EUROPÄISCHE
KOMMISSION

Brüssel, den 12.7.2016
C(2016) 4176 final

DURCHFÜHRUNGSBESCHLUSS DER KOMMISSION

vom 12.7.2016

gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes

(Text von Bedeutung für den EWR)

DURCHFÜHRUNGSBESCHLUSS DER KOMMISSION

vom 12.7.2016

gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes

(Text von Bedeutung für den EWR)

DIE EUROPÄISCHE KOMMISSION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union,

gestützt auf die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr[1], insbesondere auf Artikel 25 Absatz 6,

nach Anhörung des Europäischen Datenschutzbeauftragten[2]

1. Einleitung

(1) Die Richtlinie 95/46/EG regelt die Übermittlung personenbezogener Daten aus Mitgliedstaaten in Drittstaaten, soweit die Übermittlung in ihren Anwendungsbereich fällt.

(2) Artikel 1 der Richtlinie 95/46/EG und die Erwägungsgründe 2 und 10 ihrer Präambel sollen nicht nur einen wirksamen und vollständigen Schutz der Grundrechte und -freiheiten natürlicher Personen, insbesondere das Grundrecht auf Achtung des Privatlebens bei der Verarbeitung personenbezogener Daten, gewährleisten, sondern auch ein hohes Schutzniveau für diese Grundrechte und -freiheiten.[3]

(3) Die Bedeutung sowohl des Grundrechts auf Achtung des Privatlebens als auch des Grundrechts auf den Schutz personenbezogener Daten, wie in Artikel 7 bzw. Artikel 8 der Charta der Grundrechte der Europäischen Union garantiert, ist vom Gerichtshof in seiner ständigen Rechtsprechung hervorgehoben worden.[4]

(4) Gemäß Artikel 25 Absatz 1 der Richtlinie 95/46/EG müssen die Mitgliedstaaten sicherstellen, dass die Übermittlung personenbezogener Daten in ein Drittland nur zulässig ist, wenn dieses Drittland ein angemessenes Schutzniveau gewährleistet und die einzelstaatlichen Vorschriften zur Umsetzung anderer Bestimmungen der Richtlinie vor der Übermittlung beachtet werden. Die Kommission kann feststellen, dass ein Drittland aufgrund seiner innerstaatlichen Rechtsvorschriften oder der von ihm eingegangenen internationalen Verpflichtungen zum Schutz der Rechte von Privatpersonen ein angemessenes Schutzniveau gewährleistet. In diesem Falle können

[1] ABl. L 281 vom 23.11.1995, S. 31.

[2] Siehe Opinion 4/2016 on the EU-U.S. Privacy Shield draft adequacy decision, veröffentlicht am 30.5.2016.

[3] Rs. C-362/13, Maximillian Schrems/Data Protection Commissioner („Schrems"), EU:C:2015:650, Rn. 39.

[4] Rs. C-553/07, Rijkeboer, EU:C:2009:293, Rn. 47; verb. Rs. C-293/12 und C-594/12, Digital Rights Ireland u. a., EU:C:2014:238, Rn. 53; Rs. C-131/12, Google Spain und Google, EU:C:2014:317, Rn. 53, 66 und 74.

– unbeschadet der Einhaltung der aufgrund anderer Bestimmungen der Richtlinie erlassenen einzelstaatlichen Vorschriften – personenbezogene Daten aus den Mitgliedstaaten übermittelt werden, ohne dass zusätzliche Garantien erforderlich sind.

(5) Gemäß Artikel 25 Absatz 2 der Richtlinie 95/46/EG sollte das Schutzniveau, das ein Drittland bietet, unter Berücksichtigung aller Umstände beurteilt werden, die bei einer Datenübermittlung oder einer Kategorie von Datenübermittlungen eine Rolle spielen, einschließlich der im betreffenden Drittland geltenden allgemeinen und sektoriellen Rechtsnormen.

(6) In der Entscheidung 2000/520/EG der Kommission[5] wurde davon ausgegangen, dass im Sinne von Artikel 25 Absatz 2 der Richtlinie 95/46/EG die „Grundsätze des sicheren Hafens“, die gemäß den vom US-Handelsministerium herausgegebenen Leitlinien – enthalten in den „Häufig gestellten Fragen“ (FAQ) – umgesetzt wurden, ein angemessenes Schutzniveau für personenbezogene Daten gewährleisten, die von der Europäischen Union an in den Vereinigten Staaten niedergelassene Organisationen übermittelt werden.

(7) In ihren Mitteilungen COM(2013) 846 final[6] und COM(2013) 847 final vom 27. November 2013[7] brachte die Kommission zum Ausdruck, dass die Grundlage der Safe-Harbor-Regelung aufgrund einer Reihe von Umständen überprüft und gestärkt werden muss, als da sind: die exponentielle Zunahme des Datenverkehrs und seine herausragende Bedeutung für die transatlantische Wirtschaft, der rasante zahlenmäßige Anstieg der Unternehmen in den USA, die sich an der Safe-Harbor-Regelung beteiligen, und die kurz zuvor bekannt gewordenen Informationen über Ausmaß und Umfang bestimmter Überwachungsprogramme der USA, die neue Fragen zum Schutzniveau aufwerfen, das mit der Safe-Harbor-Vereinbarung gewährleistet werden soll. Zudem benannte die Kommission eine Reihe von Mängeln und Schwachstellen der Safe-Harbor-Regelung.

(8) Auf der Grundlage der von der Kommission zusammengetragenen Fakten, von Erkenntnissen der hochrangigen Kontaktgruppe EU-USA[8] und Informationen der Ad-hoc-Arbeitsgruppe EU-USA über Überwachungsprogramme der USA[9] gab die Kommission 13 Empfehlungen für eine Bestandsaufnahme der Safe-Harbor-Regelung ab. Bei diesen Empfehlungen ging es vor allem um die Stärkung der materiellen Datenschutzvorschriften, eine höhere Transparenz der Datenschutzbestimmungen selbstzertifizierter US-Unternehmen, eine bessere Beaufsichtigung, Kontrolle und Durchsetzung der Einhaltung dieser Grundsätze durch die amerikanischen Behörden,

---

5 Entscheidung 2000/520/EG der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des „sicheren Hafens“ und der diesbezüglichen „Häufig gestellten Fragen“ (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA (ABl. L 215 vom 28.8.2000, S. 7).

6 Mitteilung der Kommission an das Europäische Parlament und den Rat über die Wiederherstellung des Vertrauens beim Datenaustausch zwischen der EU und den USA, COM(2013) 846 final vom 27.11.2013.

7 Mitteilung der Kommission an das Europäische Parlament und den Rat über die Funktionsweise der Safe-Harbor-Regelung aus Sicht der EU-Bürger und der in der EU niedergelassenen Unternehmen, COM(2013) 847 final vom 27.11.2013.

8 Siehe z. B. Rat der Europäischen Union, Final Report by EU-US High Level Contact Group on information sharing and privacy and personal data protection, Note 9831/08, 28.5.2008, im Internet abrufbar unter: http://www.europarl.europa.eu/document/activities/cont/201010/20101019ATT88359/20101019ATT88359EN.pdf.

9 Report on the Findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection, 27.11.2013, im Internet abrufbar unter: http://ec.europa.eu/justice/data-protection/files/report-findings-of-the-ad-hoc-eu-us-working-group-on-data-protection.pdf.

die Verfügbarkeit erschwinglicher Streitbeilegungsmechanismen und die Schaffung der Voraussetzungen dafür, dass von der in der Kommissionsentscheidung 2000/520/EG vorgesehenen Ausnahmeregelung in Bezug auf die nationale Sicherheit nur so weit Gebrauch gemacht wird, wie dies unbedingt notwendig und angemessen ist.

(9) In seinem Urteil vom 6. Oktober 2015 in der Rechtssache C-362/14 Maximilian Schrems/Data Protection Commissioner[10] erklärte der Gerichtshof die Entscheidung 2000/520/EG der Kommission für ungültig. Ohne inhaltliche Prüfung der Datenschutzgrundsätze der Safe-Harbor-Regelung gelangte der Gerichtshof zu der Auffassung, die Kommission habe in ihrer Entscheidung nicht festgestellt, dass die USA aufgrund ihrer innerstaatlichen Rechtsvorschriften oder ihrer internationalen Verpflichtungen tatsächlich ein angemessenes Schutzniveau „gewährleisten“.[11]

(10) Wie der Gerichtshof erläuterte, bedeutet „angemessener Rechtsschutz“ in Artikel 25 Absatz 6 der Richtlinie 95/46/EG nicht, dass das Schutzniveau exakt dem in der EU-Rechtsordnung garantierten Niveau entsprechen muss, wohl aber, dass der Drittstaat ein Schutzniveau der Grundrechte und -freiheiten gewährleisten muss, dass dem in der Europäischen Union durch die Richtlinie 95/46/EG im Lichte der Charta der Grundrechte garantierten Niveau „der Sache nach gleichwertig“ ist. Auch wenn sich die Mittel, auf die ein Drittstaat zurückgreift, von den in der Europäischen Union herangezogenen Mitteln unterscheiden können, müssen sie sich gleichwohl in der Praxis als wirksam erweisen.[12]

(11) Der Gerichtshof kritisierte, dass die Entscheidung 2000/520 keine Feststellung dazu enthält, ob es in den Vereinigten Staaten staatliche Regeln gibt, die dazu dienen, etwaige Eingriffe – zu denen die staatlichen Stellen dieses Landes in Verfolgung berechtigter Ziele wie der nationalen Sicherheit berechtigt wären – in die Grundrechte der Personen, deren Daten aus der Union in die Vereinigten Staaten übermittelt werden, zu begrenzen, und auch nichts über das Bestehen eines wirksamen Rechtsschutzes gegen derartige Eingriffe aussagt.[13]

(12) Die Kommission hatte 2014 Gespräche mit den amerikanischen Behörden aufgenommen, um die Stärkung der Safe-Harbor-Regelung entsprechend den 13 Empfehlungen in der Mitteilung COM(2013) 847 final zu erörtern. Nach dem Urteil des Gerichtshofs der Europäischen Union in der Rechtssache Schrems wurden die Gespräche intensiviert, um zu einem neuen Angemessenheitsbeschluss zu gelangen, der den Anforderungen von Artikel 25 der Richtlinie 95/46/EG in der Auslegung durch den Gerichtshof gerecht wird. Die Schriftstücke, die dem vorliegenden Beschluss beigefügt sind und auch im Bundesregister der USA veröffentlicht werden, sind das Ergebnis dieser Gespräche. Die Datenschutzgrundsätze (Anhang II) bilden zusammen mit den in den Anhängen I, III bis VII enthaltenen offiziellen Erklärungen und Zusagen verschiedener Behörden der USA den „EU-US-Datenschutzschild“.

(13) Die Kommission hat die Rechtslage und die gängige Praxis in den USA, darunter auch die offiziellen Erklärungen und Verpflichtungen, sorgfältig analysiert. Aufgrund der in den Erwägungsgründen (136)-(140) dargelegten Erkenntnisse gelangt die Kommission zu dem Schluss, dass die Vereinigten Staaten ein angemessenes Schutzniveau für

[10] Siehe Fußnote 3.
[11] Schrems, Rn. 97.
[12] Schrems, Rn. 73-74.
[13] Schrems, Rn. 88-89.

personenbezogene Daten gewährleisten, die im Rahmen des EU-US-Datenschutzschilds aus der Europäischen Union an selbstzertifizierte Organisationen.

2. Der „EU-US-Datenschutzschild“

(14) Der EU-US-Datenschutzschild beruht auf einem System der Selbstzertifizierung, wonach sich amerikanische Organisationen zu einem Katalog von Datenschutzgrundsätzen verpflichten – den Rahmengrundsätzen des EU-US-Datenschutzschilds einschließlich der Zusatzgrundsätze (im Folgenden insgesamt „Grundsätze“) –, die vom Handelsministerium der USA herausgegeben wurden und in Anhang II des vorliegenden Beschlusses enthalten sind. Er erfasst sowohl die für die Datenverarbeitung Verantwortlichen als auch die Auftragsverarbeiter (Beauftragten) mit der Maßgabe, dass sich die Auftragsverarbeiter vertraglich verpflichten, nur auf Weisung des Verantwortlichen in der EU zu handeln und Letzteren dabei zu unterstützen, Privatpersonen die Wahrnehmung ihrer Rechte im Rahmen der Grundsätze zu erleichtern.[14]

(15) Unbeschadet der Einhaltung innerstaatlicher Vorschriften, die gemäß Richtlinie 95/46/EG erlassen wurden, hat der vorliegende Beschluss die Wirkung, dass die Übermittlung von Daten von einem für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter in der EU an Organisationen in den USA, die sich durch Selbstzertifizierung beim Handelsministerium zur Einhaltung der Grundsätze verpflichtet haben, zulässig ist. Die Grundsätze gelten ausschließlich für die Verarbeitung personenbezogener Daten durch US-Organisationen, soweit die Verarbeitung durch diese Organisation nicht in den Anwendungsbereich des EU-Rechts fällt.[15] Der Datenschutzschild berührt nicht die Anwendung des Unionsrechts auf die Verarbeitung personenbezogener Daten in den Mitgliedstaaten.[16]

(16) Der Schutz, der personenbezogenen Daten durch den Datenschutzschild gewährt wird, gilt für alle Betroffenen in der EU[17], deren personenbezogene Daten aus der EU an

---

[14] Siehe Anhang II, Abschnitt III.10.a. Entsprechend der Begriffsbestimmung in Abschnitt I.8.c. bestimmt der für die Verarbeitung Verantwortliche in der EU den Zweck und die Mittel der Verarbeitung personenbezogener Daten. Außerdem muss aus dem Vertrag mit dem Beauftragten deutlich hervorgehen, ob eine Weitergabe der Daten gestattet ist (siehe Abschnitt III.10.a.ii.2.).

[15] Dies gilt auch für die Übermittlung von Personaldaten aus der EU im Zusammenhang mit einem Beschäftigungsverhältnis. In den Grundsätzen heißt es, dass die Verantwortung „in erster Linie“ beim Arbeitgeber in der EU liegt (siehe Anhang II, Abschnitt III.9.d.i.), und zudem wird klargestellt, dass hier nicht die Grundsätze zur Anwendung kommen, sondern die Rechtsvorschriften der EU und/oder des betreffenden Mitgliedstaats. Siehe Anhang II, Abschnitt III.9.a.i., b.ii., c.i., d.i.

[16] Dies gilt auch, wenn für die Verarbeitung technische Mittel eingesetzt werden, die sich in der EU befinden, aber von einer außerhalb der EU ansässigen Organisation genutzt werden (siehe Artikel 4 Absatz 1 Buchstabe c der Richtlinie 95/46/EG). Ab 25. Mai 2018 regelt die Datenschutz-Grundverordnung (DSGVO) die Verarbeitung personenbezogener Daten i) im Rahmen der Tätigkeit einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union (auch wenn die Verarbeitung in den USA stattfindet) oder ii) von betroffenen Personen, die sich in der Union befinden, durch einen nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiter, wenn die Datenverarbeitung im Zusammenhang damit steht, a) ihnen Waren oder Dienstleistungen anzubieten, unabhängig davon, ob von den betroffenen Personen eine Zahlung zu leisten ist, oder b) ihr Verhalten zu beobachten, soweit ihr Verhalten in der Union erfolgt. Siehe Artikel 3 Absatz 1 Buchstabe 2 der 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.

[17] Der vorliegende Beschluss ist für den EWR von Bedeutung. Das Abkommen über den Europäischen Wirtschaftsraum (EWR-Abkommen) regelt die Ausweitung des EU-Binnenmarkts auf die drei EWR-

Organisationen in den USA übermittelt werden, die sich beim Handelsministerium durch Selbstzertifizierung zu den Grundsätzen bekannt haben.

(17) Die Grundsätze gelten unmittelbar vom Zeitpunkt der Zertifizierung an. Eine Ausnahme bildet der Grundsatz Verantwortlichkeit für die Weitergabe in dem Falle, dass eine Organisation, die dem Datenschutzschild durch Selbstzertifizierung beitritt, bereits vorher geschäftliche Beziehungen zu Dritten unterhielt. Da es einige Zeit in Anspruch nehmen kann, diese geschäftlichen Beziehungen mit den Regeln, die nach dem Grundsatz der Verantwortlichkeit für die Weitergabe zu befolgen sind, in Einklang zu bringen, ist die Organisation gehalten, dies so schnell wie möglich zu bewerkstelligen und auf keinen Fall später als neun Monate nach der Selbstzertifizierung (sofern diese in den ersten zwei Monaten nach dem Tag erfolgt, an dem der Datenschutzschild in Kraft tritt). In dieser Übergangszeit muss die Organisation die Grundsätze der Informationspflicht und Wahlmöglichkeit anwenden (was dem Betroffenen in der EU ein „Opt-out" ermöglicht) und bei der Übermittlung personenbezogener Daten an einen als Beauftragten fungierenden Dritten sicherstellen, dass Letzterer zumindest das gleiche Schutzniveau vorsieht wie die Grundsätze.[18] Diese Übergangszeit sorgt für ein vernünftiges und ausgewogenes Verhältnis zwischen der Achtung des Grundrechts auf Datenschutz und dem legitimen Interesse von Unternehmen an einem ausreichenden zeitlichen Spielraum für die Umstellung auf die neue Regelung, sofern dies auch von ihren geschäftlichen Beziehungen zu Dritten abhängt.

(18) Das System wird vom Handelsministerium auf der Grundlage der Zusagen verwaltet und überwacht, die in den Erklärungen des Handelsministers der USA dargelegt sind (Anhang I des vorliegenden Beschlusses). Im Hinblick auf die Durchsetzung der Grundsätze haben die Federal Trade Commission (FTC) und das Verkehrsministerium Erklärungen abgegeben, die in Anhang IV und Anhang V des vorliegenden Beschlusses enthalten sind.

2.1. Datenschutzgrundsätze

(19) Im Zuge ihrer Selbstzertifizierung unter dem EU-US-Datenschutzschild müssen sich Organisationen dazu verpflichten, die Grundsätze einzuhalten.[19]

(20) Nach dem *Grundsatz der Informationspflicht* sind Organisationen gehalten, die betroffenen Personen über eine Reihe von Kernpunkten zu unterrichten, die mit der Verarbeitung ihrer personenbezogenen Daten zusammenhängen (z. B. Art der

---

Staaten Island, Liechtenstein und Norwegen. Das Datenschutzrecht der Union, darunter die Richtlinie 95/46/EG, ist in das EWR-Abkommen einbezogen und wurde in Anhang XI aufgenommen. Der Gemeinsame EWR-Ausschuss muss über die Aufnahme des vorliegenden Beschlusses in das EWR-Abkommen entscheiden. Sobald der Beschluss für Island, Liechtenstein und Norwegen gilt, erstreckt sich der Datenschutzschild auch auf diese drei Staaten, so dass alle Bezugnahmen auf die EU und ihre Mitgliedstaaten in der Datenschutzschild-Regelung so zu interpretieren sind, dass auch Island, Liechtenstein und Norwegen darin eingeschlossen sind.

[18] Siehe Anhang II, Abschnitt III.6.e.

[19] Besondere Regeln, die zusätzliche Garantien vorsehen, gelten für Personaldaten, die im Rahmen eines Beschäftigungsverhältnisses erhoben werden, wie im Zusatzgrundsatz „Personaldaten" der Datenschutzgrundsätze dargelegt ist (siehe Anhang II, Abschnitt III.9). Beispielsweise sollten Arbeitgeber den individuellen Datenschutzbedürfnissen der Arbeitnehmer angemessen Rechnung tragen, indem sie den Zugang zu den personenbezogenen Daten beschränken, bestimmte Daten anonymisieren bzw. ihnen Codes oder Pseudonyme zuordnen. Vor allem aber sind die Organisationen verpflichtet, bei solchen Daten mit den Datenschutzbehörden der Europäischen Union zusammenzuarbeiten und deren Rat zu befolgen.

erhobenen Daten, Zweck der Verarbeitung, Zugangsrecht und Wahlmöglichkeit, Bedingungen für die Weitergabe und Haftungsfragen). Es sind noch weitere Sicherungen eingebaut, namentlich die Verpflichtung der Organisationen, ihre Datenschutzbestimmungen (in denen die Grundsätze ihren Niederschlag finden) offenzulegen und Links zur Website des Handelsministeriums (wo weitere Angaben zur Selbstzertifizierung, zu den Rechten der betroffenen Personen und zu verfügbaren Rechtsbehelfen zu finden sind), zu der im Erwägungsgrund 30 erwähnten Datenschutzschild-Liste und zur Website eines geeigneten Anbieters alternativer Streitbeilegungsverfahren anzubringen.

(21) Nach dem *Grundsatz der Datenintegrität und Zweckbindung* müssen personenbezogene Daten darauf beschränkt werden, was für den Zweck der Verarbeitung erheblich ist, und sie müssen für den vorgesehenen Zweck hinreichend zuverlässig, genau, vollständig und aktuell sein. Eine Organisation darf personenbezogene Daten nicht in einer Weise verarbeiten, die mit dem ursprünglichen Erhebungszweck oder mit dem Zweck unvereinbar ist, dem der Betroffene nachträglich zugestimmt hat. Die Organisationen müssen sicherstellen, dass die Daten für den vorgesehenen Zweck zuverlässig, genau, vollständig und aktuell sind.

(22) Wenn ein neuer (geänderter) Verwendungszweck sich zwar deutlich vom ursprünglichen Zweck unterscheidet, aber mit diesem dennoch vereinbar ist, gibt der *Grundsatz der Wahlmöglichkeit* den betroffenen Personen das Recht auf Widerspruch („Opt-out"). Dieser Grundsatz hebt aber das ausdrückliche Verbot einer unzulässigen Verarbeitung nicht auf.[20] Für das Direktmarketing gelten spezielle Regelungen, wonach Betroffene in der Regel „jederzeit" der Verwendung personenbezogener Daten widersprechen können.[21] Im Falle sensibler Daten müssen die Organisationen normalerweise die ausdrückliche Zustimmung der betroffenen Person („Opt-in") einholen.

(23) Nach dem *Grundsatz der Datenintegrität und Zweckbindung* können aber personenbezogene Informationen nur so lange in einer Form gespeichert werden, durch die eine natürliche Person identifiziert werden kann oder identifizierbar wird (d. h. als personenbezogene Daten), wie dies dem Zweck/den Zwecken dient, für die sie ursprünglich erhoben oder nachträglich autorisiert wurden. Diese Verpflichtung hindert Mitglieder des Datenschutzschilds nicht daran, weiterhin personenbezogene Daten über längere Zeiträume zu verarbeiten, aber nur solange und soweit die Verarbeitung nach vernünftigem Ermessen einem der folgenden spezifischen Zwecke dient: Archivierung im öffentlichen Interesse, Journalismus, Literatur und Kunst, wissenschaftliche und historische Forschung und statistische Analyse. Eine längere Speicherung personenbezogener Daten für einen dieser Zwecke unterliegt den in den Grundsätzen enthaltenen Garantien.

---

[20] Dies betrifft alle Datenübermittlungen im Rahmen des Datenschutzschilds, auch wenn es um Daten geht, die im Rahmen des Beschäftigungsverhältnisses erhoben wurden. Zwar kann eine selbstzertifizierte US-Organisation Personaldaten im Prinzip auch für andere Zwecke verwenden, die nicht mit der Beschäftigung zusammenhängen (z. B. bestimmte Marketingbotschaften), doch muss sie dabei das Verbot unzulässiger Verarbeitung beachten und sich an die *Grundsätze der Informationspflicht und Wahlmöglichkeit* halten. Da US-Organisationen Mitarbeiter wegen der Ausübung dieses Wahlrechts nicht maßregeln dürfen, auch nicht durch Einschränkung der beruflichen Möglichkeiten, ist gewährleistet, dass die Mitarbeiter trotz ihres Unterstellungsverhältnisses und der damit verbundenen Abhängigkeit keinem Druck ausgesetzt sind und sie somit wirklich frei entscheiden können.

[21] Siehe Anhang II, Abschnitt III.12.

(24) Nach dem *Grundsatz der Sicherheit* müssen Organisationen, die personenbezogene Daten erstellen, verwalten, verwenden oder verbreiten, „angemessene und geeignete" Sicherheitsvorkehrungen treffen und dabei die Risiken berücksichtigen, die sich aus der Verarbeitung und der Art der Daten ergeben. Im Falle der Unterauftragsverarbeitung müssen die Organisationen einen Vertrag mit dem Unterauftragsverarbeiter abschließen, der das gleiche Schutzniveau sicherstellt, wie es die Grundsätze bieten, und für dessen ordnungsgemäße Umsetzung sorgen.

(25) Nach dem *Grundsatz des Auskunftsrechts*[22] haben betroffene Personen das Recht, ohne Angabe von Gründen und gegen eine nicht übermäßige Gebühr von einer Organisation die Auskunft einzuholen, ob die Organisation sie betreffende personenbezogene Daten verarbeitet, und sich die Daten binnen einer angemessenen Frist übermitteln zu lassen. Dieses Recht darf nur in Ausnahmefällen eingeschränkt werden; jede Verweigerung oder Einschränkung des Auskunftsrechts muss notwendig und hinreichend gerechtfertigt sein, wobei die Organisation die Beweislast dafür trägt, dass die Voraussetzungen erfüllt sind. Die Betroffenen müssen die Möglichkeit haben, die personenbezogenen Daten zu korrigieren, zu ändern oder zu löschen, wenn sie falsch sind oder unter Verletzung der Grundsätze verarbeitet wurden. In Bereichen, in denen eine hohe Wahrscheinlichkeit besteht, dass Unternehmen personenbezogene Daten automatisch verarbeiten, um Entscheidungen mit Auswirkungen auf einzelne Personen zu treffen (z. B. Kreditvergabe, Hypothekenangebote, Stellenbesetzung), bietet das US-Recht spezifische Schutzvorkehrungen bei ablehnenden Entscheidungen.[23] In der Regel sehen diese Gesetze vor, dass die Betroffenen das Recht haben, über die konkreten Gründe für die Entscheidung (z. B. die Verweigerung eines Kredits) unterrichtet zu werden, bei unvollständigen oder ungenauen Informationen (sowie der Berücksichtigung unzulässiger Faktoren) Einspruch zu erheben und Rechtsschutz in Anspruch zu nehmen. Diese Regeln bieten Schutz in der aller Voraussicht nach überschaubaren Zahl von Fällen, in denen automatisierte Entscheidungen von einer dem Datenschutzschild angehörenden Organisation selbst getroffen werden.[24] Da aber in der modernen digitalen Wirtschaft die automatisierte Verarbeitung (einschließlich Profiling) zunehmend als Grundlage für Entscheidungen dient, die sich auf einzelne Personen auswirken, bedarf dieser Bereich einer intensiven Kontrolle. Um diese Kontrolle zu erleichtern, wurde mit den US-Behörden vereinbart, dass ein Dialog über automatisierte Entscheidungsprozesse, einschließlich eines Meinungsaustauschs über Gemeinsamkeiten und Unterschiede der diesbezüglichen Konzepte der EU und der USA, im Rahmen der ersten jährlichen Überprüfung und gegebenenfalls auch weiterer Überprüfungen stattfindet.

(26) Nach dem *Grundsatz des Rechtsschutzes, der Durchsetzung und der Haftung*[25] müssen die teilnehmenden Organisationen robuste Mechanismen schaffen, um die Einhaltung der anderen Datenschutzgrundsätze sicherzustellen und Betroffenen in der EU Rechtsschutz zu gewähren, deren personenbezogenen Daten in nicht rechtskonformer Weise verarbeitet wurden, was auch wirksame Rechtsbehelfe einschließt. Hat sich eine

---

22 Siehe auch Zusatzgrundsatz „Auskunftsrecht" (Anhang II, Abschnitt III.8).

23 Siehe z. B. Equal Credit Opportunity Act (ECOA, 15 U.S.C. 1691 ff.), Fair Credit Reporting Act (FRCA, 15 USC § 1681 ff.), oder Fair Housing Act (FHA, 42 U.S.C. 3601 ff.).

24 Bei der Übermittlung personenbezogener Daten, die in der EU erhoben wurden, besteht die vertragliche Beziehung zumeist zwischen einer Privatperson (Kunden) und dem für die Verarbeitung Verantwortlichen, der in der Regel auch die Entscheidung über die automatisierte Verarbeitung trifft und sich dabei an die EU-Datenschutzregeln halten muss. Möglich ist zum Beispiel ein Szenario, bei dem die Verarbeitung durch eine dem Datenschutzschild angehörende Organisation erfolgt, die im Auftrag des EU-Verantwortlichen handelt.

25 Siehe auch Zusatzgrundsatz „Beschwerdeverfahren und Durchsetzung" (Anhang II, Abschnitt III.11).

Organisation freiwillig für die Selbstzertifizierung[26] unter dem EU-US-Datenschutzschild entschieden, ist für sie die effektive Einhaltung der Grundsätze zwingend. Damit die Organisation weiterhin auf der Grundlage des Datenschutzschilds personenbezogene Daten aus der Europäischen Union empfangen kann, muss sie ihre Beteiligung daran jährlich neu zertifizieren. Überdies müssen die Organisationen Maßnahmen ergreifen, um sich zu vergewissern[27], dass die veröffentlichten Datenschutzbestimmungen den Grundsätzen entsprechen und tatsächlich eingehalten werden. Dies kann entweder durch ein System der Selbstkontrolle erfolgen, das interne Verfahren einschließen muss, die sicherstellen, dass die Mitarbeiter in der Umsetzung der Datenschutzbestimmungen der Organisation unterwiesen werden und die Einhaltung in regelmäßigen Abständen objektiv überprüft wird, oder aber externe Überprüfungen, zu denen Audits und Stichprobenkontrollen gehören können. Zudem muss die Organisation für ein wirksames Rechtsschutzinstrument sorgen, das sich mit derartigen Beschwerden befasst (siehe dazu auch Erwägungsgrund 43), und den Ermittlungs- und Durchsetzungsbefugnissen der FTC, des Verkehrsministeriums oder einer anderen dazu autorisierten staatlichen Instanz der USA unterliegen, die effektiv für die Einhaltung der Grundsätze sorgt.

(27) Besondere Regeln gelten für die „Weitergabe“, d. h. die Übermittlung personenbezogener Daten von einer Organisation an einen als für die Verarbeitung Verantwortlicher oder Auftragsverarbeiter fungierenden Dritten unabhängig davon, ob Letzterer sich in den USA oder einem Drittstaat außerhalb der Vereinigten Staaten (und der Union) befindet. Diese Regeln sollen gewährleisten, dass die für personenbezogene Daten von betroffenen Personen in der EU geltenden Schutzvorkehrungen nicht ausgehöhlt werden und nicht umgangen werden können, indem man sie an Dritte weiterleitet. Von besonderer Bedeutung ist dies für die relativ komplexen Verarbeitungsketten, wie sie für die digitale Wirtschaft von heute charakteristisch sind.

(28) Nach dem *Grundsatz der Verantwortlichkeit für die Weitergabe*[28] kann die Weitergabe nur i) für begrenzte und genau bezeichnete Zwecke, ii) auf der Grundlage eines Vertrages (oder vergleichbaren Regelung in einem Konzern[29]) und iii) nur dann erfolgen, wenn der Vertrag das gleiche Schutzniveau wie die Grundsätze gewährleistet, was die Verpflichtung einschließt, dass die Anwendung der Grundsätze nur in dem Maße eingeschränkt werden darf, das für die nationale Sicherheit, die Strafverfolgung und andere im öffentlichen Interesse liegende Belange erforderlich ist.[30] Dies ist in Verbindung mit dem Grundsatz der Informationspflicht und bei der Weitergabe an einen als für die Verarbeitung Verantwortlichen fungierenden Dritten[31]

---

26 Siehe auch Zusatzgrundsatz „Selbstzertifizierung“ (Anhang II, Abschnitt III.6).

27 Siehe auch Zusatzgrundsatz „Anlassunabhängige Kontrolle“ (Anhang II, Abschnitt III.7).

28 Siehe auch Zusatzgrundsatz „Obligatorische Verträge bei Weitergabe“ (Anhang II, Abschnitt III.10).

29 Siehe Zusatzgrundsatz „Obligatorische Verträge bei Weitergabe“ (Anhang II, Abschnitt III.10.b). Dieser Grundsatz gestattet zwar Übermittlungen auf der Grundlage nichtvertraglicher Instrumente (z. B. konzerninterne Compliance- und Kontrollprogramme), doch geht aus dem Text deutlich hervor, dass diese Instrumente stets „die Kontinuität des Schutzes personenbezogener Daten im Rahmen der Grundsätze“ gewährleisten müssen. Da die selbstzertifizierten US-Organisationen weiterhin für die Einhaltung der Grundsätze verantwortlich sind, besteht für sie ein starker Anreiz, sich solcher Instrumente zu bedienen, die sich in der Praxis als wirksam erweisen.

30 Siehe Anhang II, Abschnitt I.5.

31 Privatpersonen haben kein Recht auf Widerspruch („Opt-out“), wenn die personenbezogenen Daten an einen Dritten übermittelt werden, der im Auftrag und auf Anweisung der US-Organisation Aufgaben wahrnimmt. Dies erfordert allerdings einen Vertrag mit dem Beauftragten, wobei die US-Organisation dafür

dem Grundsatz der Wahlmöglichkeit zu sehen, wonach betroffene Personen (unter anderem) über die Art/Identität des Drittempfängers, den Zweck der Weitergabe sowie die vorhandenen Wahlmöglichkeiten unterrichtet werden müssen und gegen die Weitergabe Einspruch erheben können (Opt-out) oder ihr im Falle sensibler Daten „ausdrücklich zustimmen“ müssen (Opt-in). Im Lichte des Grundsatzes der *Datenintegrität und Zweckbindung* ergibt sich aus der Verpflichtung, das gleiche Schutzniveau wie die Grundsätze vorzusehen, dass der Dritte die an ihn übermittelten personenbezogenen Informationen nur für Zwecke verarbeiten darf, die nicht mit den Zwecken unvereinbar sind, für die sie ursprünglich erhoben oder nachträglich vom Betroffenen autorisiert wurden.

(29) Die Verpflichtung, das gleiche Schutzniveau vorzusehen wie die Grundsätze, gilt für alle Dritten, die an der Verarbeitung der so übermittelten Daten beteiligt sind unabhängig von ihrem Standort (ob in der USA oder einem anderen Drittland), aber auch für den Fall, dass der ursprüngliche Drittempfänger selbst diese Daten einem anderen Drittempfänger übermittelt, beispielsweise für Zwecke der Weiterverarbeitung. In allen Fällen muss der Vertrag mit dem Drittempfänger die Bestimmung enthalten, dass Letzterer die dem Datenschutzschild angehörende Organisation benachrichtigt, wenn er zu dem Schluss kommt, dass er diese Verpflichtung nicht länger einhalten kann. Wenn diese Situation eintritt, wird die Verarbeitung durch den Dritten eingestellt oder sind andere sinnvolle und geeignete Schritte zu unternehmen, um Abhilfe zu schaffen.[32] Falls in der (Weiter-)Verarbeitungskette Compliance-Probleme auftreten, muss die dem Datenschutzschild angehörende Organisation, die als Verantwortliche für die personenbezogenen Daten fungiert, den Nachweis erbringen, dass sie für das Ereignis, das den Schaden bewirkt hat, nicht verantwortlich ist, da sie andernfalls haftbar gemacht werden kann, wie im *Grundsatz des Rechtsschutzes, der Durchsetzung und Haftung* geregelt. Zusätzliche Schutzmaßnahmen sind für den Fall der Weitergabe an einen im Auftrag handelnden Dritten vorgesehen.[33]

2.2. Transparenz, Verwaltung und Überwachung des EU-US-Datenschutzschilds

(30) Der EU-US-Datenschutzschild sieht Überwachungs- und Durchsetzungsmechanismen vor, um zu überprüfen und sicherzustellen, dass selbstzertifizierte US-Unternehmen die Grundsätzen einhalten und Verstöße geahndet werden. Diese Mechanismen werden in den Grundsätzen (Anhang II), in den Zusagen des Handelsministeriums (Anhang I), der FTC (Anhang IV) und des Verkehrsministeriums (Anhang V) beschrieben.

---

verantwortlich ist, durch Ausübung ihres Weisungsrechts für den im Rahmen der Grundsätze garantierten Rechtsschutz zu sorgen.

[32] Je nachdem, ob der Dritte als für die Verarbeitung Verantwortlicher oder Auftragsverarbeiter (Beauftragter) fungiert, ergibt sich eine unterschiedliche Situation. Im erstgenannten Fall muss der Vertrag mit dem Dritten vorsehen, dass Letzterer die Verarbeitung einstellt oder andere sinnvolle und geeignete Schritte unternimmt, um Abhilfe zu schaffen. Im zweiten Fall ist es Sache der dem Datenschutzschild angehörenden Organisation als Verantwortliche für die Verarbeitung, deren Weisungen der Beauftragte unterliegt, diese Maßnahmen zu ergreifen.

[33] In solch einem Fall muss die US-Organisation auch sinnvolle und geeignete Schritte unternehmen, um i) sicherzustellen, dass der Beauftragte die übermittelten personenbezogenen Daten tatsächlich auf eine Weise verarbeitet, die mit den Verpflichtungen der Organisation im Rahmen der Grundsätze in Einklang stehen, und ii) eine nicht autorisierte Verarbeitung zu unterbinden und Abhilfe zu schaffen, sobald sie davon Kenntnis erlangt.

(31) Um die ordnungsgemäße Anwendung des EU-US-Datenschutzschilds zu gewährleisten, ist es erforderlich, dass interessierte Seiten wie betroffene Personen, Datenexporteure und nationale Datenschutzbehörden die den Datenschutzgrundsätzen beigetretenen Organisationen als solche erkennen können. Zu diesem Zweck hat es das US-Handelsministerium übernommen, eine Liste der Organisationen zu führen und der Öffentlichkeit zugänglich zu machen, welche die Befolgung der Grundsätze bescheinigt und in die Zuständigkeit zumindest einer der in Anhang I und II dieses Beschlusses genannten Durchsetzungsbehörden fallen („Datenschutzschild-Liste“).[34] Das Handelsministerium aktualisiert die Liste auf der Grundlage der jährlichen Anträge auf erneute Zertifizierung und streicht die Organisationen, die ausscheiden oder nicht mehr dem EU-US-Datenschutzschild angehören. Außerdem führt es ein amtliches Verzeichnis der Organisationen, die von der Liste gestrichen wurden, und macht es der Öffentlichkeit zugänglich, wobei in jedem Falle die Gründe für die Streichung angegeben werden. Des Weiteren erstellt es einen Link zur Liste der FTC-Fälle, die mit der Durchsetzung des Datenschutzschilds in Verbindung stehen, auf der Website der FTC.

(32) Das Handelsministerium macht sowohl die Datenschutzschild-Liste als auch die Anträge auf Erneuerung der Zertifizierung über die dafür vorgesehene Website der Öffentlichkeit zugänglich. Die selbstzertifizierten Organisationen müssen ihrerseits für die Datenschutzschild-Liste die Webadresse des Ministeriums angeben. Wenn die Datenschutzbestimmungen einer Organisation online verfügbar sind, müssen sie mit einem Hyperlink zur Website des Datenschutzschilds versehen sein sowie mit einem Hyperlink zur Website oder dem Beschwerdeformular der unabhängigen Beschwerdestelle, die offene Beschwerden prüft. Das Handelsministerium überprüft bei der Zertifizierung und erneuten Zertifizierung einer Organisation für die Regelung systematisch, ob deren Datenschutzbestimmungen den Grundsätzen entsprechen.

(33) Organisationen, die fortwährend gegen die Grundsätze verstoßen haben, werden von der Datenschutzschild-Liste gestrichen und müssen die im Rahmen des EU-US-Datenschutzschilds empfangenen Daten zurückgeben oder löschen. In anderen Fällen der Streichung, etwa beim freiwilligen Ausscheiden oder beim Unterbleiben der erneuten Zertifizierung, kann die Organisation die betreffenden Daten behalten, wenn sie sich dem Handelsministerium gegenüber jährlich dazu verpflichtet, die Grundsätze weiterhin anzuwenden, oder für den angemessenen Schutz der personenbezogenen Daten durch andere zulässige Mittel sorgt (z. B. durch einen Vertrag, der den Anforderungen der von der Kommission gebilligten einschlägigen Standardklauseln vollauf genügt). In diesem Falle muss die Organisation eine Kontaktstelle benennen, die innerhalb der Organisation für alle mit dem Datenschutzschild zusammenhängenden Fragen zuständig ist.

(34) Das Handelsministerium überwacht Organisationen, die nicht mehr dem EU-US-Datenschutzschild angehören, weil sie freiwillig ausgeschieden sind oder die Zertifizierung abgelaufen ist, um sich zu vergewissern, ob sie die zuvor im Rahmen der Regelung empfangenen personenbezogenen Daten zurückgeben, löschen oder speichern.[35] Falls sie diese Daten speichern, sind sie verpflichtet, die Grundsätze zu beachten. In Fällen, in denen das Handelsministerium Organisationen wegen fortgesetzter Verstöße gegen die Grundsätze von der Liste gestrichen hat, stellt es

[34] Informationen über die Verwaltung der Datenschutzschild-Liste sind in Anhang I und Anhang II zu finden (Abschnitt I.3, Abschnitt I.4, III.6.d und Abschnitt III.11.g).

[35] Siehe z. B. Anhang II, Abschnitt I.3, Abschnitt III.6.f. und Abschnitt III.11.g.i.

sicher, dass die im Rahmen der Regelung empfangenen Daten zurückgegeben oder gelöscht werden.

(35) Wenn eine Organisation aus welchem Grund auch immer den EU-US-Datenschutzschild verlässt, muss sie alle öffentlichen Erklärungen entfernen, die darauf hindeuten, dass sie sich weiterhin am EU-US-Datenschutzschild beteiligt oder Anspruch auf die damit verbundenen Vorteile hat, vor allem jegliche Bezugnahme auf den EU-US-Datenschutzschild in den von ihr veröffentlichten Datenschutzbestimmungen. Das Handelsministerium sucht zielgerichtet nach falschen Angaben zur Beteiligung an der Regelung, auch bei früheren Mitgliedern, und geht dagegen vor.[36] Bei falschen Angaben über die Einhaltung der Datenschutzgrundsätze, die eine Organisation der Öffentlichkeit gegenüber in Form von irreführenden Erklärungen oder Praktiken macht, werden die FTC, das Verkehrsministerium oder andere Vollzugsbehörden der USA tätig; falsche Angaben gegenüber dem Handelsministerium unterliegen dem False Statements Act (18 U.S.C. § 1001).[37]

(36) Das Handelsministerium wacht von Amts wegen über falsche Angaben zur Beteiligung am Datenschutzschild oder die missbräuchliche Verwendung des entsprechenden Gütesiegels, und die Datenschutzbehörden können Organisationen zur Nachprüfung an eine dafür eingerichtete Kontaktstelle des Ministeriums verweisen. Wenn eine Organisation den EU-US-Datenschutzschild verlassen hat, keinen Antrag auf erneute Zertifizierung stellt oder aus der Datenschutzschild-Liste gestrichen wird, stellt das Handelsministerium kontinuierlich sicher, dass aus den veröffentlichten Datenschutzbestimmungen alle Bezugnahmen auf den Datenschutzschild entfernt wurden, die auf eine weitere Beteiligung der Organisation hindeuten, und verweist in dem Fall, dass weiterhin falsche Angaben gemacht werden, die Angelegenheit an die FTC, das Verkehrsministerium oder eine andere zuständige Behörde, damit diese gegebenenfalls tätig werden. Sie übermittelt zudem Fragebögen an Organisationen, deren Selbstzertifizierung ausläuft oder die freiwillig aus dem EU-US-Datenschutzschild ausgeschieden sind, um zu prüfen, ob die Organisation die personenbezogenen Dateien, die sie während der Beteiligung am EU-US-Datenschutzschild empfangen hat, zurückgibt, löscht oder auf sie weiterhin die Datenschutzgrundsätze anwendet, und um festzustellen, falls die Organisation die personenbezogenen Daten behält, wer innerhalb der Organisation als ständiger Ansprechpartner für Fragen im Zusammenhang mit dem Datenschutzschild fungieren wird.

(37) Das Handelsministerium überwacht bei selbstzertifizierten Organisationen von Amts wegen kontinuierlich die Einhaltung der Grundsätze[38], auch durch die Übersendung detaillierter Fragebögen. Es führt zudem systematisch Kontrollen durch, wenn konkrete (und ernst gemeinte) Beschwerden eingehen, wenn eine Organisation auf Anfragen keine zufriedenstellenden Antworten gibt oder deutliche Anhaltspunkte darauf schließen lassen, dass eine Organisation die Grundsätze nicht einhält. Das Ministerium stimmt diese Kontrollen bei Bedarf mit den zuständigen Datenschutzbehörden ab.

2.3. Rechtsschutzinstrumente, Umgang mit Beschwerden und Rechtsdurchsetzung

[36] Siehe Anhang I, Abschnitt „Aufdeckung und Handhabung von Fällen, in denen zu Unrecht eine Beteiligung an Regelung geltend gemacht wird“

[37] Siehe Anhang II, Abschnitt III.6.h. und Abschnitt III.11.f.

[38] Siehe Anhang I.

(38) Der EU-US-Datenschutzschild verpflichtet durch den *Grundsatz des Rechtsschutzes, der Durchsetzung und der Haftung* die Organisationen dazu, den von Verstößen betroffenen Personen Rechtsbehelfe zu garantieren und somit Betroffenen in der EU die Möglichkeit einzuräumen, Beschwerden wegen der Nichteinhaltung der Grundsätze durch selbstzertifizierte US-Unternehmen einzulegen und eine Klärung herbeizuführen, erforderlichenfalls durch eine Entscheidung, die wirksam Abhilfe schafft.

(39) Im Rahmen ihrer Selbstzertifizierung müssen die Organisationen den Anforderungen des *Grundsatzes des Rechtsschutzes, der Durchsetzung und der Haftung* gerecht werden, indem sie effektive und stets verfügbare unabhängige Rechtsschutzmechanismen vorsehen, durch die Beschwerden und Streitigkeiten bearbeitet und rasch geklärt werden können, ohne dass für den Einzelnen Kosten entstehen.

(40) Die Organisationen können sich für unabhängige Beschwerdestellen in der Europäischen Union oder in den Vereinigten Staaten entscheiden. Dies schließt die Möglichkeit ein, sich freiwillig zur Zusammenarbeit mit den Datenschutzbehörden der EU zu verpflichten. Wenn eine Organisation Personaldaten verarbeitet, besteht allerdings diese Wahlmöglichkeit nicht, da eine Zusammenarbeit mit den Datenschutzbehörden dann zwingend vorgeschrieben ist. Als Alternativen dazu kommen eine unabhängige alternative Streitbeilegung oder im Privatsektor entwickelte *Datenschutzprogramme*, welche die Datenschutzgrundsätze in ihre Regeln inkorporieren, in Betracht. Letztere müssen entsprechend den Anforderungen des Grundsatzes des Rechtsschutzes, der Durchsetzung und der Haftung wirksame Durchsetzungsmechanismen vorsehen. Die Organisationen sind verpflichtet, bei Problemen mit der Einhaltung für Abhilfe zu sorgen. Zudem müssen sie angeben, dass sie den Ermittlungs- und Durchsetzungsbefugnissen der FTC, des Verkehrsministeriums oder einer anderen autorisierten staatlichen Stelle der USA unterliegen.

(41) Folglich bietet die Datenschutzschild-Regelung betroffenen Personen eine Reihe von Möglichkeiten, ihr Recht durchzusetzen, Beschwerden über Verstöße selbstzertifizierter US-Unternehmen einzureichen und eine Klärung herbeizuführen, erforderlichenfalls durch eine Entscheidung, die wirksam Abhilfe schafft. Privatpersonen können eine Beschwerde direkt an eine Organisation, eine von der Organisation benannte unabhängige Schiedsstelle, nationale Datenschutzbehörden oder die FTC richten.

(42) In Fällen, in denen die Beschwerden durch keines dieser Rechtsschutz- oder Durchsetzungsinstrumente geklärt werden konnten, haben Privatpersonen auch das Recht, ein verbindliches Schiedsverfahren im Rahmen des Datenschutzschild-Panels zu beantragen (Anlage 1 zu Anhang II des vorliegenden Beschlusses). Wenn man von diesem Panel absieht, dessen Anrufung die Ausschöpfung bestimmter Rechtsbehelfe voraussetzt, können sich Privatpersonen frei für ein Rechtsschutzinstrument ihrer Wahl entscheiden und sind nicht verpflichtet, ein bestimmtes Instrument zu bevorzugen oder eine bestimmte Reihenfolge einzuhalten. Allerdings ergibt sich eine gewisse logische Reihenfolge, die es ratsam ist einzuhalten, wie nachstehend dargelegt.

(43) Erstens können betroffene Personen in der EU durch direkte Kontakte zum *selbstzertifizierten US-Unternehmen* ihre Rechte geltend machen und Verstößen gegen die Datenschutzgrundsätze nachgehen. Um eine Klärung zu erleichtern, muss die

Organisation einen wirksamen Rechtsschutzmechanismus vorsehen, mit dem derartigen Beschwerden abgeholfen wird. Deshalb müssen die Datenschutzbestimmungen einer Organisation präzise Angaben zu einer Kontaktstelle innerhalb oder außerhalb der Organisation enthalten, die Beschwerden entgegennimmt (auch zu einer entsprechenden Niederlassung in der Europäischen Union, die Anfragen und Beschwerden bearbeitet), sowie Angaben zu den unabhängigen Beschwerdestellen.

(44) Nach Eingang einer individuellen Beschwerde, auch wenn sie nicht direkt eingereicht, sondern von einer Datenschutzbehörde an das Handelsministerium weitergeleitet wurde, muss die Organisation innerhalb einer Frist von 45 Tagen der betroffenen Person in der EU darauf antworten. Die Antwort muss eine Aussage dazu enthalten, ob die Beschwerde begründet ist, und falls dies zutrifft, darlegen, wie die Organisation den Missstand zu beheben gedenkt. Des Weiteren sind die Organisationen verpflichtet, unverzüglich auf Anfragen und andere Auskunftsbegehren des Handelsministeriums oder einer Datenschutzbehörde (sofern sich die Organisation zur Zusammenarbeit mit den Datenschutzbehörden[39] verpflichtet hat) zu reagieren, die sich auf die Einhaltung der Datenschutzgrundsätze beziehen. Überdies müssen die Organisationen ihre Unterlagen zur Umsetzung ihrer Datenschutzbestimmungen aufbewahren und sie auf Anforderung im Rahmen einer Überprüfung oder einer Beschwerde über Verstöße einer unabhängigen Stelle oder der FTC (bzw. einer anderen für die Untersuchung unlauterer und irreführender Praktiken zuständigen Behörde der USA) zur Verfügung stellen.

(45) Zweitens können Privatpersonen eine Beschwerde auch direkt bei der von einer Organisation benannten *unabhängigen Beschwerdestelle* (entweder in den USA oder in der EU) einreichen, die Individualbeschwerden (sofern sie nicht offensichtlich unbegründet oder nicht ernsthaft sind) nachgeht und eine Klärung herbeiführt sowie Privatpersonen kostenlos angemessenen Rechtsschutz gewährt. Die von dieser Stelle verfügten Sanktionen und Abhilfemaßnahmen müssen hinreichend effektiv sein, damit sich die Organisationen an die Grundsätze halten, und sollten darauf gerichtet sein, dass die Folgen der Verstöße von der Organisation abgestellt oder rückgängig gemacht werden und, je nach Sachlage, die in Frage stehenden personenbezogenen Daten nicht weiter bearbeitet und/oder gelöscht werden sowie die festgestellten Verstöße öffentlich bekannt gemacht werden. Die von einer Organisation benannten unabhängigen Beschwerdestellen sind verpflichtet, auf ihren öffentlichen Websites einschlägige Informationen zum EU-US-Datenschutzschild und zu den in diesem Rahmen erbrachten Dienstleistungen zu veröffentlichen. Alljährlich müssen sie einen Bericht vorlegen, der zusammengefasste statistische Angaben zu diesen Dienstleistungen enthält.[40]

(46) Im Rahmen seiner Überprüfungsverfahren vergewissert sich das Handelsministerium, dass selbstzertifizierte US-Unternehmen tatsächlich bei den unabhängigen Beschwerdestellen registriert sind, die sie angegeben haben. Sowohl die Organisationen als auch die zuständigen unabhängigen Beschwerdestellen sind

[39] Die vom Panel der Datenschutzbehörden benannte zuständige Behörde, wie im Zusatzgrundsatz „Die Rolle der Datenschutzbehörden“ vorgesehen (Anhang II, Abschnitt III.5).

[40] Der Jahresbericht muss folgende Angaben enthalten: 1) die Gesamtzahl der im Berichtsjahr eingegangen Beschwerden, die den Datenschutzschild betreffen; 2) die eingegangen Beschwerden nach Kategorien; 3) qualitative Angaben zur Streitbeilegung, z. B. die Bearbeitungsdauer von Beschwerden; und 4) die Ergebnisse der eingegangenen Beschwerden, namentlich Anzahl und Art der verfügten Abhilfemaßnahmen oder Sanktionen

gehalten, rasch auf Anfragen und Auskunftsbegehren des Handelsministeriums zu reagieren, die mit dem Datenschutzschild im Zusammenhang stehen.

(47) Sofern die Organisation der Entscheidung einer Beschwerdestelle oder Einrichtung der freiwilligen Selbstkontrolle nicht nachkommt, muss die besagte Stelle das Handelsministerium und die FTC (oder eine andere für die Untersuchung unlauterer und irreführender Praktiken zuständige amerikanische Behörde) bzw. ein zuständiges Gericht davon in Kenntnis setzen.[41] Wenn sich eine Organisation weigert, der abschließenden Entscheidung einer Einrichtung der freiwilligen Selbstkontrolle, unabhängigen Beschwerdestelle oder staatlichen Einrichtung nachzukommen und diese Stelle zu dem Schluss gelangt, dass eine Organisation häufig gegen die Grundsätze verstößt, wird dies als fortgesetzte Missachtung der Grundsätze gewertet und hat zur Folge, dass das Handelsministerium nach Setzung einer Frist von 30 Tagen, in der sich die betreffende Organisation dazu äußern kann, die Organisation von der Liste streicht.[42] Sollte sich diese nach Streichung von der Liste weiterhin auf die Zertifizierung beim Datenschutzschild berufen, verweist das Ministerium den Fall an die FTC oder eine andere Durchsetzungsinstanz.[43]

(48) Drittens können Privatpersonen ihre Beschwerden auch bei einer nationalen *Datenschutzbehörde* einreichen. Die Organisationen sind verpflichtet, bei der Prüfung und Klärung einer Beschwerde durch eine nationale Datenschutzbehörde mitzuwirken, wenn es um Personaldaten geht, die im Rahmen eines Beschäftigungsverhältnisses erhoben wurden, oder wenn sie sich freiwillig der Kontrolle durch die Datenschutzbehörden unterstellt haben. Vor allem müssen sie Anfragen beantworten, die von den Datenschutzbehörden abgegebenen Empfehlungen befolgen, auch bei Abhilfe- oder Ausgleichsmaßnahmen, und den Datenschutzbehörden gegenüber schriftlich bestätigen, dass derartige Maßnahmen ergriffen wurden.

(49) Die Feststellungen und Vorgaben der Datenschutzbehörden erfolgen durch ein informelles Gremium, das von diesen auf Unionsebene eingerichtet wird[44], so dass ein einheitlicher schlüssiger Ansatz beim Umgang mit einer konkreten Beschwerde gewährleistet ist. Das Gremium gibt erst dann eine Empfehlung ab, wenn beide Parteien hinreichend Gelegenheit zur Stellungnahme oder zum Vorlegen von Beweisen hatten. Es wird sich bemühen, die Empfehlung so rasch zur Verfügung zu stellen, wie ein ordnungsgemäßes Vorgehen dies erlaubt, in der Regel binnen 6 Tagen nach Eingang einer Beschwerde. Kommt die Organisation den Empfehlungen des Gremiums nicht binnen 25 Tagen nach und hat sie keine befriedigende Erklärung für die Verzögerung gegeben, so teilt das Gremium seine Absicht mit, die Angelegenheit an die FTC (oder eine andere zuständige amerikanische Durchsetzungsinstanz) zu verweisen oder gelangt zu dem Schluss, dass eine gravierende Verletzung der Verpflichtungen zur Kooperation vorliegt. Im erstgenannten Fall kann dies zu Durchsetzungsmaßnahmen auf der Grundlage von § 5 des FTC Act (oder eines vergleichbaren Gesetzes) führen. Im zweiten Fall unterrichtet das Gremium das Handelsministerium, welches daraufhin das Verhalten der Organisation als

---

41 Siehe Anhang II, Abschnitt III.11.e.

42 Siehe Anhang II, Abschnitt III.11.g, insbesondere Punkt (ii) und (iii).

43 Siehe Anhang I, Abschnitt „Aufdeckung und Handhabung von Fällen, in denen zu Unrecht eine Beteiligung an der Regelung geltend gemacht wird".

44 Die Geschäftsordnung des informellen Gremiums der Datenschutzbehörden sollte von diesen auf der Grundlage ihrer Kompetenz für die Arbeitsorganisation und die gegenseitige Zusammenarbeit erarbeitet werden.

fortgesetzte Missachtung der Grundsätze wertet, was ihre Streichung aus der Datenschutzschild-Liste nach sich zieht.

(50) Wenn die Datenschutzbehörde, bei der die Beschwerde eingegangen ist, nichts oder zu wenig unternommen hat, um der Beschwerde abzuhelfen, hat die Privatperson die Möglichkeit, diese Vorgehensweise (bzw. Untätigkeit) vor den Gerichten des jeweiligen Mitgliedstaats anzufechten.

(51) Einzelpersonen können auch dann Beschwerden bei Datenschutzbehörden einreichen, wenn das DPA Panel nicht von der betreffenden Organisation als Beschwerdestelle benannt wurde. In diesen Fällen kann die Datenschutzbehörde die Beschwerden entweder an das Handelsministerium oder die FTC weiterleiten. Um die Zusammenarbeit in Angelegenheiten, die individuelle Beschwerden und Verstöße von Mitgliedsorganisationen des Datenschutzschilds betreffen, zu erleichtern und zu vertiefen, richtet das Handelsministerium eine spezielle Kontaktstelle ein, die als Bindeglied fungiert und bei Anfragen von Datenschutzbehörden zur Einhaltung der Grundsätze durch eine bestimmte Organisation behilflich ist.[45] Die FTC hat ihrerseits zugesagt, eine spezielle Kontaktstelle einzurichten[46] und die Datenschutzbehörden gemäß dem U.S. SAFE WEB Act bei den Ermittlungen zu unterstützen.[47]

(52) Viertens hat das Handelsministerium zugesagt, Beschwerden über Verstöße einer Organisation gegen die Grundsätze entgegenzunehmen, zu überprüfen und nach Möglichkeit zu klären. Zu diesem Zweck sieht das Handelsministerium spezielle Verfahren vor, wonach Datenschutzbehörden Beschwerden einer dafür eingerichteten Kontaktstelle vorlegen und dann bei den Unternehmen weiterverfolgen, um eine Klärung zu erleichtern. Um die Bearbeitung von Individualbeschwerden zu beschleunigen, setzt sich die Kontaktstelle direkt mit der jeweiligen Datenschutzbehörde in Verbindung, um Compliance-Probleme zu erörtern und sie vor allem innerhalb einer Frist von höchstens 90 Tagen nach Vorlage der Beschwerde über den aktuellen Stand zu unterrichten. Dies ermöglicht es betroffenen Personen, Beschwerden über Verstöße selbstzertifizierter US-Unternehmen direkt bei den nationalen Datenschutzbehörden einzureichen, die sie dann an das Handelsministerium als der für die Verwaltung des EU-US-Datenschutzschilds zuständigen Behörde weiterleiten. Das Handelsministerium hat auch zugesichert, bei der jährlichen Überprüfung der Funktionsweise des EU-US-Datenschutzschilds einen Bericht zu erstellen, der in aggregierter Form die im Laufe des Jahres bei ihm eingegangenen Beschwerden analysiert.[48]

(53) Wenn das Handelsministerium auf der Grundlage seiner Überprüfungen von Amts wegen, von Beschwerden oder sonstigen Informationen zu dem Schluss kommt, dass eine Organisation fortwährend gegen die Datenschutzgrundsätze verstoßen hat, streicht es diese Organisation von der Datenschutzschild-Liste. Die Weigerung, der abschließenden Entscheidung einer Einrichtung der freiwilligen Selbstkontrolle, unabhängigen Beschwerdestelle oder staatlichen Einrichtung, einschließlich einer Datenschutzbehörde, nachzukommen, wird als fortgesetzte Missachtung der Grundsätze gewertet.

---

[45] Siehe Anhang I, Abschnitte „Ausbau der Zusammenarbeit mit den Datenschutzbehörden“ und „Erleichterung der Lösungsfindung bei Beschwerden wegen Verletzung der Datenschutzvorschriften“ und Anhang II, Abschnitt II.7.e.

[46] Siehe Anhang IV, p.6.

[47] Ebenda.

[48] Siehe Anhang I, Abschnitt „Erleichterung der Lösungsfindung bei Beschwerden wegen Verletzung der Datenschutzvorschriften”.

(54) Fünftens muss sich eine dem Datenschutzschild angehörende Organisation den Ermittlungs- und Durchsetzungsbefugnissen der US-Behörden, insbesondere der *Federal Trade Commission*[49], unterwerfen, die effektiv für die Einhaltung der Grundsätze sorgen. Die FTC behandelt vorrangig Fälle der Missachtung der Datenschutzgrundsätze, die von unabhängigen Beschwerdestellen oder Einrichtungen der freiwilligen Selbstkontrolle, vom Handelsministerium und Datenschutzbehörden (aus eigener Initiative oder aufgrund von Beschwerden) an sie überwiesen werden, um festzustellen, ob gegen § 5 des FTC Act verstoßen wurde.[50] Die FTC hat zugesagt, ein standardisiertes Befassungsverfahren einzurichten, eine Kontaktstelle für von den Datenschutzbehörden überwiesene Fälle zu benennen und Informationen darüber auszutauschen. Überdies nimmt sie Beschwerden direkt von Privatpersonen entgegen und leitet von sich aus Ermittlungen ein, die den Datenschutzschild betreffen, insbesondere im Rahmen breiter angelegter Untersuchungen zu Fragen des Datenschutzes.

(55) Die FTC kann mit Zustimmung der Parteien behördliche Anordnungen („consent orders“) erlassen, um die Einhaltung der Grundsätze sicherzustellen, und überwacht systematisch die Befolgung derartiger Anordnungen. Bei Nichtbefolgung kann die FTC den Fall an ein zuständiges Gericht überweisen, um zivilrechtliche Sanktionen und sonstige Abhilfemaßnahmen zu erwirken, was auch etwaigen Schadenersatz für die Folgen des rechtswidrigen Verhaltens einschließt. Wahlweise kann die FTC auch direkt bei einem Bundesgericht eine einstweilige Verfügung, ein Unterlassungsurteil oder andere Abhilfemaßnahmen beantragen. Jeder „consent order“, der an eine dem Datenschutzschild angehörende Organisation ergeht, enthält Bestimmungen über die Selbstkontrolle[51], und die Organisationen sind gehalten, jene Teile eines der FTC vorgelegten Compliance- oder Sachstandsberichts, die den Datenschutzschild betreffen, öffentlich zu machen. Darüber hinaus führt die FTC eine Online-Liste der Unternehmen, die Anordnungen der FTC oder eines Gerichts im Zusammenhang mit dem Datenschutzschild unterliegen.

(56) Sechstens kann eine betroffene Person in der EU, sofern es nicht gelingt, einen Streit mithilfe einer dieser Möglichkeiten beizulegen, als letztes Mittel das *Datenschutzschild-Panel*, ein verbindliches Schiedsforum, in Anspruch nehmen. Die Organisationen müssen Privatpersonen darüber informieren, dass sie sich unter bestimmten Voraussetzungen für diese Möglichkeit entscheiden können, und sind verpflichtet, darauf zu reagieren, sobald eine Privatperson dieses Verfahren wählt, indem sie eine Mitteilung an die betroffene Organisation sendet.[52]

(57) Das Panel besteht aus einem Pool von mindestens 20 Schiedsrichtern, die vom Handelsministerium und der Kommission aufgrund ihrer Unabhängigkeit, Integrität

---

[49] Um dem Datenschutzschild beizutreten, muss eine Organisation öffentlich ihre Bereitschaft erklären, die Grundsätze einzuhalten, ihre Datenschutzbestimmungen im Einklang mit diesen Grundsätzen offenlegen und diese vollständig umsetzen. Ein Verstoß der Organisation gegen diese Grundsätze ist gemäß Abschnitt 5 des FTC Act zur Verhinderung unlauterer und irreführender Praktiken, die im Handel erfolgen oder den Handel beeinträchtigen, verfolgbar.

[50] Nach Informationen der FTC ist diese nicht befugt, im Bereich des Datenschutzes Vor-Ort-Begehungen durchzuführen. Allerdings kann sie Organisationen gegenüber die Herausgabe von Schriftstücken und die Anhörung von Zeugen anordnen (siehe § 20 des FTC Act) und die Gerichte anrufen, um diese Anordnungen bei Nichtbefolgung durchzusetzen.

[51] Anordnungen der FTC oder Gerichtsbeschlüsse können es Unternehmen zur Auflage machen, Datenschutzprogramme umzusetzen und der FTC regelmäßig Compliance-Berichte oder unabhängige externe Bewertungen dieser Programme vorzulegen.

[52] Siehe Anhang II, Abschnitt II.1.xi and III.7.c.

und Kenntnis des Datenschutzrechts der USA und der Europäischen Union benannt werden. Bei jedem Streit wählen die Parteien aus diesem Pool ein aus ein bis drei[53] Schiedsrichtern bestehendes Panel aus. Maßgeblich für die Schiedsverfahren sind Standardregeln, die zwischen dem Handelsministerium und der Kommission zu vereinbaren sind. Diese Regeln ergänzen den bereits vorhandenen Rahmen, der mehrere Merkmale enthält, welche die Zugänglichkeit dieses Instruments für Betroffene in der EU sehr erleichtern: i) Sie können sich bei der Ausarbeitung ihrer Beschwerde vor dem Panel von ihrer nationalen Datenschutzbehörde unterstützen lassen; ii) das Schiedsverfahren findet zwar in den Vereinigten Staaten statt, doch können sich betroffene Personen in der EU für eine Teilnahme per Video- oder Telefonkonferenz entscheiden, die für den Einzelnen mit keinen Kosten verbunden ist; iii) zwar ist in der Regel Englisch die Verfahrenssprache, doch werden auf einen begründeten Antrag hin normalerweise[54] Dolmetscher für die mündliche Verhandlung sowie Übersetzer bereitgestellt, ohne dass sich daraus Kosten für die betroffene Person ergeben; iv) jede Partei muss selbst für die anfallenden Anwaltsgebühren aufkommen, wenn sie sich vor dem Panel von einem Anwalt vertreten lässt; das Handelsministerium wird aber einen Fonds mit jährlichen Beiträgen der Mitgliedsorganisationen des Datenschutzschilds einrichten, der bis zu einem von den amerikanischen Behörden in Abstimmung mit der Kommission festzulegenden Höchstbeitrag die erstattungsfähigen Kosten des Schiedsverfahrens abdeckt.

(58) Das Datenschutzschild-Panel ist befugt, „einzelfallbezogene, nichtmonetäre billigkeitsrechtliche Ansprüche“[55] anzuerkennen, um Verstöße gegen die Grundsätze abzustellen. Zwar berücksichtigt das Panel dabei die bereits von anderen Instrumenten des Datenschutzschilds erwirkten Abhilfemaßnahmen, doch steht es Privatpersonen frei, das Schiedsverfahren in Anspruch zu nehmen, wenn sie die anderen Abhilfemaßnahmen für unzureichend erachten. Damit können betroffene Personen in der EU in allen Fällen auf das Schiedsverfahren zurückgreifen, in denen die Vorgehensweise oder Untätigkeit der zuständigen amerikanischen Behörden (beispielsweise der FTC) nicht zu einer zufriedenstellenden Klärung ihrer Beschwerden geführt hat. Das Schiedsverfahren kann nicht in Anspruch genommen werden, wenn eine Datenschutzbehörde rechtlich befugt ist, bei einem selbstzertifizierten US-Unternehmen die in Frage stehende Beschwerde selbst zu klären, nämlich in solchen Fällen, in denen die Organisation entweder bei der Verarbeitung von Personaldaten im Rahmen eines Beschäftigungsverhältnisses zur Zusammenarbeit mit den Datenschutzbehörden und zur Befolgung ihrer Empfehlungen verpflichtet ist oder eine solche Verpflichtung freiwillig eingegangen ist. Einzelpersonen können den Schiedsspruch auf der Grundlage des Federal Arbitration Act vor amerikanischen Gerichten durchsetzen, so dass ihnen ein Rechtsbehelf zur Verfügung steht, falls sich ein Unternehmen nicht daran hält.

(59) Siebtens: Wenn sich eine Organisation nicht an ihre Zusage hält, die Grundsätze und die veröffentlichten Datenschutzbestimmungen einzuhalten, bieten die Rechtsvorschriften der US-Bundesstaaten gegebenenfalls zusätzliche Möglichkeiten, um im Rahmen des Deliktrechts und in Fällen von arglistiger Täuschung, unlauteren

[53] Die Anzahl der Schiedsrichter ist zwischen den Parteien zu vereinbaren.

[54] Das Panel kann allerdings in einem konkreten Fall zu dem Schluss gelangen, dass eine Kostenübernahme nicht gerechtfertigt oder unverhältnismäßig wäre.

[55] Privatpersonen können im Schiedsverfahren keinen Schadenersatz geltend machen, doch schließt die Inanspruchnahme des Schiedsverfahrens nicht die Möglichkeit aus, vor ordentlichen Gerichten der USA auf Schadensersatz zu klagen.

oder irreführenden Handlungen oder Praktiken bzw. Vertragsbruch rechtlich gegen sie vorzugehen.

(60) Wenn eine Datenschutzbehörde ferner nach Eingang der Beschwerde einer betroffenen Person in der EU zu der Feststellung gelangt, dass die Übermittlung der personenbezogenen Daten einer Person an eine amerikanische Organisation unter Verstoß gegen das EU-Datenschutzrecht durchgeführt wird, einschließlich der Fälle, in denen der Datenexporteur Anlass zu der Annahme hat, dass die amerikanische Organisation sich nicht an die Grundsätze hält, kann sie auch ihre Befugnisse gegenüber dem Datenexporteur ausüben und erforderlichenfalls die Aussetzung der Datenübermittlung anordnen.

(61) In Anbetracht der in diesem Abschnitt dargelegten Informationen geht die Kommission davon aus, dass die vom Handelsministerium der USA herausgegebenen Datenschutzgrundsätze als solche ein Schutzniveau personenbezogener Daten gewährleisten, das dem Niveau der in der Richtlinie 95/46/EG verankerten materiell-rechtlichen Grundsätze der Sache nach gleichwertig ist.

(62) Zudem garantieren die Transparenzpflichten und die Verwaltung sowie Überprüfung der Einhaltung des Datenschutzschilds durch das Handelsministerium die wirksame Anwendung der Datenschutzgrundsätze.

(63) Des Weiteren geht die Kommission davon aus, dass insgesamt gesehen die vom Datenschutzschild vorgesehenen Rechtsschutz- und Durchsetzungsinstrumente es gestatten, Verstöße von dem Datenschutzschild angehörenden Organisationen gegen die Grundsätze in der Praxis aufzudecken und zu ahnden, und dass damit den betroffenen Personen Rechtsbehelfe an die Hand gegeben werden, um Zugang zu den sie betreffenden personenbezogenen Daten zu erlangen und letzten Endes die Korrektur oder Löschung dieser Daten zu erwirken.

3. Abfrage und Nutzung personenbezogener Daten, die im Rahmen des EU-US-Datenschutzschilds übermittelt werden, durch staatliche Stellen der USA

(64) Wie aus Anhang II Abschnitt I.5 hervorgeht, wird die Einhaltung der Grundsätze so weit eingeschränkt, wie dies aus Gründen der nationalen Sicherheit, des öffentlichen Interesses oder der Strafverfolgung erforderlich ist.

(65) Die Kommission hat die Einschränkungen und Garantien bewertet, die im amerikanischen Recht für im Rahmen des EU-US-Datenschutzschilds übermittelte Daten gelten, welche durch staatliche Einrichtungen der USA aus Gründen der nationalen Sicherheit, der Strafverfolgung oder anderer im öffentlichen Interesse liegender Ziele gesammelt und genutzt werden. Überdies hat die Regierung der USA über das Amt des Director of National Intelligence (ODNI)[56] der Kommission gegenüber detaillierte Erklärungen abgegeben und Zusagen gemacht, die in Anhang VI dieses Beschlusses enthalten sind. In einem Schreiben, das vom Außenminister unterzeichnet wurde und diesem Beschluss als Anhang III beigefügt

[56] Der Director of National Intelligence (DNI) ist Leiter der Intelligence Community und berät den Präsidenten und den National Security Council. Siehe Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-458 vom 17.12.2004. Unter anderem soll das ODNI die Anforderungen an die Aufklärungstätigkeit der Intelligence Community festlegen sowie die Anordnung, Erhebung, Analyse, Aufbereitung und Verbreitung nachrichtendienstlicher Erkenntnisse leiten und verwalten, unter anderem durch die Erarbeitung von Leitlinien für die Gewinnung, Nutzung und Weitergabe von Informationen und Aufklärungsdaten. Siehe Sec. 1.3 (a), (b) of E.O. 12333.

ist, hat sich die Regierung der USA zudem verpflichtet, eine neue Aufsichtsinstanz für Eingriffe aus Gründen der nationalen Sicherheit ins Leben zu rufen, die Ombudsperson des Datenschutzschilds (Privacy Shield Ombudsperson), die von der Intelligence Community unabhängig ist. Außerdem werden in einer Erklärung des Justizministeriums der USA, die in Anhang VII des vorliegenden Beschlusses enthalten ist, die Einschränkungen und Garantien dargelegt, die für die Sammlung und Nutzung von Daten durch staatliche Stellen für Zwecke der Strafverfolgung und andere im öffentlichen Interesse liegende Ziele gelten. Um für größere Transparenz zu sorgen und die Rechtsverbindlichkeit dieser Zusagen zu unterstreichen, werden alle aufgeführten und diesem Beschluss beigefügten Schriftstücke im Bundesregister der USA veröffentlicht.

(66) Auf die Feststellungen der Kommission zu den Beschränkungen der Sammlung und Nutzung von personenbezogenen Daten, die aus der Europäischen Union in die Vereinigten Staaten übermittelt werden, durch staatliche Stellen der USA und zum Vorhandensein eines effektiven Rechtsschutzes wird nachfolgend näher eingegangen.

3.1. Sammlung und Nutzung durch staatliche Stellen der USA aus Gründen der nationalen Sicherheit

(67) Aus der Analyse der Kommission geht hervor, dass die Rechtsvorschriften der USA die Sammlung und Nutzung von im Rahmen des EU-US-Datenschutzschilds übermittelten personenbezogenen Daten für Zwecke der nationalen Sicherheit einer Reihe von Beschränkungen unterwerfen sowie Aufsichtsverfahren und Rechtsschutzinstrumente vorsehen, die hinreichende Garantien für den wirksamen Schutz dieser Daten vor rechtswidrigen Eingriffen und Missbrauch enthalten.[57] Seit dem Jahr 2013, in dem die Kommission ihre zwei Mitteilungen veröffentlichte (siehe Erwägungsgrund 7), ist der rechtliche Rahmen spürbar verstärkt worden, wie im Folgenden dargelegt.

3.1.1. Einschränkungen

(68) Nach der Verfassung der USA fällt die Gewährleistung der nationalen Sicherheit in die Zuständigkeit des Präsidenten als Oberbefehlshaber, Staatsoberhaupt und, soweit die Auslandsaufklärung betroffen ist, Verantwortlicher für die Außenpolitik der USA.[58] Der Kongress ist zwar befugt, ihm Beschränkungen aufzuerlegen, und hat von diesem Recht mehrfach Gebrauch gemacht, doch kann der Präsident innerhalb dieser Grenzen die Aktivitäten der amerikanischen Intelligence Community lenken, insbesondere durch Executive Orders oder Presidential Directives. Dies gilt natürlich auch für Bereiche, in denen keine Vorgaben des Kongresses zu befolgen sind. Zwei zentrale Rechtsvorschriften dieser Art sind die Executive Order 12333 („E.O. 12333“)[59] und die Presidential Policy Directive 28.

---

57 Siehe Schrems, Rn. 91.

58 Artikel II der Verfassung der USA. Siehe auch Einleitung zur PPD-28.

59 E.O. 12333: United States Intelligence Activities, Federal Register Vol. 40, No. 235 (8.12.1981). Soweit die Executive Order für die Öffentlichkeit zugänglich ist, regelt sie die Ziele, die Ausrichtung, die Aufgaben und die Arbeitsgebiete der nachrichtendienstlichen Tätigkeit in den USA (wie auch die Kompetenzen der einzelnen Nachrichtendienste) und legt die allgemeinen Parameter für die Gestaltung der Aufklärungsarbeit fest (insbesondere den Erlass spezifischer Verfahrensregeln). Nach § 3.2 des E.O. 12333 ist es Aufgabe des Präsidenten, mit Unterstützung des National Security Council und des DNI die Direktiven, Verfahren und Leitlinien vorzugeben, die zur Umsetzung der Executive Order erforderlich sind.

(69) Die am 17. Januar 2014 erlassene Presidential Policy Directive 28 („PPD-28“) bringt eine Reihe von Einschränkungen für die „Signalaufklärung“ mit sich.[60] Diese Verordnung ist für die Nachrichtendienste der USA verbindlich[61] und bleibt auch bei einem Regierungswechsel in Kraft.[62] Die PPD-28 ist für Personen außerhalb der USA, darunter Betroffene in der EU, von besonderer Bedeutung. Sie enthält unter anderem folgende Festlegungen:

a) Die Signalaufklärung muss gesetzlich geregelt oder vom Präsidenten autorisiert sein und muss im Einklang mit der Verfassung der USA (insbesondere dem 4. Zusatzartikel) und dem amerikanischen Recht stehen;

b) alle Personen sind unabhängig von ihrer Nationalität oder ihrem Wohnort würde- und respektvoll zu behandeln;

c) alle Personen haben berechtigte Datenschutzinteressen beim Umgang mit ihren personenbezogenen Informationen;

d) die Privatsphäre und die bürgerlichen Freiheiten sind integraler Bestandteil aller Überlegungen bei der Planung der signalerfassenden Aufklärung in den USA;

e) die Signalaufklärung der USA muss daher angemessene Garantien für die personenbezogenen Informationen aller Privatpersonen unabhängig von ihrer Nationalität oder ihres Wohnorts einschließen.

(70) In der PPD-28 ist festgelegt, dass die Signalaufklärung ausschließlich dann zum Einsatz kommt, wenn dies der Auslandsaufklärung oder Spionageabwehr dient und im Interesse der Regierung oder einzelner Ministerien liegt, nicht aber zu anderen Zwecken (etwa um US-Unternehmen einen Wettbewerbsvorteil zu verschaffen). Dem ODNI zufolge sollten die Nachrichtendienste „wann immer dies praktikabel erscheint, die Erhebung auf spezifische Aufklärungsziele oder -themen im Ausland konzentrieren, indem sie Selektoren (z. B. konkrete Objekte, Suchkriterien und Identifikatoren) heranziehen“.[63] Darüber hinaus bieten die Erklärungen des ODNI die Gewähr, dass Entscheidungen über die Nachrichtengewinnung nicht dem Ermessen einzelner Geheimdienstmitarbeiter überlassen bleiben, sondern Gegenstand der Strategien und Verfahren sind, die von den verschieden Nachrichtendiensten der USA zur Umsetzung der PPD-28 zu erarbeiten sind.[64] Dementsprechend erfolgen die Ermittlung und die Festlegung geeigneter Selektoren im Rahmen des „National Intelligence Priorities Framework“ (NIPF), der dafür sorgt, dass die Schwerpunkte der nachrichtendienstlichen Tätigkeit auf hoher politischer Ebene bestimmt und regelmäßig überprüft werden, damit sie jederzeit den Anforderungen der nationalen Sicherheit genügen und mögliche Risiken, auch eine Gefährdung der Privatsphäre,

---

60 Nach der E.O. 12333 soll der Direktor der National Security Agency (NSA) als operativer Leiter der signalerfassenden Aufklärung für eine einheitliche Organisation der Aktivitäten in diesem Bereich sorgen.

61 Eine Begriffsbestimmung des Terminus „Intelligence Community“ findet sich in § 3.5 (h) des E.O. 12333 mit Nr. 1 der PPD-28.

62 Siehe Memorandum by the Office of Legal Counsel, Department of Justice, to President Clinton, 29.1.2000. Nach diesem Rechtsgutachten haben Presidental Directives „materiell-rechtlich gesehen die gleiche Rechtswirkung wie eine Executive Order“.

63 Erklärungen des ODNI (Anhang VI), S. 3.

64 Siehe § 4(b),(c) der PPD-28. Nach öffentlich vorliegenden Informationen bestätigte die 2015 vorgenommene Überprüfung die bestehenden sechs Zielsetzungen. Siehe ODNI, Signals Intelligence Reform, 2016 Progress Report.

berücksichtigen.[65] Auf dieser Grundlage untersuchen und benennen Mitarbeiter der Nachrichtendienste konkrete Suchkriterien, anhand derer Erkenntnisse aus dem Ausland gewonnen werden können, die den Schwerpunkten entsprechen.[66] Die Suchkriterien oder Selektoren müssen regelmäßig daraufhin überprüft werden, ob sie weiterhin wertvolle Erkenntnisse entsprechend den gesetzten Schwerpunkten liefern.[67]

(71) Außerdem heißt es in der PPD-28, dass die Datensammlung immer[68] so „zielgenau wie möglich" erfolgen und die Intelligence Community vorrangig auf andere Informationen und auf geeignete und machbare Alternativen zurückgreifen soll,[69] worin eine allgemeine Bevorzugung gezielter Erfassung gegenüber der Sammelerhebung zum Ausdruck kommt. Den Zusicherungen des ODNI zufolge wird so vor allem sichergestellt, dass eine Sammelerhebung nicht „massenhaft" oder „anlassunabhängig" erfolgt und dass die Ausnahme nicht zur Regel wird.[70]

(72) Zwar heißt es in der PPD-28, dass Nachrichtendienste unter bestimmten Umständen auf die Sammelerhebung zurückgreifen müssen, beispielweise um neue oder sich abzeichnende Bedrohungen zu erkennen, aber die Dienste sind gehalten, Alternativen den Vorzug zu geben, die eine gezielte Signalaufklärung ermöglichen.[71] Die Sammelerhebung wird folglich nur gestattet. wenn die gezielte Erhebung mithilfe von Selektoren – d. h. zielgenauen Suchkriterien wie der E-Mail-Adresse oder Telefonnummer einer Zielperson – „aufgrund technischer oder operativer Erwägungen" nicht möglich ist.[72] Dies gilt sowohl für die Art und Weise, in der Signalaufklärungsdaten erhoben werden, als auch für die Datensammlung selbst.[73]

(73) Den Erklärungen des ODNI zufolge sind die Nachrichtendienste bemüht, auch wenn sie nicht auf zielgenaue Suchkriterien zurückgreifen können, die Datenerhebung „so weit wie möglich" einzugrenzen. Dazu setzen sie „Filter und andere technische Mittel ein, um die Datensammlung auf solche Kommunikationsvorgänge zu konzentrieren,

---

65 Erklärung des ODNI (Anhang VI), S. 6 (mit Bezugnahme auf die Intelligence Community Directive 204). Siehe auch § 3 der PPD-28.

66 Erklärungen des ODNI (Anhang VI), S. 6. Siehe beispielsweise NSA Civil Liberties and Privacy Office (NSA CLPO), NSA's Civil Liberties and Privacy Protections for Targeted SIGINT Activities under Executive Order 12333, 7.10.2014. Siehe auch ODNI Status Report 2014. Bei Anträgen auf Datenzugriff nach § 702 des FISA (des Gesetzes, das die Überwachung der Auslandsaufklärung regelt) gelten vom FISC (dem dafür zuständigen Gericht) gebilligte Minimierungsverfahren. Siehe NSA CLPO, NSA's Implementation of Foreign Intelligence Surveillance Act Section 702, 16.4.2014.

67 Siehe Signal Intelligence Reform, 2015 Anniversary Report. Siehe auch Erklärungen des ODNI (Anhang VI), S. 6, 8-9, 11.

68 Siehe Erklärung des ODNI (Anhang VI), S. 3.

69 Es sei auch darauf verwiesen, dass gemäß § 2.4 der E.O. 12333 die Nachrichtendienste „die mit den geringsten Eingriffen verbundenen Erhebungsmethoden verwenden sollen, die in den Vereinigten Staaten praktikabel sind". Was die Grenzen einer Ersetzung der Sammelerhebung durch gezielte Sammlungen anbelangt, siehe die Ergebnisse einer Einschätzung des National Research Council, die von der Agentur der Europäischen Union für Grundrechte veröffentlicht wurde: Surveillance by intelligence services: fundamental rights, safeguards and remedies in the EU (2015), S. 18

70 Erklärungen des ODNI (Anhang VI), S. 4.

71 Siehe auch § 5(d) der PPD-28, wonach der Director of National Intelligence in Abstimmung mit den Leitern der einschlägigen Nachrichtendienste und dem Office of Science and Technology Policy dem Präsidenten einen „Bericht über die Möglichkeiten zur Erstellung einer Software vorzulegen hat, die der Intelligence Community die Aufgabe erleichtern würde, die Sammelerhebung verstärkt durch gezielte Informationsgewinnung zu ersetzen". Nach öffentlich vorliegenden Informationen lautete das Fazit des Berichts, dass „keine softwaregestützte Alternative verfügbar ist, die bei der Aufdeckung bestimmter Gefahren für die nationale Sicherheit die Sammelerhebung vollständig ersetzen kann". Siehe Signals Intelligence Reform, 2015 Anniversary Report.

72 Siehe Erklärungen des ODNI (Anhang VI), S. 3.

73 Erklärungen des ODNI (Anhang VI), S. 3.

die nachrichtendienstliche Erkenntnisse versprechen“ (und berücksichtigen damit die von US-Politikern gemäß dem im Erwägungsgrund 70 dargestellten Prozess aufgestellten Anforderungen). Im Ergebnis wird die Sammelerhebung zumindest auf zweierlei Weise zielgerichtet eingesetzt: Erstens werden damit immer konkrete Ziele der Auslandsaufklärung verfolgt (z. B. Signalaufklärung zur Erlangung von Erkenntnissen über Terroristengruppen, die in einer bestimmten Region operieren) und vor allem diesbezügliche Kommunikationsdaten erhoben. Wie das ODNI dazu ausführte, ist dies auch daran abzulesen, dass „die Signalaufklärung der Vereinigten Staaten nur einen Bruchteil der Kommunikationsvorgänge im Internet erfasst“.[74] Zweitens ist den Erläuterungen des ODNI zu entnehmen, dass die Filter und sonstigen technischen Mittel so konzipiert sind, dass die Erhebung „so präzise wie möglich“ erfolgt, um den Anteil „nichtrelevanter“ Informationen auf ein Mindestmaß zu reduzieren.

(74) Letztendlich beschränkt aber selbst in dem Fall, dass die Vereinigten Staaten die Sammelerhebung von Signalaufklärungsdaten für erforderlich halten, die PPD-28 unter den in den Erwägungsgründen (70)-(73) dargelegten Voraussetzungen die Nutzung derartiger Informationen auf einen spezifischen Katalog von sechs Zielsetzungen der nationalen Sicherheit, um die Privatsphäre und die bürgerlichen Freiheiten aller Personen unabhängig von ihrer Nationalität und ihrem Wohnort zu schützen.[75] Diese zulässigen Zielsetzungen umfassen Maßnahmen zur Aufdeckung und Abwehr von Bedrohungen, die sich aus Spionage, Terrorismus, Massenvernichtungswaffen, Bedrohungen der Netz- und Informationssicherheit, möglichen Anschlägen auf die Streitkräfte und militärisches Personal ergeben, sowie von länderübergreifenden kriminellen Bedrohungen, die mit den anderen fünf Zielsetzungen im Zusammenhang stehen, und unterliegen einer zumindest jährlichen Überprüfung. Den Erklärungen der amerikanischen Regierung zufolge haben die Nachrichtendienste ihre Analyseverfahren und -standards für die Abfrage ungeprüfter Signalaufklärungsdaten verschärft, um diesen Anforderungen zu genügen. Gezielte Abfragen „stellen sicher, dass den Analysten nur Vorgänge vorgelegt werden, die einen potenziellen Erkenntniswert aufweisen“.[76]

(75) Von Belang sind diese Einschränkungen insbesondere für personenbezogene Daten, die im Rahmen des EU-US-Datenschutzschilds übermittelt werden, vor allem wenn die Sammlung der Daten außerhalb der Vereinigten Staaten erfolgt, was die Übermittlung über transatlantische Kabel zwischen der EU und den USA einschließt. Wie von den US-Behörden in den Erklärungen des ODNI bestätigt wurde, gelten die in diesem Beschluss dargelegten Beschränkungen und Garantien – darunter jene der PPD-28 – für eine solche Sammlung.[77]

(76) Diese Prinzipien bringen den Wesensinhalt der Grundsätze der Notwendigkeit und der Verhältnismäßigkeit zum Ausdruck, auch wenn diese Begriffe nicht ausdrücklich verwendet werden. Die gezielte Sammlung hat eindeutig Vorrang, wohingegen die Sammelerhebung auf (Ausnahme-)Situationen beschränkt wird, in denen die gezielte

---

[74] Erklärungen des ODNI (Anhang VI). Hiermit wird konkret auf die Bedenken eingegangen, die von den nationalen Datenschutzbehörden in ihrer Stellungnahme zum Entwurf des Angemessenheitsbeschlusses vorgebracht wurden. Siehe Article 29 Data Protection Working Party, Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision (angenommen am 13.4.2016), S. 38 mit Nr. 47.

[75] Siehe § 2 der PPD-28.

[76] Erklärungen des ODNI (Anhang VI), S. 4. Siehe auch Intelligence Community Directive 203.

[77] Erklärungen des ODNI (Anhang VI), S. 2. Es gelten auch die in der E.O. 12333 festgelegten Einschränkungen (wonach z. B. die gewonnenen Erkenntnisse den vom Präsidenten gesetzten Schwerpunkten der nachrichtendienstlichen Tätigkeit entsprechen müssen).

Sammlung aus technischen oder operativen Gründen nicht möglich ist. Selbst wenn sich die *Sammelerhebung* nicht vermeiden lässt, ist die weitere *„Nutzung"* derartiger Daten *stark eingeschränkt* und nur für konkrete und berechtigte Zielsetzungen der nationalen Sicherheit zulässig.[78]

(77) Da es sich um eine Direktive des Präsidenten in seiner Eigenschaft als Staatsoberhaupt handelt, sind ihre Bestimmungen für die gesamte Intelligence Community verbindlich und inzwischen durch Regeln und Verfahren der Nachrichtendienste weiter ausgestaltet worden, die die allgemeinen Grundsätze in konkrete Anleitungen für die alltägliche Praxis umsetzen. Der Kongress ist zwar selbst nicht an die PPD-28 gebunden, hat aber gleichfalls Schritte eingeleitet, um sicherzustellen, dass die Erhebung und die Abfrage personenbezogener Daten in den USA gezielt und nicht „anlassunabhängig" erfolgen.

(78) Aus den verfügbaren Informationen, darunter den Erklärungen der amerikanischen Regierung, ergibt sich, dass nach der Übermittlung von Daten an Organisationen mit Sitz in den USA, die sich für eine Selbstzertifizierung unter dem EU-US-Datenschutzschild entschieden haben, die amerikanischen Nachrichtendienste personenbezogene Daten nur sammeln dürfen[79], wenn ihr Antrag mit dem Foreign Intelligence Surveillance Act (FISA) im Einklang steht oder über einen National Security Letter (NSL) des Federal Bureau of Investigation (FBI) erfolgt[80]. Der FISA sieht verschiedene Rechtsgrundlagen vor, die herangezogen werden können, um die im Rahmen des EU-US-Datenschutzschilds von betroffenen Personen in der EU übermittelten personenbezogenen Daten zu erheben (und anschließend zu verarbeiten). Abgesehen von § 104 FISA[81], der die herkömmliche individuelle elektronische Überwachung zum Gegenstand hat, und § 402 FISA[82], der den Einsatz von Geräten

---

78 Siehe Schrems, Rn. 93.

79 Darüber hinaus kann die Erhebung von Daten durch den FBI auch auf der Grundlage von autorisierten Strafverfolgungsmaßnahmen erfolgen (siehe Abschnitt 3.2 des vorliegenden Beschlusses).

80 Für weitere Erläuterungen zur Verwendung von NSL siehe Erklärungen des ODNI (Anhang VI), S. 13-14 mit Nr. 38. Daraus geht hervor, dass das FBI nur auf NSL zurückgreifen darf, um nichtinhaltliche Informationen im Rahmen einer autorisierten Ermittlung zu Fragen der nationalen Sicherheit zu beantragen, die dem Schutz vor internationalem Terrorismus und verdeckten nachrichtendienstlichen Aktivitäten dient. Was die Datenübermittlung unter dem EU-US-Datenschutzschild anbelangt, ist die wichtigste Rechtsgrundlage wohl der Electronic Communications Privacy Act (18 U.S.C. § 2709), der vorschreibt, dass ein Antrag auf Informationen über Teilnehmer oder Bewegungsdaten einen „Begriff verwende[n muss], der konkret eine Person, eine Stelle, eine Telefonnummer oder ein Konto bezeichnet".

81 50 U.S.C. § 1804. Diese Rechtsgrundlage erfordert eine „Darlegung der Fakten und Umstände, auf die sich die Annahme des Antragstellers stützt, dass (A) das Ziel der elektronischen Überwachung eine ausländische Macht oder ein Vertreter einer ausländischen Macht ist", worunter auch Nicht-US-Bürger fallen können, die sich am internationalen Terrorismus oder an der internationalen Weitergabe von Massenvernichtungswaffen (einschließend vorbereitender Maßnahmen) beteiligen (50 U.S.C. § 1801 (b)(1)). Daraus ergibt sich aber nur ein theoretischer Zusammenhang mit der Übermittlung personenbezogener Daten unter dem EU-US-Datenschutzschild, denn bei der Darlegung der Tatsachen ist auch die Annahme zu begründen, dass „alle Objekte oder Orte, die elektronisch überwacht werden sollen, bereits von einer ausländischen Macht oder einem Vertreter einer ausländischen Macht genutzt werden oder dies beabsichtigt ist". In jedem Falle erfordert die Inanspruchnahme dieser Rechtsgrundlage einen Antrag an den FISC, der unter anderem zu beurteilen hat, ob diese Annahme auf der Grundlage der vorgelegten Tatsachen vermutlich zutrifft.

82 50 U.S.C. § 1842 mit § 1841(2) und § 3127 des Titels 18. Diese Rechtsgrundlage betrifft nicht den Inhalt der Kommunikation, sondern Informationen über den Kunden oder Teilnehmer, der einen Dienst in Anspruch nimmt (z. B. Name, Anschrift, Telefonnummer, Dauer/Art der Dienstleistung, Zahlungsquelle/-modalitäten). Sie erfordert die Beantragung einer Anordnung des FISC (oder eines U.S. Magistrate Judge) und die Verwendung eines konkreten Suchbegriffs im Sinne von § 1841(4), d. h. eines Begriffs, der eine Person, ein Konto usw. präzise bezeichnet und den Suchbereich möglichst stark eingrenzen soll.

zur Rufnummernerfassung von ausgehenden und eingehenden Anrufen regelt, sind die beiden wichtigsten Rechtsgrundlagen § 501 des FISA (vormals § 215 des U.S. PATRIOT ACT) und § 702 des FISA.[83]

(79) In diesem Zusammenhang untersagt der USA FREEDOM Act, der am 2. Juni 2015 in Kraft getreten ist, die Sammelerhebung von Daten auf der Grundlage von § 402 des FISA (Rufnummernerfassung), § 501 des FISA (vormals § 215 des U.S. PATRIOT ACT)[84] und durch die Verwendung von NSL und verlangt stattdessen die Anwendung konkreter „Suchkriterien".[85]

(80) Wenngleich der FISA weitere Rechtsgrundlagen für die nachrichtendienstliche Tätigkeit auf nationaler Ebene enthält, wozu auch die Signalaufklärung gehört, zeigt die Bewertung der Kommission, dass diese Rechtsgrundlagen im Falle der Übermittlung personenbezogener Daten unter dem EU-US-Datenschutzschild ebenfalls Eingriffe staatlicher Behörden auf die gezielte Sammlung und den gezielten Zugang einschränken.

(81) Dies betrifft eindeutig die herkömmliche individuelle elektronische Überwachung gemäß § 104 FISA[86]. Im Falle von § 702 FISA, der die Grundlage für zwei wichtige Aufklärungsprogramme der amerikanischen Nachrichtendienste (PRISM, UPSTREAM) bildet, erfolgt die Suche gezielt durch die Verwendung individueller Selektoren, die konkrete Kommunikationseinrichtungen identifizieren, so etwa die E-Mail-Adresse oder die Telefonnummer der Zielperson, aber nicht Stichwörter oder gar die Namen von Zielpersonen.[87] Wie das Privacy and Civil Liberties Oversight Board (PCLOB) zum Ausdruck gebracht hat, geht es bei der Überwachung gemäß § 702 „ausschließlich um konkrete Zielpersonen [die nicht Bürger der USA sind], deren Auswahl eine Einzelfallprüfung voraussetzt".[88] Aufgrund einer „Auslaufklausel" muss

---

[83] Während § 501 des FISA (vormals § 215 des U.S. PATRIOT ACT) das FBI autorisiert, einen Gerichtsbeschluss zu beantragen, der auf die Herausgabe „materieller Objekte" (insbesondere Metadaten der telefonischen Kommunikation, aber auch Geschäftsunterlagen) gerichtet ist, gestattet § 702 des FISA den amerikanischen Nachrichtendiensten gegebenenfalls den Zugriff auf Informationen, einschließlich des Inhalts von Online-Kommunikation, die ihren Ausgangspunkt in den USA haben, sich aber an bestimmte Nicht-US-Bürger außerhalb der Vereinigten Staaten richten.

[84] Dieser Bestimmung zufolge kann das FBI den Zugriff auf „materielle Objekte" (z. B. Unterlagen, Schriftstücke, Akten) beantragen, sofern es dem Foreign Intelligence Surveillance Court (FISC) gegenüber hinlänglich begründet, dass diese für konkrete Ermittlungen des FBI von Belang sind. Bei seinen Recherchen muss das FBI vom FISC bestätigte Suchbegriffe verwenden, bei denen der „begründete und formulierbare Verdacht" eines Zusammenhangs mit einer oder mehreren ausländischen Mächten oder deren Vertretern besteht, die sich am internationalen Terrorismus oder vorbereitenden Handlungen beteiligen. Siehe PCLOB, § 215 Report, S. 59; NSA CLPO, Transparency Report: The USA Freedom Act Business Records FISA Implementation, 15.1.2016, S. 4-6.

[85] Erklärungen des ODNI (Anhang VI), S. 13 (n. 38).

[86] Siehe Fußnote 81.

[87] PCLOB, § 702 Report, S. 32-33 mit weiterführenden Informationen. Nach Angaben ihrer Datenschutzabteilung muss sich die NSA vergewissern, dass zwischen Zielperson und Selektor eine Verbindung besteht, die zu erwartenden ausländischen Aufklärungsdaten dokumentieren, die Daten von zwei ranghohen NSA-Analysten überprüfen und bestätigen lassen und den gesamten Ablauf für spätere Überprüfungen durch das ODNI und das Justizministerium nachvollziehbar machen. Siehe NSA CLPO, NSA's Implementation of Foreign Intelligence Act Section 702, 16.4.2014.

[88] PLCOB, § 702 Report, S. 111. Siehe auch Erklärung des ODNI (Anhang VI), S. 9 („Die Sammlung gemäß § 702 des [FISA] erfolgt nicht ‚massenhaft und anlassunabhängig', sondern ist strikt auf die Sammlung ausländischer Aufklärungsdaten einzeln benannter legitimer Zielpersonen gerichtet") sowie S. 13, Nr. 36 (mit Bezugnahme auf ein Gutachten des FISC aus dem Jahr 2014); NSA CLPO, NSA's Implementation of Foreign Intelligence Act Section 702, 16.4.2014. Selbst im Rahmen von UPSTREAM darf die NSA nur die Überwachung der elektronischen Kommunikation beantragen, die an vorgegebene Selektoren gerichtet ist, von diesen ausgeht oder diese betrifft.

§ 702 des FISA im Jahre 2017 überprüft werden, und die Kommission muss zu diesem Zeitpunkt eine Neubewertung der Garantien vornehmen, die betroffenen Personen in der EU zur Verfügung stehen.

(82) Überdies hat die Regierung der USA der Europäischen Kommission in ihren Erklärungen ausdrücklich zugesichert, dass die Intelligence Community der USA „keine systematische anlassunabhängige Überwachung von Personen betreibt, was normale europäische Bürger einschließt“.[89] Was in den USA erhobene personenbezogene Daten anbelangt, wird diese Erklärung durch empirische Erkenntnisse untermauert, wonach die *Zugriffsanfragen* über NSL und gemäß FISA sowohl einzeln betrachtet als auch zusammengenommen nur eine relativ kleine Anzahl von Zielpersonen betreffen, wenn man den Datenverkehr im Internet insgesamt betrachtet.[90]

(83) Im Hinblick auf den *Zugang* zu erhobenen Daten und die *Datensicherheit* schreibt die PPD-28 vor, dass der Zugriff „auf befugte Mitarbeiter zu beschränken ist, die diese Informationen für die Erfüllung ihres Auftrags benötigen“ und dass personenbezogene Daten „unter Bedingungen zu verarbeiten und zu speichern sind, die hinreichenden Schutz gewährleisten und den Zugriff unbefugter Personen verhindern, was mit den für sensible Informationen geltenden Garantien im Einklang steht“. Mitarbeiter der Nachrichtendienste sind auf angemessene Weise hinreichend mit den in der PPD-28 dargelegten Grundsätzen vertraut zu machen.[91]

(84) Was abschließend die *Speicherung* und *Weitergabe* personenbezogener Daten betrifft, die Nachrichtendienste der USA von Betroffenen in der EU erheben, verlangt PPD-28, dass alle Personen (einschließlich Nicht-US-Bürger) würde- und respektvoll zu behandeln sind, dass alle Personen berechtigte Datenschutzinteressen beim Umfang mit ihren personenbezogenen Daten haben und dass die Nachrichtendienste folglich dafür sorgen müssen, dass für derartige Daten angemessene Schutzvorkehrungen

---

89 Erklärungen des ODNI (Anhang VI), S. 18. Siehe auch S. 6, wonach die anwendbaren Verfahren „das deutliche Bemühen erkennen lassen, die willkürliche und anlassunabhängige Sammlung von Signalaufklärungsdaten zu verhindern und – ausgehend von den höchsten Ebenen staatlicher Verwaltung – dem Grundsatz der Verhältnismäßigkeit Geltung zu verschaffen“.

90 Siehe Statistical Transparency Report Regarding Use of National Security Authorities, 22.4.2015. Zum Gesamtvolumen des Datenverkehrs im Internet siehe beispielsweise Fundamental Rights Agency, Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU (2015), S. 15-16. Nach einer freigegebenen Stellungnahme des FISC aus dem Jahre 2011 entfallen über 90 % der gemäß § 702 des FISA überwachten elektronischen Kommunikation auf das Programm PRISM, weniger als 10 % hingegen auf UPSTREAM. Siehe FISC, Memorandum Opinion, 2011 WL 10945618 (FISA Ct., 3.10.2011), n. 21 (abrufbar unter: http://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf).

91 Siehe § 4(a)(ii) der PPD-28. Siehe auch ODNI, Safeguarding the Personal Information of all People: A Status Report on the Development and Implementation of Procedures under Presidential Policy Directive 28, Juli 2014, S. 5, wonach „das Vorgehen der Nachrichtendienste auf die Stärkung der vorhandenen Analysemethoden und -standards gerichtet sein sollte, denen zufolge die Analysten bestrebt sein müssen, Anfragen oder Suchbegriffe und -methoden so zu strukturieren, dass sie Aufklärungsdaten bezeichnen, die für einen begründeten nachrichtendienstlichen oder strafrechtlichen Zweck von Belang sind; bei Anfragen zu Personen die Kategorien der Aufklärungsdaten in den Mittelpunkt stellen, die den nachrichtendienstlichen oder strafrechtlichen Erfordernissen entsprechen; und die Überprüfung personenbezogener Informationen, die für nachrichtendienstliche oder strafrechtliche Zwecke nicht relevant sind, auf ein Mindestmaß reduzieren.“ Siehe z. B. CIA, Signals Intelligence Activities, S. 5; FBI, Presidential Policy Directive 28 Policies and Procedures, S. 3. Nach dem 2016 Progress Report on the Signals Intelligence Reform haben Nachrichtendienste (darunter FBI, CIA und NSA) Schritte eingeleitet, um ihre Mitarbeiter für die Anforderungen der PPD-28 zu sensibilisieren, indem sie neue Schulungsmaßnahmen einführen oder bestehende Maßnahmen entsprechend anpassen.

getroffen werden, „die vernünftiger Weise so konzipiert sind, dass sie deren Weitergabe und Speicherung auf ein Mindestmaß beschränken“.[92]

(85) Den Erläuterungen der US-Regierung zufolge bedeutet dieses Erfordernis, dass die Nachrichtendienste nicht alle „theoretisch möglichen Maßnahmen“ ergreifen dürfen, sondern „ihre Bemühungen um den Schutz der legitimen Interessen auf dem Gebiet des Datenschutzes und der bürgerlichen Freiheiten mit den praktischen Erfordernissen der Signalaufklärung in Einklang zu bringen haben“.[93] In dieser Hinsicht werden Nicht-US-Bürger auf der Grundlage von Verfahren, die der Justizminister gebilligt hat, ebenso behandelt wie US-Bürger.[94]

(86) Nach diesen Regeln ist die Speicherung im Allgemeinen auf einen Zeitraum von höchsten fünf Jahren begrenzt, sofern dem nicht ein konkretes Gerichtsurteil oder – nach sorgfältiger Prüfung von Datenschutzfragen und Berücksichtigung der Auffassung des ODNI Civil Liberties Protection Officer sowie der Datenschutz- und Bürgerrechtsbeauftragten der Behörde – eine ausdrückliche Entscheidung des Director of National Intelligence entgegensteht, wonach eine längere Speicherung im Interesse der nationalen Sicherheit liegt.[95] Eine Weitergabe ist auf Fälle beschränkt, in denen die Informationen für den eigentlichen Zweck der Erhebung von Belang sind und daher einem autorisierten Zweck der Auslandsaufklärung oder Strafverfolgung dienen.[96]

(87) Den Zusicherungen der US-Regierung zufolge dürfen personenbezogene Daten nicht einfach deshalb weitergegeben werden, weil die betreffende Person kein US-Bürger ist. Vielmehr „würde Signalaufklärung über die alltäglichen Aktivitäten eines ausländischen Staatsangehörigen nicht als Auslandsaufklärung angesehen, die man allein aus diesem Grund weitergeben oder dauerhaft speichern darf, ohne dass sie einem autorisierten Zweck der Auslandsaufklärung dient“.[97]

(88) Aufgrund der geschilderten Sachlage gelangt die Kommission zu dem Schluss, dass in den Vereinigten Staaten Regeln gelten, die darauf abzielen, Eingriffe aus Gründen der

---

92 Den Erklärungen des ODNI zufolge gelten diese Beschränkungen unabhängig davon, ob die Informationen durch Sammelerhebung oder gezielte Erfassung gewonnen wurden, und unabhängig von der Nationalität der betroffenen Person.

93 Erklärungen des ODNI (Anhang VI), S. 4.

94 Siehe § 4(a)(i) der PPD-28 in Verbindung mit § 2.3 der E.O. 12333.

95 § 4(a)(i) der PPD-28; Erklärungen des ODNI (Anhang VI), S. 7. Bei personenbezogenen Daten, die gemäß § 702 des FISA erhoben werden, sehen beispielsweise die vom FISC gebilligten Minimierungsverfahren der NSA in der Regel vor, dass die Metadaten und der ungeprüfte Inhalt bei PRISM für maximal fünf Jahre gespeichert werden, bei UPSTREAM für höchstens zwei Jahre. Die NSA hält diese Vorgaben mithilfe eines automatisierten Verfahrens ein, das bei Ablauf der Speicherfrist die Daten löscht. Siehe NSA § 702 FISA Minimization Procedures, § 7 in Verbindung mit § 6(a)(1); NSA CLPO, NSA's Implementation of Foreign Intelligence Surveillance Act Section 702, 16.4.2014. Auch nach § 501 des FISA (vormals § 215 des U.S. PATRIOT ACT) ist die Speicherung auf fünf Jahre begrenzt, sofern die personenbezogenen Daten nicht Bestandteil einer ordnungsgemäß gebilligten Weitergabe von Auslandsaufklärungsdaten sind oder das Justizministerium die NSA schriftlich davon in Kenntnis setzt, dass sie Gegenstand einer Erhaltungsanordnung in einem anhängigen oder zu erwartenden Rechtsstreit sind. Siehe auch NSA, CLPO, Transparency Report: The USA Freedom Act Business Records FISA Implementation, 15.1.2016.

96 Insbesondere gilt, dass im Falle von § 501 des FISA (vormals § 215 des U.S. PATRIOT ACT) die Weitergabe personenbezogener Daten nur zum Zwecke der Terrorismusbekämpfung oder des Nachweises einer Straftat erfolgen darf und im Falle von § 702 FISA nur dann, wenn dies einem begründeten Ziel der Auslandsaufklärung oder der Strafverfolgung dient. Vgl. NSA, CLPO, NSA's Implementation of Foreign Intelligence Surveillance Act Section 702, 16.4.2014; Transparency Report: The USA Freedom Act Business Records FISA Implementation, 15.1.2016. Siehe auch NSA's Civil Liberties and Privacy Protections for Targeted SIGINT Activities under Executive Order 12333, 7.10.2014.

97 Erklärungen des ODNI (Anhang VI), S. 7 (mit Bezugnahme auf die Intelligence Community Directive (ICD) 203).

nationalen Sicherheit in die Grundrechte von Personen, deren personenbezogene Daten im Rahmen des EU-US-Datenschutzschilds aus der EU in die USA übermittelt werden, auf das absolut notwendige Maß zu begrenzen, das für die Erreichung des jeweiligen legitimen Ziels erforderlich ist.

(89) Wie die hier vorgenommene Analyse gezeigt hat, gewährleistet das amerikanische Recht, dass Überwachungsmaßnahmen nur zur Erlangung von Daten zur Auslandsaufklärung dienen – was ein legitimes politisches Ziel darstellt[98] – und möglichst zielgenau ausgeführt werden. Insbesondere wird die Sammelerhebung nur in Ausnahmefällen genehmigt, in denen eine gezielte Sammlung nicht möglich ist, und geht mit zusätzlichen Schutzvorkehrungen einher, um die Menge der erhobenen Daten und den anschließenden Zugang (der nur für spezifische Zwecke gestattet wird) auf ein Mindestmaß zu begrenzen.

(90) Nach Einschätzung der Kommission entspricht dies dem Maßstab, den der Gerichtshof im Urteil Schrems angelegt hat, wonach Gesetze, die Eingriffe in die von Artikel 7 und 8 der Charta garantierten Grundrechte vorsehen, „Mindestanforderungen"[99] vorschreiben und eine Regelung „nicht auf das absolut Notwendige beschränkt ist […], die generell die Speicherung aller personenbezogenen Daten sämtlicher Personen, deren Daten aus der Union in die Vereinigten Staaten übermittelt wurden, gestattet, ohne irgendeine Differenzierung, Einschränkung oder Ausnahme anhand des verfolgten Ziels vorzunehmen und ohne ein objektives Kriterium vorzusehen, das es ermöglicht, den Zugang der Behörden zu den Daten und deren spätere Nutzung auf ganz bestimmte, strikt begrenzte Zwecke zu beschränken, die den sowohl mit dem Zugang zu diesen Daten als auch mit deren Nutzung verbundenen Eingriff zu rechtfertigen vermögen."[100] Auch wird es keine unbeschränkte Sammlung und Speicherung von Daten aller Personen geben. Die der Kommission gegenüber abgegebenen Erklärungen, darunter die Zusicherung, dass die US-Aktivitäten zur Signalaufklärung nur einen Bruchteil der Kommunikationsvorgänge im Internet berühren, schließen zudem die Möglichkeit aus, „generell[101] auf den Inhalt elektronischer Kommunikation zuzugreifen".

3.1.2. Wirksamer Rechtsschutz

(91) Die Kommission hat sowohl die Aufsichtsinstrumente geprüft, die in den USA bei Eingriffen der US-Nachrichtendienste in die dorthin übermittelten personenbezogenen Daten zur Verfügung stehen, als auch die Rechtsbehelfe, die betroffene Privatpersonen in der EU in Anspruch nehmen können.

Aufsicht

---

98 Der Gerichtshof hat klargestellt, dass die nationale Sicherheit ein legitimes politisches Ziel darstellt. Siehe Schrems, Rn. 88. Siehe auch sein Urteil in der Rechtssache Digital Rights Ireland u. a., Rnn. 42-44 und 51, in dem es heißt, dass die Bekämpfung schwerer Kriminalität, insbesondere der organisierten Kriminalität und des Terrorismus, möglicherweise in hohem Maße vom Einsatz moderner Ermittlungstechniken abhängt. Anders als bei strafrechtlichen Ermittlungen, bei denen es in der Regel um die nachträgliche Feststellung der Verantwortlichkeit und Schuld geht, steht bei der nachrichtendienstlichen Tätigkeit häufig die Abwehr von Gefahren für die nationale Sicherheit vor Eintritt eines Schadens im Vordergrund. Deshalb müssen sich derartige Ermittlung oft auf einen größeren Kreis möglicher Akteure („Zielpersonen") und ein größeres räumliches Gebiet erstrecken. Vgl. EGMR, Weber und Saravia/Deutschland, Entscheidung vom 29.6.2006, Antrag Nr. 54934/00, Rnn. 105-118 (zur „strategischen Überwachung").

99 Schrems, Rn. 91 und weitere Bezugnahmen.

100 Schrems, Rn. 93.

101 Vgl. Schrems, Rn. 94.

(92) Die Intelligence Community der USA unterliegt der Kontrolle und Aufsicht durch verschiedene Einrichtungen aller drei Gewalten des Staates. Dazu zählen interne und externe Exekutivorgane, eine Reihe von Kongressausschüssen sowie die Gerichte, die speziell die Aktivitäten im Rahmen des Foreign Intelligence Surveillance Act beaufsichtigen.

(93) Erstens unterliegt jegliche nachrichtendienstliche Tätigkeit von US-Behörden einer umfassenden Beaufsichtigung durch die Exekutive.

(94) Gemäß PPD-28, § 4(a)(iv), umfassen die Maßnahmen und Verfahren der Nachrichtendienste „geeignete Schritte, um die Überwachung der Durchsetzung von Garantien zum Schutz personenbezogener Informationen zu erleichtern"; diese Schritte sollten auch regelmäßige Audits einschließen.[102]

(95) Dazu wurden mehrere Ebenen der Überwachung eingerichtet, darunter Bürgerrechts- oder Datenschutzbeauftragte, Generalinspekteure, das ODNI Civil Liberties and Privacy Office, das PCLOB und das Intelligence Oversight Board des Präsidenten. Für die Überwachungsaufgaben stehen in sämtlichen Behörden Compliance-Mitarbeiter zur Verfügung.[103]

(96) Wie von der US-Regierung erläutert[104], sind *Bürgerrechts- oder Datenschutzbeauftragte* mit Überwachungsfunktionen in verschiedenen Abteilungen mit nachrichtendienstlichen Aufgaben und in Nachrichtendiensten tätig.[105] Zwar unterscheiden sich die konkreten Befugnisse dieser Beauftragten in beschränktem Maße in Abhängigkeit von der Rechtsgrundlage, doch umfassen sie in der Regel die Aufsicht über Verfahren, mit denen sichergestellt werden soll, dass die betreffende Abteilung/der betreffende Nachrichtendienst die Belange des Datenschutzes und der bürgerlichen Freiheiten hinreichend beachtet und geeignete Vorkehrungen getroffen hat, um Beschwerden von Einzelpersonen nachzugehen, die der Meinung sind, dass ihre Privatsphäre oder ihre Bürgerrechte verletzt wurden (in manchen Fällen, so im ODNI, sind die Beauftragten selbst zur Untersuchung von Beschwerden befugt).[106] Der Leiter der Abteilung/des Nachrichtendiensts muss sicherstellen, dass die Beauftragten alle Informationen und Zugang zu allen Materialien erhalten, die sie für die Wahrnehmung ihrer Aufgaben benötigen. Die Bürgerrechts- und Datenschutzbeauftragten übermitteln dem Kongress und dem PCLOB regelmäßig einen Bericht mit Angaben zur Anzahl und Art der bei der der Abteilung/beim Nachrichtendienst eingegangenen Beschwerden sowie einem Überblick über die Bearbeitung der Beschwerden, die durchgeführten Überprüfungen und Recherchen und die Auswirkungen der von den Beauftragten geleisteten Arbeit.[107] Nach Einschätzung der nationalen Datenschutzbehörden ist die interne Überwachung durch

---

[102] ODNI, Safeguarding the Personal Information of all People: A Status Report on the Development and Implementation of Procedures under Presidential Policy Directive 28, S. 7. Siehe beispielsweise CIA, Signals Intelligence Activities, S. 6 (Compliance); FBI, Presidential Policy Directive 28 Policies and Procedures, Sec. III (A)(4), (B)(4); NSA, PPD-28 Section 4 Procedures, 12.1.2015, Sec. 8.1, 8.6(c).

[103] Beispielsweise beschäftigt die NSA im Direktionsbereich „Compliance" über 300 Compliance-Mitarbeiter. Siehe Erklärungen des ODNI (Anhang VI), S. 7.

[104] Siehe Ombudsstelle (Anhang III), Punkt 6(b) (i) bis (iii).

[105] Siehe 42 U.S.C. § 2000ee-1. Dazu zählen beispielsweise das Außenministerium, das Justizministerium (einschließlich FBI), das Heimatschutzministerium, das Verteidigungsministerium, die NSA, die CIA und das ODNI.

[106] Wenn beim ODNI Civil Liberties and Privacy Office eine Beschwerde eingeht, erfolgt nach Angaben der US-Regierung eine Abstimmung mit anderen Nachrichtendiensten über die Bearbeitung der Beschwerde innerhalb der Intelligence Community. Siehe Ombudsstelle (Anhang III), Punkt 6(b) (ii).

[107] Siehe 42 U.S.C. § 2000ee-1 (f)(1),(2).

Bürgerrechts- und Datenschutzbeauftragte als „relativ robust“ anzusehen, auch wenn diese nicht das erforderliche Maß an Unabhängigkeit aufweisen.[108]

(97) Darüber hinaus hat jeder Nachrichtendienst seinen eigenen *Generalinspekteur*, der unter anderem für die Kontrolle der Auslandsaufklärung zuständig ist.[109] Im ODNI besteht ein Büro des Generalinspekteurs mit umfassender Zuständigkeit für die gesamte Intelligence Community, das befugt ist, Beschwerden oder Hinweisen auf rechtswidriges Verhalten oder Amtsmissbrauch nachzugehen, die mit Programmen und Aktivitäten des ODNI und/oder der Intelligence Community im Zusammenhang stehen.[110] Generalinspekteure sind rechtlich unabhängige[111] Instanzen, die für die Durchführung von Audits und Untersuchungen im Zusammenhang mit den nachrichtendienstlichen Programmen und Aktivitäten der jeweiligen Behörde zuständig sind, darunter auch für Missbrauchsfälle oder Rechtsverstöße.[112] Sie haben Zugriff auf alle Unterlagen, Berichte, Audits, Überprüfungen, Dokumente, Schriftstücke, Empfehlungen oder sonstiges einschlägiges Material, dessen Herausgabe sie notfalls unter Strafandrohung anordnen können, und sind zur Beweisaufnahme berechtigt.[113] Zwar können die Generalinspekteure nur Empfehlungen für Korrekturmaßnahmen abgeben, die nicht bindend sind, doch werden ihre Berichte, auch über die ergriffenen (oder unterlassenen) Folgemaßnahmen, öffentlich gemacht und darüber hinaus dem Kongress übermittelt, der auf dieser Grundlage seine Kontrollfunktion wahrnehmen kann.[114]

(98) Darüber hinaus wurde das *Privacy and Civil Liberties Oversight Board*, eine parteiübergreifende unabhängige Behörde[115] der Exekutive, deren fünf Mitglieder[116] vom Präsidenten mit Zustimmung des Senats für eine Amtszeit von sechs Jahren

---

108 Article 29 Data Protection Working Party, Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision (angenommen am 13.4.2016), S. 41.

109 Erklärungen des ODNI (Anhang VI), S. 7. Siehe beispielsweise NSA, PPD-28 Section 4 Procedures, 12.1.2015, Sec. 8.1; CIA, Signals Intelligence Activities, S. 7 (Responsibilities).

110 Dieser Generalinspekteur (dessen Amt seit Oktober 2010 besteht) wird mit Zustimmung des Senats vom Präsidenten ernannt und kann vom Präsidenten, nicht aber vom DNI abberufen werden.

111 Generalinspekteure genießen Kündigungsschutz und können nur vom Präsidenten abberufen werden, der dem Kongress schriftlich die Gründe für die Abberufung darlegen muss. Dies bedeutet aber nicht zwangsläufig, dass sie keinerlei Weisungen unterliegen. In bestimmten Fällen kann der Leiter der Regierungsstelle den Generalinspekteur daran hindern, einen Audit oder eine Untersuchung einzuleiten, durchzuführen oder abzuschließen, wenn dies geboten erscheint, um wichtige nationale (Sicherheits-)Interessen zu wahren. Allerdings muss darüber der Kongress unterrichtet werden, der den Behördenleiter gegebenenfalls zur Verantwortung ziehen kann. Siehe beispielsweise Inspector General Act of 1978, § 8 (IG of the Department of Defense); § 8E (IG of the DOJ), § 8G (d)(2)(A),(B) (IG of the NSA); 50. U.S.C. § 403q (b) (IG for the CIA); Intelligence Authorization Act For Fiscal Year 2010, Sec 405(f) (IG for the Intelligence Community). Nach Einschätzung der nationalen Datenschutzbehörden dürften die Generalinspekteure „*dem Kriterium organisatorischer Unabhängigkeit im Sinne des EuGH und des Europäischen Gerichtshofs für Menschenrechte (EGMR) zumindest von dem Zeitpunkt an genügen, an dem das neue Ernennungsverfahren für alle gilt.*“ Siehe Article 29 Data Protection Working Party, Opinion 01/2016 on the EU-U.S. Privacy Shield adequacy decision (angenommen am 13.4.2016), S. 40.

112 Siehe Erklärungen des ODNI (Anhang VI), S. 7. Siehe auch Inspector General Act of 1978, as amended, Pub. L. 113-126 of 7.7.2014.

113 Siehe Inspector General Act of 1978, § 6.

114 Siehe Erklärungen des ODNI (Anhang VI), S. 7. Siehe auch Inspector General Act of 1978, §§ 4(5), 5. Gemäß § 405(b)(3),(4) des Intelligence Authorization Act For Fiscal Year 2010, Pub. L. 111-259 vom 7.10.2010 informiert der Generalinspekteur für die Intelligence Community den DNI sowie den Kongress über notwendige Korrekturmaßnahmen und deren Fortgang.

115 Nach Einschätzung der nationalen Datenschutzbehörden hat das PCLOB in der Vergangenheit „seine eigenständigen Befugnisse unter Beweis gestellt“. Siehe Article 29 Data Protection Working Party, Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision (angenommen am 13.4.2016), S. 42.

116 Außerdem hat das PCLOB noch 20 weitere Mitarbeiter. Siehe https://www.pclob.gov/about-us/staff.html.

ernannt werden, mit der Aufgabe betraut, auf dem Gebiet der Terrorismusbekämpfung und ihrer Umsetzung für den Schutz der Privatsphäre und der bürgerlichen Freiheiten zu sorgen. Bei der Überprüfung der Tätigkeit der Nachrichtendienste hat sie Zugriff auf alle einschlägigen Unterlagen von Behörden wie Berichte, Audits, Überprüfungen, Dokumente, Schriftstücke und Empfehlungen, einschließlich der Geheimhaltung unterliegenden Informationen, kann Befragungen durchführen und Zeugen vernehmen. Die Behörde erhält Berichte von Bürgerrechts- und Datenschutzbeauftragten verschiedener Regierungsstellen[117], kann ihnen gegenüber Empfehlungen abgeben und erstattet regelmäßig den Ausschüssen des Kongresses und dem Präsidenten Bericht.[118] Das PCLOB hat die Aufgabe, im Rahmen seines Auftrags einen Bericht zu erstellen, in dem die Umsetzung der PPD-28 bewertet wird.

(99) Ergänzt werden die genannten Aufsichtsmechanismen durch das *Intelligence Oversight Board*, das innerhalb des Intelligence Advisory Board des Präsidenten eingerichtet wurde, um die Einhaltung der Verfassung und aller einschlägigen Vorschriften durch die US-Nachrichtendienste zu überwachen.

(100) Um die Aufsicht zu erleichtern, werden die Nachrichtendienste dazu angehalten, Informationssysteme zu konzipieren, die die Erfassung, Aufzeichnung und Nachprüfung von Anfragen und anderen Formen der Beschaffung personenbezogener Daten ermöglichen.[119] Die Kontroll- und Compliance-Gremien kontrollieren regelmäßig die Verfahren der Nachrichtendienste zum Schutz der personenbezogenen Informationen, die bei der Signalaufklärung anfallen, und die Einhaltung dieser Verfahren.[120]

(101) Die Aufsichtstätigkeit geht zudem mit umfassenden Berichtspflichten bei fehlender Rechtsbefolgung einher. Insbesondere müssen die behördlichen Verfahren sicherstellen, dass im Falle eines wichtigen Compliance-Problems, bei dem es um personenbezogene Daten geht, die per Signalaufklärung von einer Person unabhängig von ihrer Nationalität erhoben wurden, das Problem unverzüglich dem Leiter des Nachrichtendienstes gemeldet wird, der seinerseits den Director of National Intelligence unterrichtet, dem es nach der PPD-28 obliegt zu entscheiden, ob Korrekturmaßnahmen erforderlich sind.[121] Überdies sind nach E.O. 12333 alle Nachrichtendienste verpflichtet, dem Intelligence Oversight Board Rechtsverstöße zu melden.[122] Diese Vorgehensweise gewährleistet, dass das Problem an die höchste Ebene der Intelligence Community weitergemeldet wird. Betrifft es einen Nicht-US-Bürger, entscheidet der Director of National Intelligence in Abstimmung mit dem Außenminister und dem Leiter der meldenden Regierungsstelle darüber, ob Schritte einzuleiten sind, um die betreffende ausländische Regierung in einer Weise davon in

---

117 Dazu zählen zumindest das Justizministerium, das Verteidigungsministerium, das Heimatschutzministerium, der Director of National Intelligence und die Central Intelligence Agency sowie andere Regierungsstellen oder Einrichtungen der Exekutive, deren Einbeziehung das PCLOB für sinnvoll erachtet.

118 Siehe 42 U.S.C. § 2000ee. Siehe auch Ombudsmechanismus (Anhang III), Punk 6(b) (iv).

119 ODNI, Safeguarding the Personal Information of all People: A Status Report on the Development and Implementation of Procedures under Presidential Policy Directive 28, S. 7-8.

120 Ebenda auf S. 8. Siehe auch Erklärungen des ODNI (Anhang VI), S. 9.

121 ODNI, Safeguarding the Personal Information of all People: A Status Report on the Development and Implementation of Procedures under Presidential Policy Directive 28, S. 7. Siehe beispielsweise NSA, PPD-28 Section 4 Procedures, 12.1.2015, Sec. 7.3, 8.7(c),(d); FBI, Presidential Policy Directive 28 Policies and Procedures, Sec. III.(A)(4), (B)(4); CIA, Signals Intelligence Activities, S. 6 (Compliance) und S. 8 (Responsibilities).

122 Siehe E.O. 12333, Sec. 1.6(c).

Kenntnis zu setzen, die mit dem Schutz der Quellen und Methoden und der US-Mitarbeiter vereinbar ist.[123]

(102) Zweitens nimmt neben diesen Aufsichtsgremien der Exekutive auch der Kongress der USA, vor allem über die *Ausschüsse des Repräsentantenhauses und des Senats für Nachrichtendienste und Justiz*, Kontrollaufgaben wahr, die alle Formen der Auslandsaufklärung, darunter die US-Signalaufklärung, betreffen. Der National Security Act besagt: „Der Präsident stellt sicher, dass die Kongressausschüsse für die Nachrichtendienste umfassend und zeitnah über die nachrichtendienstliche Tätigkeit der Vereinigten Staaten unterrichtet werden, auch über wichtige bevorstehende nachrichtendienstliche Operationen, wie dieses Unterkapitel es erfordert.“[124] Des Weiteren heißt es: „Der Präsident stellt sicher, dass den Kongressausschüssen für die Nachrichtendienste illegale nachrichtendienstliche Aktivitäten unverzüglich gemeldet werden, ebenso Korrekturmaßnahmen, die im Zusammenhang mit illegalen Aktivitäten ergriffen wurden bzw. geplant sind.“[125] Die Mitglieder dieser Ausschüsse haben Zugriff auf Informationen, die der Geheimhaltung unterliegen, sowie auf nachrichtendienstliche Methoden und Programme.[126]

(103) In späteren Gesetzen wurden die Berichtspflichten erweitert und präzisiert, soweit sie die Nachrichtendienste, die jeweiligen Generalinspekteure und den Justizminister betreffen. Beispielsweise heißt es im FISA, dass der Justizminister die Ausschüsse des Senats und des Repräsentantenhauses für Nachrichtendienste und Justiz über Aktivitäten der Regierung im Rahmen bestimmter Paragrafen des FISA „umfassend zu unterrichten“ habe.[127] Das Gesetz verpflichtet die Regierung auch dazu, den Kongressausschüssen „Kopien sämtlicher Entscheidungen, Anordnungen oder Stellungnahmen des Foreign Intelligence Surveillance Court oder des Foreign Intelligence Surveillance Court of Review zukommen zu lassen, die eine wichtige Auslegung oder Interpretation“ der FISA-Bestimmungen beinhalten. Bei der Überwachung gemäß § 702 FISA erfolgt die Aufsicht mittels gesetzlich vorgeschriebener Berichte an die Ausschüsse für Nachrichtendienste und Justiz sowie häufiger Informationsgespräche und Anhörungen. Dazu zählen ein halbjährlicher Bericht des Justizministers über die Anwendung von § 702 des FISA, dem die Compliance-Berichte des Justizministeriums und des ODNI und eine Beschreibung von Verstößen beigefügt sind,[128] und eine gesonderte halbjährliche Einschätzung des Justizministers und des DNI, der die Einhaltung der Verfahren zur zielgenauen Sammlung und Minimierung dokumentiert, darunter auch die Einhaltung der Verfahren, die sicherstellen sollen, dass die Sammlung einem begründeten Ziel der Auslandsaufklärung dient.[129] Der Kongress erhält auch Berichte der Generalinspekteure, die befugt sind, die Einhaltung der Verfahren zur zielgenauen Sammlung und Minimierung und der Leitlinien des Justizministers zu bewerten.

(104) Gemäß dem USA FREEDOM Act von 2015 muss die US-Regierung alljährlich gegenüber dem Kongress (und der Öffentlichkeit) unter anderem die Anzahl der beantragten und genehmigten FISA-Anordnungen und -Direktiven sowie die geschätzte Anzahl der von Überwachungsmaßnahmen betroffenen US-Bürger und

123 PPD-28, Sec. 4(a)(iv).

124 Siehe § 501(a)(1) (50 U.S.C. § 413(a)(1)). Diese Bestimmungen regeln die allgemeinen Anforderungen an die Kontrolltätigkeit des Kongresses im Bereich der nationalen Sicherheit.

125 Siehe § 501(b) (50 U.S.C. § 413(b)).

126 Vgl. § 501(d) (50 U.S.C. § 413(d)).

127 Siehe 50 U.S.C. §§ 1808, 1846, 1862, 1871, 1881f.

128 Siehe 50 U.S.C. § 1881f.

129 Siehe 50 U.S.C. § 1881a(l)(1).

Nicht-US-Bürger offenlegen.[130] Das Gesetz verlangt zudem, die Öffentlichkeit zusätzlich über die Anzahl der erteilten NSL zu unterrichten, wiederum aufgeschlüsselt nach US-Bürgern und Nicht-US-Bürgern (wobei gleichzeitig aber den Empfängern von FISA-Anordnungen und -Zertifizierungen sowie NSL-Auskunftsersuchen gestattet wird, unter bestimmten Voraussetzungen Transparenzberichte vorzulegen).[131]

(105) Drittens kann bei nachrichtendienstlichen Aktivitäten von US-Behörden auf der Grundlage des FISA eine Überprüfung und in manchen Fällen die vorherige Genehmigung der Maßnahmen durch den *FISA Court* (FISC)[132], einem unabhängigen Gericht[133], verlangt werden, dessen Entscheidung vor dem Foreign Intelligence Court of Review (FISCR)[134] und in letzter Instanz vor dem Obersten Gericht der Vereinigten Staaten angefochten werden kann.[135] Im Falle der vorherigen Genehmigung müssen die antragstellenden Behörden (FBI, NSA, CIA usw.) einen Antragsentwurf bei Juristen der Abteilung Nationale Sicherheit des Justizministeriums einreichen, die die Angelegenheit prüfen und erforderlichenfalls zusätzliche Informationen anfordern.[136] In der Endfassung muss der Antrag dann vom Justizminister, seinem ersten Stellvertreter oder dem Stellvertreter für nationale Sicherheit gebilligt werden.[137] Das Justizministerium legt den Antrag anschließend dem FISC vor, das ihn prüft und eine vorläufige Entscheidung über das weitere Vorgehen trifft.[138] Findet eine Anhörung

---

130 Siehe USA FREEDOM Act of 2015, Pub. L. No. 114-23, § 602(a). Des Weiteren besagt § 402: „Der Director of National Intelligence prüft in Abstimmung mit dem Justizminister die Möglichkeit der Freigabe einer jeden Entscheidung, Anordnung oder Stellungnahme des Foreign Intelligence Surveillance Court bzw. des Foreign Intelligence Surveillance Court of Review (wie in § 601(e) definiert), die eine bedeutsame Auslegung oder Interpretation einer gesetzlichen Bestimmung enthält, darunter auch eine neuartige oder bedeutsame Auslegung oder Interpretation des Terminus ‚konkreter Suchbegriff', und macht abhängig von dieser Prüfung jede Entscheidung, Anordnung oder Stellungnahme dieser Art im größtmöglichen Umfang öffentlich."

131 USA FREEDOM Act, § 602(a), 603(a).

132 Bei bestimmten Formen der Überwachung kann wahlweise ein U.S. Magistrate Judge, der öffentlich vom Obersten Richter der Vereinigten Staaten benannt wird, die Befugnis erhalten, Anträge zu prüfen und Anordnungen zu erlassen.

133 Das FISC besteht aus elf Richtern, die vom Obersten Richter der Vereinigten Staaten ernannt werden. Es handelt sich dabei um amtierende Richter von US-Bundesbezirksgerichten, die zuvor vom Präsidenten ernannt und vom Senat bestätigt wurden. Die auf Lebenszeit ernannten Richter können nur aus schwerwiegenden Gründen abberufen werden und gehören dem FISC jeweils sieben Jahre an. Laut FISA müssen die Richter aus mindestens sieben verschiedenen US-Gerichtsbezirken kommen. Siehe § 103 FISA (50 U.S.C. 1803 (a)); PCLOB, Sec. 215 Report, S. 174-187. Den Richtern stehen erfahrene Rechtsassistenten zur Seite, die das juristische Personal darstellen und Rechtsgutachten zu Auskunftsersuchen erstellen. Siehe PCLOB, Sec. 215 Report, S. 178; Letter from the Honourable Reggie B. Walton, Presiding Judge, U.S. Foreign Intelligence Surveillance Court, to the Honourable Patrick J. Leahy, Chairman, Committee on the Judiciary, U.S. Senate (July 29, 2013) („Walton Letter"), S. 2-3.

134 Das FISCR besteht aus drei Richtern, die vom Obersten Richter der Vereinigten Staaten benannt und aus Richtern an US-Bezirksgerichten oder Berufungsgerichten ausgewählt werden. Sie gehören dem FISCR jeweils sieben Jahre an. Siehe § 103 FISA (50 U.S.C. § 1803 (b)).

135 Siehe 50 U.S.C. §§ 1803 (b), 1861 a (f), 1881 a (h), 1881 a (i)(4).

136 Zum Beispiel zusätzliche Angaben über die Zielperson der Überwachung, technische Informationen über die Überwachungsmethode oder Zusicherungen über die Nutzung und Weitergabe der erhobenen Daten. Siehe PCLOB, Sec. 215 Report, S. 177.

137 50 U.S.C. §§ 1804 (a), 1801 (g).

138 Das FISC kann dem Antrag stattgeben, weitere Informationen anfordern, eine Anhörung für notwendig befinden oder auf eine mögliche Ablehnung des Antrags hinweisen. Auf der Grundlage dieser vorläufigen Entscheidung stellt die Regierung ihren endgültigen Antrag. Dieser kann aufgrund der Berücksichtigung der vorläufigen Stellungnahme des Richters größere Änderungen gegenüber dem ursprünglichen Antrag enthalten. Zwar wird ein hoher Prozentsatz der endgültigen Anträge vom FISC gebilligt, doch weist ein erheblicher Anteil davon deutliche Änderungen gegenüber dem ursprünglichen Antrag auf, so etwa 24 %

statt, ist das FISC befugt, Beweismittel zu erheben, wozu auch die Einholung von Gutachten gehören kann.[139]

(106) Das FISC (und das FISCR) werden von einer ständigen Expertengruppe unterstützt, die aus fünf Sachverständigen für nationale Sicherheit und Bürgerrechte besteht.[140] Das Gericht benennt ein Mitglied dieser Gruppe als „Amicus curiae", damit er bei der Prüfung eines Antrags auf Anordnung oder Überprüfung mitwirkt, der nach Auffassung des Gerichts eine neuartige oder bedeutsame Interpretation des Rechts beinhaltet, es sei denn, das Gericht hält eine solche Benennung nicht für angebracht.[141] Auf diese Weise soll vor allem sichergestellt werden, dass Datenschutzbelange bei der gerichtlichen Prüfung hinreichend Berücksichtigung finden. Das Gericht kann auch eine Einzelperson oder Organisation als Amicus curiae benennen, um bestimmte rechtliche Aspekte zu beleuchten, sofern ihm dies geboten erscheint, oder auf Antrag einer Einzelperson oder einer Organisation gestatten, einen Amicus-curiae-Schriftsatz („brief") einzureichen.[142]

(107) Bei den zwei Rechtsgrundlagen für eine Überwachung im Rahmen des FISA, die für die Datenübermittlung unter dem EU-US-Privacy Shield am wichtigsten sind, geht das FISC bei der Aufsicht unterschiedlich vor.

(108) Gemäß § 501 des FISA[143], der den Zugriff auf „materielle Objekte (darunter Bücher, Unterlagen, Schriftstücke, Dokumente und andere Objekte)" gestattet, muss der Antrag an das FISC eine Darlegung des Sachverhalts enthalten, dem zufolge gewichtige Gründe dafür sprechen, dass die aufgeführten materiellen Objekte für eine autorisierte Ermittlung (nicht aber für eine Bedrohungsanalyse) von Belang sind, die auf die Beschaffung von Auslandsaufklärungsdaten gerichtet ist, deren Gegenstand keine US-Bürger sind, oder die dem Schutz vor internationalem Terrorismus oder geheimen nachrichtendienstlichen Aktivitäten dient. Zudem muss der Antrag die Minimierungsverfahren aufführen, die der Justizminister für die Speicherung und Weitergabe der erhobenen Aufklärungsdaten festgelegt hat. [144]

(109) Hingegen autorisiert das FISC nach § 702 des FISA[145] keine individuellen Überwachungsmaßnahmen; vielmehr genehmigt es Überwachungsprogramme (wie PRISM oder UPSTREAM) auf der Grundlage jährlicher Zertifizierungen, die vom Justizminister und dem Director of National Intelligence vorgenommen werden. § 702 des FISA gestattet die gezielte Überwachung von Personen, die sich mit hinreichender Bestimmtheit außerhalb der Vereinigten Staaten aufhalten, um Auslandsaufklärungsdaten zu erlangen.[146] Die gezielte Überwachung durch die NSA erfolgt in zwei Schritten: Zunächst identifizieren Analysten der NSA Nicht-US-Bürger, die sich im Ausland befinden und deren Überwachung nach Einschätzung der

---

der Anträge, denen im Zeitraum von Juli bis September 2013 stattgegeben wurde. Siehe PCLOB, Sec. 215 Report, S. 179; Walton Letter, S. 3.

139 PCLOB, Sec. 215 Report, S.179, Nr. 619.

140 50 U.S.C. § 1803 (i)(1),(3)(A). Mit dieser neuen Regelung wird eine Empfehlung des PCLOB umgesetzt, eine Gruppe von Sachverständigen für Datenschutz und Bürgerrechte zu bilden, die als „Amicus curiae" fungieren können, um das Gericht mit juristischen Argumenten zur Wahrung der Belange des Datenschutzes und der Bürgerrechte zu unterstützen. Siehe PCLOB, Sec. 215 Report, S. 183-187.

141 50 U.S.C. § 1803 (i)(2)(A). Nach Informationen des ODNI sind solche Ernennungen bereits erfolgt. Siehe Signals Intelligence Reform, 2016 Progress Report.

142 50 U.S.C. § 1803 (i)(2)(B).

143 50 U.S.C. § 1861

144 50 U.S.C. § 1861 (b).

145 50 U.S.C. § 1881.

146 50 U.S.C. § 1881a (a).

Analysten zu den in der Zertifizierung angegebenen Auslandsaufklärungsdaten führt. Sobald diese Personen identifiziert sind und ihre gezielte Überwachung nach einem gründlichen Kontrollverfahren innerhalb der NSA genehmigt wurde[147], werden Selektoren, die Kommunikationseinrichtungen (wie E-Mail-Adressen) identifizieren, „aktiviert“ (d. h. erstellt und angewandt).[148] Wie bereits angemerkt, enthalten die vom FISC zu bestätigenden Zertifizierungen keine Informationen über die einzelnen zu überwachenden Personen, sondern beziehen sich auf Kategorien von Auslandsaufklärungsdaten.[149] Das FISC beurteilt nicht – anhand eines hinreichenden Verdachts oder sonstigen Kriteriums –, ob die Personen vorschriftsgemäß als Zielpersonen für die Beschaffung von Auslandsaufklärungsdaten ausgewählt wurden,[150] sondern überprüft die Einhaltung der Bestimmung, dass „ein wesentlicher Zweck der Datenerhebung darin besteht, Auslandsaufklärungsdaten zu erlangen“[151]. Laut § 702 des FISA ist es nämlich der NSA nur dann gestattet, den Datenverkehr von Nicht-US-Bürgern außerhalb der USA zu erheben, wenn die begründete Annahme besteht, dass ein bestimmtes Kommunikationsmittel verwendet wird, um Daten zu übermitteln, die für die Auslandsaufklärung von Interesse sind (z. B. weil sie mit dem internationalen Terrorismus, der Weitergabe von Kernwaffen oder feindseligen Cyberaktivitäten in Verbindung stehen). Entscheidungen dieser Art sind gerichtlich anfechtbar.[152] Auch müssen die Zertifizierungen Verfahren zur zielgenauen Erfassung und Minimierung vorsehen.[153] Der Justizminister und der Director of National Intelligence überprüfen die Einhaltung der Grundsätze, und die Behörden sind verpflichtet, jegliche Verstöße dagegen dem FISC[154] (sowie dem Kongress und dem Intelligence Oversight Board des Präsidenten) zu melden, der daraufhin die Genehmigung abändern kann.[155]

(110) Um die Effektivität der Überwachung durch das FISC zu erhöhen, hat sich die US-Regierung überdies bereit erklärt, eine Empfehlung des PCLOB umzusetzen, dem

147 PCLOB, Sec. 702 Report, p. 46.

148 50 U.S.C. § 1881a (h).

149 50 U.S.C. § 1881a (g). Nach Angaben des PCLOB betrafen diese Kategorien bisher hauptsächlich den internationalen Terrorismus und Themen wie den Erwerb von Massenvernichtungswaffen. Siehe PCLOB, Sec. 702 Report, S. 25.

150 PCLOB, Sec. 702 Report, S. 27.

151 50 U.S.C. § 1881a.

152 „Liberty and Security in a Changing World“, Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies, 12.12.2013, S. 152.

153 50 U.S.C.1881a (i).

154 Regel 13(b) der Verfahrensordnung des FISC verpflichtet die Regierung dazu, dem Gericht unverzüglich eine schriftliche Mitteilung zukommen zu lassen, wenn sich herausstellt, dass eine vom Gericht erteilte Genehmigung oder Bestätigung auf eine Weise umgesetzt worden ist, die mit dieser Genehmigung oder Bestätigung bzw. dem geltenden Recht nicht im Einklang steht. Auch muss die Regierung das Gericht schriftlich über die Fakten und Umstände unterrichten, die für diesen Verstoß relevant sind. Im Regelfall übermittelt die Regierung eine endgültige Mitteilung gemäß Regel 13(a), sobald die einschlägigen Tatsachen bekannt sind und unbefugt erhobene Daten vernichtet wurden. Siehe Walton Letter, S. 10.

155 50 U.S.C. § 1881 (l). Siehe auch PCLOB, Sec. 702 Report, S. 66-76; NSA CLPO, NSA's Implementation of Foreign Intelligence Surveillance Act Section 702, 16.4.2014. Die Erhebung personenbezogener Daten für nachrichtendienstliche Zwecke gemäß § 702 des FISA unterliegt innerhalb der Exekutive sowohl einer internen als auch einer externen Überwachung. Zur internen Überwachung gehören interne Compliance-Programme zur Einschätzung und Kontrolle der Einhaltung von Verfahren zur zielgenauen Sammlung und Minimierung; die Meldung von Verstößen – intern wie extern – an das ODNI, das Justizministerium, den Kongress und das FISC; und jährliche Prüfberichte, die an die gleichen Gremien gehen. Die externe Überwachung besteht hauptsächlich in der Prüfung der zielgenauen Sammlung und Minimierung durch das ODNI, das Justizministerium und die Generalinspekteure, die ihrerseits dem Kongress und dem FISC Mitteilung machen, auch zu Verstößen. Schwerwiegende Verstöße sind dem FISC unverzüglich zu melden, andere in einem vierteljährlichen Bericht. Siehe PCLOB, Sec. 702 Report, S. 66-77.

FICS Unterlagen zu Entscheidungen über eine zielgenaue Erfassung nach § 702 zukommen zu lassen, darunter eine Stichprobe der „tasking sheets“ (Überwachungspläne), damit das FISC beurteilen kann, wie in der Praxis die Vorgabe eingehalten wird, dass die Erhebung der Auslandsaufklärung dienen muss.[156] Zugleich hat die US-Regierung Maßnahmen eingeleitet, um die NSA-Verfahren für eine zielgenaue Erfassung weiter zu entwickeln, dass der Zweck der diesbezüglichen Entscheidungen – die Auslandsaufklärung – noch besser zum Ausdruck kommt.[157]

Rechtsschutz für Privatpersonen

(111) Nach amerikanischem Recht steht Betroffenen in der EU eine Reihe von Möglichkeiten offen, wenn sie in Erfahrung bringen wollen, ob ihre personenbezogenen Daten von US-Nachrichtendiensten verarbeitet (erhoben, genutzt, usw.) wurden, und sofern dies der Fall ist, ob die im amerikanischen Recht geltenden Einschränkungen befolgt wurden. Diese betreffen im Wesentlichen drei Bereiche: Eingriffe gemäß FISA; der vorsätzliche gesetzwidrige Zugriff auf personenbezogene Daten durch Regierungsbeamte; und der Zugang zu Informationen gemäß dem Freedom of Information Act (FOIA).[158]

(112) Erstens bietet der Foreign Intelligence Surveillance Act eine Reihe von Rechtsschutzinstrumenten, die auch Nicht-US-Bürger in Anspruch nehmen können, um gegen rechtswidrige elektronische Überwachung[159] vorzugehen. Beispielsweise haben Privatpersonen die Möglichkeit, eine Zivilklage auf Schadenersatz gegen die Vereinigten Staaten anzustrengen, wenn Informationen, die sie betreffen, gesetzwidrig und vorsätzlich genutzt oder offengelegt wurden[160]; US-Regierungsbeamte in persönlicher Eigenschaft (nach dem Grundsatz der Rechtsscheinhaftung) auf Schadenersatz zu verklagen[161]; und die Rechtmäßigkeit der Überwachung anzufechten (und auf die Unterdrückung der Informationen hinzuwirken), sofern die US-Regierung beabsichtigt, in den Vereinigten Staaten direkt oder mittelbar aus der elektronischen Überwachung gewonnene Erkenntnisse in einem Gerichts- oder Verwaltungsverfahren gegen die betroffene Person zu verwenden oder offenzulegen.[162]

(113) Zweitens hat die US-Regierung die Kommission auf eine Reihe zusätzlicher Möglichkeiten hingewiesen, die betroffene Personen in der EU nutzen könnten, um rechtlich gegen Regierungsbeamte wegen des rechtswidrigen Zugangs zu, oder der Verarbeitung personenbezogener Daten, auch für vorgebliche Ziele der nationalen Sicherheit, vorzugehen (Computer Fraud and Abuse Act[163]; Electronic Communications Privacy Act[164]; und Right to Financial Privacy Act[165]). All diese Klagegründe betreffen spezifische Daten, Zielpersonen und/oder Arten des Zugriffs

156 PCLOB, Recommendations Assessment Report, 29.1.2015, S. 20.
157 PCLOB, Recommendations Assessment Report, 29.1.2015, S.16.
158 Zudem besagt § 10 des Classified Information Procedures Act, dass in jedem Strafverfahren, in dem die Vereinigten Staaten nachweisen müssen, dass bestimmtes Material der Geheimhaltung unterliegt (z. B. weil es aus Gründen der nationalen Sicherheit vor einer nicht autorisierten Offenlegung geschützt werden muss), die Vereinigten Staaten dem Angeklagten mitteilen müssen, auf welche Teile des Materials sie sich mit hinreichender Bestimmtheit stützen werden, um nachzuweisen, dass für das Verfahren relevante Informationen der Geheimhaltung unterliegen.
159 Siehe Erklärungen des ODNI (Anhang VI), S. 16.
160 18 U.S.C. § 2712.
161 50 U.S.C. § 1810.
162 50 U.S.C. § 1806.
163 18 U.S.C. § 1030.
164 18 U.S.C. §§ 2701-2712.
165 12 U.S.C. § 3417.

(z. B. Fernzugriff auf einen Computer über das Internet) und können unter bestimmten Umständen in Anspruch genommen werden (z. B. vorsätzliches Handeln, Überschreitung der Befugnisse, erlittener Schaden).[166] Eine allgemeinere Möglichkeit des Rechtsschutzes bietet der Administrative Procedure Act (5 U.S.C. § 702), wonach „eine Person, die durch Handlungen einer Behörde einen Schaden oder Nachteil erleidet", berechtigt ist, eine gerichtliche Nachprüfung zu beantragen. Dazu gehört die Möglichkeit, das Gericht zu ersuchen, „Handlungen, Feststellungen und Schlussfolgerungen einer Behörde, die für ... willkürlich, mutwillig, die Befugnisse überschreitend oder anderweitig rechtswidrig befunden werden, für null und nichtig zu erklären".[167]

(114) Darüber hinaus benannte die US-Regierung den Freedom of Information Act als Mittel, mit dem Nicht-US-Bürger Zugang zu vorhandenen Unterlagen von Bundesbehörden erlangen können, auch zu solchen, die personenbezogene Daten der betreffenden Personen enthalten.[168] Aufgrund seines zentralen Anliegens eröffnet der FOIA einerseits keine Möglichkeit für individuellen Rechtschutz gegen Eingriffe in personenbezogene Daten als solche, wobei das Gesetz andererseits vom Grundsatz her Privatpersonen den Zugang zu relevanten Informationen ermöglichen könnte, die sich im Besitz von bundesweit operierenden Nachrichtendiensten befinden. Aber auch in dieser Hinsicht sind die Möglichkeiten anscheinend begrenzt, weil die Behörden Informationen zurückhalten können, die unter detailliert aufgeführte Ausnahmeregelungen fallen, wozu der Zugriff auf Informationen gehört, die zum einen aus Gründen der nationalen Sicherheit der Geheimhaltung unterliegen und zum anderen strafrechtliche Ermittlungen betreffen.[169] Allerdings kann die Inanspruchnahme dieser Ausnahmeregelungen durch bundesweit tätige Nachrichtendienste von Privatpersonen angefochten werden, was einen Antrag auf sowohl eine behördliche als auch eine gerichtliche Überprüfung einschließt.

(115) Auch wenn Privatpersonen, einschließlich Betroffene in der EU, eine Reihe von Rechtsschutzinstrumenten zur Verfügung steht, wenn sie aus Gründen der nationalen Sicherheit rechtswidrig (elektronisch) überwacht wurden, steht doch fest, dass zumindest einige Rechtsgrundlagen, die US-Nachrichtendienste nutzen können (z. B. E.O. 12333), nicht dazu gehören. Selbst wenn Nicht-US-Bürger im Prinzip auf gerichtliche Rechtsbehelfe zurückgreifen können, beispielsweise auf der Grundlage des FISA im Falle der Überwachung, sind die verfügbaren Klagemöglichkeiten begrenzt[170], denn Klagen von Einzelpersonen (auch US-Bürgern) werden abgewiesen,

166 Erklärungen des ODNI (Anhang VI), S. 17.

167 5 U.S.C. § 706(2)(A).

168 5 U.S.C. § 552. Ähnliche Rechtsvorschriften existieren auf der Ebene der einzelnen Bundesstaaten.

169 Wenn dies zutrifft, erhält die betroffene Person in der Regel nur eine Standardantwort, in der die Behörde das Vorhandensein von Unterlagen weder bestätigt noch dementiert. Siehe ACLU v. CIA, 710 F.3d 422 (D.C. Cir. 2014).

170 Siehe Erklärungen des ODNI (Anhang VI), S. 16. Den gegebenen Erläuterungen zufolge setzen die verfügbaren Klagemöglichkeiten entweder das Vorliegen eines Schadens voraus (18 U.S.C. § 2712; 50 U.S.C. § 1810) oder den Nachweis, dass die Regierung beabsichtigt, in den Vereinigten Staaten direkt oder mittelbar aus der elektronischen Überwachung gewonnene Erkenntnisse in einem Gerichts- oder Verwaltungsverfahren gegen die betroffene Person zu verwenden (50 U.S.C. § 1806). Wie aber wiederholt vom Europäischen Gerichtshof unterstrichen wurde, kommt es für die Feststellung des Vorliegens eines Eingriffs in das Grundrecht auf Achtung der Privatsphäre nicht darauf an, ob die Betroffenen durch den Eingriff Nachteile erlitten haben. Siehe Schrems, Rn. 89 mit weiteren Verweisen.

wenn diese ihre „Klagebefugnis“ nicht nachweisen können[171], was den Zugang zu den ordentlichen Gerichten einschränkt.[172]

(116) Um eine zusätzliche Rechtsschutzmöglichkeit zu schaffen, die allen Betroffenen in der EU offensteht, hat die US-Regierung beschlossen, als neue Einrichtung einen Ombudsmechanismus ins Leben zu rufen, wie er im Schreiben des US-Außenministers an die Kommission beschrieben wird, das Bestandteil von Anhang III zum vorliegenden Beschluss ist. Er basiert auf der gemäß PPD-28 erfolgenden Benennung eines Senior Coordinator (im Range eines Under-Secretary [Staatssekretärs]) im Außenministerium, der als Ansprechpartner für ausländische Regierungen fungiert, die Bedenken im Zusammenhang mit der US-Signalaufklärung vorbringen, geht aber deutlich darüber hinaus.

(117) Im Einklang mit den verbindlichen Zusagen der US-Regierung wird der Ombudsmechanismus dafür sorgen, dass Beschwerden von Privatpersonen korrekt geprüft und geklärt werden und die betreffenden Personen von unabhängiger Seite die Bestätigung erhalten, dass die amerikanischen Rechtsvorschriften eingehalten bzw. Verstöße abgestellt wurden.[173] Der neu geschaffene Mechanismus besteht aus der „Ombudsperson des Datenschutzschilds“, d. h. dem Staatssekretär und weiterem Personal, sowie anderen Stellen, die für die Beaufsichtigung der verschiedenen Nachrichtendienste zuständig sind und auf deren Mitwirkung sich die Ombudsperson des Datenschutzschilds bei der Bearbeitung von Beschwerden stützt. Vor allem wenn eine individuelle Beschwerde die Vereinbarkeit der Überwachung mit US-Recht in Zweifel zieht, kann die Ombudsperson auf unabhängige Kontrollgremien mit Ermittlungsbefugnissen (wie die Generalinspekteure oder das PCLOB) zurückgreifen. In jedem Falle garantiert der Außenminister, dass die Ombudsperson bei der Beantwortung individueller Beschwerden über alle dafür benötigten Informationen verfügt.

(118) Durch diese „mehrgliedrige Struktur“ garantiert der Ombudsmechanismus eine unabhängige Kontrolle und individuellen Rechtsschutz. Zudem stellt die Zusammenarbeit mit anderen Kontrollgremien die notwendige Sachkompetenz sicher. Da der Mechanismus die Ombudsperson des Datenschutzschilds dazu verpflichtet, die Einhaltung der Grundsätze oder das Abstellen von Verstößen zu bestätigen, ist er ein Beleg für die Bereitschaft der US-Regierung insgesamt, Beschwerden von EU-Bürgern nachzugehen und einer Klärung zuzuführen.

(119) Erstens nimmt die Ombudsperson des Datenschutzschilds – anders als eine rein auf Regierungsebene agierende Einrichtung – individuelle Beschwerden entgegen und reagiert darauf. Beschwerden dieser Art können an die Kontrollgremien der Mitgliedstaaten gerichtet werden, die für die Beaufsichtigung der Nachrichtendienste und/oder die Verarbeitung von personenbezogene Daten durch staatliche Behörden

---

[171] Dieses Kriterium ergibt sich aus Artikel III der amerikanischen Verfassung, wonach sich die richterliche Gewalt nur auf reale Fälle und Streitigkeiten erstreckt.

[172] Siehe Clapper v. Amnesty Int'l USA, 133 S.Ct. 1138, 1144 (2013). Was die Verwendung von NSL anbelangt, schreibt der USA FREEDOM Act (§ 502(f)-503) vor, dass Verpflichtungen zur Geheimhaltung regelmäßig überprüft werden müssen und Empfänger von NSL darüber zu unterrichten sind, wenn die Faktenlage die Verpflichtung zur Geheimhaltung nicht länger rechtfertigt (siehe Erklärungen des ODNI (Anhang VI), S. 13). Allerdings ist dies keine Garantie dafür, dass Betroffene in der EU Kenntnis von der Überwachung ihrer Daten erhalten.

[173] Sofern der Beschwerdeführer den Zugang zu Schriftstücken beantragt, die sich im Besitz von staatlichen Behörden der USA befinden, gelten die im Freedom of Information Act verankerten Regeln und Verfahren. Dies schließt die Möglichkeit ein, sich im Falle der Ablehnung des Antrags unter den im FOIA genannten Voraussetzungen an ein Gericht (und nicht an ein unabhängiges Aufsichtsgremium) zu wenden.

zuständig sind, damit sie diese einer zentralen Stelle der EU vorlegen, die sie an die Ombudsperson des Datenschutzschilds weiterleitet.[174] Dies wird für EU-Bürger von Vorteil sein, da sie sich in ihrer eigenen Sprache an eine nahe gelegene innerstaatliche Instanz wenden können. Es ist Aufgabe dieser Instanz, Privatpersonen bei der Formulierung von Anträgen an die Ombudsperson des Datenschutzschilds zu unterstützen, die alle grundlegenden Informationen enthalten und daher als „vollständig" gelten können. Antragsteller brauchen nicht nachzuweisen, dass im Zuge der Signalaufklärung wirklich ein Zugriff der US-Regierung auf ihre personenbezogenen Daten stattgefunden hat.

(120) Zweitens sichert die US-Regierung zu, dafür zu sorgen, dass sich die Ombudsperson des Datenschutzschilds bei der Erfüllung ihrer Aufgaben auf die Zusammenarbeit mit anderen im amerikanischen Recht vorgesehenen unabhängigen Überwachungs- und Kontrollgremien stützen kann. Dazu gehören bisweilen innerstaatliche Nachrichtendienste, insbesondere wenn ein Antrag als auf Einsicht in Dokumente gemäß dem Freedom of Information Act gerichtet zu interpretieren ist. In anderen Fällen, vor allem wenn die Anträge die Vereinbarkeit von Überwachung mit US-Recht betreffen, werden unabhängige Kontrollgremien (z. B. Generalinspekteure) einbezogen, die dafür zuständig und befugt sind, gründliche Ermittlungen durchzuführen (insbesondere durch Zugang zu allen einschlägigen Dokumenten und die Befugnis, Informationen und Erklärungen einzuholen) und gegen Verstöße vorzugehen.[175] Auch kann die Ombudsperson des Datenschutzschilds Angelegenheiten an das PCLOB zur Prüfung weiterleiten.[176] Wenn eines der Kontrollgremien Verstöße feststellt, muss die betreffende Einrichtung der Intelligence Community (z. B. ein Nachrichtendienst) die Verstöße abstellen, da die Ombudsperson nur dann in der Lage ist, der betroffenen Person eine „positive" Antwort zu geben (in dem Sinne, dass etwaige Verstöße abgestellt worden sind), wozu sich die US-Regierung verpflichtet hat. Im Rahmen dieser Zusammenarbeit wird die Ombudsperson des Datenschutzschilds auch über den Ausgang der Ermittlungen unterrichtet, und sie wird über alle Mittel verfügen, um sicherzugehen, dass sie sämtliche Informationen erhält, die sie für die Abfassung ihrer Antwort benötigt.

(121) Hinzu kommt, dass die Ombudsperson des Datenschutzschilds von der US Intelligence Community unabhängig ist und somit nicht ihren Weisungen unterliegt.[177] Dies ist von erheblicher Bedeutung, da die Ombudsperson „bestätigen" muss, i) dass

---

174 Die Arbeitsweise des Ombudsmechanismus (Anhang III), Abschnitt 4(f) ist so geregelt, dass sich die Privacy Shield Ombudsperson direkt mit der EU-Stelle für die Bearbeitung von Individualbeschwerden in Verbindung setzt, die ihrerseits für die Kommunikation mit den Antragstellern zuständig ist. Wenn direkte Kontakte Bestandteil der „zugrundeliegenden Prozesse" sind, die den beantragten Rechtsschutz ermöglichen (z. B. eine Zugangsanfrage gemäß FOIA, siehe Abschnitt 5), erfolgen diese Kontakte im Einklang mit den anwendbaren Verfahren.

175 Siehe Ombudsmechanismus (Anhang III), Abschnitt 2(a). Siehe auch Erwägungsgründe 96-97.

176 Siehe Ombudsmechanismus (Anhang III), Abschnitt 2(c). Nach den von der US-Regierung gegebenen Erläuterungen soll das PCLOB kontinuierlich die Maßnahmen und Verfahren (sowie deren Durchführung) jener US-Behörden überwachen, die für die Bekämpfung des Terrorismus zuständig sind, um in Erfahrung zu bringen, ob ihre Aktionen „hinreichend die Privatsphäre und die Bürgerrechte schützen und mit den geltenden Gesetzen, Regelungen und Maßnahmen auf diesem Gebiet vereinbar sind". Es soll auch „Berichte und andere Informationen von Datenschutz- und Bürgerrechtsbeauftragten entgegennehmen und prüfen und gegebenenfalls Empfehlungen abgeben, die ihre Tätigkeit betreffen".

177 Siehe Roman Zakharov/Russland, Urteil vom 4.12.2015 (Große Kammer des EGMR), Antrag Nr. 47143/06, Rn. 275 („auch wenn es im Prinzip wünschenswert ist, die aufsichtsrechtliche Kontrolle einem Richter anzuvertrauen, kann die Beaufsichtigung durch nichtgerichtliche Organe als mit der Konvention vereinbar betrachtet werden, sofern das Aufsichtsorgan unabhängig von den die Überwachung durchführenden Behörden ist und mit hinreichenden und effektiven Aufsichtsbefugnissen ausgestattet ist".)

der Beschwerde ordnungsgemäß nachgegangen wurde und ii) dass die einschlägigen amerikanischen Rechtsvorschriften – darunter vor allem die in Anhang VI aufgeführten Einschränkungen und Garantien – befolgt wurden bzw. bei Nichteinhaltung der Grundsätze der Verstoß abgestellt wurde. Um diese unabhängige Bestätigung abgeben zu können, benötigt die Ombudsperson des Datenschutzschilds hinreichende Informationen über die Ermittlungen, damit sie die Richtigkeit der Antwort auf die Beschwerde beurteilen kann. Darüber hinaus hat der Außenminister zugesagt, dass der Staatssekretär die Aufgabe als Ombudsperson des Datenschutzschilds objektiv und ohne ungebührliche Einflussnahme, die sich auf die zu erteilende Antwort auswirken würde, wahrnehmen kann.

(122) Insgesamt gewährleistet dieser Mechanismus, dass individuelle Beschwerden gründlich untersucht und geklärt werden und dass zumindest im Bereich der Überwachung unabhängige Kontrollgremien mit der notwendigen Sachkompetenz und den erforderlichen Ermittlungsbefugnissen mitwirken und die Ombudsperson ihre Aufgaben ohne ungebührliche, insbesondere politische Einflussnahme wahrnehmen kann. Zudem können Privatpersonen Beschwerden einreichen, ohne dass sie den Nachweis oder auch nur Anhaltspunkte dafür erbringen müssen, dass sie Gegenstand einer Überwachung sind oder waren.[178] Angesichts dieser Gegebenheiten ist die Kommission davon überzeugt, dass hinreichende und wirksame Garantien gegen Missbrauch vorhanden sind.

(123) Aufgrund der hier geschilderten Sachlage gelangt die Kommission zu dem Schluss, dass die Vereinigten Staaten einen wirksamen Rechtsschutz vor Eingriffen ihrer Nachrichtendienste in die Grundrechte von Personen gewährleistet, deren Daten im Rahmen des EU-US-Datenschutzschilds aus der Europäischen Union in die Vereinigten Staaten übermittelt werden.

(124) In diesem Zusammenhang nimmt die Kommission das Urteil des Gerichtshofs in der Rechtssache Schrems zur Kenntnis, in dem es heißt: „Desgleichen verletzt eine Regelung, die keine Möglichkeit für den Bürger vorsieht, mittels eines Rechtsbehelfs Zugang zu den ihn betreffenden personenbezogenen Daten zu erlangen oder ihre Berichtigung oder Löschung zu erwirken, den Wesensgehalt des in Art. 47 der Charta verankerten Grundrechts auf wirksamen gerichtlichen Rechtsschutz.“[179] Die Analyse der Kommission hat bestätigt, dass derartige Rechtsbehelfe in den Vereinigten Staaten vorhanden sind, auch durch die Einrichtung des Ombudsmechanismus. Dieser Mechanismus ermöglicht eine unabhängige Kontrolle mit Ermittlungsbefugnissen. Im Rahmen der ständigen Überwachung des Datenschutzschilds durch die Kommission, wozu auch die gemeinsame jährliche Überprüfung gehört, an der sich die Ombudsperson beteiligen soll, wird die Wirksamkeit dieses Mechanismus überprüft.

3.2. Zugang zu und Verarbeitung von Daten durch staatliche Behörden der USA aus Gründen der Strafverfolgung und des öffentlichen Interesses

(125) Im Hinblick auf Eingriffe in personenbezogene Daten, die im Rahmen des EU-US-Datenschutzschilds aus Gründen der Strafverfolgung übermittelt werden, hat die

[178] Siehe Kennedy/Vereinigtes Königreich, Urteil vom 18.5.2010, Antrag Nr. 26839/05, Rn. 167.

[179] Schrems, Rn. 95. Wie aus den Randnummern 91 und 96 des Urteils deutlich hervorgeht, betrifft Randnummer 95 das Schutzniveau, das die Rechtsordnung der Union garantiert und dem das Schutzniveau im Drittland „in der Sache gleichwertig“ sein muss. Gemäß Rn. 73 und 74 des Urteils erfordert dies nicht, dass das Schutzniveau oder die Mittel, auf die das Drittland zurückgreift, identisch sind, doch müssen sich die Mittel in der Praxis als wirksam erweisen.

Regierung der USA (über das Justizministerium) Zusicherungen zu den dafür geltenden Einschränkungen und Garantien gemacht, die nach Einschätzung der Kommission ein hinreichendes Schutzniveau gewährleisten.

(126) Nach diesen Informationen erfordern gemäß viertem Zusatzartikel zur Verfassung der USA[180] Durchsuchungen und Beschlagnahmen, die von Strafverfolgungsbehörden vorgenommen werden, grundsätzlich[181] eine gerichtliche Anordnung bei Vorliegen eines „hinreichenden Tatverdachts". In den wenigen Sonder- und Ausnahmefällen, in denen diese Anforderung nicht gilt[182], unterliegt die Strafverfolgung einer Prüfung der „Zumutbarkeit".[183] Ob eine Durchsuchung oder Beschlagnahme zumutbar ist, „wird zum einen daran gemessen, inwieweit sie in die Privatsphäre der betreffenden Person eingreift, und zum anderen daran, inwieweit sie zur Förderung legitimer staatlicher Interessen erforderlich ist."[184] Ganz allgemein garantiert der vierte Zusatzartikel den Schutz der Privatsphäre und der Menschenwürde und bietet Schutz vor willkürlichen Eingriffen von Staatsbeamten.[185] Diese Konzepte entsprechen den Grundsätzen der Notwendigkeit und Verhältnismäßigkeit im EU-Recht. Wenn die Strafverfolgungsbehörden die beschlagnahmten Objekte nicht länger als Beweismittel benötigen, sind sie zurückzugeben.[186]

(127) Auch wenn sich das Recht, das der vierte Zusatzartikel enthält, nicht auf Nicht-US-Bürger erstreckt, die ihren Wohnsitz außerhalb der USA haben, profitieren diese dennoch indirekt von diesem Rechtsschutz, weil amerikanische Unternehmen über die personenbezogenen Daten verfügen und die Strafverfolgungsbehörden ihnen gegenüber in jedem Falle einer gerichtlichen Genehmigung bedürfen (oder zumindest den Grundsatz der Verhältnismäßigkeit beachten müssen). [187] Weiteren Schutz bieten bestimmte staatliche Behörden sowie die Leitlinien des Justizministeriums, die den Datenzugriff zu Zwecken der Strafverfolgung nach Grundsätzen, die dem Prinzip der Notwendigkeit und Verhältnismäßigkeit entsprechen, einschränken (indem z. B. das FBI verpflichtet wird, die mit den geringsten Eingriffen verbundenen

---

180 Der vierte Zusatzartikel lautet: „Das Recht des Volkes auf Sicherheit der Person und der Wohnung, der Urkunden und des Eigentums vor willkürlicher Durchsuchung, Verhaftung und Beschlagnahme darf nicht verletzt werden, und Haussuchungs- und Haftbefehle dürfen nur bei Vorliegen eines eidlich oder eidesstattlich erhärteten Rechtsgrundes ausgestellt werden und müssen die zu durchsuchende Örtlichkeit und die in Gewahrsam zu nehmenden Personen oder Gegenstände genau bezeichnen." Nur Richter dürfen Durchsuchungsbefehle ausstellen. Bundesrichterliche Genehmigungen zum Kopieren elektronisch gespeicherter Informationen unterliegen zudem Regel 41 der Strafprozessordnung der USA.

181 Der Oberste Gerichtshof hat wiederholt Durchsuchungen ohne richterliche Anordnung als „Ausnahmefälle" bezeichnet. Siehe z. B. *Johnson v. United States*, 333 U.S. 10, 14 (1948); *McDonald v. United States*, 335 U.S. 451, 453 (1948); *Camara v. Municipal Court*, 387 U.S. 523, 528-29 (1967); *G.M. Leasing Corp. v. United States*, 429 U.S. 338, 352-53, 355 (1977). Auch betont er immer wieder, es sei „ein fundamentaler Verfassungsgrundsatz auf diesem Gebiet, dass Durchsuchungen ohne Mitwirkung der Justiz, d. h. ohne vorherige Genehmigung durch einen Richter, laut viertem Zusatzartikel ihrem Wesen nach willkürlich sind, wenn man von einigen konkret benannten und klar umrissenen Ausnahmen absieht." Siehe z. B. *Coolidge v. New Hampshire*, 403 U.S. 443, 454-55 (1971); *G.M. Leasing Corp. v. United States*, 429 U.S. 338, 352-53, 358 (1977).

182 City of Ontario, Cal. v. Quon, 130 S. Ct. 2619, 2630 (2010).

183 PCLOB, Sec. 215 Report, S. 107, mit Verweis auf Maryland v. King, 133 S. Ct. 1958, 1970 (2013).

184 PCLOB, Sec. 215 Report, S.107, mit Verweis auf Samson v. California, 547 U.S. 843, 848 (2006).

185 City of Ontario, Cal. v. Quon, 130 S. Ct. 2619, 2630 (2010), 2627.

186 Siehe z. B. *United States v Wilson*, 540 F.2d 1100 (D.C. Cir. 1976).

187 Vgl. Roman Zakharov/Russland, Urteil vom 4.12.2015 (Große Kammer des EGMR), Antrag Nr. 47143/06, Rn. 269. Dort heißt es: „Das Erfordernis, einem Kommunikationsanbieter vor Erlangung des Zugangs zu den Kommunikationsvorgängen einer Person eine Abhörgenehmigung vorzulegen, gehört zu den wichtigsten Schutzvorkehrungen gegen einen Missbrauch durch die Strafverfolgungsbehörden und stellt sicher, dass für das Abhören in allen Fällen die dafür vorgeschriebene Genehmigung eingeholt wird."

Ermittlungsmethoden anzuwenden und die Auswirkungen auf die Privatsphäre und die Bürgerrechte zu berücksichtigen).[188] Den Erklärungen der US-Regierung zufolge gilt das gleiche oder ein noch höheres Schutzniveau bei strafrechtlichen Ermittlungen auf einzelstaatlicher Ebene (wenn diese auf Rechtsvorschriften der Bundesstaaten basieren).[189]

(128) Obwohl eine vorherige Genehmigung durch ein Gericht oder eine Grand Jury (eine Ermittlungseinrichtung, deren Mitglieder von einem Richter oder Magistrate ausgewählt werden) nicht in allen Fällen erforderlich ist[190], sind behördliche Anordnungen zur Herausgabe von Daten auf einzelne Fälle beschränkt und können einer unabhängigen gerichtlichen Überprüfung unterzogen werden, zumindest wenn die Regierung sie vor Gericht durchsetzen will.[191]

(129) Das Gleiche gilt für behördliche Anordnungen zur Herausgabe von Daten für im öffentlichen Interesse liegende Zwecke. Den Erklärungen der US-Regierung zufolge gibt es zudem materiell-rechtliche Beschränkungen dahingehend, dass Behörden nur den Zugriff auf Daten beantragen können, die für Angelegenheiten innerhalb ihres Verantwortungsbereichs von Belang sind, und den Grundsatz der Zumutbarkeit beachten müssen.

(130) Darüber hinaus gewährt das amerikanische Recht Privatpersonen eine Reihe gerichtlicher Rechtsbehelfe gegen staatliche Behörden oder einzelne Mitarbeiter, sofern diese Behörden personenbezogene Daten verarbeiten. Diese Rechtsschutzmöglichkeiten, die insbesondere der Administrative Procedure Act (APA), der Freedom of Information Act (FOIA) und der Electronic Communications Privacy Act (ECPA) einräumen, stehen alle Personen unabhängig von ihrer Nationalität offen, sofern die erforderlichen Voraussetzungen gegeben sind.

(131) Nach den Bestimmungen des Administrative Procedure Act[192] kann „eine Person, die durch Handlungen einer Behörde einen Schaden oder Nachteil erleidet“, eine gerichtliche Nachprüfung beantragen. [193] Dazu gehört die Möglichkeit, das Gericht zu ersuchen, „Handlungen, Feststellungen und Schlussfolgerungen einer Behörde, die für ... willkürlich, mutwillig, die Befugnisse überschreitend oder anderweitig rechtswidrig befunden werden, für null und nichtig zu erklären.“[194]

---

188 Erklärungen des DOJ (Anhang VII), S. 4 mit weiteren Verweisen.

189 Erklärungen des DOJ (Anhang VII), Nr. 2.

190 Nach den Informationen, die der Kommission übermittelt wurden, betrifft dies – wenn man einzelne Bereiche ausklammert, die aller Voraussicht nach für den Datenverkehr im Rahmen des EU-US-Datenschutzschilds nicht relevant sind (z. B. Ermittlungen zu Betrug im Gesundheitswesen, zum Kindesmissbrauch oder zu Verstößen gegen das Betäubungsmittelgesetz) –, in erster Linie bestimmte Behörden aufgrund des Electronic Communications Privacy Act (ECPA) bei Auskunftsbegehren zu Basis-, Verbindungs- und Abrechnungsdaten von Teilnehmern (18 U.S.C. § 2703(c)(1)), (2), z. B. Adressen, Art und Dauer der Verbindungen, und zum Inhalt von E-Mails, die mehr als 180 Tage alt sind (18 U.S.C. § 2703 (a), (b)). Im letztgenannten Fall muss allerdings die betroffene Person darüber unterrichtet werden und hat somit die Möglichkeit, das Auskunftsbegehren vor Gericht anzufechten. Siehe auch den Überblick in DOJ, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, Ch. 3: The Stored Communications Act, S. 115-138.

191 Den Erklärungen der US-Regierung zufolge können die Empfänger von behördlichen Anordnungen zur Herausgabe von Daten diese vor Gericht mit der Begründung anfechten, sie seien unverhältnismäßig, d. h. überzogen, repressiv oder belastend. Siehe Erklärungen des DOJ (Anhang VII), S. 2.

192 5 U.S.C. § 702.

193 Im Allgemeinen unterliegen nur „endgültige“ Maßnahmen einer Behörde, nicht aber „vorbereitende, verfahrensmäßige oder vorläufige“ Maßnahmen der gerichtlichen Nachprüfung. Siehe 5 U.S.C. § 704.

194 5 U.S.C. § 706(2)(A).

(132) Konkreter ist in diesem Zusammenhang Titel II des Electronic Communications Privacy Act[195], der ein System gesetzlich verankerter Datenschutzrechte beinhaltet und somit unmittelbar den Zugriff der Strafverfolgungsbehörden auf den Inhalt leitungsgebundener, mündlicher oder elektronischer Kommunikationsvorgänge regelt, die von Drittanbietern gespeichert werden.[196] Er stellt den rechtswidrigen (d. h. nicht gerichtlich autorisierten oder anderweitig zulässigen) Zugriff auf derartige Kommunikationsvorgänge unter Strafe und räumt betroffenen Personen die Möglichkeit ein, vor einem Bundesgericht der USA eine Klage auf eigentlichen und pönalen Schadensersatz einzureichen sowie billigkeitsrechtliche Ansprüche gegen einen Regierungsbeamten, der vorsätzlich derartige rechtswidrige Handlungen begangen hat, oder die Vereinigten Staaten geltend zu machen.

(133) Auch hat nach dem Freedom of Information Act (FOIA, 5 U.S.C. § 552) jede Person das Recht, Zugang zu Unterlagen von Bundesbehörden zu erlangen und nach Ausschöpfung aller behördlichen Rechtsbehelfe dieses Recht gerichtlich durchzusetzen, sofern die Unterlagen nicht durch eine Ausnahmeregelung oder Strafverfolgungsklausel vor der Offenlegung geschützt sind.[197]

(134) Darüber hinaus gewähren verschiedene weitere Gesetze Privatpersonen das Recht, wegen der Verarbeitung ihrer personenbezogener Daten staatliche Behörden der USA oder Beamte zu verklagen, so etwa der Wiretap Act[198], der Computer Fraud and Abuse

---

195 18 U.S.C. §§ 2701-2712.

196 Der ECPA schützt Kommunikationsdaten, die sich im Besitz von zwei dort aufgeführten Kategorien von Netzbetreibern befinden, nämlich Anbietern: i) elektronischer Kommunikationsdienste, z. B. Telefon oder E-Mail; ii) elektronischer Dienste zur Fernspeicherung oder -verarbeitung.

197 Diese Ausnahmen sind jedoch klar umrissen. Beispielsweise ist nach 5 U.S.C. § 552 (b)(7) die Berufung auf den FOIA ausgeschlossen bei „Unterlagen oder Informationen, die zu Strafverfolgungszwecken zusammengetragen wurden, aber nur soweit die Herausgabe derartiger Unterlagen oder Informationen der Strafverfolgung A) nach vernünftigem Ermessen die Rechtsdurchsetzung behindern könnte, B) eine Person ihres Rechts auf ein ordentliches Verfahren oder eine unparteiische richterliche Entscheidung berauben würde, (C) nach vernünftigem Ermessen einen unzulässigen Eingriff in die Privatsphäre darstellen könnte, D) nach vernünftigem Ermessen zur Enttarnung von vertraulichen Quellen führen könnte, was staatliche, kommunale oder ausländische Behörden bzw. Dienststellen oder private Einrichtungen, die Informationen auf vertraulicher Grundlage zur Verfügung stellten, ebenso betrifft wie die auf vertraulichen Quellen beruhenden Unterlagen oder Informationen, die von einer Strafverfolgungsbehörde im Zuge strafrechtlicher Ermittlungen oder von einer Behörde im Rahmen gesetzlicher nachrichtendienstlicher Ermittlungen zusammengetragen wurden, (E) Techniken und Verfahren strafrechtlicher Ermittlungen und Strafverfolgungen oder Leitlinien für strafrechtliche Ermittlungen und Strafverfolgungen offenlegen würde und dies nach vernünftigem Ermessen die Gefahr einer Umgehung des Gesetzes heraufbeschwören würde, oder F) nach vernünftigem Ermessen das Leben oder die körperliche Unversehrtheit einer Person gefährden könnte.“ Zudem gilt: „Wenn ein Antrag auf Zugang zu Unterlagen gestellt wird [deren Herausgabe nach vernünftigem Ermessen die Rechtsdurchsetzung behindern könnte] und – A) die Ermittlungen oder das Verfahren einen möglichen Verstoß gegen das Strafrecht betreffen; und B) Grund zur Annahme besteht, dass i) die Person, gegen die Ermittlungen oder ein Verfahren im Gange sind, davon keine Kenntnis hat und ii) die Offenlegung des Vorhandenseins der Unterlagen nach vernünftigem Ermessen die Rechtsdurchsetzung behindern könnte, kann die Behörde, jedoch nur solange diese Umstände fortbestehen, die Unterlagen als Informationen behandeln, die nicht den Bestimmungen dieses Paragrafen unterliegen.“ (5 U.S.C. § 552 (c)(1)).

198 18 U.S.C. §§ 2510 ff. Nach dem Wiretap Act (18 U.S.C. § 2520) kann eine Person, deren leitungsgebundene, mündliche oder elektronische Kommunikation überwacht, offengelegt oder vorsätzlich verwendet wird, eine Zivilklage gegen die Vereinigten Staaten wegen Verstoßes gegen den Wiretap Act einreichen, unter bestimmten Umständen auch gegen einen einzelnen Regierungsbeamten. Zur Erhebung von Adressen oder anderen nichtinhaltlichen Informationen (z. B. IP-Adresse, Adressen von gesendeten/empfangenen E-Mails) siehe auch das Kapitel „Pen Registers and Trap and Trace Devices“ von Titel 18 (18 U.S.C. §§ 3121-3127 und zu Zivilklagen § 2707).

Act[199], der Federal Torts Claim Act[200], der Right to Financial Privacy Act[201] und der Fair Credit Reporting Act.[202]

(135) Die Kommission gelangt daher zu dem Schluss, dass in den Vereinigten Staaten Regeln gelten, die darauf gerichtet sind, jegliche Eingriffe in die Grundrechte von Personen, deren personenbezogene Daten im Rahmen des EU-US-Datenschutzschilds aus der Europäischen Union in die Vereinigten Staaten übermittelt werden, aus Gründen der Strafverfolgung[203] oder für andere im öffentlichen Interesse liegende Zwecke auf das für die Erreichung solcher legitimen Ziele absolut notwendige Maß zu beschränken, und dass damit ein wirksamer Rechtsschutz vor derartigen Eingriffen gewährleistet ist.

4. Angemessener Rechtsschutz im Rahmen des EU-US-Datenschutzschilds

(136) Im Licht dieser Feststellungen geht die Kommission davon aus, dass die Vereinigten Staaten einen angemessenen Rechtsschutz für personenbezogene Daten gewährleisten, die im Rahmen des EU-US-Datenschutzschilds aus der Europäischen Union an selbstzertifizierte Organisationen in den Vereinigten Staaten übermittelt werden.

(137) Insbesondere geht die Kommission davon aus, dass die vom US-Handelsministerium herausgegebenen Datenschutzgrundsätze insgesamt ein Schutzniveau für personenbezogene Daten gewährleisten, das der Sache nach dem Niveau gleichwertig ist, wie es durch die in der Richtlinie 95/46/EG verankerten Grundsätze garantiert wird.

(138) Zudem garantieren die Transparenzpflichten und die Verwaltung des Datenschutzschilds durch das Handelsministerium die wirksame Anwendung der Datenschutzgrundsätze.

(139) Des Weiteren geht die Kommission davon aus, dass insgesamt betrachtet die vom Datenschutzschild vorgesehenen Aufsichts- und Beschwerdeverfahren es gestatten, Verstöße dem Datenschutzschild angehörender Organisationen gegen die Grundsätze

---

199 18 U.S.C. § 1030. Dem Computer Fraud and Abuse Act zufolge kann jedermann eine Person, unter bestimmten Umständen auch einen einzelnen Regierungsbeamten, wegen eines vorsätzlichen nicht autorisierten Zugriffs (oder wegen Überschreitung der Zugriffsbefugnisse) verklagen, der darauf zielt, Informationen von einem Finanzinstitut, einem Computersystem der US-Regierung oder einem genau bezeichneten Computer zu erlangen.

200 28 U.S.C. §§ 2671 ff. Der Federal Tort Claims Act ermöglicht Privatpersonen unter bestimmten Umständen, eine Klage gegen die Vereinigten Staaten wegen „einer fahrlässigen oder rechtswidrigen Handlung oder Unterlassung eines Angestellten der Regierung im Rahmen der Ausübung seines Amts oder seiner Tätigkeit“ einzureichen.

201 12 U.S.C. §§ 3401 ff. Nach dem Right to Financial Privacy Act können Privatpersonen unter bestimmten Umständen die Vereinigten Staaten wegen der gesetzwidrigen Erlangung oder Offenlegung geschützter Finanzunterlagen verklagen. Der Zugriff des Staates auf geschützte Finanzunterlagen ist im Allgemeinen untersagt, sofern er sich nicht auf eine rechtmäßige Anordnung zur Herausgabe oder Durchsuchung stützt oder vorbehaltlich bestimmter Einschränkungen auf eine formale schriftliche Aufforderung, von der die betroffene Person in Kenntnis zu setzen ist.

202 15 U.S.C. §§ 1681-1681x. Der Fair Credit Reporting Act räumt die Möglichkeit ein, gegen jede Person und unter bestimmten Voraussetzungen auch gegen eine staatliche Behörde rechtliche Schritte einzuleiten, die bei der Erstellung, Verbreitung und Verwendung von Verbraucherkreditauskünften nicht die Anforderungen (insbesondere an die rechtliche Ermächtigung) erfüllt.

203 Der Gerichtshof hat anerkannt, dass die Strafverfolgung ein legitimes politisches Ziel darstellt. Siehe verb. Rs. C-293/12 und C-594/12, Digital Rights Ireland u. a., EU:C:2014:238, Rn. 42. Siehe auch Artikel 8 Absatz 2 EGMR und das Urteil des Europäischen Gerichtshofs für Menschenrechte in Weber and Saravia v. Germany, Antrag Nr. 54934/00, Rn. 104.

in der Praxis aufzudecken und zu ahnden, und dass damit den betroffenen Personen Rechtsbehelfe an die Hand gegeben werden, um Zugang zu den sie betreffenden personenbezogenen Daten zu erlangen und letztlich die Korrektur oder Löschung dieser Daten zu erwirken.

(140) Schließlich kommt die Kommission aufgrund der verfügbaren Informationen über die Rechtsordnung der USA, einschließlich der Erklärungen und Zusagen der US-Regierung, zu dem Schluss, dass jegliche Eingriffe in die Grundrechte von Personen, deren Daten im Rahmen des EU-US-Datenschutzschilds aus Gründen der nationalen Sicherheit, der Strafverfolgung oder für andere im öffentlichen Interesse liegende Zwecke aus der Europäischen Union in die Vereinigten Staaten übermittelt werden, sowie die deshalb den selbstzertifizierten Organisationen bei der Einhaltung der Grundsätze auferlegten Beschränkungen auf das für die Erreichung solcher legitimen Ziele absolut notwendige Maß beschränkt werden und dass damit ein wirksamer Rechtsschutz vor derartigen Eingriffen gewährleistet ist.

(141) Die Kommission schließt daraus, dass somit den im Licht der Charta der Grundrechte der Europäischen Union geltenden Anforderungen von Artikel 25 der Richtlinie 95/46/EG entsprochen wird, wie sie der Gerichtshof vor allem im Urteil Schrems erläutert hat.

5. Maßnahmen der Datenschutzbehörden und Unterrichtung der Kommission

(142) Im Urteil Schrems stellte der Gerichtshof klar, dass die Kommission nicht berechtigt ist, die von Datenschutzbehörden aus Artikel 28 der Richtlinie 95/46/EG abgeleiteten Befugnisse (darunter die Befugnis, Datenübermittlungen auszusetzen) einzuschränken, wenn eine Person im Rahmen einer Eingabe aufgrund dieser Bestimmung in Frage stellt, dass eine Angemessenheitsentscheidung der Kommission mit dem Schutz der Privatsphäre sowie der Freiheiten und Grundrechte unvereinbar ist.[204]

(143) Um die Funktionsweise des Datenschutzschilds wirksam überwachen zu können, sollte die Kommission von den Mitgliedstaaten über einschlägige Maßnahmen der Datenschutzbehörden unterrichtet werden.

(144) Der Gerichtshof befand des Weiteren, dass entsprechend Artikel 25 Absatz 6 Unterabsatz 2 der Richtlinie 95/46/EG die Mitgliedstaaten und ihre Organe die notwendigen Maßnahmen treffen müssen, um Rechtsakte der Unionsorgane umzusetzen, denn für diese gilt grundsätzlich eine Vermutung der Rechtmäßigkeit, so dass sie Rechtswirkungen entfalten, solange sie nicht zurückgenommen, im Rahmen einer Nichtigkeitsklage für nichtig erklärt oder infolge eines Vorabentscheidungsersuchens oder einer Einrede der Rechtswidrigkeit für ungültig erklärt wurden. Folglich ist eine Angemessenheitsentscheidung der Kommission gemäß Artikel 25 Absatz 6 der Richtlinie 95/46/EG für alle Organe der Mitgliedstaaten bindend, an die sie gerichtet ist, einschließlich ihrer unabhängigen Kontrollstellen.[205] Wenn bei einer Kontrollstelle eine Beschwerde eingegangen ist, die die Vereinbarkeit einer Angemessenheitsentscheidung der Kommission mit dem Grundrecht der Achtung der Privatsphäre und des Datenschutzes in Frage stellt, und die Kontrollstelle die darin enthaltenen Rügen für begründet erachtet, ist es insoweit Sache des nationalen Gesetzgebers, Rechtsbehelfe vorzusehen, die es der

[204] Schrems, Rn. 40ff., 101-103.
[205] Schrems, Rn. 51, 52 und 62.

Kontrollstelle ermöglichen, die von ihr für begründet erachteten Rügen vor den nationalen Gerichten geltend zu machen, damit diese, wenn sie die Zweifel teilen, das Verfahren aussetzen und den Gerichtshof um eine Vorabentscheidung über deren Gültigkeit ersuchen.[206]

6. Regelmäßige Überprüfung der Feststellung der Angemessenheit

(145) In Anbetracht der Tatsache, dass sich das von der US-Rechtsordnung gewährte Schutzniveau ändern kann, überprüft die Kommission nach Annahme des vorliegenden Beschlusses in regelmäßigen Abständen, ob die Feststellungen zur Angemessenheit des Schutzniveaus, das die Vereinigten Staaten im Rahmen des EU-US-Datenschutzschild gewährleistet, noch sachlich und rechtlich gerechtfertigt sind. Eine solche Überprüfung ist auf alle Fälle erforderlich, wenn die Kommission Kenntnisse erlangt, die in dieser Hinsicht begründete Zweifel aufkommen lassen.[207]

(146) Daher wird die Kommission kontinuierlich den mit dem EU-US-Datenschutzschild geschaffenen Gesamtrahmen für die Übermittlung personenbezogener Daten sowie die Einhaltung der Erklärungen und Zusagen, die in den diesem Beschluss beigefügten Schriftstücken enthalten sind, durch die US-Behörden überwachen. Um diesen Prozess zu erleichtern, haben die USA zugesichert, die Kommission über wesentliche Änderungen des US-Rechts zu unterrichten, wenn sie für den Datenschutzschild relevant sind und den Datenschutz sowie die Beschränkungen und Schutzvorkehrungen für den Zugriff staatlicher Behörden auf personenbezogene Daten betreffen. Zudem unterliegt der Beschluss einer gemeinsamen jährlichen Überprüfung, die sich auf alle Aspekte der Funktionsweise des EU-US-Datenschutzschilds erstreckt, darunter die Handhabung der aus Gründen der nationalen Sicherheit und Strafverfolgung gewährten Ausnahmen von den Grundsätzen. Da die Feststellung der Angemessenheit auch von Entwicklungen des Unionsrechts beeinflusst werden kann, bewertet die Kommission überdies das vom Datenschutzschild gebotene Schutzniveau nach dem Inkrafttreten der Datenschutz-Grundverordnung.

(147) Zur Durchführung der in den Anhängen I, II und VI erwähnten gemeinsamen jährlichen Überprüfung führt die Kommission Gespräche mit dem Handelsministerium und der FTC, die gegebenenfalls von Vertretern anderer an der Umsetzung der Modalitäten des Datenschutzschilds beteiligten Regierungsstellen sowie – bei Angelegenheiten der nationalen Sicherheit – von Vertretern des ODNI, anderen Nachrichtendiensten und der Ombudsperson begleitet werden. Die Teilnahme an dieser Zusammenkunft steht Datenschutzbehörden der EU und Vertretern der Artikel-29-Datenschutzgruppe offen.

(148) Im Rahmen der gemeinsamen jährlichen Überprüfung wird die Kommission das Handelsministerium um eine umfassende Unterrichtung über alle relevanten Gesichtspunkte der Funktionsweise des EU-US-Datenschutzschilds ersuchen, wozu auch die von den Datenschutzbehörden an das Handelsministerium überwiesenen Fälle und die Ergebnisse der von Amts wegen vorgenommenen Kontrollen der Einhaltung gehören. Die Kommission wird auch um Erklärungen nachsuchen, die Fragen oder Angelegenheiten betreffen, welche mit dem EU-US-Datenschutzschild und seiner Handhabung zusammenhängen und sich aus allen verfügbaren Informationen ergeben, so etwa in nach dem USA FREEDOM Act zulässigen

[206] Schrems, Rn. 65.
[207] Schrems, Rn. 76.

Transparenzberichten, öffentlich zugänglichen Berichten von bundesweiten US-Nachrichtendiensten, Datenschutzbehörden und Datenschutzgruppen, Medienberichten oder anderen möglichen Quellen. Um die diesbezügliche Aufgabe der Kommission zu erleichtern, sollten die Mitgliedstaaten die Kommission über Fälle unterrichten, in denen Maßnahmen der Organe, die in den USA für die Gewährleistung der Einhaltung der Grundsätze zuständig sind, diesem Ziel nicht gerecht werden, und über Anhaltspunkte dafür, dass die Maßnahmen von staatlichen Behörden der USA, die für die nationale Sicherheit oder die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten zuständig sind, nicht das erforderliche Schutzniveau gewährleisten.

(149) Auf der Grundlage der gemeinsamen jährlichen Überprüfung wird die Kommission einen öffentlich zugänglichen Bericht erstellen, der dem Europäischen Parlament und dem Rat vorgelegt wird.

7. Aussetzung des Angemessenheitsbeschlusses

(150) Wenn die Kommission anhand der durchgeführten Kontrollen oder sonstiger verfügbarer Informationen zu dem Schluss gelangt, dass das vom Datenschutzschild gebotene Schutzniveau nicht mehr als dem Schutzniveau der Union in der Sache gleichwertig anzusehen ist, oder eindeutige Anhaltspunkte dafür erkennt, dass in den Vereinigten Staaten eine wirksame Einhaltung der Grundsätze möglicherweise nicht länger gewährleistet ist oder die Maßnahmen von staatlichen Behörden der USA, die für die nationale Sicherheit oder die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten zuständig sind, nicht das erforderliche Schutzniveau gewährleisten, setzt sie das Handelsministerium davon in Kenntnis und ersucht darum, dass geeignete Maßnahmen getroffen werden, um innerhalb einer angemessenen Frist die Frage der potenziellen Nichteinhaltung der Grundsätze zügig zu klären. Wenn die US-Behörden nach Ablauf der Frist nicht zufriedenstellend nachweisen können, dass der EU-US-Datenschutzschild weiterhin eine wirksame Einhaltung und ein angemessenes Schutzniveau garantiert, leitet die Kommission das Verfahren ein, das zur teilweisen oder vollständigen Aussetzung oder zur Aufhebung des vorliegenden Beschlusses führt.[208] Wahlweise kann die Kommission vorschlagen, den Beschluss abzuändern, indem beispielsweise der Anwendungsbereich der Angemessenheitsfeststellung auf Datenübertragungen beschränkt wird, die zusätzlichen Auflagen unterliegen.

(151) Die Kommission leitet das Verfahren zur Aussetzung oder Aufhebung des Beschlusses insbesondere ein, sofern

a) es Anhaltspunkte dafür gibt, dass sich die US-Behörden nicht an die Erklärungen und Zusagen halten, die in den diesem Beschluss beigefügten Schriftstücken enthalten sind und unter anderem die Bedingungen und Einschränkungen betreffen, denen der Zugriff amerikanischer Behörden auf personenbezogene Daten, die im Rahmen des Datenschutzschilds übertragen werden, aus Gründen der

[208] Vom Zeitpunkt des Inkrafttretens der Datenschutz-Grundverordnung an macht die Kommission von ihrer Befugnis Gebrauch, in hinreichend begründeten Fällen äußerster Dringlichkeit einen sofort geltenden Durchführungsrechtsakt zu erlassen, der den vorliegenden Beschluss aussetzt, sofort in Kraft tritt, ohne dass er vorher dem zuständigen Komitologieausschuss vorgelegt wurde, und für einen Zeitraum von höchstens sechs Monaten in Kraft bleibt.

Strafverfolgung, der nationalen Sicherheit oder des öffentlichen Interesses unterliegt;

b) Beschwerden von betroffenen Personen in der EU nicht wirksam nachgegangen wird; dabei berücksichtigt die Kommission sämtliche Umstände, die sich auf die Möglichkeiten von betroffenen Personen in der EU auswirken, ihre Rechte durchzusetzen, wozu insbesondere die freiwillige Verpflichtung selbstzertifizierter US-Unternehmen gehört, mit den Datenschutzbehörden zusammenzuarbeiten und ihre Empfehlungen zu befolgen; oder

c) die Ombudsperson des Datenschutzschilds nicht zeitnah und angemessen auf Anfragen von betroffenen Personen in der EU reagiert.

(152) Die Kommission wird die Einleitung des Verfahrens, das zur Änderung, Aussetzung oder Aufhebung des vorliegenden Beschlusses führt, auch in Erwägung ziehen, wenn im Rahmen der gemeinsamen jährlichen Überprüfung der Funktionsweise des EU-US-Datenschutzschilds oder bei anderer Gelegenheit das Handelsministerium oder andere Regierungsstellen, die an der Umsetzung des Datenschutzschilds beteiligt sind, oder bei Angelegenheiten der nationalen Sicherheit Vertreter der US Intelligence Community oder die Ombudsstelle nicht für die Informationen und Klarstellungen sorgen, die erforderlich sind, um die Einhaltung der Datenschutzgrundsätze, die Wirksamkeit der Beschwerdeverfahren oder die Absenkung des notwendigen Schutzniveaus zu beurteilen, die auf Maßnahmen der bundesweiten US-Nachrichtendienste zurückzuführen ist, vor allem auf die Sammlung und/oder den Zugang zu personenbezogenen Daten, die nicht auf das absolut notwendige und vertretbare Maß beschränkt ist. Dabei berücksichtigt die Kommission den Umfang, in dem die relevanten Informationen aus anderen Quellen beschafft werden können, darunter Berichte von selbstzertifizierten US-Unternehmen, wie dies gemäß USA FREEDOM Act zulässig ist.

(153) Die durch Artikel 29 der Richtlinie 95/46/EG eingesetzte Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten hat zu dem Schutzniveau, das der EU-US-Datenschutzschild bietet, eine Stellungnahme abgegeben[209], die bei der Ausarbeitung des vorliegenden Beschlusses berücksichtigt wurde.

(154) Das Europäische Parlament hat eine Entschließung zur transatlantischen Datenübermittlung verabschiedet.[210]

(155) Die im vorliegenden Beschluss vorgesehenen Maßnahmen stehen im Einklang mit der Stellungnahme des gemäß Artikel 31 Absatz 1 der Richtlinie 95/46/EG eingesetzten Ausschusses. —

[209] Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision, angenommen am 13.4.2016.

[210] Entschließung des Europäischen Parlaments vom 26. Mai 2016 zur transatlantischen Datenübermittlung ((2016/2727(RSP)).

HAT FOLGENDEN BESCHLUSS ERLASSEN:

Artikel 1

(1) Im Sinne von Artikel 25 Absatz 2 der Richtlinie 95/46/EG gewährleisten die Vereinigten Staaten ein angemessenes Schutzniveau für personenbezogene Daten, die im Rahmen des EU-US-Datenschutzschilds aus der Europäischen Union an Organisationen in den Vereinigten Staaten übermittelt werden.

(2) Der EU-US-Datenschutzschild besteht aus den Grundsätzen, die am 7. Juli 2016 vom US-Handelsministerium herausgegeben wurden und in Anhang II aufgeführt sind, und den offiziellen Erklärungen und Zusagen, die in den Schriftstücken der Anhänge I und III bis VII enthalten sind.

(3) Im Sinne von Absatz 1 werden personenbezogene Daten im Rahmen des EU-US-Datenschutzschilds übermittelt, wenn sie aus der Europäischen Union an US-Organisationen übermittelt werden, die in der „Datenschutzschild-Liste“ aufgeführt sind, welche in Übereinstimmung mit Abschnitt I und III der Grundsätze in Anhang II vom US-Handelsministerium geführt und der Öffentlichkeit zugänglich gemacht wird.

Artikel 2

Die Anwendung anderer Bestimmungen der Richtlinie 95/46/EG als Artikel 25 Absatz 1, die sich auf die Verarbeitung personenbezogener Daten in den Mitgliedstaaten beziehen, insbesondere Artikel 4, bleibt von diesem Beschluss unberührt.

Artikel 3

Wenn die zuständigen Behörden in den Mitgliedstaaten ihre Befugnisse gemäß Artikel 28 Absatz 3 der Richtlinie 95/46/EG ausüben und die Datenübertragungen an eine im Einklang mit Abschnitt I und III der Grundsätze in Anhang II in der Datenschutzschild-Liste aufgeführte Organisation in den Vereinigten Staaten aussetzen oder endgültig verbieten, um Privatpersonen im Hinblick auf die Verarbeitung ihrer personenbezogenen Daten zu schützen, setzt der betreffende Mitgliedstaat die Kommission unverzüglich davon in Kenntnis.

Artikel 4

(1) Die Kommission überwacht kontinuierlich die Funktionsweise des EU-US-Datenschutzschilds, um zu überprüfen, ob die Vereinigten Staaten weiterhin ein angemessenes Schutzniveau für personenbezogene Daten gewährleisten, die in diesem Rahmen aus der Europäischen Union an Organisationen in den Vereinigten Staaten übermittelt werden.

(2) Die Mitgliedstaaten und die Kommission unterrichten sich gegenseitig über Fälle, in denen es Anhaltspunkte gibt, dass die staatlichen Einrichtungen in den Vereinigten Staaten, die zur Durchsetzung der in Anhang II dargelegten Grundsätze gesetzlich befugt sind, nicht für wirksame Verfahren zur Aufdeckung und Kontrolle sorgen, mit denen Verstöße gegen die Grundsätze ermittelt und geahndet werden können.

(3) Die Mitgliedstaaten und die Kommission unterrichten sich gegenseitig über Anhaltspunkte dafür, dass die Eingriffe der US-Behörden, die für die nationale Sicherheit, die Strafverfolgung oder andere im öffentlichen Interesse liegende Aufgaben zuständig sind, in das Recht von Privatpersonen auf den Schutz ihrer personenbezogenen Daten über das

absolut notwendige Maß hinausgehen und/oder dass kein wirksamer Rechtsschutz vor derartigen Eingriffen besteht.

(4) Binnen eines Jahres, nachdem die Mitgliedstaaten von diesem Beschluss in Kenntnis gesetzt wurden, und anschließend alljährlich überprüft die Kommission die Feststellung in Artikel 1 Absatz 1 anhand aller verfügbaren Informationen, einschließlich der Informationen, die ihr im Zuge der in den Anhängen I, II und VI erwähnten gemeinsamen jährlichen Überprüfung zugegangen sind.

(5) Die Kommission erstattet dem gemäß Artikel 31 der Richtlinie 95/46 eingerichteten Ausschuss über alle sachdienlichen Erkenntnisse Bericht.

(6) Die Kommission legt gemäß dem in Artikel 31 Absatz 2 der Richtlinie 95/46/EG angeführten Verfahren Entwürfe von Maßnahmen zur Aussetzung, Änderung oder Aufhebung des vorliegenden Beschlusses oder zur Änderung seines Anwendungsbereichs vor, wenn es unter anderem Anhaltspunkte dafür gibt,

- dass sich die US-Behörden nicht an die Erklärungen und Zusagen halten, die in den diesem Beschluss beigefügten Schriftstücken enthalten sind und unter anderem die Bedingungen und Einschränkungen betreffen, denen der aus Gründen der Strafverfolgung, der nationalen Sicherheit oder des öffentlichen Interesses erfolgende Zugriff amerikanischer Behörden auf personenbezogene Daten, die im Rahmen des Datenschutzschilds übertragen werden, unterliegt;
- dass Beschwerden von betroffenen Personen in der EU systematisch nicht wirksam nachgegangen wird;
- dass die Ombudsperson des Datenschutzschilds systematisch nicht zeitnah und angemessen auf Anfragen von betroffenen Personen in der EU so antwortet, wie es Anhang III Abschnitt 4 Buchstabe e erfordert.

Die Kommission legt ebenfalls Entwürfe derartiger Maßnahmen vor, wenn die mangelnde Zusammenarbeit der Einrichtungen, die für ein ordnungsgemäßes Funktionieren des EU-US-Datenschutzschilds sorgen sollen, die Kommission daran hindert festzustellen, ob die Feststellung in Artikel 1 Absatz 1 davon in Frage gestellt wird.

Artikel 5

Die Mitgliedstaaten ergreifen alle für die Umsetzung des vorliegenden Beschlusses erforderlichen Maßnahmen.

Artikel 6

Dieser Beschluss ist an die Mitgliedstaaten gerichtet.

Geschehen zu Brüssel am 12.7.2016

Für die Kommission
Věra JOUROVÁ
Mitglied der Kommission

BEGLAUBIGTE AUSFERTIGUNG
Für den Generalsekretär

Jordi AYET PUIGARNAU
Direktor der Kanzlei
EUROPÄISCHE KOMMISSION