere Verstöße werden mit geeigneten abschreckenden straf-, zivil- oder verwaltungsrechtlichen Sanktionen geahndet.

2. Die in Absatz 1 genannten Maßnahmen umfassen gegebenenfalls die Einstellung der Übermittlung personenbezogener Daten an nicht unter dieses Abkommen fallende Behörden einzelner Gebietseinheiten der Vertragsparteien, die personenbezogene Daten nicht wirksam geschützt haben, wobei der Zweck dieses Abkommens und insbesondere die darin festgelegten Zweck- und Verwendungsbeschränkungen und Weitergabebestimmungen zu berücksichtigen sind.

3. Bei Verdacht auf eine nicht ordnungsgemäße Anwendung dieses Artikels kann eine Vertragspartei die andere Vertragspartei auffordern, ihr sachdienliche Informationen zu übermitteln, darunter gegebenenfalls auch Informationen über die Maßnahmen, die gemäß diesem Artikel getroffen wurden.

Artikel 15: Automatisierte Entscheidungen

Entscheidungen, die die rechtmäßigen Interessen der betroffenen Personen erheblich beeinträchtigen, dürfen nicht ausschließlich auf eine automatisierte, ohne menschliches Zutun erfolgende Verarbeitung von personenbezogenen Daten gestützt sein, es sei denn, dies ist nach internem Recht zulässig und es gibt geeignete Garantien einschließlich der Möglichkeit, das Eingreifen eines Menschen zu erwirken.

Artikel 16: Zugang

1. Die Vertragsparteien stellen sicher, dass jede Person Zugang zu ihren personenbezogenen Daten beantragen und vorbehaltlich der in Absatz 2 festgelegten Einschränkungen erhalten kann. Maßgeblich für die Beantragung eines solchen Zugangs bei einer zuständigen Behörde und die Zugangsgewährung durch eine zuständige Behörde ist der geltende Rechtsrahmen des Staates, in dem der Antrag gestellt wird.

2. Der Zugang zu derartigen Daten kann im Einzelfall angemessenen, den berechtigten Interessen der betroffenen Person Rechnung tragenden Beschränkungen nach internem Recht unterworfen werden, um

a) die Rechte und Freiheiten - einschließlich der Privatsphäre - anderer zu schützen;

b) die öffentliche und die nationale Sicherheit zu schützen;

c) sensible Strafverfolgungsdaten zu schützen;

d) Behinderungen behördlicher oder gerichtlicher Ermittlungen, Untersuchungen oder Verfahren zu vermeiden;

e) Beeinträchtigungen der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung zu vermeiden;

f) sonstige in den Rechtsvorschriften über die Informationsfreiheit und den Zugang der Öffentlichkeit zu Dokumenten genannte Interessen zu schützen.

3. Betroffenen Personen dürfen für den Zugang zu ihren personenbezogenen Daten keine übermäßigen Kosten auferlegt werden.

4. Betroffene Personen können eine Aufsichtsbehörde oder einen Vertreter ermächtigen, den Zugang in ihrem Namen zu beantragen, sofern dies nach geltendem internen Recht zulässig ist.

5. Wird der Zugang verweigert oder Einschränkungen unterworfen, teilt die mit dem Antrag befasste zuständige Behörde der betroffenen Person oder ihrem ordnungsgemäß ermächtigten Vertreter nach Absatz 4 die Gründe für die Zugangsverweigerung beziehungsweise -einschränkung mit.

Artikel 17: Berichtigung

1. Die Vertragsparteien stellen sicher, dass jede betroffene Person die Berichtigung oder Bereinigung eigener personenbezogener Daten, die ihres Erachtens ungenau sind oder nicht ordnungsgemäß verarbeitet wurden, erwirken kann. Die Berichtigung oder Bereinigung kann die Ergänzung, Löschung, Sperrung oder sonstige Maßnahmen oder Verfahren zur Beseitigung von Ungenauigkeiten oder von Folgen einer nicht ordnungsgemäßen Verarbeitung einschließen. Maßgeblich für die Beantragung einer solchen Berichtigung oder Bereinigung bei einer zuständigen Behörde und für die Genehmigung einer solchen Berichtigung oder Bereinigung durch eine zuständige Behörde ist der geltende Rechtsrahmen des Staates, in dem der Antrag gestellt wird.

2. Falls die zuständige Behörde, der die Daten übermittelt wurden,

a) nach Eingang eines Antrags nach Absatz 1,

b) nach Benachrichtigung durch den Übermittler der Daten oder

c) aufgrund eigener Ermittlungen oder Nachforschungen

zu dem Schluss gelangt, dass Daten, die ihr im Rahmen dieses Abkommens übermittelt wurden, ungenau sind oder nicht ordnungsgemäß verarbeitet wurden, so ergreift sie geeignete Maßnahmen zur Ergänzung, zur Löschung, zur Sperrung oder zu sonstigen Berichtigungs- oder Bereinigungsverfahren.

3. Betroffene Personen können eine Aufsichtsbehörde oder einen Vertreter ermächtigen, die Berichtigung oder Bereinigung in ihrem Namen zu beantragen, sofern dies nach geltendem internen Recht zulässig ist.

4. Wird die Berichtigung oder Bereinigung verweigert oder Einschränkungen unterworfen, teilt die mit dem Antrag befasste zuständige Behörde der betroffenen Person oder ihrem ordnungsgemäß ermächtigten Vertreter nach Absatz 3 die Gründe für die Berichtigungs- oder Bereinigungsverweigerung beziehungsweise -einschränkung mit.

Artikel 18: Behördlicher Rechtsbehelf

1. Die Vertragsparteien stellen sicher, dass jede betroffene Person einen behördlichen Rechtsbehelf einlegen kann, wenn sie der Ansicht ist, dass ihr Antrag auf Zugang nach Artikel 16 oder ihr Antrag auf Berichtigung ungenauer oder nicht ordnungsgemäß verarbeiteter Daten nach Artikel 17 zu Unrecht abgelehnt wurde. Maßgeblich für die Einlegung eines solchen Rechtsbehelfs bei einer zuständigen Behörde und die Gewährung

eines solchen Rechtsbehelfs durch eine zuständige Behörde ist der geltende Rechtsrahmen des Staates, in dem die Einlegung erfolgt.

2. Betroffene Personen können eine Aufsichtsbehörde oder einen Vertreter ermächtigen, in ihrem Namen einen behördlichen Rechtsbehelf einzulegen, sofern dies nach geltendem internen Recht zulässig ist.

3. Die zuständige Behörde, bei der der Rechtsbehelf eingelegt wird, führt geeignete Nachforschungen und Überprüfungen durch und erteilt unverzüglich eine schriftliche Antwort (auch auf elektronischem Weg), in der sie gegebenenfalls mitteilt, welche Abhilfemaßnahmen ergriffen wurden. Die Belehrung über das Verfahren für die Einlegung eines weiteren behördlichen Rechtsbehelfs erfolgt gemäß Artikel 20.

Artikel 19: Gerichtlicher Rechtsbehelf

1. Die Vertragsparteien sehen in ihren geltenden Rechtsrahmen vor, dass jeder Bürger einer Vertragspartei vorbehaltlich etwaiger Bestimmungen, wonach zunächst die Möglichkeiten des behördlichen Rechtsbehelfs ausgeschöpft werden müssen, in folgenden Fällen eine gerichtliche Überprüfung beantragen kann:

a) Verweigerung des Zugangs zu Aufzeichnungen mit personenbezogenen Daten der betroffenen Person durch eine zuständige Behörde,

b) Verweigerung der Änderung von Aufzeichnungen mit personenbezogenen Daten der betroffenen Person durch eine zuständige Behörde und

c) bewusst oder vorsätzlich erfolgte unrechtmäßige Offenlegung derartiger Daten, die auch einen Schadensersatz nach sich ziehen kann.

2. Maßgeblich für die Beantragung und Genehmigung einer solchen gerichtlichen Überprüfung ist der geltende Rechtsrahmen des Staates, in dem der Rechtsbehelf eingelegt wird.

3. Die Absätze 1 und 2 berühren nicht etwaige sonstige Möglichkeiten für eine gerichtliche Überprüfung, die in Bezug auf die Verarbeitung personenbezogener Daten nach dem Recht des Staates, in dem der Rechtsbehelf eingelegt wird, bestehen.

4. Im Falle der Aussetzung oder Kündigung dieses Abkommens bilden Artikel 26 Absatz 2 und Artikel 29 Absatz 3 keine Grundlage für einen gerichtlichen Rechtsbehelf, der nach dem Recht der betreffenden Vertragspartei nicht mehr verfügbar ist.

Artikel 20: Transparenz

1. Die Vertragsparteien belehren jede betroffene Person über ihre personenbezogenen Daten; diese Belehrung kann von den zuständigen Behörden durch Veröffentlichung allgemeiner Bekanntmachungen oder durch eine spezifische Belehrung vorgenommen werden, wobei für die Form und den Zeitpunkt der Belehrung das Recht maßgeblich ist, dem die die Belehrung vornehmende Behörde unterliegt, und in der Belehrung Folgendes mitzuteilen ist:

a) die Zwecke, zu denen die betreffenden Daten von der Behörde verarbeitet werden,

b) die Zwecke, zu denen die Daten an andere Behörden weitergegeben werden dürfen,

c) die für die Verarbeitung der Daten maßgeblichen Gesetze oder Vorschriften,

d) etwaige Dritte, denen gegenüber die Daten offengelegt werden und

e) zur Verfügung stehende Möglichkeiten für den Zugang zu den Daten, für ihre Berichtigung oder Bereinigung oder für einen Rechtsbehelf.

2. Diese Belehrungspflicht gilt vorbehaltlich angemessener Beschränkungen nach internem Recht für die in Artikel 16 Absatz 2 Buchstaben a bis f genannten Zwecke.

Artikel 21: Wirksame Aufsicht

1. Die Parteien müssen über eine oder mehrere Aufsichtsbehörden verfügen, die

a) gegebenenfalls von sich aus unabhängige Aufsichtsfunktionen und -befugnisse ausüben, die Überprüfungs-, Untersuchungs- und Eingriffsmaßnahmen einschließen,

b) befugt sind, von betroffenen Personen eingereichte Beschwerden, die sich auf Maßnahmen zur Umsetzung dieses Abkommens beziehen, entgegenzunehmen und diesen nachzugehen und

c) befugt sind, bei Zuwiderhandlungen im Zusammenhang mit diesem Abkommen gegebenenfalls eine strafrechtliche Verfolgung einleiten oder Disziplinarmaßnahmen verhängen zu lassen.

2. Die Europäische Union stellt sicher, dass durch ihre Datenschutzbehörden und durch die Datenschutzbehörden der Mitgliedstaaten eine Aufsicht im Sinne dieses Artikels erfolgt.

3. Die Vereinigten Staaten stellen sicher, dass durch mehr als eine ihrer Behörden (Generalinspektoren, Datenschutzbeauftragte, Rechnungshöfe, für die Überwachung des Schutzes der Privatsphäre und der bürgerlichen Freiheiten zuständige Stellen, sonstige für den Schutz der Privatsphäre und der bürgerlichen Freiheiten zuständige Nachprüfungsinstanzen der Exekutive und der Legislative usw.) eine kumulative Aufsicht im Sinne dieses Artikels erfolgt.

Artikel 22: Zusammenarbeit zwischen den Aufsichtsbehörden

1. Die für die Aufsicht im Sinne von Artikel 21 zuständigen Behörden konsultieren einander erforderlichenfalls bezüglich der Ausübung der in diesem Abkommen vorgesehenen Aufgaben im Hinblick auf eine effiziente Umsetzung der Artikel 16, 17 und 18.

2. Die Vertragsparteien richten nationale Kontaktstellen ein, die bei der Ermittlung der im Einzelfall zu kontaktierenden Aufsichtsbehörde behilflich sind.

Artikel 23: Gemeinsame Überprüfung

1. Die Vertragsparteien führen regelmäßig eine gemeinsame Überprüfung der Strategien und Verfahren zur Umsetzung dieses Abkommens sowie ihrer Wirksamkeit durch. Dabei achten sie besonders auf eine wirksame Umsetzung der Schutzklauseln der Artikel 14 (Rechenschaftspflicht), 16 (Zugang), 17 (Berichtigung), 18 (behördlicher Rechtsbehelf) und 19 (gerichtlicher Rechtsbehelf).

2. Die gemeinsame Überprüfung erfolgt erstmals spätestens drei Jahre nach dem Inkrafttreten dieses Abkommens und danach in regelmäßigen Abständen. Die Vertragsparteien legen gemeinsam vorab die Einzelheiten und Bedingungen der gemeinsamen Überprüfung fest und unterrichten einander über die Zusammensetzung ihrer jeweiligen Delegationen, denen auch Vertreter der in Artikel 21 (wirksame Kontrolle) genannten Aufsichtsbehörden sowie Vertreter von Strafverfolgungs- und Justizbehörden angehören müssen. Die Ergebnisse der gemeinsamen Überprüfung werden veröffentlicht.

3. Falls die Vertragsparteien oder die Vereinigten Staaten und ein Mitgliedstaat ein anderes Abkommen geschlossen haben, dessen Gegenstand ebenfalls in den Anwendungsbereich dieses Abkommens fällt und das ebenfalls gemeinsame Überprüfungen vorsieht, so werden die letztgenannten gemeinsamen Überprüfungen nicht dupliziert, und ihre Ergebnisse fließen - soweit relevant - in die Ergebnisse der im Rahmen dieses Abkommens durchgeführten gemeinsamen Überprüfung ein.

Artikel 24: Notifikation

1. Die Vereinigten Staaten notifizieren der Europäischen Union sämtliche Benennungen, die amerikanische Behörden in Bezug auf Artikel 19 vornehmen, sowie etwaige Änderungen der betreffenden Angaben.

2. Die Vertragsparteien ergreifen angemessene Maßnahmen, um einander den Erlass von Rechtsvorschriften beziehungsweise die Annahme von Regelungen zu notifizieren, die die Umsetzung dieses Abkommens wesentlich beeinflussen; dies geschieht nach Möglichkeit, bevor diese wirksam werden.

Artikel 25: Konsultation

Bei etwaigen Streitigkeiten über die Auslegung oder Anwendung dieses Abkommens konsultieren die Vertragsparteien einander, um zu einer einvernehmlichen Lösung zu gelangen.

Artikel 26: Aussetzung

1. Im Fall einer erheblichen Verletzung dieses Abkommens kann jede Vertragspartei dieses Abkommen durch schriftliche Notifikation an die andere Vertragspartei auf diplomatischem Weg ganz oder teilweise aussetzen. Eine solche schriftliche Notifikation kann erst erfolgen, wenn die Vertragsparteien einander während eines angemessenen Zeitraums konsultiert, jedoch dabei keine Lösung gefunden haben; die Aussetzung tritt nach einer Frist von zwanzig Tagen ab dem Datum des Eingangs einer entsprechenden Notifikation in Kraft. Die

aussetzende Vertragspartei kann die Aussetzung nach schriftlicher Notifikation an die andere Vertragspartei aufheben. Die Aufhebung wird unmittelbar nach Eingang einer entsprechenden Notifikation wirksam.

2. Ungeachtet einer etwaigen Aussetzung dieses Abkommens dürfen personenbezogene Daten, die in den Anwendungsbereich dieses Abkommens fallen und vor der Aussetzung übermittelt wurden, weiterhin gemäß den Bestimmungen dieses Abkommens verarbeitet werden.

Artikel 27: Räumlicher Geltungsbereich

1. Dieses Abkommen gilt nur dann für Dänemark, das Vereinigte Königreich oder Irland, wenn die Europäische Kommission den Vereinigten Staaten schriftlich notifiziert, dass Dänemark, das Vereinigte Königreich oder Irland beschlossen hat, dass das Abkommen auf sein Hoheitsgebiet Anwendung findet.

2. Falls die Europäische Kommission den Vereinigten Staaten vor Inkrafttreten dieses Abkommens notifiziert, dass dieses Abkommen auf Dänemark, das Vereinigte Königreich oder Irland Anwendung findet, gilt das Abkommen für das Hoheitsgebiet des betreffenden Staates ab dem Tag des Inkrafttretens dieses Abkommens.

3. Falls die Europäische Kommission den Vereinigten Staaten nach Inkrafttreten des Abkommens notifiziert, dass das Abkommen auf Dänemark, das Vereinigte Königreich oder Irland Anwendung findet, gilt das Abkommen für das Hoheitsgebiet des betreffenden Staates ab dem ersten Tag des Monats nach Eingang der Notifikation bei den Vereinigten Staaten.

Artikel 28: Geltungsdauer des Übereinkommens

Dieses Abkommen wird auf unbegrenzte Zeit geschlossen.

Artikel 29: Inkrafttreten und Kündigung

1. Dieses Abkommen tritt am ersten Tag des Monats in Kraft, der auf den Tag folgt, an dem die Vertragsparteien einander den Abschluss ihrer internen Verfahren für das Inkrafttreten notifiziert haben.

2. Dieses Abkommen kann von jeder Vertragspartei jederzeit durch schriftliche Notifikation an die andere Vertragspartei auf diplomatischem Wege gekündigt werden. Die Kündigung wird dreißig Tage nach dem Tag des Eingangs dieser Notifikation wirksam.

3. Ungeachtet einer Kündigung dieses Abkommens dürfen personenbezogene Daten, die in den Anwendungsbereich dieses Abkommens fallen und vor der Kündigung übermittelt wurden, weiterhin gemäß den Bestimmungen dieses Abkommens verarbeitet werden.

ZU URKUND DESSEN haben die unterzeichneten Bevollmächtigten ihre Unterschriften unter dieses Abkommen gesetzt.

Geschehen zu […] am […] 201. in zwei Urschriften in englischer Sprache. Nach dem EU-Recht wird das Abkommen von der EU ebenfalls in bulgarischer, dänischer, deutscher, estnischer, finnischer, französischer, griechischer, irischer, italienischer, kroatischer, lettischer, litauischer, maltesischer, niederländischer, polnischer, portugiesischer, rumänischer, schwedischer, slowakischer, slowenischer, spanischer, tschechischer und ungarischer Sprache abgefasst. Die Verbindlichkeit dieser zusätzlichen Sprachfassungen kann im Wege eines diplomatischen Notenwechsels zwischen den Vereinigten Staaten und der Europäischen Union festgestellt werden. Bei Abweichungen zwischen verbindlichen Sprachfassungen gilt die englische Fassung.