EUROPÄISCHE
KOMMISSION

Brüssel, den 10.1.2017
COM(2017) 7 final

MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT

Austausch und Schutz personenbezogener Daten in einer globalisierten Welt

1. EINLEITUNG

Der Schutz personenbezogener Daten ist Teil des gemeinsamen europäischen Regelwerks und in Artikel 8 der EU-Charta der Grundrechte verankert. Seit über 20 Jahren kommt dem Datenschutz im EU-Recht ein zentraler Stellenwert zu, angefangen bei der Datenschutzrichtlinie aus dem Jahr 1995[1] („Richtlinie von 1995“) bis hin zur Verabschiedung der Datenschutz-Grundverordnung[2] und der Polizei-Richtlinie[3] im Jahr 2016.

Präsident Juncker betonte in seiner Rede zur Lage der Europäischen Union am 14. September 2016: „*Europäer sein heißt, ein Anrecht darauf zu haben, dass die eigenen personenbezogenen Daten durch strenge europäische Gesetze geschützt werden. [...] Denn in Europa spielt der Schutz der Privatsphäre eine Rolle. Das ist eine Frage der Menschenwürde.*“

Der Wunsch nach dem Schutz personenbezogener Daten ist jedoch nicht auf Europa beschränkt. Verbraucher auf der ganzen Welt legen immer mehr Wert auf ihre Privatsphäre. Unternehmen wiederum erkennen, dass ein guter Schutz der Privatsphäre ihnen einen Wettbewerbsvorteil verschafft, da er das Vertrauen in ihre Dienstleistungen erhöht. Viele von ihnen, vor allem Unternehmen mit globaler Reichweite, passen ihre Datenschutzregeln an diejenigen der Datenschutz-Grundverordnung an, zum einen, weil sie in der EU Geschäfte machen wollen, zum anderen, weil sie sie als beispielhaft ansehen.

Auch einige Länder und regionale Organisationen außerhalb der EU, ob in unserer unmittelbaren Nachbarschaft oder in Asien, Lateinamerika oder Afrika, führen neue Datenschutzvorschriften ein bzw. aktualisieren bestehende Vorschriften, um die Chancen der globalen digitalen Wirtschaft zu nutzen und der wachsenden Nachfrage nach mehr Datensicherheit und Schutz der Privatsphäre zu begegnen. Auch wenn zwischen der Herangehensweise der einzelnen Länder und dem Grad des Ausbaus ihrer Rechtsvorschriften Unterschiede bestehen, so gibt es doch Anzeichen für eine Aufwärtskonvergenz, d. h. eine Angleichung nach oben bei wichtigen Datenschutzgrundsätzen, insbesondere in einigen Regionen der Welt[4]. Eine größere Kompatibilität der einzelnen Datenschutzsysteme würde den grenzüberschreitenden Verkehr personenbezogener Daten erleichtern, ob für kommerzielle Zwecke oder die Zusammenarbeit von Behörden (z. B. im Bereich der Strafverfolgung). Die EU sollte vor diesem Hintergrund die Chance nutzen, ihre

---

1 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. L 281 vom 23.11.1995).

2 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1). Sie trat am 24. Mai 2016 in Kraft und findet ab dem 25. Mai 2018 Anwendung.

3 Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119 vom 4.5.2016, S. 89). Sie trat am 5. Mai 2016 in Kraft. Die EU-Mitgliedstaaten müssen sie bis spätestens 6. Mai 2018 in nationales Recht umsetzen.

4 Siehe „Data protection regulations and international data flows: Implications for trade and development“, UNCTAD (2016): http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf

Datenschutzwerte zu fördern und den Datenverkehr zu erleichtern, indem sie sich für eine größere Konvergenz der Rechtssysteme einsetzt. Daher werden in der vorliegenden Mitteilung im Einklang mit dem Arbeitsprogramm der Kommission[5] der strategische Rahmen der Kommission für „Angemessenheitsbeschlüsse" sowie andere Instrumente für Datenübermittlungen und den internationalen Datenschutz erläutert.

2. DAS DATENSCHUTZ-REFORMPAKET DER EU – EIN MODERNER RECHTSRAHMEN FÜR EINEN GUT GESCHÜTZTEN INTERNATIONALEN DATENVERKEHR

Durch die Reform der EU-Datenschutzvorschriften im April 2016 wurde ein System geschaffen, das zum einen ein hohes Schutzniveau gewährleistet und zum anderen die Nutzung der Chancen der globalen Informationsgesellschaft ermöglicht. Durch Verbesserung der Kontrolle, die die Bürger über ihre personenbezogenen Daten erhalten, wird mit der Reform auch das Vertrauen der Verbraucher in die digitale Wirtschaft gestärkt. Die Harmonisierung und Vereinfachung des rechtlichen Umfelds machen es für heimische wie auch ausländische Unternehmen leichter und weniger aufwendig, in der EU Geschäfte zu tätigen und zu diesem Zweck auch Daten international auszutauschen. Die EU bietet so Offenheit für den internationalen Datenverkehr bei maximalem Schutz für den Einzelnen. Sie hat das Potenzial, sich zu einer Drehscheibe für Datendienste zu entwickeln, die sowohl einen freien Datenverkehr als auch Vertrauen voraussetzen.

2.1 Ein umfassender, einheitlicher und vereinfachter EU-Datenschutzrahmen

Durch die Reform erhält die EU einen umfassenden Rechtsrahmen für die Verarbeitung personenbezogener Daten sowohl im privaten als auch im öffentlichen Sektor, der die kommerziellen Aspekte (Datenschutz-Grundverordnung) und die Strafverfolgung (Polizei-Richtlinie) abdeckt.

Ab Mai 2018 – dem Geltungsbeginn der Datenschutz-Grundverordnung – wird es statt der bisherigen 28 nationalen Regelungen ein einheitliches Regelwerk für ganz Europa geben. Mit dem neuen „Verfahren der Zusammenarbeit und Kohärenz" wird dafür gesorgt, dass in der EU nur eine Datenschutzbehörde für die Aufsicht über ein Unternehmen, das Daten grenzüberschreitend verarbeitet, zuständig ist. Die einheitliche Auslegung der neuen Vorschriften wird gewährleistet. So wird in grenzüberschreitenden Fällen, an denen mehrere nationale Datenschutzbehörden beteiligt sind, ein einziger Beschluss gefasst, damit sichergestellt ist, dass für gemeinsame Probleme gemeinsame Lösungen gefunden werden. Darüber hinaus schafft die Datenschutz-Grundverordnung gleiche Bedingungen für EU-Unternehmen und in Drittländern ansässige Unternehmen, denn Letztere werden dieselben Vorschriften anwenden müssen wie EU-Unternehmen, wenn sie in der EU Waren und Dienstleistungen anbieten oder individuelle Verhaltensweisen beobachten wollen. Ein größeres Vertrauen der Verbraucher kommt sowohl den in der EU als auch den in Drittländern ansässigen Wirtschaftsteilnehmern zugute.

[5] Arbeitsprogramm der Kommission 2017 „Für ein Europa, das schützt, stärkt und verteidigt", COM(2016) 710 final vom 25.10.2016, S. 12 und Anhang 1.

Die Polizei-Richtlinie enthält gemeinsame Regeln für die Verarbeitung personenbezogener Daten von Einzelpersonen – Verdächtigen, Opfern oder Zeugen – im Strafverfahren, wobei den Besonderheiten von Polizei und Strafjustiz Rechnung getragen wird. Die Harmonisierung der Datenschutzvorschriften im Bereich der Strafverfolgung, einschließlich der Bestimmungen für internationale Datenübermittlungen, wird die grenzüberschreitende Zusammenarbeit zwischen Polizei- und Justizbehörden sowohl innerhalb der EU als auch mit den internationalen Partnern erleichtern und dadurch die Voraussetzungen für eine wirksamere Bekämpfung der Kriminalität schaffen. Dies ist ein wichtiger Beitrag zur Europäischen Sicherheitsagenda[6].

2.2 Ein neues und breit gefächertes Instrumentarium für internationale Datenübermittlungen

Von Anfang an waren in den Datenschutzvorschriften der EU verschiedene Möglichkeiten für internationale Datenübermittlungen vorgesehen. Dabei geht es vor allem darum sicherzustellen, dass bei der Übermittlung personenbezogener Daten von Europäern ins Ausland der Schutz der Daten erhalten bleibt. Im Laufe der Jahre entwickelten sich diese Vorschriften zum Maßstab für die Regelungen vieler Länder zum internationalen Datenverkehr. Die Konzeption der neuen EU-Vorschriften für internationale Datenübermittlungen bleibt im Wesentlichen die gleiche wie bei der Richtlinie von 1995, doch durch die Reform wird die Anwendung einfacher und klarer und es werden neue Instrumente für Datenübermittlungen eingeführt.

Gemäß dem EU-Recht besteht eine der Möglichkeiten der Übermittlung personenbezogener Daten in Drittländer darin, dies auf der Grundlage eines „Angemessenheitsbeschlusses“ der Kommission zu tun, in dem festgestellt wird, dass ein Drittland ein Datenschutzniveau vorsieht, das dem Schutz in der EU „der Sache nach gleichwertig“[7] ist. Mit einem solchen Beschluss wird der freie Verkehr personenbezogener Daten in dieses Drittland ermöglicht, ohne dass der Datenexporteur weitere Garantien bieten oder eine Genehmigung einholen muss. Interessierten Ländern und internationalen Organisationen steht ein detaillierter, umfassender Katalog der Elemente zur Verfügung, die die Kommission zu berücksichtigen hat, wenn sie die Angemessenheit des Schutzes, den ein ausländisches System bietet, beurteilt[8]. Die Kommission kann jetzt auch Angemessenheitsbeschlüsse im Bereich der

---

6 Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen „Die Europäische Sicherheitsagenda“, COM(2015) 185 final vom 28.4.2015.

7 Urteil des Gerichtshofs der Europäischen Union vom 6. Oktober 2015 in der Rechtssache C-362/14, Maximilian Schrems gegen Data Protection Commissioner, Randnummern 73, 74 und 96. Siehe auch Erwägungsgrund 104 der Datenschutz-Grundverordnung und Erwägungsgrund 67 der Polizei-Richtlinie, in denen auf ein in der Sache gleichwertiges Schutzniveau verwiesen wird.

8 Siehe Artikel 45 der Datenschutz-Grundverordnung. Gemäß Artikel 45 Absatz 2 muss die Kommission bei ihrer Prüfung unter anderem die Rechtsstaatlichkeit, die Achtung der Menschenrechte und Grundfreiheiten sowie die einschlägigen Rechtsvorschriften berücksichtigen, auch in Bezug auf Datenschutz, öffentliche Sicherheit, Verteidigung, nationale Sicherheit und Strafrecht sowie Zugang der Behörden zu personenbezogenen Daten. Voraussetzungen hierfür sind wirksame und durchsetzbare Rechte, einschließlich verwaltungsrechtlicher und gerichtlicher Rechtsbehelfe für die Betroffenen, und eine gut funktionierende unabhängige Aufsichtsbehörde, die für die Einhaltung und Durchsetzung der Datenschutzbestimmungen sorgt. Die Einhaltung rechtsverbindlicher Übereinkünfte, insbesondere des

Strafverfolgung erlassen.[9] Aufbauend auf der Praxis gemäß der Richtlinie von 1995 sehen die reformierten Bestimmungen außerdem ausdrücklich vor, dass die Angemessenheit für ein bestimmtes Gebiet oder einen bestimmten Sektor oder Wirtschaftszweig in einem Drittland festgestellt werden kann („teilweise“ Angemessenheit).[10]

Wenn kein Angemessenheitsbeschluss erlassen wurde, sind internationale Datenübermittlungen mithilfe einer Reihe alternativer Übermittlungsinstrumente möglich, die einen angemessenen Datenschutz gewährleisten[11]. Die Reform formalisiert und erweitert die Möglichkeiten zur Nutzung der vorhandenen Instrumente wie Standardvertragsklauseln[12] und verbindliche interne Datenschutzvorschriften[13]. Zum Beispiel können Standardvertragsklauseln jetzt in Verträge zwischen in der EU ansässigen Auftragsverarbeitern und Auftragsverarbeitern in Nicht-EU-Ländern aufgenommen werden[14]. Auch die verbindlichen internen Datenschutzvorschriften, die bislang auf Vereinbarungen zwischen Unternehmen derselben Unternehmensgruppe beschränkt waren, können nun von Unternehmen genutzt werden, die als Gruppe eine gemeinsame Wirtschaftstätigkeit ausüben, aber nicht notwendigerweise zur selben Unternehmensgruppe gehören.[15] Mit der Reform wird außerdem der bürokratische Aufwand reduziert, indem Datenübermittlungen in ein Drittland, die sich auf Standardvertragsklauseln oder verbindliche interne Datenschutzvorschriften stützen, nicht mehr grundsätzlich vorab bei den Datenschutzbehörden angemeldet und von ihnen genehmigt werden müssen.[16] Dies stellt eine erhebliche Vereinfachung des EU-Systems für internationale Datenübermittlungen dar, denn die derzeit unterschiedlichen Anforderungen der einzelnen Mitgliedstaaten werden häufig als erhebliches Hindernis für den Datenverkehr gesehen, vor allem von kleineren Unternehmen[17].

Außerdem werden mit der Reform neue Instrumente für internationale Datenübermittlungen eingeführt.[18] Die für die Datenverarbeitung Verantwortlichen und die Auftragsverarbeiter

---

Übereinkommens Nr. 108 des Europarats und die Beteiligung an multilateralen oder regionalen Systemen für den Datenschutz werden ebenfalls berücksichtigt.

9 Polizei-Richtlinie: Die Kriterien für die Prüfung der Angemessenheit sind in Artikel 36 Absatz 2 festgelegt.

10 Siehe Artikel 45 Absatz 1 der Datenschutz-Grundverordnung und Artikel 36 Absatz 1 der Polizei-Richtlinie.

11 Siehe z. B. Mitteilung der Kommission an das Europäische Parlament und den Rat zu der Übermittlung personenbezogener Daten aus der EU in die Vereinigten Staaten von Amerika auf der Grundlage der Richtlinie 95/46/EG nach dem Urteil des Gerichtshofs in der Rechtssache C-362/14 (Schrems), COM(2015) 566 final vom 6.11.2015.

12 Die Standardvertragsklauseln nennen die jeweiligen Datenschutzverpflichtungen des Datenexporteurs in der EU und des Datenimporteurs in einem Drittland.

13 Die verbindlichen internen Datenschutzvorschriften sind interne Regeln, die eine multinationale Unternehmensgruppe für Datenübermittlungen an ihr angehörende Unternehmen mit Standort in Ländern festlegt, in denen kein angemessenes Schutzniveau gewährleistet ist. Zwar werden verbindliche interne Datenschutzvorschriften bereits auf der Grundlage der Richtlinie von 1995 genutzt, doch wird ihre Rolle als Instrument für die Datenübermittlung mit der Datenschutz-Grundverordnung kodifiziert und formalisiert.

14 Siehe Artikel 46 Absatz 2 Buchstaben c und d sowie Erwägungsgrund 168 der Datenschutz-Grundverordnung.

15 Siehe Artikel 46 Absatz 2 Buchstabe b, Artikel 47 und Erwägungsgrund 110 der Datenschutz-Grundverordnung.

16 Siehe Artikel 46 Absatz 2 der Datenschutz-Grundverordnung.

17 Dass Registrierungsanforderungen ein Handelshemmnis für viele Unternehmen, insbesondere KMU, darstellen, wurde z. B. im UNCTAD-Bericht (S. 34) hervorgehoben.

18 Siehe Artikel 46 Absatz 2 Buchstaben e und f der Datenschutz-Grundverordnung.

werden unter bestimmten Voraussetzungen[19] genehmigte Verhaltensregeln oder Zertifizierungsverfahren (z. B. Datenschutzsiegel oder -prüfzeichen) verwenden können, um für „geeignete Garantien“ zu sorgen. Dies dürfte die Entwicklung von stärker maßgeschneiderten Lösungen für internationale Datenübermittlungen ermöglichen, die beispielsweise den Besonderheiten und Bedürfnissen eines bestimmten Sektors/Wirtschaftszweigs oder bestimmter Datenströme Rechnung tragen. Ferner wird es so möglich, geeignete Garantien für die Übermittlung von Daten zwischen Behörden oder öffentlichen Stellen auf der Grundlage internationaler Übereinkünfte oder Verwaltungsvereinbarungen vorzusehen[20]. Schließlich sind in der Datenschutz-Grundverordnung sogenannte „Ausnahmen“[21] (z. B. Einwilligung, Erfüllung eines Vertrags oder wichtige Gründe des öffentlichen Interesses) vorgesehen, die es Einrichtungen erlauben, in bestimmten Situationen ihre Datenübermittlungen auch ohne Angemessenheitsbeschluss und unabhängig vom Rückgriff auf eines der oben genannten Instrumente vorzunehmen. Insbesondere enthält die Verordnung eine neue, wenn auch begrenzte Ausnahmeregelung für Übermittlungen zur Wahrung der berechtigten Interessen[22] eines Unternehmens.

Schließlich ermöglicht die Reform der Kommission die Entwicklung von Mechanismen der internationalen Zusammenarbeit, um die Durchsetzung von Datenschutzvorschriften zu erleichtern, unter anderem durch Amtshilfevereinbarungen.[23] Damit wird der Beitrag anerkannt, den eine engere Zusammenarbeit zwischen den Aufsichtsbehörden auf internationaler Ebene leisten könnte, um sowohl für einen wirksameren Schutz der individuellen Rechte als auch für eine größere Rechtssicherheit für Unternehmen zu sorgen.

3. INTERNATIONALE DATENÜBERMITTLUNGEN IN DER WIRTSCHAFT: ERLEICHTERUNG DES HANDELS DURCH SCHUTZ DER PRIVATSPHÄRE

Die Achtung der Privatsphäre ist eine Voraussetzung für stabile, sichere und wettbewerbsfähige globale Handelsströme. Die Privatsphäre ist keine Handelsware.[24] Das Internet und die Digitalisierung von Waren und Dienstleistungen hat die Weltwirtschaft verändert, und die grenzüberschreitende Übermittlung von Daten, einschließlich personenbezogener Daten, gehört zum Geschäftsalltag der europäischen Unternehmen aller Größen und Branchen. Da der Handelsverkehr zunehmend mit der Übermittlung personenbezogener Daten verbunden ist, sind der Schutz und die Sicherheit dieser Daten zu einem ausschlaggebenden Faktor für das Vertrauen der Verbraucher geworden. So geben beispielsweise zwei Drittel der Europäer an, es bereite ihnen Sorge, dass sie keine Kontrolle über die von ihnen im Internet bereitgestellten Informationen haben, und die Hälfte der

---

19 Verantwortliche in Drittländern können dann mittels vertraglicher oder sonstiger rechtlich bindender Zusagen, dass sie die Datenschutzbestimmungen dieser Instrumente anwenden, die verbindliche und durchsetzbare Verpflichtung eingehen, Verhaltensregeln oder ein Zertifizierungsverfahren der EU einzuhalten. Siehe Artikel 42 Absatz 2 der Datenschutz-Grundverordnung.

20 Siehe Artikel 46 Absatz 2 Buchstabe a und Absatz 3 Buchstabe b der Datenschutz-Grundverordnung.

21 Siehe Artikel 49 der Datenschutz-Grundverordnung.

22 Siehe Artikel 49 Absatz 1 Unterabsatz 2.

23 Siehe Artikel 50 der Datenschutz-Grundverordnung.

24 Siehe z. B. Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen „Handel für alle – Hin zu einer verantwortungsbewussteren Handels- und Investitionspolitik“, COM(2015) 497 final vom 14.10.2015, S. 7.

Befragten befürchtet, sie könnten einem Betrug zum Opfer fallen.[25] Gleichzeitig sehen sich europäische Unternehmen, die in bestimmten Drittländern tätig sind, zunehmend mit protektionistischen Beschränkungen konfrontiert, die sich nicht durch den legitimen Schutz der Privatsphäre rechtfertigen lassen.

Im digitalen Zeitalter müssen die Förderung eines hohen Maßes an Datenschutz und die Erleichterung des internationalen Handels daher Hand in Hand gehen. Da der Schutz personenbezogener Daten in Handelsübereinkünften nicht verhandelbar ist[26], umfassen die EU-Regeln für internationale Datenübermittlungen wie oben dargelegt ein breit gefächertes Instrumentarium, um den Datenverkehr in verschiedenen Situationen zu ermöglichen und gleichzeitig ein hohes Schutzniveau zu gewährleisten.

3.1. Angemessenheitsbeschlüsse

Eine Angemessenheitsfeststellung ermöglicht den freien Verkehr personenbezogener Daten aus der EU in Drittländer, ohne dass der EU-Datenexporteur zusätzliche Garantien bieten muss oder zusätzlichen Bedingungen unterliegt. Mit einem solchen Beschluss wird festgestellt, dass die Rechtsordnung des betreffenden Landes ein angemessenes Schutzniveau bietet, und somit anerkannt, dass sein System mit dem der EU-Mitgliedstaaten vergleichbar ist. Auf dieser Grundlage werden Datenübermittlungen in dieses Land Datenübermittlungen innerhalb der EU gleichgestellt, woraus ein bevorrechtigter Zugang zum Binnenmarkt der EU resultiert, der Handelskanäle für EU-Wirtschaftsteilnehmer eröffnet. Wie oben dargelegt, erfordert diese Anerkennung ein Schutzniveau, das dem innerhalb der Union gewährleisteten Schutzniveau der „Sache nach gleichwertig“[27] ist. Dazu bedarf es einer umfassenden Bewertung des Systems des Drittlands, einschließlich seiner Vorschriften über den Zugang zu personenbezogenen Daten durch öffentliche Behörden zu Zwecken der Rechtsdurchsetzung, der nationalen Sicherheit und anderen Zwecken des öffentlichen Interesses.

Allerdings erfordert die Angemessenheitsfeststellung keine Eins-zu-eins-Übereinstimmung mit den EU-Vorschriften, wie 2015 vom Gerichtshof im *Schrems*-Urteil bestätigt wurde[28]. Die Frage ist vielmehr, ob das ausländische System insgesamt aufgrund des Wesensgehalts der Rechte auf Privatsphäre sowie ihrer wirksamen Anwendung, Durchsetzbarkeit und Überwachung das erforderliche hohe Maß an Schutz bietet. Die bisher angenommenen Angemessenheitsbeschlüsse zeigen, dass es der Kommission möglich ist, eine breite Palette von Systemen für den Schutz der Privatsphäre, die auf verschiedenen Rechtstraditionen beruhen, als angemessen anzuerkennen. Diese Beschlüsse betreffen Länder, die eng mit der Europäischen Union und ihren Mitgliedstaaten verbunden sind (Schweiz, Andorra, die Färöer, Guernsey, Jersey, Insel Man), wichtige Handelspartner (Argentinien, Kanada, Israel, die Vereinigten Staaten) und Länder, die eine Vorreiterrolle bei der Entwicklung von Datenschutzgesetzen in ihrer Region spielen (Neuseeland, Uruguay).

---

25 Special Eurobarometer 431 - Data protection (Juni 2015).

26 Politische Leitlinien von Präsident Juncker: *Ein neuer Start für Europa: Meine Agenda für Jobs, Wachstum, Fairness und demokratischen Wandel.*

27 Siehe Fußnote 7.

28 Siehe Punkt 74 des *Schrems*-Urteils.

Bei den Beschlüssen betreffend Kanada und die Vereinigten Staaten handelt es sich um Feststellungen einer „teilweisen" Angemessenheit. Der Beschluss betreffend Kanada gilt nur für private Unternehmen, die unter den „Personal Information Protection and Electronic Documents Act" fallen. Bei dem unlängst angenommenen Beschluss über den EU-US-Datenschutzschild[29] handelt es sich um einen spezifischen Fall, da er sich in Ermangelung allgemeiner Datenschutzvorschriften in den USA[30] auf Verpflichtungen der beteiligten Unternehmen stützt, die in dieser Regelung vorgesehenen hohen Datenschutzstandards anzuwenden, die dann auch nach US-Recht durchsetzbar sind. Darüber hinaus stützt sich der Datenschutzschild auf die spezifischen Erklärungen und Zusicherungen der US-Regierung in Bezug auf den Zugang zu Zwecken der nationalen Sicherheit[31], die die Angemessenheitsfeststellung untermauern. Die Einhaltung dieser Verpflichtungen wird von der Kommission genau überwacht werden und Teil der jährlichen Überprüfung des Funktionierens des Rechtsrahmens sein.

In den vergangenen Jahren haben weltweit immer mehr Länder neue Vorschriften über den Datenschutz und die Privatsphäre erlassen oder einen entsprechenden Prozess in Gang gesetzt. 2015 verfügten insgesamt 109 Länder über Datenschutzgesetze, ein erheblicher Anstieg gegenüber den 76 Ländern, die Mitte 2011 gezählt wurden[32]. Rund 35 weitere Länder arbeiten derzeit Entwürfe für Datenschutzgesetze aus[33]. Diese neuen oder modernisierten Rechtsvorschriften beruhen in der Regel auf einer Reihe gemeinsamer Grundsätze, darunter die Anerkennung des Datenschutzes als Grundrecht, die Annahme übergreifender Rechtsvorschriften auf diesem Gebiet, das Vorhandensein durchsetzbarer individueller Rechte auf Privatsphäre und die Errichtung einer unabhängigen Aufsichtsbehörde. Dies bietet neue Möglichkeiten für die weitere Erleichterung des Datenverkehrs – insbesondere durch Angemessenheitsfeststellungen – bei gleichzeitiger Gewährleistung eines kontinuierlich hohen Niveaus des Schutzes personenbezogener Daten.

Nach EU-Recht setzt eine Angemessenheitsfeststellung voraus, dass Datenschutzvorschriften vorhanden sind, die mit denen der EU vergleichbar sind[34]. Dies betrifft sowohl den umfassenden Schutz personenbezogener Daten als auch die entsprechenden Aufsichts- und Rechtsbehelfsmechanismen des Drittlands.

---

29 Durchführungsbeschluss (EU) 2016/1250 vom 12. Juli 2016.

30 Die Kommission fordert die USA auf, ihre Bemühungen um die Schaffung eines umfassenden Systems für den Schutz der Privatsphäre und den Datenschutz fortzusetzen, das auf längere Sicht Konvergenz zwischen den Systemen beider Seiten ermöglicht. Siehe Mitteilung der Kommission an das Europäische Parlament und den Rat: Transatlantischer Datenaustausch: Wiederherstellung des Vertrauens durch starke Schutzvorkehrungen, COM(2016) 117 final vom 29.2.2016.

31 Dazu zählt insbesondere die Anwendung der „Presidential Policy Directive 28" (PPD-28), die eine Reihe von Einschränkungen und Garantien für Maßnahmen der „Signalaufklärung" sowie die Ernennung eines eigenen Ombudsmannes für Beschwerden von Personen aus der EU auf diesem Gebiet vorsieht.

32 G. Greenleaf, „Global data privacy laws 2015: 109 countries, with European laws now in a minority", (2015) 133 Privacy Laws & Business International Report, 14-17.

33 UNCTAD-Studie, S. 8 und 42 (siehe Fußnote 4).

34 In diesem Zusammenhang berücksichtigt die Kommission bei der Beurteilung der Angemessenheit auch die Verpflichtungen des Drittlands aus rechtsverbindlichen Übereinkünften, insbesondere ob es Vertragspartei des Übereinkommens Nr. 108 des Europarats und seines Zusatzprotokolls ist. Siehe Artikel 45 Absatz 2 Buchstabe c und Erwägungsgrund 105 der Datenschutz-Grundverordnung.

Im Rahmen ihrer Regelung für Angemessenheitsfeststellungen sollten nach Ansicht der Kommission folgende Kriterien zugrunde gelegt werden, wenn geprüft wird, mit welchen Drittländern ein Dialog über die Angemessenheit des Schutzniveaus geführt werden sollte[35]:

i) der Umfang der (tatsächlichen oder potenziellen) Handelsbeziehungen der EU zu dem jeweiligen Drittland, einschließlich der Frage, ob ein Freihandelsabkommen besteht oder entsprechende Verhandlungen im Gange sind,

ii) der Umfang der Übermittlung personenbezogener Daten aus der EU in das Drittland, der die geografischen und/oder kulturellen Bindungen widerspiegelt,

iii) die Vorreiterrolle des Drittlandes im Bereich des Schutzes der Privatsphäre und des Datenschutzes, die als Modell für andere Länder in der Region dienen könnte,[36] und

iv) die allgemeinen politischen Beziehungen zu dem Drittland, insbesondere in Bezug auf die Förderung gemeinsamer Werte und Ziele auf internationaler Ebene.

Auf der Grundlage dieser Erwägungen wird die Kommission aktiv mit den wichtigsten Handelspartnern in Ost- und Südostasien zusammenarbeiten, 2017 zunächst mit Japan und Korea[37] sowie – abhängig von Fortschritten bei der Modernisierung der Datenschutzvorschriften – mit Indien, aber auch mit Ländern in Lateinamerika (insbesondere Mercosur-Ländern) und in der Europäischen Nachbarschaft, die Interesse an einer „Angemessenheitsfeststellung“ geäußert haben. Die Kommission begrüßt ferner Interessenbekundungen aus anderen Drittländern, die bereit sind, in diesen Fragen zusammenzuarbeiten. Die Gespräche über eine mögliche Angemessenheitsfeststellung müssen beiden Seiten gerecht werden, alle notwendigen Klarstellungen in Bezug auf die Datenschutzvorschriften der EU liefern und der Erkundung von Möglichkeiten dienen, die Konvergenz der Rechtsvorschriften und Vorgehensweisen der Drittländer zu verbessern.

In bestimmten Fällen kann es angebracht sein, statt eines landesweiten Ansatzes andere Optionen zu nutzen, wie eine teilweise oder sektorspezifische Angemessenheitsfeststellung (z. B. für Finanzdienstleistungen oder IT-Sektoren), die geografische Gebiete oder auch Industriezweige betreffen kann, die einen wichtigen Teil der Wirtschaft des jeweiligen Drittlands darstellen. Dies muss vor dem Hintergrund von Aspekten geprüft werden wie beispielsweise Art und Stand der Regelung für den Schutz der Privatsphäre (eigenständiges Gesetz, mehrere oder sektorale Gesetze usw.), verfassungsrechtliche Struktur des Drittlandes oder besonders hohes Aufkommen des Datenverkehrs aus der EU in bestimmten Wirtschaftszweigen.

---

[35] Bei Ländern, mit denen ein einschlägiges Interesse an einer Zusammenarbeit im Bereich innere Sicherheit und Rechtsdurchsetzung besteht, wird die Kommission die Möglichkeit spezifischer Angemessenheitsfeststellungen im Rahmen der Polizei-Richtlinie prüfen (siehe Abschnitt 4).

[36] Dies könnte insbesondere für Entwicklungs- und Schwellenländer gelten, da der Schutz personenbezogener Daten sowohl ein zentrales Element der Rechtsstaatlichkeit als auch ein wichtiger Faktor für die Wettbewerbsfähigkeit der Wirtschaft ist.

[37] Japan und Korea haben in jüngster Zeit Rechtsvorschriften erlassen bzw. modernisiert, um umfassende Datenschutzregelungen einzuführen.

Die Annahme eines Angemessenheitsbeschlusses erfordert die Aufnahme eines spezifischen Dialogs und enger Formen der Zusammenarbeit mit dem betreffenden Drittland. Angemessenheitsbeschlüsse sind „lebendige“ Dokumente, die von der Kommission genau überwacht und angepasst werden müssen, falls es in dem betreffenden Drittland zu Neuentwicklungen hinsichtlich des Datenschutzniveaus kommt[38]. Zu diesem Zweck werden mindestens alle vier Jahre periodische Überprüfungen stattfinden, um die aufgetretenen Fragen zu erörtern und bewährte Methoden zwischen engen Partnern auszutauschen[39]. Dieses dynamische Konzept gilt auch für bereits nach der Richtlinie von 1995 angenommene Angemessenheitsbeschlüsse, die überprüft werden müssen, falls sie dem geltenden Standard nicht mehr entsprechen[40]. Die betreffenden Drittländer werden daher ersucht, die Kommission von sämtlichen einschlägigen Änderungen in Recht und Praxis zu unterrichten, die seit der Annahme des Angemessenheitsbeschlusses erfolgt sind. Dies ist von wesentlicher Bedeutung, um die Kontinuität dieser Beschlüsse im Rahmen der neuen reformierten Vorschriften sicherzustellen[41].

Die EU-Datenschutzvorschriften dürfen nicht Gegenstand von Verhandlungen über Freihandelsabkommen sein[42]. Auch wenn der Dialog über den Datenschutz und die Handelsverhandlungen mit Drittländern getrennt stattfinden müssen, ist ein Beschluss über die Angemessenheit – auch teilweiser oder sektorspezifischer Art – der beste Weg, um gegenseitiges Vertrauen aufzubauen, einen reibungslosen Verkehr personenbezogener Daten zu gewährleisten und damit Handelsströme zu erleichtern, die die Übermittlung personenbezogener Daten an das betreffende Drittland umfassen. Solche Beschlüsse können daher Handelsverhandlungen erleichtern oder bestehende Handelsabkommen ergänzen und so deren Nutzen verstärken. Durch die Förderung der Konvergenz der Schutzniveaus in der EU und dem Drittland verringert eine Angemessenheitsfeststellung gleichzeitig das Risiko, dass dieses Land Gründe des Schutzes personenbezogener Daten geltend macht, um ungerechtfertigte Datenlokalisierungs- und -speicherungsanforderungen aufzuerlegen. Wie in der Mitteilung „Handel für alle“ dargelegt, wird die Kommission darüber hinaus – unter strikter Einhaltung und unbeschadet der EU-Datenschutzvorschriften – die Handelsabkommen der EU nach Möglichkeit dazu nutzen, Vorschriften für den

---

38 Nach Artikel 45 Absätze 4 und 5 der Datenschutz-Grundverordnung überwacht die Kommission fortlaufend die Entwicklungen in Drittländern und hat die Befugnis, Angemessenheitsbeschlüsse zu widerrufen, zu ändern oder auszusetzen, wenn sie feststellt, dass das betreffende Land kein angemessenes Schutzniveau mehr gewährleistet.

39 Artikel 45 Absatz 3 der Datenschutz-Grundverordnung.

40 Nach Artikel 97 Absatz 2 Buchstabe a der Datenschutz-Grundverordnung übermittelt die Kommission 2020 einen Bewertungsbericht an das Europäische Parlament und den Rat.

41 Als Konsequenz aus dem *Schrems*-Urteil, in dem festgestellt wurde, dass die Kommission ihre Kompetenzen überschritten hat, als sie mit der Safe-Harbor-Entscheidung die Befugnisse der Datenschutzbehörden einschränkte, Datenübermittlungen auszusetzen oder zu verbieten, erließ die Kommission am 16. Dezember 2016 einen „Omnibus“-Änderungsbeschluss, dem zufolge ähnliche Bestimmungen in Angemessenheitsbeschlüssen gestrichen und durch Bestimmungen ersetzt werden, die lediglich Informationspflichten zwischen den Mitgliedstaaten und der Kommission für Fälle vorsehen, in denen eine Datenschutzbehörde Datenübermittlungen in Drittländer aussetzt oder verbietet. Mit diesem Omnibus-Beschluss wird auch die Verpflichtung der Kommission eingeführt, entsprechende Entwicklungen in dem Drittland zu überwachen. Siehe ABl. L 344 vom 17.12.2016, S. 83.

42 Vor allem ist eine Angemessenheitsfeststellung ein einseitiger Durchführungsbeschluss der Kommission, der im Einklang mit dem EU-Datenschutzrecht steht und sich auf die darin enthaltenen Kriterien stützt.

elektronischen Geschäftsverkehr und den grenzüberschreitenden Datenverkehr festzulegen und gegen neue Formen des digitalen Protektionismus vorzugehen[43].

Die Kommission wird

- Beratungen über etwaige Angemessenheitsbeschlüsse für die wichtigsten Handelspartner in Ost- und Südostasien – beginnend mit Japan und Korea im Jahr 2017, aber möglicherweise auch für andere strategisch wichtige Partner wie Indien –, für Länder in Lateinamerika, insbesondere die Mercosur-Länder, und Länder der europäischen Nachbarschaft Vorrang einräumen,

- das Funktionieren der bestehenden Angemessenheitsbeschlüsse sorgfältig überwachen; dies bezieht sich insbesondere auf die Umsetzung des EU-US-Datenschutzschilds, vor allem durch den Mechanismus der gemeinsamen jährlichen Überprüfung,

- mit Ländern, die an der Annahme solider Datenschutzvorschriften interessiert sind, zusammenarbeiten, sie unterstützen und die Konvergenz ihrer Vorschriften mit den Datenschutzgrundsätzen der EU fördern.

3.2. Alternative Mechanismen für die Datenübermittlung

In den Datenschutzvorschriften der EU wurde stets anerkannt, dass es keine Patentlösung für internationale Datenübermittlungen gibt. Dies gilt erst recht für die aus der Reform hervorgegangenen Vorschriften. Auch wenn Angemessenheitsfeststellungen nur für diejenigen Drittländer verfügbar sein werden, die die einschlägigen Kriterien erfüllen, bietet die Datenschutz-Grundverordnung eine Vielfalt von Mechanismen, die so flexibel sind, dass sie an alle möglichen unterschiedlichen Fälle der Datenübermittlung angepasst werden können. Es können Instrumente entwickelt werden, die den besonderen Bedürfnissen oder Anforderungen bestimmter Industriezweige, Geschäftsmodelle und/oder Wirtschaftsteilnehmer Rechnung tragen. Dabei könnte es sich beispielsweise um Standardvertragsklauseln handeln, die auf die Anforderungen eines bestimmten Sektors zugeschnitten sind (z. B. spezifische Garantien für die Verarbeitung sensibler Daten im Gesundheitssektor) oder sich auf spezifische Arten von Verarbeitungsvorgängen beziehen, die in bestimmten Drittländern vorwiegend genutzt werden (z. B. Auslagerung von Dienstleistungen, die für europäische Unternehmen durchgeführt werden). Zu diesem Zweck könnten entweder neue Standardklauseln angenommen werden oder bestehende Klauseln durch zusätzliche Garantien ergänzt werden, die von technischen über organisatorische bis hin zu auf das jeweilige Geschäftsmodell bezogenen Lösungen reichen könnten.[44] Auf bestimmte sektorale Anforderungen kann durch verbindliche interne Datenschutzvorschriften eingegangen werden, die für Gruppen von Unternehmen gelten, die an einer gemeinsamen Wirtschaftstätigkeit beteiligt sind, beispielsweise in der Reiseindustrie. Für internationale

[43] Siehe Mitteilung „Handel für alle“, S. 12 (Fußnote 24).

[44] Siehe Artikel 46 Absatz 2 Buchstaben c und d sowie Erwägungsgrund 109 der Datenschutz-Grundverordnung, in denen ausgeführt wird, dass Anpassungen genehmigter Musterklauseln möglich sind, solange diese weder mittelbar noch unmittelbar im Widerspruch zu den Musterklauseln stehen noch die Grundrechte und Grundfreiheiten der betroffenen Personen beschneiden.

Datenübermittlungen zwischen Auftragsverarbeitern könnte die Entwicklung von eigens dafür vorgesehenen Standardvertragsklauseln und/oder von verbindlichen internen Datenschutzvorschriften für Auftragsverarbeiter nützlich sein. Schließlich bieten neue Übermittlungsmechanismen – wie genehmigte Verhaltensregeln und Zertifizierungen für akkreditierte Dritte – der Industrie die Möglichkeit, maßgeschneiderte Lösungen für internationale Datenübermittlungen einzuführen, wobei ihnen gleichzeitig die Wettbewerbsvorteile zugute kommen, die beispielsweise mit einem Datenschutzsiegel oder -prüfzeichen verbunden sind. Einige dieser Instrumente können als übermittlungsspezifische Mechanismen oder als Teil allgemeinerer Instrumente konzipiert werden, mit denen die Einhaltung aller Bestimmungen der Datenschutz-Grundverordnung nachgewiesen wird, wie etwa genehmigte Verhaltensregeln.

Die Kommission wird mit der Industrie, der Zivilgesellschaft und den Datenschutzbehörden zusammenarbeiten, damit bei internationalen Datenübermittlungen das volle Potenzial des Instrumentariums der Datenschutz-Grundverordnung ausgeschöpft werden kann. Der laufende Dialog mit den Interessenträgern im Rahmen der Durchführung der Reform wird einen Beitrag zur Ermittlung der diesbezüglichen Handlungsprioritäten leisten. Eine davon könnte der Abschluss bereits begonnener Arbeiten sein, wie die Erstellung von Standardvertragsklauseln für Verträge zwischen Auftragsverarbeitern in Zusammenarbeit mit der Artikel-29-Datenschutzgruppe (die 2018 durch den Europäischen Datenschutzausschuss ersetzt wird)[45]. Denkbar wäre auch die Entwicklung neuer Komponenten der EU-Infrastruktur für die Einhaltung der Vorschriften, indem die Kommission beispielsweise Anforderungen und technische Standards für die Schaffung und Funktionsweise von Zertifizierungsverfahren festlegt, einschließlich der Aspekte, die internationale Datenübermittlungen betreffen[46]. Einige dieser Maßnahmen können durch Arbeiten auf internationaler Ebene ergänzt werden, insbesondere mit Organisationen, die ähnliche Verfahren für Datenübermittlungen entwickelt haben. So könnte beispielsweise geprüft werden, wie die Konvergenz zwischen verbindlichen internen Datenschutzvorschriften nach EU-Recht und den Cross Border Privacy Rules der APEC (Asiatisch-Pazifische Wirtschaftskooperation)[47] gefördert werden kann, sowohl hinsichtlich der anzuwendenden Standards als auch hinsichtlich der Anwendungsverfahren des jeweiligen Systems. Dies dürfte zur Förderung weltweit hoher Datenschutzstandards bei gleichzeitiger Annäherung der unterschiedlichen Ansätze für den Schutz der Privatsphäre und den Datenschutz beitragen, es den Wirtschaftsteilnehmern erleichtern, zwischen verschiedenen Systemen zu wechseln, und zur Erarbeitung entsprechender Politikkonzepte führen.

---

45 Derzeit existieren keine Standardvertragsklauseln für Verträge zwischen Auftragsverarbeitern in der EU und Auftragsverarbeitern in Drittländern.

46 Artikel 43 Absätze 8 und 9 der Datenschutz-Grundverordnung.

47 Siehe Gemeinsame Referenzgrundlage APEC/EU von 2014 für die Struktur der verbindlichen internen Datenschutzvorschriften der EU und der Cross Border Privacy Rules (CBPR) der APEC, in der die Anforderungen beider Systeme hinsichtlich Regelkonformität und Zertifizierung verglichen werden: http://www.apec.org/~/media/Files/Groups/ECSG/20140307_Referential-BCR-CBPR-reqs.pdf.

Die Kommission wird

- mit den Interessenträgern zusammenarbeiten, um alternative Verfahren für die Übermittlung personenbezogener Daten zu entwickeln, die den besonderen Bedürfnissen oder Anforderungen bestimmter Industriezweige, Geschäftsmodelle und/oder Wirtschaftsteilnehmer angepasst sind.

3.3 Internationale Zusammenarbeit zum Schutz personenbezogener Daten

3.3.1. Förderung von Datenschutzstandards im Rahmen multilateraler Instrumente und Foren

Der EU-Rechtsrahmen für den Datenschutz dient Drittländern oft als Bezugsgrundlage für die Ausarbeitung von Rechtsvorschriften in diesem Bereich. Die EU wird den Dialog mit ihren internationalen Partnern auf bilateraler wie multilateraler Ebene aktiv fortsetzen, um die Konvergenz durch die Entwicklung hoher interoperabler Standards für den Schutz personenbezogener Daten zu fördern. Dies trägt zu einem wirksameren Schutz der Rechte von Personen und gleichzeitig zum Abbau der Hindernisse für den grenzüberschreitenden Datenverkehr als wichtigem Element des freien Handels bei.

Insbesondere fördert die Kommission den Beitritt von Drittstaaten zum Übereinkommen Nr. 108 des Europarats und seinem Zusatzprotokoll.[48] Das Übereinkommen, das auch Nichtmitgliedern des Europarats offensteht und bereits von 50 Ländern ratifiziert wurde, darunter von einigen afrikanischen und südamerikanischen Staaten[49], stellt das einzige verbindliche multilaterale Instrument auf dem Gebiet des Datenschutzes dar. Es wird derzeit überarbeitet, und die Kommission wird die zügige Annahme der modernisierten Fassung aktiv fördern, damit die EU Vertragspartei werden kann. Das Übereinkommen wird dieselben Grundsätze widerspiegeln, die auch in den neuen EU-Datenschutzvorschriften enthalten sind, und somit zur Konvergenz mit Blick auf einen Katalog hoher Datenschutzstandards beitragen.

Der G20-Gipfel im Jahr 2017 wird der EU eine weitere Gelegenheit bieten, auf Konvergenz bezüglich des Grundsatzes hinzuarbeiten, dass hohe Datenschutzstandards ein wesentliches Element bei der Weiterentwicklung einer globalen Informationsgesellschaft darstellen, die in der Lage ist, Innovation, Wachstum und sozialen Wohlstand zu fördern[50].

Die Kommission sieht auch der Zusammenarbeit mit wichtigen neuen Akteuren wie dem Sonderberichterstatter der Vereinten Nationen für das Recht auf Privatheit[51] sowie einem weiteren Ausbau der Arbeitsbeziehungen mit regionalen Organisationen wie der APEC

[48] Übereinkommen des Europarats vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (SEV Nr. 108) und Zusatzprotokoll von 2001 zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Kontrollstellen und grenzüberschreitendem Datenverkehr (SEV Nr. 181).

[49] Mauritius, Senegal und Uruguay haben das Übereinkommen ratifiziert. Darüber hinaus wurden Cabo Verde, Marokko und Tunesien zum Beitritt aufgefordert.

[50] Siehe auch OECD-Ministererklärung vom 23. Juni 2016 über Innovation, Wachstum und sozialen Wohlstand in der digitalen Wirtschaft („Erklärung von Cancún“).

[51] Siehe http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx.

erwartungsvoll entgegen. Ziel ist es, eine weltweite Kultur der Achtung der Rechte auf Privatsphäre und den Schutz personenbezogener Daten zu fördern.

Als Teil ihrer umfassenderen Bemühungen um die Verbesserung des Bewusstseins für die Privatsphäre und die Stärkung der Datenschutzgarantien weltweit billigte die Europäische Kommission am 15. November 2016 ein Projekt im Rahmen des Partnerschaftsinstruments, mit dem die Zusammenarbeit mit den Partnerländern in diesem Bereich vertieft werden soll[52]. Darunter fällt beispielsweise die Finanzierung von Ausbildungs- und Sensibilisierungsmaßnahmen. Im Gegenzug profitiert die EU im Rahmen der Umsetzung der Reform vom Austausch bewährter Methoden und von den Erfahrungen anderer mit neuen Herausforderungen beim Schutz der Privatsphäre und mit neuentwickelten rechtlichen oder technischen Lösungen, auch im Hinblick auf die Durchsetzung, die Instrumente für die Einhaltung der Vorschriften (z. B. Zertifizierungsverfahren, Abschätzungen der Folgen für die Privatsphäre) oder den Schutz bestimmter Datensätze (z. B. Daten von Kindern).

3.3.2. Zusammenarbeit bei der Rechtsdurchsetzung

Angesichts der globalen Reichweite multinationaler Unternehmen, die riesige Mengen von personenbezogenen Daten in einer Vielzahl von Ländern verarbeiten, wächst das Erfordernis, die Zusammenarbeit mit den für den Schutz der Privatsphäre zuständigen Durchsetzungs- und Aufsichtsbehörden von Drittländern zu vertiefen. Durch Probleme der Nichteinhaltung der Datenschutzvorschriften oder Verstöße gegen den Datenschutz werden häufig Menschen in mehr als einem Rechtsraum beeinträchtigt. In solchen Fällen könnte der Schutz von Personen durch gemeinsame Maßnahmen wirksamer gestaltet werden. Ein klareres rechtliches Umfeld, in dem gemeinsame Auslegungsinstrumente und Durchsetzungsmethoden auf globaler Ebene entwickelt werden, würde gleichzeitig auch den Wirtschaftsteilnehmern zugute kommen.

In der grenzfreien und vernetzten Welt des Datenverkehrs ist es daher an der Zeit, die Zusammenarbeit zwischen den Durchsetzungsbehörden zu verstärken[53]. Die EU ist bereit, ihren Beitrag zu leisten. Wie oben erwähnt, ermöglicht die Datenschutz-Grundverordnung der Kommission, Mechanismen der internationalen Zusammenarbeit zu entwickeln, um die wirksame Durchsetzung von Rechtsvorschriften zum Schutz personenbezogener Daten zu erleichtern, unter anderem durch Regelungen über gegenseitige Amtshilfe. In diesem Kontext sollte die Möglichkeit der Ausarbeitung eines Rahmenübereinkommens für die Zusammenarbeit zwischen den Datenschutzbehörden der EU und den Durchsetzungsbehörden bestimmter Drittländer geprüft werden, wobei auch die Erfahrungen der Kommission in

---

[52] Durchführungsbeschluss C(2016) 7198 der Kommission zur Billigung der zweiten Phase des Jahresaktionsprogramms 2016 (JAP 2016) im Rahmen des Partnerschaftsinstruments.

[53] Zu den bestehenden Netzen gehört das Global Privacy Enforcement Network (GPEN), das 2010 unter Schirmherrschaft der OECD ins Leben gerufen wurde. Dabei handelt es sich um ein informelles Netz von für den Schutz der Privatsphäre zuständigen Durchsetzungsbehörden, an dem die EU-Datenschutzbehörden beteiligt sind und das unter anderem mit der Zusammenarbeit bei der Rechtsdurchsetzung, dem Austausch bewährter Methoden bei der Bewältigung grenzübergreifender Herausforderungen und der Unterstützung gemeinsamer Durchsetzungsinitiativen und Sensibilisierungskampagnen beauftragt ist. Es ist nicht mit neuen rechtsverbindlichen Verpflichtungen der Beteiligten verbunden und legt den Schwerpunkt auf die Erleichterung der Zusammenarbeit bei der Durchsetzung der Datenschutzgesetze für den Privatsektor. Siehe https://privacyenforcement.net/.

anderen Bereichen der Rechtsdurchsetzung, wie Wettbewerb und Verbraucherschutz, genutzt werden können.

Die Kommission wird

- die rasche Verabschiedung der modernisierten Fassung des Europarats-Übereinkommens Nr. 108 mit dem Ziel des Beitritts der EU als Vertragspartei fördern und Drittländer ebenfalls zum Beitritt ermutigen,

- multilaterale Foren wie die Vereinten Nationen, die G20 und die APEC nutzen, um eine weltweite Kultur der Achtung der Datenschutzrechte zu fördern,

- Mechanismen für die internationale Zusammenarbeit mit wichtigen internationalen Partnern entwickeln, um eine wirksame Durchsetzung zu erleichtern.

4. WIRKSAMERE ZUSAMMENARBEIT BEI DER RECHTSDURCHSETZUNG UND SOLIDE DATENSCHUTZGARANTIEN

Der Austausch personenbezogener Daten ist ein fester Bestandteil der Verhütung, Ermittlung und Verfolgung von Straftaten. In einer vernetzten Welt, in der Kriminalität in der Regel nicht an nationalen Grenzen haltmacht, ist ein rascher Austausch personenbezogener Daten entscheidend für die erfolgreiche Zusammenarbeit bei der Rechtsdurchsetzung und die wirksame Bekämpfung von Kriminalität. Diesem Austausch müssen solide Datenschutzgarantien zugrunde liegen. Dies trägt auch zum Aufbau von Vertrauen zwischen den Rechtsdurchsetzungsbehörden und zur Stärkung der Rechtssicherheit bei der Sammlung und beim Austausch von Informationen bei.

Die in der Polizei-Richtlinie enthaltenen Bestimmungen für internationale Datenübermittlungen regeln den Datenaustausch zwischen Durchsetzungsbehörden innerhalb und außerhalb der EU sowie in bestimmten Fällen Datenübermittlungen von Durchsetzungsbehörden an andere Stellen. Mit der Richtlinie wird die Möglichkeit von Angemessenheitsfeststellungen im Bereich der Strafverfolgung eingeführt. Die Kommission wird die Möglichkeit solcher Angemessenheitsfeststellungen für qualifizierte Drittländer fördern, insbesondere für Länder, mit denen eine enge und rasche Zusammenarbeit bei der Bekämpfung von Kriminalität und Terrorismus erforderlich ist und bereits ein umfangreicher Austausch personenbezogener Daten stattfindet. Vor diesem Hintergrund wird die Kommission Gesprächen über Angemessenheitsbeschlüsse mit denjenigen Drittländern Vorrang einräumen, die auf diesem Gebiet besonders wichtige Partner sind.

Alternativ ist das im Dezember 2016 geschlossene Datenschutz-Rahmenabkommen[54] zwischen der EU und den USA ein erfolgreiches Beispiel dafür, wie die Zusammenarbeit im

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

Bereich der Rechtsdurchsetzung mit einem wichtigen internationalen Partner durch die Aushandlung einer Reihe solider Datenschutzgarantien verbessert werden kann. Indem das Rahmenabkommen bestehende Rechtsinstrumente, auf die sich der Datenaustausch stützt, automatisch ergänzt (insbesondere bilaterale Abkommen auf Ebene sowohl der EU als auch der Mitgliedstaaten), bringt es dem Einzelnen sofortige und unmittelbare Vorteile und stärkt die Zusammenarbeit bei der Rechtsdurchsetzung durch die Erleichterung des Informationsaustauschs. Da das Rahmenabkommen eine Grundlage für künftige Datenübermittlungsvereinbarungen mit den USA schafft, fällt auch die Notwendigkeit weg, dieselben Garantien immer wieder neu auszuhandeln. Das Rahmenabkommen ist das erste bilaterale internationale Abkommen mit einem umfassenden Katalog von im Einklang mit dem Besitzstand der EU stehenden Rechten und Pflichten auf dem Gebiet des Schutzes personenbezogener Daten. Es eignet sich daher als Vorbild für die Aushandlung ähnlicher Abkommen mit Drittländern, nicht nur im Bereich der justiziellen und polizeilichen Zusammenarbeit, sondern auch in anderen Bereichen der Durchsetzung staatlicher Maßnahmen (z. B. Wettbewerbspolitik, Verbraucherschutz). Dies gilt sowohl für den Austausch zwischen Regierungen als auch für Datenübermittlungen zwischen privaten Unternehmen und Durchsetzungsbehörden. Es könnte der EU auch den Abschluss von Abkommen über den Datenaustausch zwischen den einschlägigen EU-Einrichtungen (insbesondere Europol und Eurojust) und Drittländern erleichtern[55]. Die Kommission wird daher die Möglichkeit prüfen, ähnliche Rahmenabkommen mit wichtigen Partnern auf dem Gebiet der Rechtsdurchsetzung zu schließen.

Darüber hinaus sieht die Polizei-Richtlinie für die Rechtsdurchsetzungsbehörden in der EU die Möglichkeit vor, abhängig von strikten Garantien und unter bestimmten Umständen Informationen direkt von einem privaten Unternehmen in einem Drittland anzufordern und in der entsprechenden Anforderung personenbezogene Informationen (in der Regel einen Namen oder eine IP-Adresse) weiterzugeben[56]. Dagegen geht die Datenschutz-Grundverordnung gezielt auf Fälle ein, in denen private Unternehmen in der EU Rechtsdurchsetzungsbehörden eines Drittlands auf Ersuchen personenbezogene Daten übermitteln: Solche Datenübermittlungen in Nicht-EU-Länder sind nur unter bestimmten Voraussetzungen zulässig, beispielsweise auf der Grundlage einer internationalen Übereinkunft oder wenn die Offenlegung aus einem wichtigen Grund des öffentlichen Interesses erfolgt, der im Recht der Union oder der Mitgliedstaaten anerkannt ist[57].

Diese Zusammenarbeit, die sich als entscheidend für die erfolgreiche Ermittlung und Verfolgung von Straftaten und Terrorismus erwiesen hat, wird in den Schlussfolgerungen des Rates zur Verbesserung der Strafjustiz im Cyberspace hervorgehoben. Der Rat hat die Kommission aufgefordert, auf der Grundlage eines gemeinsamen Konzepts der EU konkrete

---

der justiziellen Zusammenarbeit in Strafsachen. http://ec.europa.eu/justice/data-protection/files/dp-umbrella-agreement_en.pdf http://ec.europa.eu/justice/data-protection/files/dp-umbrella-agreement_en.pdf

[55] Der Abschluss von operativen Abkommen mit Europol und Eurojust stellt auch eine wichtige Etappe im Dialog über die Visaliberalisierung mit bestimmten Drittländern dar, u. a. im Kontext des laufenden Dialogs mit der Türkei.

[56] Siehe Artikel 39 und Erwägungsgrund 73 der Polizei-Richtlinie.

[57] Siehe Artikel 48 und Erwägungsgrund 115 der Datenschutz-Grundverordnung.

Maßnahmen zu treffen, die Zusammenarbeit mit den Diensteanbietern zu verstärken, die Rechtshilfe effizienter zu gestalten und Lösungen für die Probleme im Zusammenhang mit der Bestimmung der Zuständigkeit für Ermittlungsmaßnahmen im Cyberspace und mit der entsprechenden Durchsetzung vorzuschlagen[58]. Diese Maßnahmen betreffen sowohl den Austausch zwischen Rechtsdurchsetzungsbehörden und Diensteanbietern innerhalb der EU als auch den Austausch mit Behörden und Unternehmen außerhalb der EU. Die Kommission wird im Juni 2017 Optionen für den Zugang zu elektronischen Beweismitteln vorstellen, wobei sie das Erfordernis einer raschen und verlässlichen Zusammenarbeit berücksichtigen wird, die sich auf die hohen Datenschutzstandards der Polizei-Richtlinie und der Datenschutz-Grundverordnung stützt – sowohl innerhalb der EU als auch bei internationalen Datenübermittlungen.

Im Einklang mit der neuen Rechtsgrundlage für Europol wird die Kommission die Bestimmungen der gemäß dem Beschluss 2009/371/JI des Rates geschlossenen Abkommen zwischen Europol und Dritten über operative Zusammenarbeit überprüfen, einschließlich der Datenschutzbestimmungen.[59] Wie in der Europäischen Sicherheitsagenda 2015 dargelegt, wird darüber hinaus das künftige Konzept der Union für den Austausch von Fluggastdatensätzen (PNR) mit Nicht-EU-Ländern dem Umstand Rechnung tragen, dass einheitliche Standards und ein besonderer Schutz der Grundrechte angewandt werden müssen. Die Kommission wird rechtlich tragfähige und nachhaltige Lösungen für den Austausch von PNR mit Drittländern erarbeiten, wobei sie unter anderem eine Modellvereinbarung über PNR in Betracht ziehen wird, um festzulegen, welche Anforderungen Drittländer erfüllen müssen, um PNR-Daten von der EU zu erhalten. Die künftige Politik in diesem Bereich hängt jedoch insbesondere von dem Gutachten des Gerichtshofs der Europäischen Union über das geplante PNR-Abkommen zwischen der EU und Kanada ab[60].

---

58 Schlussfolgerungen des Rates vom 9. Juni 2016 zur Verbesserung der Strafjustiz im Cyberspace: http://data.consilium.europa.eu/doc/document/ST-10007-2016-INIT/de/pdf. Die Kommission wurde im Anschluss an ihren Fortschrittsbericht an den Rat vom Dezember 2016 beauftragt, dem Rat in diesen Fragen bis Juni 2017 Ergebnisse vorzulegen.

59 Siehe Artikel 25 Absatz 4 der Verordnung (EU) 2016/794 des Europäischen Parlaments und des Rates vom 11. Mai 2016 über die Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (Europol) und zur Ersetzung und Aufhebung der Beschlüsse 2009/371/JI, 2009/934/JI, 2009/935/JI, 2009/936/JI und 2009/968/JI des Rates (ABl. L 135 vom 24.5.52016. S. 53-114). Die Kommission muss bis 14. Juni 2021 einen Bewertungsbericht über die mit Europol vor dem 1. Mai 2017 geschlossenen Kooperationsabkommen vorlegen.

60 Gutachten des Gerichtshofs zu dem Entwurf des PNR-Abkommens zwischen der EU und Kanada von 2014, vom Europäischen Parlament beim Gerichtshof beantragt (Gutachten 1/15). Der Gerichtshof wurde ersucht, die Vereinbarkeit des Entwurfs des Abkommens mit der EU-Charta der Grundrechte zu prüfen.

WIRKSAMERE ZUSAMMENARBEIT BEI DER RECHTSDURCHSETZUNG UND SOLIDE DATENSCHUTZGARANTIEN

Die Kommission wird

- die Möglichkeit prüfen, im Rahmen der Polizei-Richtlinie Angemessenheitsbeschlüsse für qualifizierte Drittländer zu fassen,

- die Aushandlung von Abkommen im Bereich der Rechtsdurchsetzung mit wichtigen internationalen Partnern nach dem Muster des Rahmenabkommens mit den USA fördern,

- Folgemaßnahmen zu den Schlussfolgerungen des Rates zur Verbesserung der Strafjustiz im Cyberspace treffen, um den grenzüberschreitenden Austausch elektronischer Beweismittel im Einklang mit den Datenschutzvorschriften zu erleichtern.

5. FAZIT

Schutz und Austausch personenbezogener Daten schließen sich nicht gegenseitig aus. Ein starkes Datenschutzsystem erleichtert den Datenverkehr, da die Verbraucher so Vertrauen zu denjenigen Unternehmen fassen, denen ein sorgfältiger Umgang mit personenbezogenen Daten ihrer Kunden wichtig ist. Hohe Datenschutzstandards stellen somit in der globalen digitalen Wirtschaft einen Vorteil dar. Dasselbe gilt für die Zusammenarbeit bei der Rechtsdurchsetzung: Garantien für den Schutz der Privatsphäre sind ein integraler Bestandteil des wirksamen und raschen Austauschs von Informationen bei der Bekämpfung der Kriminalität auf der Grundlage von gegenseitigem Vertrauen und Rechtssicherheit.

Nach Abschluss der Reform der Datenschutzvorschriften sollte die EU mit Drittländern in diesem Bereich proaktiv zusammenarbeiten. Sie sollte sich sowohl auf bilateraler als auch auf multilateraler Ebene um eine größere Aufwärtskonvergenz der Datenschutzgrundsätze weltweit bemühen. Dies ist für Bürger wie Unternehmen von Interesse und Vorteil. Der neue Rechtsrahmen für den Datenschutz bietet der EU die Instrumente, die erforderlich und geeignet sind, um diese Ziele zu erreichen. Auf der Grundlage des in dieser Mitteilung dargelegten strategischen Konzepts wird die Kommission aktiv mit den wichtigsten Drittländern zusammenarbeiten, um die Möglichkeit von Angemessenheitsbeschlüssen zu prüfen (beginnend mit Japan und Korea im Jahr 2017), um die Angleichung der Regelungen an die EU-Standards zu fördern und die Handelsbeziehungen zu erleichtern. Gleichzeitig wird die EU die gesamte Bandbreite alternativer Übermittlungsinstrumente nutzen, um die Datenschutzrechte zu sichern und die Wirtschaftsteilnehmer zu unterstützen, wenn es darum geht, Daten an Länder zu übermitteln, deren nationales Recht kein angemessenes Datenschutzniveau gewährleistet. Diese Instrumente sollten außerdem verwendet werden, um die Zusammenarbeit zwischen den Aufsichts- und Rechtsdurchsetzungsbehörden der EU und ihren internationalen Partnern weiter zu erleichtern. Die Kommission wird die Kohärenz

zwischen der internen und der externen Dimension der EU-Datenschutzpolitik sicherstellen und einen hohen Datenschutz auf internationaler Ebene fördern, um die Zusammenarbeit bei der Rechtsdurchsetzung zu verbessern, einen Beitrag zum freien Handel zu leisten und weltweit hohe Standards für den Schutz personenbezogener Daten zu entwickeln.