Amtsblatt der Europäischen Union

L 207

Ausgabe in deutscher Sprache

Rechtsvorschriften

59. Jahrgang

1. August 2016

Inhalt

[1] Text von Bedeutung für den EWR

DE

Bei Rechtsakten, deren Titel in magerer Schrift gedruckt sind, handelt es sich um Rechtsakte der laufenden Verwaltung im Bereich der Agrarpolitik, die normalerweise nur eine begrenzte Geltungsdauer haben.

Rechtsakte, deren Titel in fetter Schrift gedruckt sind und denen ein Sternchen vorangestellt ist, sind sonstige Rechtsakte.

II

(Rechtsakte ohne Gesetzescharakter)

BESCHLÜSSE

DURCHFÜHRUNGSBESCHLUSS (EU) 2016/1250 DER KOMMISSION

vom 12. Juli 2016

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

(Bekannt gegeben unter Aktenzeichen C(2016) 4176)

(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 — 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.

([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. Mai 2016.
([3]) Rs. C-362/14, 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.

(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, die Verfügbarkeit erschwinglicher Streitbeilegungsmechanismen und die Schaffung der Voraussetzungen dafür, dass von der in der Entscheidung 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 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/EG 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]).

([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. November 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. November 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. Mai 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. November 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.

([10]) Siehe Fußnote 3.

([11]) Schrems, Rn. 97.

([12]) Schrems, Rn. 73-74.

([13]) Schrems, Rn. 88-89.

(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 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]).

([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).

(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 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 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.

([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-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, sodass 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.

(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.

(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.

([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.

([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.

(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 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 Vertrags (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]) 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

([25]) Siehe auch Zusatzgrundsatz „Beschwerdeverfahren und Durchsetzung" (Anhang II, Abschnitt III.11).
([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 verantwortlich ist, durch Ausübung ihres Weisungsrechts für den im Rahmen der Grundsätze garantierten Rechtsschutz zu sorgen.

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.

(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 den Anhängen 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

([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.

([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.

denen das Handelsministerium Organisationen wegen fortgesetzter Verstöße gegen die Grundsätze von der Liste gestrichen hat, stellt es 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*

(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

([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.

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]).

([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

(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 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]), sodass 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 60 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 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]).

([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.
([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, S. 6.
([47]) Ebenda.

(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.

(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]).

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

([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.

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

([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.

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 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.

([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.

([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. Dezember 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, 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]).

([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. Januar 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.
([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. Oktober 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. April 2014.
([67]) Siehe Signal Intelligence Reform, 2015 Anniversary Report. Siehe auch Erklärungen des ODNI (Anhang VI), S. 6, 8-9, 11.

(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 ([72]).

(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, 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" ([73]). 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 ([74]). Diese zulässigen Zielsetzungen umfassen Maßnahmen zur

([68]) Siehe Fußnote 63.

([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 Fußnote 63.

([73]) 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. April 2016), S. 38 mit Nr. 47.

([74]) Siehe § 2 der PPD-28.

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" ([75]).

(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 ([76]).

(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 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 ([77]).

(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 ([78]), 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 ([79]). Der FISA sieht verschiedene Rechtsgrundlagen vor, die herangezogen werden können, um die im

([75]) Erklärungen des ODNI (Anhang VI), S. 4. Siehe auch Intelligence Community Directive 203.
([76]) 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).
([77]) Siehe Schrems, Rn. 93.
([78]) 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).
([79]) 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".

Rahmen des EU-US-Datenschutzschilds von betroffenen Personen in der EU übermittelten personenbezogenen Daten zu erheben (und anschließend zu verarbeiten). Abgesehen von § 104 FISA ([80]), der die herkömmliche individuelle elektronische Überwachung zum Gegenstand hat, und § 402 FISA ([81]), der den Einsatz von Geräten 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 ([82]).

(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) ([83]) und durch die Verwendung von NSL und verlangt stattdessen die Anwendung konkreter „Suchkriterien" ([84]).

(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 ([85]). 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 ([86]). Wie das Privacy and Civil

([80]) 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.

([81]) 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.

([82]) 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.

([83]) 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. Januar 2016, S. 4-6.

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

([85]) Siehe Fußnote 81.

([86]) 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. April 2014.

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" ([87]). Aufgrund einer „Auslaufklausel" muss § 702 des FISA im Jahr 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" ([88]). 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 ([89]).

(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 ([90]).

(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 getroffen werden, „die vernünftiger Weise so konzipiert sind, dass sie deren Weitergabe und Speicherung auf ein Mindestmaß beschränken" ([91]).

([87]) 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. April 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.

([88]) 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".

([89]) Siehe Statistical Transparency Report Regarding Use of National Security Authorities, 22. April 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. Oktober 2011), n. 21 (abrufbar unter: http://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf).

([90]) 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.

([91]) 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.

(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" ([92]). In dieser Hinsicht werden Nicht-US-Bürger auf der Grundlage von Verfahren, die der Justizminister gebilligt hat, ebenso behandelt wie US-Bürger ([93]).

(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 ([94]). 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 ([95]).

(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" ([96]).

(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 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 ([97]) — und möglichst zielgenau ausgeführt werden. Insbesondere wird die Sammelerhebung nur in

([92]) Erklärungen des ODNI (Anhang VI), S. 4.
([93]) Siehe § 4(a)(i) der PPD-28 in Verbindung mit § 2.3 der E.O. 12333.
([94]) § 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. April 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. Januar 2016.
([95]) 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. April 2014; Transparency Report: The USA Freedom Act Business Records FISA Implementation, 15. Januar 2016. Siehe auch NSA's Civil Liberties and Privacy Protections for Targeted SIGINT Activities under Executive Order 12333, 7. Oktober 2014.
([96]) Erklärungen des ODNI (Anhang VI), S. 7 (mit Bezugnahme auf die Intelligence Community Directive (ICD) 203).
([97]) 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. Juni 2006, Antrag Nr. 54934/00, Rnn. 105-118 (zur „strategischen Überwachung").

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" ([98]) 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." ([99]) 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" ([100]) 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

(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 ([101]).

([98]) Schrems, Rn. 91 und weitere Bezugnahmen.
([99]) Schrems, Rn. 93.
([100]) Vgl. Schrems, Rn. 94.
([101]) 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. Januar 2015, Sec. 8.1, 8.6(c).

(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 ([102]).

(96) Wie von der US-Regierung erläutert ([103]), sind *Bürgerrechts- oder Datenschutzbeauftragte* mit Überwachungsfunktionen in verschiedenen Abteilungen mit nachrichtendienstlichen Aufgaben und in Nachrichtendiensten tätig ([104]). 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) ([105]). 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 ([106]). Nach Einschätzung der nationalen Datenschutzbehörden ist die interne Überwachung durch Bürgerrechts- und Datenschutzbeauftragte als „relativ robust" anzusehen, auch wenn diese nicht das erforderliche Maß an Unabhängigkeit aufweisen ([107]).

(97) Darüber hinaus hat jeder Nachrichtendienst seinen eigenen *Generalinspekteur*, der unter anderem für die Kontrolle der Auslandsaufklärung zuständig ist ([108]). 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 ([109]). Generalinspekteure sind rechtlich unabhängige ([110]) 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 ([111]). Sie haben Zugriff auf alle Unterlagen, Berichte, Audits, Überprüfungen, Dokumente, Schriftstücke, Empfehlungen oder sonstiges einschlägiges Material, dessen

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

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

([104]) 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.

([105]) 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).

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

([107]) Article 29 Data Protection Working Party, Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision (angenommen am 13. April 2016), S. 41.

([108]) Erklärungen des ODNI (Anhang VI), S. 7. Siehe beispielsweise NSA, PPD-28 Section 4 Procedures, 12. Januar 2015, Sec. 8.1; CIA, Signals Intelligence Activities, S. 7 (Responsibilities).

([109]) 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.

([110]) 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. April 2016), S. 40.

([111]) Siehe Erklärungen des ODNI (Anhang VI), S. 7. Siehe auch Inspector General Act of 1978, as amended, Pub. L. 113-126 vom 7. Juli 2014.

Herausgabe sie notfalls unter Strafandrohung anordnen können, und sind zur Beweisaufnahme berechtigt ([112]). 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 ([113]).

(98) Darüber hinaus wurde das *Privacy and Civil Liberties Oversight Board*, eine parteiübergreifende unabhängige Behörde ([114]) der Exekutive, deren fünf Mitglieder ([115]) vom Präsidenten mit Zustimmung des Senats für eine Amtszeit von sechs Jahren 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 ([116]), kann ihnen gegenüber Empfehlungen abgeben und erstattet regelmäßig den Ausschüssen des Kongresses und dem Präsidenten Bericht ([117]). 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 ([118]). 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 ([119]).

(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 ([120]). Überdies sind nach E.O. 12333 alle Nachrichtendienste verpflichtet, dem Intelligence Oversight Board Rechtsverstöße zu melden ([121]). Diese Vorgehensweise

([112]) Siehe Inspector General Act of 1978, § 6.
([113]) 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. Oktober 2010 informiert der Generalinspekteur für die Intelligence Community den DNI sowie den Kongress über notwendige Korrekturmaßnahmen und deren Fortgang.
([114]) 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. April 2016), S. 42.
([115]) Außerdem hat das PCLOB noch 20 weitere Mitarbeiter. Siehe https://www.pclob.gov/about-us/staff.html.
([116]) 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.
([117]) Siehe 42 U.S.C. § 2000ee. Siehe auch Ombudsmechanismus (Anhang III), Punk 6(b)(iv).
([118]) 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.
([119]) Ebenda auf S. 8. Siehe auch Erklärungen des ODNI (Anhang VI), S. 9.
([120]) 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. Januar 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).
([121]) Siehe E.O. 12333, Sec. 1.6(c).

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 Kenntnis zu setzen, die mit dem Schutz der Quellen und Methoden und der US-Mitarbeiter vereinbar ist ([122]).

(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." ([123]) 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." ([124]) Die Mitglieder dieser Ausschüsse haben Zugriff auf Informationen, die der Geheimhaltung unterliegen, sowie auf nachrichtendienstliche Methoden und Programme ([125]).

(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 ([126]). 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 ([127]), 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 ([128]). 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 Nicht-US-Bürger offenlegen ([129]). 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

([122]) PPD-28, Sec. 4(a)(iv).
([123]) 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.
([124]) Siehe § 501(b) (50 U.S.C. § 413(b)).
([125]) Vgl. § 501(d) (50 U.S.C. § 413(d)).
([126]) Siehe 50 U.S.C. §§ 1808, 1846, 1862, 1871, 1881f.
([127]) Siehe 50 U.S.C. § 1881f.
([128]) Siehe 50 U.S.C. § 1881a(l)(1).
([129]) 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."

Empfängern von FISA-Anordnungen und -Zertifizierungen sowie NSL-Auskunftsersuchen gestattet wird, unter bestimmten Voraussetzungen Transparenzberichte vorzulegen) ([130]).

(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) ([131]), einem unabhängigen Gericht ([132]), verlangt werden, dessen Entscheidung vor dem Foreign Intelligence Court of Review (FISCR) ([133]) und in letzter Instanz vor dem Obersten Gericht der Vereinigten Staaten angefochten werden kann ([134]). 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 ([135]). In der Endfassung muss der Antrag dann vom Justizminister, seinem ersten Stellvertreter oder dem Stellvertreter für nationale Sicherheit gebilligt werden ([136]). Das Justizministerium legt den Antrag anschließend dem FISC vor, das ihn prüft und eine vorläufige Entscheidung über das weitere Vorgehen trifft ([137]). Findet eine Anhörung statt, ist das FISC befugt, Beweismittel zu erheben, wozu auch die Einholung von Gutachten gehören kann ([138]).

(106) Das FISC (und das FISCR) werden von einer ständigen Expertengruppe unterstützt, die aus fünf Sachverständigen für nationale Sicherheit und Bürgerrechte besteht ([139]). 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 ([140]). 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 ([141]).

([130]) USA FREEDOM Act, § 602(a), 603(a).

([131]) 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.

([132]) 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.

([133]) 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)).

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

([135]) 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.

([136]) 50 U.S.C. §§ 1804 (a), 1801 (g).

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

([138]) PCLOB, Sec. 215 Report, S. 179, Nr. 619.

([139]) 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.

([140]) 50 U.S.C. § 1803 (i)(2)(A). Nach Informationen des ODNI sind solche Ernennungen bereits erfolgt. Siehe Signals Intelligence Reform, 2016 Progress Report.

([141]) 50 U.S.C. § 1803 (i)(2)(B).

(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 ([142]), 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 ([143]).

(109) Hingegen autorisiert das FISC nach § 702 des FISA ([144]) 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 ([145]). 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 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 ([146]), werden Selektoren, die Kommunikationseinrichtungen (wie E-Mail-Adressen) identifizieren, „aktiviert" (d. h. erstellt und angewandt) ([147]). 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 ([148]). Das FISC beurteilt nicht — anhand eines hinreichenden Verdachts oder sonstigen Kriteriums —, ob die Personen vorschriftsgemäß als Zielpersonen für die Beschaffung von Auslandsaufklärungsdaten ausgewählt wurden ([149]), sondern überprüft die Einhaltung der Bestimmung, dass „ein wesentlicher Zweck der Datenerhebung darin besteht, Auslandsaufklärungsdaten zu erlangen" ([150]). 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 ([151]). Auch müssen die Zertifizierungen Verfahren zur zielgenauen Erfassung und Minimierung vorsehen ([152]). Der Justizminister und der Director of National

([142]) 50 U.S.C. § 1861
([143]) 50 U.S.C. § 1861 (b).
([144]) 50 U.S.C. § 1881.
([145]) 50 U.S.C. § 1881a (a).
([146]) PCLOB, Sec. 702 Report, S. 46.
([147]) 50 U.S.C. § 1881a (h).
([148]) 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.
([149]) PCLOB, Sec. 702 Report, S. 27.
([150]) 50 U.S.C. § 1881a.
([151]) „Liberty and Security in a Changing World", Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies, 12. Dezember 2013, S. 152.
([152]) 50 U.S.C.1881a (i).

Intelligence überprüfen die Einhaltung der Grundsätze, und die Behörden sind verpflichtet, jegliche Verstöße dagegen dem FISC ([153]) (sowie dem Kongress und dem Intelligence Oversight Board des Präsidenten) zu melden, der daraufhin die Genehmigung abändern kann ([154]).

(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 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 ([155]). 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 ([156]).

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) ([157]).

(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 ([158]) 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 ([159]); US-Regierungsbeamte in persönlicher Eigenschaft (nach dem Grundsatz der Rechtsscheinhaftung) auf Schadenersatz zu verklagen ([160]); 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 ([161]).

(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

([153]) 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.

([154]) 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. April 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.

([155]) PCLOB, Recommendations Assessment Report, 29. Januar 2015, S. 20.

([156]) PCLOB, Recommendations Assessment Report, 29. Januar 2015, S. 16.

([157]) 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.

([158]) Siehe Erklärungen des ODNI (Anhang VI), S. 16.

([159]) 18 U.S.C. § 2712.

([160]) 50 U.S.C. § 1810.

([161]) 50 U.S.C. § 1806.

Zugangs zu, oder der Verarbeitung personenbezogener Daten, auch für vorgebliche Ziele der nationalen Sicherheit, vorzugehen (Computer Fraud and Abuse Act ([162]); Electronic Communications Privacy Act ([163]); und Right to Financial Privacy Act ([164])). All diese Klagegründe betreffen spezifische Daten, Zielpersonen und/oder Arten des Zugriffs (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) ([165]). 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" ([166]).

(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 ([167]). 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 ([168]). 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 ([169]), denn Klagen von Einzelpersonen (auch US-Bürgern) werden abgewiesen, wenn diese ihre „Klagebefugnis" nicht nachweisen können ([170]), was den Zugang zu den ordentlichen Gerichten einschränkt ([171]).

(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.

([162]) 18 U.S.C. § 1030.
([163]) 18 U.S.C. §§ 2701-2712.
([164]) 12 U.S.C. § 3417.
([165]) Erklärungen des ODNI (Anhang VI), S. 17.
([166]) 5 U.S.C. § 706(2)(A).
([167]) 5 U.S.C. § 552. Ähnliche Rechtsvorschriften existieren auf der Ebene der einzelnen Bundesstaaten.
([168]) 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).
([169]) 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.
([170]) Dieses Kriterium ergibt sich aus Artikel III der amerikanischen Verfassung, wonach sich die richterliche Gewalt nur auf reale Fälle und Streitigkeiten erstreckt.
([171]) 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.

(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 ([172]). 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 zuständig sind, damit sie diese einer zentralen Stelle der EU vorlegen, die sie an die Ombudsperson des Datenschutzschilds weiterleitet ([173]). 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 ([174]). Auch kann die Ombudsperson des Datenschutzschilds Angelegenheiten an das PCLOB zur Prüfung weiterleiten ([175]). 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,

([172]) 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.

([173]) 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 „zugrunde liegenden 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.

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

([175]) 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".

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 ([176]). Dies ist von erheblicher Bedeutung, da die Ombudsperson „bestätigen" muss, i) dass 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 ([177]). 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." ([178]) 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 Regierung der USA (über das Justizministerium) Zusicherungen zu den dafür geltenden Einschränkungen und Garantien gemacht, die nach Einschätzung der Kommission ein hinreichendes Schutzniveau gewährleisten.

([176]) Siehe Roman Zakharov/Russland, Urteil vom 4. Dezember 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".)

([177]) Siehe Kennedy/Vereinigtes Königreich, Urteil vom 18. Mai 2010, Antrag Nr. 26839/05, Rn. 167.

([178]) 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.

(126) Nach diesen Informationen erfordern gemäß viertem Zusatzartikel zur Verfassung der USA ([179]) Durchsuchungen und Beschlagnahmen, die von Strafverfolgungsbehörden vorgenommen werden, grundsätzlich ([180]) eine gerichtliche Anordnung bei Vorliegen eines „hinreichenden Tatverdachts". In den wenigen Sonder- und Ausnahmefällen, in denen diese Anforderung nicht gilt ([181]), unterliegt die Strafverfolgung einer Prüfung der „Zumutbarkeit" ([182]). 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." ([183]) Ganz allgemein garantiert der vierte Zusatzartikel den Schutz der Privatsphäre und der Menschenwürde und bietet Schutz vor willkürlichen Eingriffen von Staatsbeamten ([184]). 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 ([185]).

(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) ([186]). 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 Ermittlungsmethoden anzuwenden und die Auswirkungen auf die Privatsphäre und die Bürgerrechte zu berücksichtigen) ([187]). 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) ([188]).

(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 ([189]), 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 ([190]).

([179]) 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.

([180]) 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).

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

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

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

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

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

([186]) 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."

([187]) Erklärungen des DOJ (Anhang VII), S. 4 mit weiteren Verweisen.

([188]) Erklärungen des DOJ (Anhang VII), Nr. 2.

([189]) 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.

([190]) 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.

(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 ([191]) kann „eine Person, die durch Handlungen einer Behörde einen Schaden oder Nachteil erleidet", eine gerichtliche Nachprüfung beantragen ([192]). 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" ([193]).

(132) Konkreter ist in diesem Zusammenhang Titel II des Electronic Communications Privacy Act ([194]), 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. ([195]) 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 ([196]).

([191]) 5 U.S.C. § 702.

([192]) Im Allgemeinen unterliegen nur „endgültige" Maßnahmen einer Behörde, nicht aber „vorbereitende, verfahrensmäßige oder vorläufige" Maßnahmen der gerichtlichen Nachprüfung. Siehe 5 U.S.C. § 704.

([193]) 5 U.S.C. § 706(2)(A).

([194]) 18 U.S.C. §§ 2701-2712.

([195]) 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.

([196]) 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)).

(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 ([197]), der Computer Fraud and Abuse Act ([198]), der Federal Torts Claim Act ([199]), der Right to Financial Privacy Act ([200]) und der Fair Credit Reporting Act ([201]).

(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 ([202]) 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 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.

([197]) 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).

([198]) 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.

([199]) 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.

([200]) 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.

([201]) 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.

([202]) 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.

(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 ([203]).

(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, sodass 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 ([204]). 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 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 ([205]).

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 ([206]).

(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.

([203]) Schrems, Rn. 40ff., 101-103.
([204]) Schrems, Rn. 51, 52 und 62.
([205]) Schrems, Rn. 65.
([206]) Schrems, Rn. 76.

(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 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 ([207]). 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 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

([207]) 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.

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 ([208]), die bei der Ausarbeitung des vorliegenden Beschlusses berücksichtigt wurde.

(154) Das Europäische Parlament hat eine Entschließung zur transatlantischen Datenübermittlung verabschiedet ([209]).

(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. —

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.

([208]) Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision, angenommen am 13. April 2016.
([209]) Entschließung des Europäischen Parlaments vom 26. Mai 2016 zur transatlantischen Datenübermittlung (2016/2727(RSP)).

(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/EG 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.

Brüssel, den 12. Juli 2016

Für die Kommission
Věra JOUROVÁ
Mitglied der Kommission

ANHANG I

Schreiben von US-Handelsministerin Penny Pritzker

7. Juli 2016

Frau Věra Jourová
Kommissionsmitglied für Justiz, Verbraucherschutz und Gleichstellungsfragen
Europäische Kommission
Rue de la Loi/Westraat 200
1049 Brüssel
Belgien

Sehr geehrte Frau Jourová,

es ist mir eine große Freude, Ihnen im Namen der Vereinigten Staaten mit diesem Schreiben eine Materialsammlung zum EU-US-Datenschutzschild zukommen zu lassen, die das Ergebnis zweijähriger produktiver Gespräche zwischen den Teams unserer beiden Seiten ist. In Kombination mit anderen öffentlichen Quellen, die der Kommission zur Verfügung stehen, bietet diese Sammlung der Kommission eine fundierte Grundlage, um eine aktuelle Angemessenheitsfeststellung vorzunehmen ([1]).

Meines Erachtens können wir auf beiden Seiten stolz auf die erzielten Verbesserungen der Regelung sein. Der Datenschutzschild stützt sich auf Grundsätze, über die beiderseits des Atlantiks ein breiter Konsens besteht und denen wir zu mehr Wirksamkeit verholfen haben. Dank unserer Zusammenarbeit bietet sich uns eine wirkliche Gelegenheit, weltweit zur Stärkung des Datenschutzes beizutragen.

Die Materialsammlung zum Datenschutzschild umfasst die Datenschutzgrundsätze sowie ein in Anlage 1 beigefügtes Schreiben der für die Programmverwaltung zuständigen International Trade Administration (ITA) des US-Handelsministeriums, in dem die Verpflichtungen erläutert werden, die unser Ministerium mit Blick auf eine wirksame Umsetzung des Datenschutzschildes eingegangen ist. Die Sammlung umfasst ferner Anlage 2 mit den Zusagen des Ministeriums zum neuen Schiedssystem, das im Rahmen des Datenschutzschildes zur Verfügung steht.

Meine Mitarbeiter sind angewiesen, alle notwendigen Ressourcen unverzüglich und vollständig auf die Realisierung des Datenschutzschildes zu konzentrieren und eine fristgemäße Umsetzung der in Anlage 1 und Anlage 2 aufgeführten Zusagen sicherzustellen.

Ferner beinhaltet die Sammlung zum Datenschutzschild weitere Dokumente anderer US-Behörden, darunter:

— ein Schreiben der Federal Trade Commission (FTC) zur internen Durchsetzung des Datenschutzschilds;

— ein Schreiben des Verkehrsministeriums zur internen Durchsetzung des Datenschutzschilds;

— zwei Schreiben des Amts des Director of National Intelligence (ODNI) zu den für die nationalen Sicherheitsbehörden in den USA geltenden Garantien und Beschränkungen;

— ein Schreiben des Außenministeriums mit einer Absichtserklärung, in der die Zusage des Außenministeriums zur Einsetzung einer neuen Ombudsstelle für den Datenschutzschild erläutert wird, die für Anfragen zu Vorgängen im Zusammenhang mit der signalerfassenden Aufklärung in den USA zuständig ist und

— ein Schreiben des Justizministeriums zu den Garantien und Beschränkungen der Abfrage von Daten durch die US-Regierung aus Gründen der Strafverfolgung und des öffentlichen Interesses.

Seien Sie versichert, dass die USA diese Zusagen sehr ernst nimmt.

([1]) Unter der Voraussetzung, dass der Beschluss über die Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes für Island, Liechtenstein und Norwegen gilt, wird die Materialsammlung zum Datenschutzschild sowohl die Europäische Union als auch diese drei Länder abdecken.

Innerhalb von 30 Tagen nach der endgültigen Annahme der Angemessenheitsfeststellung wird das vollständige Paket zum Datenschutzschild zur Veröffentlichung an das *Bundesregister* übermittelt.

Wir freuen uns auf unsere Zusammenarbeit bei der Umsetzung des Datenschutzschildes und der Einleitung der nächsten Phase in diesem Prozess.

Hochachtungsvoll

Penny Pritzker

Anlage 1

Schreiben des geschäftsführenden Staatssekretärs für internationalen Handel Ken Hyatt

Frau Věra Jourová
Kommissionsmitglied für Justiz, Verbraucherschutz und Gleichstellungsfragen
Europäische Kommission
Rue de la Loi/Westraat 200
1049 Brüssel
Belgien

Sehr geehrte Frau Jourová,

es ist mir eine große Freude, im Namen der International Trade Administration zu erläutern, welche Verbesserungen für den Schutz personenbezogener Daten mit den Rahmengrundsätzen des EU-US-Datenschutzschilds („Datenschutzschild" oder „Regelung") verbunden sind und welche Verpflichtungen das Handelsministerium („Ministerium") eingegangen ist, um eine wirksame Funktionsweise des Datenschutzschilds zu gewährleisten. Mit dem Abschluss dieser historischen Regelung sind wichtige Fortschritte für den Datenschutz und für Unternehmen auf beiden Seiten des Atlantiks verknüpft. EU-Bürgern bietet sie die Gewissheit, dass ihre Daten geschützt werden und sie bei etwaigen Bedenken über Rechtsmittel verfügen. Zudem trägt die damit verbundene Sicherheit zum Wachstum der transatlantischen Wirtschaft bei, weil sie ein Garant dafür ist, dass Tausende von Unternehmen in Europa und den USA auch weiterhin grenzüberschreitend investieren und Geschäfte abschließen können. Das Datenschutzschild ist das Ergebnis unserer zweijährigen umfassenden Bemühungen und Zusammenarbeit mit Ihnen, unseren Kolleginnen und Kollegen in der Europäischen Kommission („Kommission"). Wir freuen uns, unsere Kooperation mit der Kommission im Sinne einer ordnungsgemäßen Funktionsweise des Datenschutzschildes fortzusetzen.

Gemeinsam mit der Kommission haben wir uns darum bemüht, den Datenschutzschild so zu gestalten, dass in den USA niedergelassene Organisationen die Möglichkeit haben, die Angemessenheitsanforderungen an den Datenschutz nach dem EU-Recht einzuhalten. Mit dem neuen Rahmen sind zahlreiche grundlegende Vorteile sowohl für Privatpersonen als auch für Unternehmen verbunden. Erstens beinhaltet es einen umfassenden Katalog von Schutzbestimmungen für die Daten von EU-Bürgern. US-Organisationen sind verpflichtet, an der Entwicklung einer einheitlichen Datenschutzstrategie mitzuwirken, sich öffentlich zur Einhaltung der Grundsätze des Datenschutzschildes zu verpflichten, damit diese Verpflichtung nach US-Recht durchsetzbar wird, die Einhaltung beim Ministerium jährlich neu zu zertifizieren, EU-Bürgern eine kostenfreie unabhängige Streitbeilegung zu ermöglichen und sich der Zuständigkeit der Federal Trade Commission („FTC"), des Verkehrsministeriums (Department of Transportation, „DOT") oder einer anderen Durchsetzungsstelle zu unterstellen. Zweitens bietet der Datenschutzschild Tausenden von Unternehmen in den USA sowie Tochtergesellschaften europäischer Unternehmen in den USA die Möglichkeit, personenbezogene Daten aus der Europäischen Union zu empfangen, was den Datenfluss im Sinne des transatlantischen Handels erleichtert. Bereits heute weist der transatlantische Geschäftsverkehr weltweit den größten Umfang auf, denn auf ihn entfallen die Hälfte der weltweiten Wirtschaftsleistung und ein Handelsvolumen im Bereich Waren und Dienstleistungen von nahezu einer Billion Dollar, was Millionen von Arbeitsplätzen diesseits und jenseits des Atlantiks sichert. Unternehmen, die den transatlantischen Datenverkehr nutzen, stammen aus allen Industriezweigen und umfassen sowohl große Vertreter aus der Gruppe der umsatzstärksten Unternehmen (Fortune Global 500) als auch viele kleine und mittlere Unternehmen (KMU). Dank des transatlantischen Datenverkehrs können US-Organisationen Daten verarbeiten, die erforderlich sind, um EU-Bürgern Waren, Dienstleistungen und Beschäftigungsmöglichkeiten anzubieten. Der Datenschutzschild orientiert sich an gemeinsamen Datenschutzgrundsätzen, mit denen die Unterschiede zwischen unseren beiden Rechtssystemen überbrückt werden, und trägt zur Förderung des Handels und der wirtschaftlichen Ziele sowohl in Europa als auch in den USA bei.

Die Entscheidung eines Unternehmens, sich mittels einer Selbstzertifizierung für diese neue Regelung zu registrieren, ist zwar freiwillig, sobald sich ein Unternehmen jedoch öffentlich zur Einhaltung des Datenschutzschildes verpflichtet hat, ist diese Zusage nach US-Recht entweder durch die Federal Trade Commission oder das Verkehrsministerium durchsetzbar, je nachdem welche Behörde die Zuständigkeit für die jeweilige Organisation übernimmt.

Positive Effekte der Grundsätze des Datenschutzschilds

Mit dem Datenschutzschild wird der Datenschutz wie folgt gestärkt:

— Bereitstellung zusätzlicher Informationen für Privatpersonen gemäß dem Grundsatz der Informationspflicht, darunter eine Erklärung über die Beteiligung einer Organisation am Datenschutzschild, ein Hinweis auf die Rechte des Einzelnen auf den Zugang zu personenbezogenen Daten und die Benennung der zuständigen unabhängigen Beschwerdestelle;

— Ausweitung des Schutzes personenbezogener Daten, die von einer dem Datenschutzschild angehörenden Organisation an für die Datenverarbeitung verantwortliche Dritte weitergegeben werden, indem die Parteien zum Abschluss eines Vertrags verpflichtet werden, der vorsieht, dass derartige Daten ausschließlich für begrenzte und genau bezeichnete Zwecke verarbeitet werden können, zu denen die Privatperson ihre Zustimmung erteilt hat, und dass der Datenempfänger dasselbe Schutzniveau gewährleistet, das auch in den Grundsätzen enthalten ist;

— Verbesserung des Schutzes personenbezogener Daten, die von einer dem Datenschutzschild angehörenden Organisation an einen Dritten weitergegeben werden, auch durch die Verpflichtung einer dem Datenschutzschild angehörenden Organisation, angemessene und geeignete Vorkehrungen zu treffen, um sicherzustellen, dass dieser Dritte die personenbezogenen Angaben tatsächlich auf eine Weise verarbeitet, die mit den Verpflichtungen der Organisation im Rahmen der Grundsätze vereinbar ist; nach Kenntnisnahme angemessene und geeignete Maßnahmen ergreift, um eine unrechtmäßige Verarbeitung zu unterbinden und zu beheben und dem Ministerium auf Anfrage eine Zusammenfassung oder eine aussagekräftige Kopie der in ihrem Vertrag mit diesem Dritten enthaltenen einschlägigen Datenschutzbestimmungen zur Verfügung zu stellen;

— Gewährleistung der Verantwortung einer dem Datenschutzschild angehörenden Organisation für die Verarbeitung der personenbezogenen Daten, die ihr auf Grundlage des Datenschutzschilds übermittelt werden und von ihr anschließend an einen Dritten weitergegeben werden, der in ihrem Auftrag tätig ist, sowie der fortgesetzten Haftung gemäß der Grundsätze für den Fall, dass der Auftragnehmer diese personenbezogenen Informationen auf eine Art und Weise verwendet, die nicht in Einklang mit den Grundsätzen steht, es sei denn, sie kann nachweisen, dass sie für den Umstand, durch den der Schaden eingetreten ist, nicht verantwortlich ist;

— Klarstellung, dass dem Datenschutzschild angehörende Organisationen personenbezogene Informationen auf diejenigen Daten beschränken müssen, die für den beabsichtigten Verwendungszweck erheblich sind;

— Anforderung an eine Organisation, jährlich beim Ministerium eine Zertifizierung ihrer Verpflichtung zur Einhaltung der Grundsätze für alle Informationen vorzunehmen, die während ihrer Teilnahme am Datenschutzschild bei ihr eingegangen sind, nachdem sie den Datenschutzschild verlassen hat und sich für die Speicherung dieser Daten entscheidet;

— Erfordernis der Bereitstellung von für den Einzelnen kostenfreien unabhängigen Beschwerdestellen;

— Anforderung an Organisationen und ihre jeweiligen unabhängigen Beschwerdestellen, rasch auf Anfragen und Auskunftsbegehren des Handelsministeriums zu reagieren, die mit dem Datenschutzschild im Zusammenhang stehen;

— Anforderung an Organisationen, auf Beschwerden im Zusammenhang mit der Einhaltung der Grundsätze, die von den Behörden der EU-Mitgliedstaaten an das Ministerium übermittelt wurden, mit der gebotenen Eile zu reagieren und

— Anforderung an eine dem Datenschutzschild angehörende Organisation, jene Teile eines der FTC vorgelegten Compliance- oder Sachstandsberichts, die den Datenschutzschild betreffen, öffentlich zu machen, wenn Anordnungen der FTC oder Gerichtsbeschlüsse wegen Nichteinhaltung gegen sie ergehen.

Verwaltung und Überwachung des Datenschutzschild-Programms durch das Handelsministerium

Das Ministerium bekräftigt seine Zusage, ein amtliches Verzeichnis der Organisationen, die sich gegenüber dem Ministerium selbst zertifiziert und eine Befolgung der Grundsätze zugesichert haben (die „Datenschutzschild-Liste“) zu führen und der Öffentlichkeit zugänglich zu machen. Diese Liste wird durch das Ministerium aktualisiert, indem Organisationen gestrichen werden, die ihre Verpflichtung freiwillig zurückziehen, die jährliche Zertifizierung gemäß den geltenden Verfahren des Ministeriums versäumen oder offensichtlich fortgesetzt die Grundsätze missachten. Außerdem führt es ein amtliches Verzeichnis der Organisationen, die sich zu einem früheren Zeitpunkt gegenüber dem US-Handelsministerium selbst zertifiziert haben, aber von der Datenschutzschild-Liste gestrichen wurden, auch wegen fortgesetzten Verstoßes gegen die Grundsätze, und macht es der Öffentlichkeit zugänglich. Das Ministerium muss die Gründe für den Ausschluss der einzelnen Organisationen benennen.

Darüber hinaus verpflichtet sich das Ministerium, Verbesserungen bei der Verwaltung und Überwachung des Datenschutzschildes vorzunehmen. Dies beinhaltet insbesondere:

Die Bereitstellung zusätzlicher Informationen auf der Website des Datenschutzschilds;

— die Pflege der Datenschutzschild-Liste sowie eines Verzeichnisses der Organisationen, die sich ursprünglich durch Selbstzertifizierung zu den Grundsätzen bekannten, aber keinen Anspruch mehr auf die Vorteile des Datenschutzschilds haben;

— Aufnahme einer Erläuterung an deutlich sichtbarer Stelle, in der klargestellt wird, dass alle von der Datenschutzschild-Liste gestrichenen Organisationen zwar keinen Anspruch mehr auf die Vorteile des Datenschutzschilds haben, jedoch mit Blick auf die personenbezogenen Informationen, die sie während ihrer Beteiligung am Datenschutzschild erhalten haben, weiterhin ihren Verpflichtungen nachkommen müssen, solange sie diese Informationen speichern und

— Erstellung eines Links zur Liste der FTC-Fälle, die mit dem Datenschutzschild in Verbindung stehen, auf der Website der FTC.

Prüfung der Selbstzertifizierungs-Anforderungen

— vor dem Abschluss der Selbstzertifizierung einer Organisation (oder der erneuten jährlichen Zertifizierung) und der Aufnahme einer Organisation in die Datenschutzschild-Liste ist zu prüfen, ob diese Organisation:

  — die erforderlichen Kontaktinformationen bereitgestellt hat;

  — die Tätigkeit der Organisation im Zusammenhang mit personenbezogenen Daten aus der EU beschrieben hat;

  — darauf hingewiesen hat, bei welchen personenbezogenen Informationen die Selbstzertifizierung zur Anwendung kommt;

  — bei Vorhandensein einer öffentlich zugänglichen Website der Organisation die Webadresse angegeben hat, auf der die Datenschutzbestimmungen eingesehen werden können, und die Datenschutzbestimmungen unter der genannten Webadresse zugänglich gemacht oder darauf hingewiesen hat, an welchem Ort die Datenschutzbestimmungen von der Öffentlichkeit eingesehen werden können, sofern eine Organisation keine öffentliche Website unterhält;

  — in die einschlägigen Datenschutzbestimmungen einen Hinweis aufgenommen hat, dass sie sich an die Grundsätze hält, und für den Fall, dass die Datenschutzbestimmungen online verfügbar sind, einen Hyperlink auf die Datenschutzschild-Website des Ministeriums angefügt hat;

  — die gesetzliche Aufsichtsbehörde benannt hat, die über Beschwerden gegen die Organisation wegen unlauteren oder irreführenden Geschäftsgebarens und wegen Verletzung von datenschutzrechtlichen Vorschriften entscheidungsbefugt ist (und in den Grundsätzen oder in einem künftigen Anhang zu den Grundsätzen aufgeführt ist);

  — sofern sie den Bestimmungen gemäß Absatz 1 Buchstabe a und Absatz 3 Buchstabe a des Grundsatzes des Rechtsschutzes, der Durchsetzung und der Haftung entsprechen will, indem sie sich zur Zusammenarbeit mit den entsprechenden Datenschutzbehörden verpflichtet, ihre Absicht erklärt hat, mit den entsprechenden Datenschutzbehörden bei der Behandlung von Beschwerden zusammenzuarbeiten, die unter Berufung auf die Grundsätze des Datenschutzschildes erhoben werden, und insbesondere dann Auskünfte zu erteilen, wenn betroffene Personen in der EU eine Beschwerde direkt an ihre nationale Datenschutzbehörde gerichtet haben;

  — alle Datenschutzprogramme angegeben hat, an denen die Organisation teilnimmt;

  — die Art der anlassunabhängigen Kontrolle (z. B. intern oder extern) benannt hat, mit der die Einhaltung der Grundsätze gewährleistet werden soll;

  — sowohl in ihrem Antrag auf Selbstzertifizierung als auch in ihren Datenschutzbestimmungen auf die unabhängige Beschwerdestelle verwiesen hat, die für die Prüfung und Lösung von Beschwerden zuständig ist;

  — in ihre entsprechenden Datenschutzbestimmungen, sofern diese online verfügbar sind, einen Hyperlink zur Website oder zum Beschwerdeformular der unabhängigen Beschwerdestelle, die ungeklärte Beschwerden prüft, eingefügt hat und

  — gegebenenfalls auf ihren Wunsch verwiesen hat, dass ihr Personaldaten zur Verwendung im Rahmen von Beschäftigungsverhältnissen aus der EU übermittelt werden, ihre Bereitschaft erklärt hat, mit den Datenschutzbehörden zusammenzuarbeiten und deren Rat zu befolgen, wenn es um die Lösung von Beschwerden über ihren Umgang mit diesen Daten geht, dem Ministerium eine Kopie ihrer Bestimmungen zum Schutz von Personaldaten übermittelt und mitgeteilt hat, wo die Datenschutzbestimmungen durch die betroffenen Mitarbeiter eingesehen werden können.

— In Zusammenarbeit mit den unabhängigen Beschwerdestellen ist zu prüfen, ob sich die Organisationen tatsächlich für die jeweiligen Mechanismen registriert haben, die in ihren Anträgen auf Selbstzertifizierung angegeben sind, sofern eine solche Registrierung erforderlich ist.

Verstärkte Bemühungen um eine Weiterbehandlung der Fälle von Organisationen, die von der Datenschutzschild-Liste gestrichen wurden

— Hinweis an Organisationen, die wegen „fortgesetzter Missachtung der Grundsätze“ von der Datenschutzschild-Liste gestrichen wurden, dass sie nicht befugt sind, im Rahmen des Datenschutzschildes erhobene Daten zu speichern und

— Übermittlung von Fragebögen an Organisationen, deren Selbstzertifizierung ausläuft oder die freiwillig aus dem Datenschutzschild ausgeschieden sind, um zu prüfen, ob die Organisation die personenbezogenen Daten, die sie während der Beteiligung am 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.

Aufdeckung und Handhabung von Fällen, in denen zu Unrecht eine Beteiligung an der Regelung geltend gemacht wird

— Prüfung der Datenschutzbestimmungen von Organisationen, die sich bereits am Datenschutzschild beteiligt haben, jedoch von der Datenschutzschild-Liste gestrichen wurden, um mögliche Fälle zu ermitteln, in denen falsche Angaben zur Beteiligung am Datenschutzschild gemacht werden.

— Wenn eine Organisation: a) den Datenschutzschild verlassen hat, b) keinen Antrag auf erneute Zertifizierung ihres Beitritts zu den Grundsätzen stellt oder c) insbesondere aufgrund „fortgesetzter Missachtung der Grundsätze" von der Beteiligung am Datenschutzschild ausgeschlossen wird, ist von Amts wegen kontinuierlich sicherzustellen, dass aus den relevanten veröffentlichten Datenschutzbestimmungen der Organisation alle Bezugnahmen auf den Datenschutzschild entfernt wurden, die auf eine weitere aktive Beteiligung der Organisation oder auf einen Anspruch auf die damit verbundenen Vorteile hindeuten. Stellt das Ministerium fest, dass diese Bezugnahmen nicht entfernt wurden, weist es die Organisation eindringlich darauf hin, dass sie die Angelegenheit einer anderen zuständigen Behörde zuzuleiten gedenkt, damit diese gegebenenfalls tätig wird, sofern die Angaben zur Beteiligung am Datenschutzschild nicht entfernt werden. Für den Fall, dass die Organisation die Bezugnahme weder entfernt noch ihren Beitritt zu den Grundsätzen des Datenschutzschildes erklärt, wird das Ministerium die Angelegenheit von Amts wegen an die FTC, das Verkehrsministerium oder eine andere zuständige Behörde verweisen oder gegebenenfalls Maßnahmen zur Einhaltung der Bestimmungen des Gütesiegels für den Datenschutzschild ergreifen.

— Einleitung weiterer Maßnahmen zur Ermittlung falscher Angaben über eine Beteiligung am Datenschutzschild oder einer missbräuchlichen Verwendung des entsprechenden Gütesiegels, auch im Rahmen von Internetrecherchen, um festzustellen, ob Abbildungen des Gütesiegels für den Datenschutzschild verwendet werden und Bezugnahmen auf den Datenschutzschild in den Datenschutzbestimmungen einer Organisation enthalten sind;

— unverzügliche Klärung aller Angelegenheiten, die bei einer Prüfung falscher Angaben zur Beteiligung am Datenschutzschild oder der missbräuchlichen Verwendung des entsprechenden Gütesiegels von Amts wegen ermittelt wurden, was auch eine im Vorangehenden beschriebene Warnung an Organisationen beinhaltet, die falsche Angaben zu ihrer Beteiligung am Datenschutzschild machen;

— Einleitung weiterer geeigneter Abhilfemaßnahmen, darunter die Beschreitung aller für das Ministerium zulässigen Rechtswege und Verweisung der Angelegenheit an die FTC, das Verkehrsministerium oder eine andere zuständige Durchsetzungsstelle und

— unverzügliche Prüfung und Behandlung von bei uns eingehenden Beschwerden über falsche Angaben zur Beteiligung.

Das Ministerium prüft die Datenschutzbestimmungen von Organisationen, um falsche Angaben zur Beteiligung am Datenschutzschild wirksamer aufdecken und dagegen vorgehen zu können. Diese Prüfung betrifft insbesondere die Datenschutzbestimmungen von Organisationen, deren Selbstzertifizierung ausgelaufen ist, weil sie es versäumt haben, ihren Betritt zu den Grundsätzen erneut zertifizieren zu lassen. Mit Hilfe dieser Prüfungen will das Ministerium feststellen, ob die Organisationen aus ihren relevanten veröffentlichten Datenschutzbestimmungen alle Bezugnahmen entfernt haben, die auf ihre weitere aktive Beteiligung am Datenschutzschild hindeuten. Im Rahmen der beschriebenen Prüfverfahren sollen Organisationen ermittelt werden, die derartige Bezugnahmen nicht entfernt haben, und anschließend in einem Schreiben der Rechtsabteilung des Ministeriums über mögliche Durchsetzungsmaßnahmen für den Fall unterrichtet werden, dass sie diese Bezugnahmen nicht streichen. Anhand von Folgemaßnahmen stellt das Ministerium sicher, dass die Organisationen die unzulässigen Bezugnahmen entweder entfernen oder ihren Beitritt zu den Grundsätzen erneut zertifizieren. Darüber hinaus ist das Ministerium auch darum bemüht, falsche Angaben zur Beteiligung am Datenschutzschild von Organisationen aufzudecken, die niemals am Datenschutzschild-Programm teilgenommen haben, und vergleichbare Abhilfemaßnahmen gegen diese Organisationen einzuleiten.

Regelmäßige Durchführung der von Amts wegen vorgenommenen Kontrollen der Einhaltung und Programmbewertungen

— kontinuierliche Überwachung der effektiven Einhaltung, auch durch die Zusendung detaillierter Fragebögen an teilnehmende Organisationen, um Problemfelder zu ermitteln, in denen es möglicherweise weiterer Folgemaßnahmen bedarf. Die genannten Einhaltungskontrollen sind insbesondere dann durchzuführen, wenn: a) dem Ministerium ernst gemeinte Beschwerden über die Einhaltung der Grundsätze durch eine Organisation zugegangen sind, b) eine Organisation keine zufriedenstellende Antwort auf eine mit dem Datenschutzschild verbundene Anfrage des Ministeriums übermittelt oder c) deutliche Anhaltspunkte darauf schließen lassen, dass eine Organisation ihren Zusagen im Zusammenhang mit dem Datenschutzschild nicht nachkommt. Das Ministerium stimmt diese Einhaltungskontrollen bei Bedarf mit den zuständigen Datenschutzbehörden ab, und

— bewertet regelmäßig die Verwaltung und Überwachung des Datenschutzschild-Programms, um sicherzustellen, dass die Kontrollbemühungen auch für neue Problemfelder geeignet sind.

Das Ministerium hat die Mittel für die Verwaltung und Überwachung des Datenschutzschild-Programms aufgestockt und darüber hinaus die Zahl der für die Verwaltung und Überwachung zuständigen Mitarbeiter verdoppelt. Wir werden auch weiterhin angemessene Mittel für derartige Maßnahmen bereitstellen, um eine effektive Überwachung und Verwaltung des Programms zu gewährleisten.

Überarbeitung der Website des Datenschutzschilds mit Blick auf ausgewählte Zielgruppen

Das Ministerium überarbeitet die Website des Datenschutzschilds, um sie auf drei Zielgruppen auszurichten: EU-Bürger, EU-Unternehmen und US-Unternehmen. Durch die Aufnahme von speziell auf EU-Bürger und EU-Unternehmen zugeschnittenen Materialien kann die Transparenz auf vielfältige Weise gesteigert werden. Für EU-Bürger werden folgende Punkte klar erläutert: 1) die Rechte, die für EU-Bürger mit dem Datenschutzschild verbunden sind, 2) die Rechtsbehelfe, die EU-Bürgern zur Verfügung stehen, wenn sie der Ansicht sind, dass eine Organisation ihrer Verpflichtung zur Einhaltung der Grundsätze nicht nachkommt und 3) die Verfügbarkeit von Informationen zur Selbstzertifizierung einer Organisation im Rahmen des Datenschutzschilds. Für EU-Unternehmen werden folgende Kontrollen erleichtert: 1) ob eine Organisation Anspruch auf die Vorteile aus dem Datenschutzschild hat, 2) welche Informationen von der Selbstzertifizierung einer Organisation im Rahmen des Datenschutzschilds abgedeckt werden, 3) welche Datenschutzbestimmungen auf diese Informationen zur Anwendung kommen und 4) anhand welcher Methoden eine Organisation die Einhaltung der Grundsätze prüft.

Ausbau der Zusammenarbeit mit den Datenschutzbehörden

Für den Ausbau der Kooperationsmöglichkeiten mit den Datenschutzbehörden richtet das Ministerium eine spezielle Kontaktstelle ein, die als Bindeglied zu den Datenschutzbehörden fungiert. Sollte eine Datenschutzbehörde, auch aufgrund einer Beschwerde durch einen EU-Bürger, den Verdacht hegen, dass eine Organisation die Grundsätze nicht einhält, kann sie sich an die spezielle Kontaktstelle im Ministerium wenden, um eine weitere Kontrolle der Organisation zu veranlassen. An die Kontaktstelle können auch Fälle überwiesen werden, in denen Organisationen falsche Angaben zu ihrer Beteiligung am Datenschutzschild machen, obgleich sie ihren Beitritt zu den Grundsätzen niemals selbst bescheinigt haben. Die Kontaktstelle unterstützt Datenschutzbehörden bei der Erfassung von Informationen zur Selbstzertifizierung oder zum bisherigen Beitritt einer Organisation zum Programm und beantwortet Anfragen der Datenschutzbehörden zur Umsetzung der spezifischen Datenschutzschild-Anforderungen. Darüber hinaus stellt das Ministerium den Datenschutzbehörden Material zum Datenschutzschild zur Verfügung, das sie auf ihre eigenen Websites stellen können, um für mehr Transparenz zugunsten von EU-Bürgern und EU-Unternehmen zu sorgen. Ein stärkeres Bewusstsein für den Datenschutzschild und die damit verbundenen Rechte und Pflichten kann die Erkennung von Problemen unmittelbar nach ihrem Auftreten begünstigen und die Einleitung geeigneter Abhilfemaßnahmen begünstigen.

Erleichterung der Lösungsfindung bei Beschwerden wegen Verletzung der Datenschutzvorschriften

An das Ministerium gerichtete Beschwerden einer Datenschutzbehörde über die Nichteinhaltung der Grundsätze durch eine dem Datenschutzschild angehörende Organisation gehen dem Ministerium über die spezielle Kontaktstelle zu. Nach Eingang ist das Ministerium nach besten Kräften um eine Klärung der Beschwerde mit der dem Datenschutzschild angehörenden Organisation bemüht. Innerhalb von 90 Tagen nach Eingang der Beschwerde unterrichtet das Ministerium die Datenschutzbehörde über den aktuellen Sachstand. Um die Einreichung derartiger Beschwerden zu erleichtern, erstellt das Ministerium ein Standardformular für Datenschutzbehörden, das bei der speziellen Kontaktstelle im Ministerium eingereicht werden kann. In der speziellen Kontaktstelle werden alle von den Datenschutzbehörden an das Ministerium übermittelten Fälle erfasst, und das Ministerium erstellt bei der jährlichen Überprüfung einen Bericht, der in aggregierter Form die im Laufe des Jahres bei ihm eingegangenen Beschwerden enthält.

Annahme von Schiedsverfahren und Auswahl von Schiedsrichtern in Abstimmung mit der Kommission

Das Ministerium kommt seinen Zusagen gemäß Anhang I nach und macht die Verfahren im Anschluss an eine Einigung bekannt.

Gemeinsame Überprüfung der Funktionsweise des Datenschutzschilds

Das Handelsministerium, die FTC und andere Stellen werden bei Bedarf jährliche Sitzungen mit der Kommission, betroffenen Datenschutzbehörden und gegebenenfalls auch Vertretern der Artikel-29-Datenschutzgruppe organisieren, auf denen das Ministerium über den aktuellen Sachstand mit Blick auf das Datenschutzschild-Programm informiert. Bei den jährlichen Sitzungen werden aktuelle Probleme im Zusammenhang mit der Funktionsweise, Durchführung, Überwachung und Durchsetzung des Datenschutzschilds, darunter die von den Datenschutzbehörden an das Ministerium übermittelten Fälle, die Ergebnisse der von Amts wegen durchgeführten Kontrollen einer Einhaltung der Grundsätze sowie möglicherweise relevante Gesetzesänderungen, erörtert. Die erste jährliche Überprüfung und gegebenenfalls anschließende Überprüfungen werden einen Dialog zu weiteren Themen wie z. B. automatische Entscheidungsprozesse, einschließlich eines Meinungsaustauschs über Gemeinsamkeiten und Unterschiede der diesbezüglichen Konzepte der EU und der USA beinhalten.

Aktualisierung von Gesetzen

Das Ministerium wird die Kommission in angemessener Weise über wesentliche Änderungen des Rechts der Vereinigten Staaten unterrichten, wenn sie für den Datenschutzschild relevant sind und den Datenschutz sowie die Beschränkungen und Schutzvorkehrungen für den Zugriff staatlicher Behörden auf personengebundene Daten und deren anschließende Verwendung betreffen.

Ausnahmen aus Gründen der nationalen Sicherheit

Der Rechtsbeauftragte im Amt des Directors of National Intelligence, Robert Litt, hat Justin Antonipillai und Ted Dean im Handelsministerium zwei Schreiben zu den Einschränkungen bei der Einhaltung der Grundsätze des Datenschutzschildes aus Gründen der nationalen Sicherheit übermittelt, die an Sie weitergeleitet wurden. In diesen Schreiben werden unter anderem die Strategien, Garantien und Beschränkungen erläutert, die für signalerfassende Aufklärung in den USA gelten. Darüber hinaus enthalten diese Schreiben Erläuterungen zur Transparenz, die von den Nachrichtendiensten in dieser Hinsicht geschaffen wurde. Die Kommission kann bei ihrer Überprüfung der Datenschutzschild-Regelung aus den in diesen Schreiben enthaltenen Informationen mit Sicherheit schließen, dass der Datenschutzschild in Übereinstimmung mit den darin aufgeführten Grundsätzen ordnungsgemäß funktioniert. Wir gehen davon aus, dass Sie bei der jährlichen Überprüfung der Datenschutzschild-Regelung künftig auf von den Nachrichtendiensten öffentlich gemachte Informationen sowie auf weitere Informationen zurückgreifen werden.

Ausgehend von den Grundsätzen des Datenschutzschilds und den Begleitschreiben und -materialien, einschließlich der Zusagen des Ministeriums zur Verwaltung und Überwachung der Grundsätze des Datenschutzschilds, rechnen wir damit, dass die Kommission die EU-US-Datenschutzschild-Regelung als ausreichend erachtet, um einen Schutz im Sinne der EU-Rechtsvorschriften zu gewährleisten, und dass Daten weiterhin an Organisationen übermittelt werden, die sich am Datenschutzschild beteiligen.

Hochachtungsvoll

Ken Hyatt

Anlage 2

Schiedsmodell

ANLAGE I

In dieser Anlage I sind die Bedingungen aufgeführt, unter denen dem Datenschutz angehörende Organisationen zur Behandlung von Ansprüchen im Schiedsverfahren nach dem Grundsatz des Rechtsschutzes, der Durchsetzung und der Haftung verpflichtet sind. Die im Folgenden beschriebene Möglichkeit des verbindlichen Schiedsverfahrens bezieht sich auf bestimmte „Restansprüche" in Bezug auf Daten, die unter den EU-US-Datenschutzschild fallen. Damit soll Privatpersonen ein zeitnaher, unabhängiger und fairer Mechanismus bereitgestellt werden, der sich mit geltend gemachten Verstößen gegen die Grundsätze befasst, die nicht von einem der gegebenenfalls in Anspruch genommenen anderen Mechanismen des Datenschutzschilds geklärt werden konnten.

A. **Anwendungsbereich**

Mit dem Schiedsverfahren können Privatpersonen bei Restansprüchen feststellen lassen, ob eine dem Datenschutzschild angehörende Organisation ihre Pflichten im Rahmen der Grundsätze gegenüber der betreffenden Person verletzt hat und ob diese Verletzung vollständig oder teilweise ungeahndet bleibt. Diese Option steht nur für diese Zwecke zur Verfügung, nicht jedoch beispielsweise bei den geregelten Abweichungen von den Grundsätzen ([1]) oder im Hinblick auf eine Behauptung zur Angemessenheit des Datenschutzschilds.

B. **Verfügbare Abhilfemaßnahmen**

Im Rahmen dieses Schiedsverfahrens ist das Datenschutzschild-Panel (bestehend aus einem oder drei von den Parteien ausgewählten Schiedsrichtern) befugt, einzelfallabhängige nichtmonetäre billigkeitsrechtliche Ansprüche (wie z. B. Zugang, Korrektur, Löschung oder Rückgabe der betreffenden Daten der Person) anzuerkennen, um die Verstöße gegen die Grundsätze abzustellen. Dieses sind die einzigen Befugnisse des Schiedsforums in Bezug auf Abhilfemaßnahmen. Bei der Prüfung von Abhilfemaßnahmen muss das Schiedsforum andere bereits von anderen Mechanismen im Rahmen des Datenschutzschilds verhängte Abhilfemaßnahmen berücksichtigen. Schadenersatz, Kosten, Gebühren oder andere derartige Maßnahmen sind nicht verfügbar. Jede Partei muss selbst für die anfallenden Anwaltsgebühren aufkommen.

C. **Voraussetzungen für das Schiedsverfahren**

Wer das Schiedsverfahren in Anspruch nehmen möchte, muss vor der Einleitung einer Schiedsklage 1) den behaupteten Verstoß direkt bei der Organisation geltend machen und der Organisation Gelegenheit geben, die Angelegenheit innerhalb der in Abschnitt III.11 d)i) der Grundsätze aufgeführten Frist zu klären, 2) das kostenlose unabhängige Beschwerdeverfahren im Rahmen der Grundsätze in Anspruch nehmen und 3) die Angelegenheit kostenlos über seine zuständige Datenschutzbehörde dem Handelsministerium zuleiten und dem Handelsministerium die Gelegenheit geben, die Angelegenheit nach Möglichkeit innerhalb der im Schreiben der International Trade Administration des Handelsministeriums gesetzten Frist zu klären.

Das Schiedsverfahren kann nicht in Anspruch genommen werden, wenn der von der Person geltend gemachte Verstoß 1) bereits Gegenstand eines verbindlichen Schiedsverfahrens war, 2) Gegenstand eines rechtskräftigen Urteils in einem Gerichtsverfahren mit der Person als Prozesspartei war oder 3) von den Parteien bereits geregelt wurde. Darüber hinaus kann das Schiedsverfahren nicht in Anspruch genommen werden, wenn eine EU-Datenschutzbehörde 1) gemäß Abschnitt III.5 oder III.9 der Grundsätze zuständig ist oder 2) befugt ist, den geltend gemachten Verstoß direkt mit der Organisation zu klären.Die Befugnis einer Datenschutzbehörde, den gleichen Anspruch gegen einen für die Verarbeitung Verantwortlichen in der EU geltend zu machen, schließt die Inanspruchnahme des Schiedsverfahrens gegen eine nicht an die Befugnis der Datenschutzbehörde gebundene andere rechtliche Einheit allein nicht aus.

D. **Verbindlichkeit von Schiedssprüchen**

Die Entscheidung einer Einzelperson, dieses verbindliche Schiedsverfahren in Anspruch zu nehmen, ist vollkommen freiwillig. Die Schiedssprüche sind für alle beteiligten Parteien verbindlich. Mit der Inanspruchnahme verzichtet die betreffende Person auf die Möglichkeit, ein anderes Forum mit der Klärung des geltend gemachten Verstoßes zu befassen; wenn jedoch diesem Verstoß mit der Anerkennung nichtmonetärer Ansprüche nicht vollständig abgeholfen wird, kann die betreffende Person dennoch Schadensersatzansprüche vor Gericht geltend machen.

([1]) Abschnitt I.5 der Grundsätze.

E. **Überprüfung und Durchsetzung**

Privatpersonen und dem Datenschutzschild angehörende Organisationen können eine gerichtliche Überprüfung und Durchsetzung der Schiedsentscheidungen nach US-Recht gemäß Federal Arbitration Act beantragen ([1]). Derartige Fälle müssen bei dem Bundesbezirksgericht eingereicht werden, dessen territoriale Zuständigkeit sich auf den Hauptgeschäftsort der dem Datenschutzschild angehörenden Organisation erstreckt.

Mit diesem Schiedsverfahren sollen individuelle Streitigkeiten geklärt werden, und die Schiedsentscheidungen sollen nicht als zur Nachahmung empfohlener oder verbindlicher Präzedenzfall bei Angelegenheiten anderer Parteien dienen, einschließlich bei künftigen Schiedsverfahren oder an Gerichten der EU oder der USA oder in Verfahren der FTC.

F. **Das Schiedsforum**

Die Parteien wählen die Schiedsrichter aus dem im Folgenden erörterten Verzeichnis der Schiedsrichter aus.

Nach geltendem Recht erstellen das US-Handelsministerium und die Europäische Kommission ein Verzeichnis mit mindestens 20 Schiedsrichtern, die aufgrund ihrer Unabhängigkeit, Integrität und Sachkenntnis ausgewählt werden. Dafür gilt Folgendes:

Die Schiedsrichter

1) verbleiben für einen Zeitraum von 3 Jahren in dem Verzeichnis, sofern keine außergewöhnlichen Umstände oder wichtigen Gründe vorliegen; dieser Zeitraum kann um weitere drei Jahre verlängert werden;

2) sind gegenüber einer der Parteien oder einer dem Datenschutzschild angehörigen Organisation bzw. gegenüber den USA, der EU oder einem EU-Mitgliedstaat oder einer anderen Regierungsbehörde, öffentlichen Behörde oder Strafverfolgungsbehörde weder weisungsgebunden noch anderweitig verpflichtet;

3) müssen als Rechtsanwalt in den USA zugelassen und im US-Privatrecht bewandert sein und Sachkenntnis im EU-Datenschutzrecht aufweisen.

G. **Schiedsverfahren**

Im Einklang mit dem geltenden Recht vereinbaren das Handelsministerium und die Europäische Kommission innerhalb von 6 Monaten nach Annahme des Angemessenheitsbeschlusses die Übernahme einer Reihe von bestehenden, etablierten US-Schiedsverfahren (wie z. B. AAA oder JAMS) zur Regelung des Verfahrens vor dem Datenschutzschild-Panel, wobei die folgenden Aspekte zugrunde gelegt werden:

1. Eine Person kann vorbehaltlich der vorstehend aufgeführten Voraussetzungen ein verbindliches Schiedsverfahren einleiten, indem sie der Organisation eine Mitteilung zukommen lässt. Die Mitteilung enthält eine Zusammenfassung der gemäß Abschnitt C unternommenen Schritte zur Klärung einer Beschwerde, eine Beschreibung des geltend gemachten Verstoßes und, nach eigener Wahl, Belegunterlagen und -materialien und/oder eine Rechtserörterung mit Bezug zum geltend gemachten Verstoß.

([1]) In Kapitel 2 des Federal Arbitration Act („FAA“) heißt es: „Eine Schiedsvereinbarung oder ein Schiedsspruch aus einem vertraglichen oder nicht vertraglichen Rechtsverhältnis, das als kommerziell gilt, einschließlich einer Transaktion, eines Vertrags oder einer Vereinbarung nach [§ 2 des FAA], fällt unter das Übereinkommen über die Anerkennung und Vollstreckung ausländischer Schiedssprüche vom 10. Juni 1958, 21 U.S.T. 2519, T.I.A.S. No. 6997 („New Yorker Übereinkommen“).“ 9 U.S.C. § 202. Weiter ist im FAA festgelegt: „Eine Schiedsvereinbarung oder ein Schiedsspruch aus einem derartigen Verhältnis, das ausschließlich zwischen Bürgern der Vereinigten Staaten besteht, fällt nur dann unter das [New Yorker] Übereinkommen, wenn dieses Verhältnis im Ausland befindliche Immobilien umfasst, eine Leistung oder Rechtsdurchsetzung im Ausland anstrebt oder in einer anderweitigen hinreichenden Beziehung zu einem oder mehreren anderen Staaten steht.“ Ebenda. Nach Kapitel 2 kann „jede Partei des Schiedsverfahrens einen Antrag bei einem nach diesem Kapitel zuständigen Gericht auf eine Anordnung zur Bestätigung des Schiedspruchs gegen eine andere Partei des Schiedsverfahrens stellen. Das Gericht bestätigt den Schiedsspruch, sofern es keinen der Gründe für eine Verweigerung oder einen Aufschub der Anerkennung oder Durchsetzung des Schiedsspruchs gemäß dem besagten [New Yorker] Übereinkommen findet.“ Ebenda § 207. Weiter heißt es in Kapitel 2: „Die Bezirksgerichte der Vereinigten Staaten … haben ungeachtet des Streitwerts die ursprüngliche Zuständigkeit für … eine Klage oder ein Verfahren [im Rahmen des New Yorker Übereinkommens].“ Ebenda § 203.
Außerdem heißt es in Kapitel 2: „Kapitel 1 gilt für Klagen und Verfahren nach diesem Kapitel, soweit jenes Kapitel nicht mit diesem Kapitel oder dem [New Yorker] Übereinkommen, wie von den Vereinigten Staaten ratifiziert, kollidiert.“ Ebenda § 208. In Kapitel 1 heißt es wiederum: „Eine schriftliche Bestimmung in einem Vertrag über eine geschäftliche Transaktion, wonach ein Streit aufgrund dieses Vertrags oder dieser Transaktion oder die Weigerung, diesen bzw. diese ganz oder teilweise zu erfüllen, im Schiedsverfahren beizulegen ist, oder eine schriftliche Vereinbarung, wonach ein bestehender Streit aufgrund dieses Vertrags, dieser Transaktion oder dieser Weigerung an ein Schiedsgericht zu verweisen ist, ist gültig, unwiderruflich und vollstreckbar, sofern nicht Gründe nach Recht oder Billigkeit für den Rücktritt von einem Vertrag vorliegen.“ Ebenda § 2. Weiter heißt es in Kapitel 1: „Jede Partei im Schiedsverfahren kann bei einem angegebenen Gericht eine Anordnung zur Bestätigung des Schiedsspruchs beantragen, woraufhin das Gericht eine derartige Anordnung erlassen muss, sofern der Schiedsspruch nicht gemäß § 10 und 11 des [FAA] aufgegeben, geändert oder korrigiert wird.“ Ebenda § 9.

2. Es werden Verfahren entwickelt, die sicherstellen, dass für einen geltend gemachten Verstoß nicht mehrere Verfahren geführt oder mehrere Abhilfemaßnahmen getroffen werden.

3. Die FTC kann parallel zum Schiedsverfahren tätig werden.

4. An den Schiedsverfahren dürfen keine Vertreter der USA, der EU oder eines EU-Mitgliedstaats oder einer anderen Regierungsbehörde, staatlichen Behörde oder Strafverfolgungsbehörde teilnehmen, wobei auf Antrag einer Person aus der EU die EU-Datenschutzbehörden Hilfe bei der Erstellung ausschließlich der Mitteilung leisten können, jedoch keinen Zugang zu Offenlegungen und anderen Materialien in Bezug auf diese Schiedsverfahren haben dürfen.

5. Ort des Schiedsverfahrens sind die Vereinigten Staaten, und die betroffene Person kann sich für eine Teilnahme per Video oder Telefonkonferenz entscheiden, die für sie mit keinen Kosten verbunden ist. Eine persönliche Anwesenheit ist nicht erforderlich.

6. Verfahrenssprache ist Englisch, wenn von den Parteien nicht anders vereinbart. Auf einen begründeten Antrag hin und unter Berücksichtigung dessen, ob sich die Person von einem Anwalt vertreten lässt, werden Dolmetscher für die mündliche Verhandlung sowie Übersetzungen der Verfahrensunterlagen bereitgestellt, ohne dass sich daraus Kosten für die Person ergeben, es sei denn, das Panel gelangt in einem konkreten Fall zu dem Schluss, dass eine Kostenübernahme nicht gerechtfertigt oder unverhältnismäßig wäre.

7. Den Schiedsrichtern vorgelegte Unterlagen werden vertraulich behandelt und nur in Verbindung mit dem Schiedsverfahren genutzt.

8. Wenn erforderlich, kann eine die Person betreffende Offenlegung zugelassen werden, wobei diese Offenlegung von den Parteien vertraulich behandelt und nur in Verbindung mit dem Schiedsverfahren genutzt wird.

9. Schiedsverfahren sollen innerhalb von 90 Tagen nach Zustellung der Mitteilung an die betreffende Organisation abgeschlossen werden, sofern von den Parteien nicht anderweitig vereinbart.

H. **Kosten**

Die Schiedsrichter sollen angemessene Maßnahmen zur Minimierung der Kosten oder Gebühren der Schiedsverfahren ergreifen.

Nach Maßgabe des geltenden Rechts wird das Handelsministerium in Abstimmung mit der Europäischen Kommission die Einrichtung eines Fonds ermöglichen, in den die dem Datenschutzschild angehörenden Organisationen einen Jahresbeitrag einzahlen, der sich zum Teil nach der Größe der Organisation richtet und die Schiedskosten, einschließlich Schiedsrichtergebühren, bis zu einer Obergrenze deckt. Der Fonds wird von einem Dritten verwaltet, der regelmäßig über die Tätigkeit des Fonds Bericht erstattet. Bei der jährlichen Überprüfung werden das Handelsministerium und die Europäische Kommission die Tätigkeit des Fonds, einschließlich der Notwendigkeit einer Anpassung des Beitrags oder der Obergrenze, kontrollieren und unter anderem die Anzahl der Schiedsverfahren sowie deren Kosten und Dauer prüfen, und zwar im gegenseitigen Einvernehmen, dass den am Datenschutzschild teilnehmenden Organisationen keine übermäßige finanzielle Belastung auferlegt wird. Rechtsanwaltsgebühren sind von dieser Bestimmung oder einem anderen Fonds im Rahmen dieser Bestimmung nicht erfasst.

ANHANG II

GRUNDSÄTZE DES EU-US-DATENSCHUTZSCHILDS VORGELEGT VOM AMERIKANISCHEN HANDELSMINISTERIUM

I. ÜBERBLICK

1. Die Vereinigten Staaten und die Europäische Union haben beide das Ziel, den Datenschutz zu verstärken, wobei die Vereinigten Staaten jedoch einen anderen Ansatz verfolgen als die Europäische Gemeinschaft. Die USA verfolgen einen sektoralen Ansatz, der auf einer Mischung von Rechtsvorschriften, Verordnungen und freiwilliger Selbstkontrolle basiert. Angesichts dieser Unterschiede und um Organisationen in den Vereinigten Staaten einen zuverlässigen Mechanismus für die Übermittlung personenbezogener Daten aus der Europäischen Union in die Vereinigten Staaten bereitzustellen und dabei gleichzeitig sicherzustellen, dass betroffene EU-Bürger weiter in den Genuss wirksamer Garantien und eines wirksamen Schutzes bei der Verarbeitung ihrer personenbezogenen Daten nach deren Übermittlung in Nicht-EU-Länder kommen, legt das Handelsministerium im Rahmen seiner gesetzlichen Befugnis, internationalen Handel zu pflegen, zu fördern und zu entwickeln (15 U.S.C. § 1512), diese Grundsätze des Datenschutzschilds, einschließlich der Zusatzgrundsätze (im Folgenden insgesamt „Grundsätze") vor. Die Grundsätze wurden in Absprache mit der Europäischen Kommission sowie mit der Industrie und anderen Interessenträgern entwickelt, um den Handel zwischen der Europäischen Union und den Vereinigten Staaten zu erleichtern. Sie sind ausschließlich für den Gebrauch durch Organisationen in den Vereinigten Staaten bestimmt, die personenbezogene Daten aus der Europäischen Union erhalten, um sich für den Datenschutzschild zu qualifizieren und so vom Angemessenheitsbeschluss der Europäischen Kommission zu profitieren ([1]). Die Grundsätze berühren nicht die Anwendung nationaler Rechtsvorschriften über die Verarbeitung personenbezogener Daten in den Mitgliedstaaten, mit denen die Richtlinie 95/46/EG (im Folgenden „Richtlinie") umgesetzt wird. Ebenso wenig schränken die Prinzipien ansonsten nach US-Recht geltende Datenschutzverpflichtungen ein.

2. Um sich auf den Datenschutzschild zur Übermittlung personenbezogener Daten aus der EU stützen zu können, muss eine Organisation gegenüber dem Handelsministerium (oder einer von ihm benannten Stelle) (im Folgenden „Ministerium") durch Selbstzertifizierung erklären, dass sie sich an die Grundsätze hält. Obwohl Entscheidungen von Organisationen, so dem Datenschutzschild beizutreten, vollkommen freiwillig sind, ist die wirksame Einhaltung der Grundsätze obligatorisch: Organisationen, die dem Ministerium eine Selbstzertifizierung bekanntgeben und öffentlich erklären, dass sie die Grundsätze befolgen, müssen diese vollständig einhalten. Um dem Datenschutzschild beizutreten, muss eine Organisation a) den Untersuchungs- und Durchsetzungsbefugnissen der Federal Trade Commission (im Folgenden „FTC"), des Verkehrsministeriums oder anderer gesetzlicher Organe, die die Einhaltung der Grundsätze effektiv gewährleisten, unterliegen (*andere von der EU anerkannte Behörden der Vereinigten Staaten können künftig als Anhang beigefügt werden*), b) öffentlich seine Bereitschaft erklären, die Grundsätze einzuhalten, c) ihre Datenschutzbestimmungen im Einklang mit diesen Grundsätzen offenlegen und d) diese vollständig umsetzen. Ein Verstoß der Organisation gegen diese Grundsätze ist gemäß Abschnitt 5 des Federal Trade Commission Act zur Verhinderung unlauterer und irreführender Praktiken, die im Handel erfolgen oder den Handel beeinträchtigen (15 U.S.C. § 45(a)), oder ähnlichen Rechtsvorschriften verfolgbar.

3. Das Handelsministerium wird eine verbindliche Liste der US-Organisationen führen und der Öffentlichkeit zugänglich machen, die sich gegenüber dem Ministerium selbst zertifiziert und zugesichert haben, die Grundsätze zu befolgen (im Folgenden „Datenschutzschild-Liste"). Das Ministerium wird eine Organisation von der Datenschutzschild-Liste streichen, wenn sie freiwillig aus dem Datenschutzschild ausscheidet oder wenn sie es versäumt, ihre jährlich fällige Zertifizierung gegenüber dem Ministerium zu erneuern. Die Streichung einer Organisation von der Datenschutz-Liste bedeutet, dass sie nicht mehr in den Genuss des Angemessenheitsbeschlusses der Europäischen Kommission zum Empfang personenbezogener Daten aus der EU kommen kann. Die Organisation muss die Grundsätze für personenbezogene Daten, die sie während der Zeit ihrer Teilnahme am Datenschutzschild erhalten hat, weiter einhalten, solange sie diese Daten speichert, und gegenüber dem Ministerium jährlich die Einhaltung zusichern; ansonsten muss die Organisation die Daten zurückgeben oder löschen oder für sie einen „angemessenen" Schutz bieten. Das Ministerium wird zudem jene Organisationen von der Datenschutzschild-Liste streichen, die die Grundsätze fortgesetzt missachten; diese Organisationen verlieren die mit dem Datenschutzschild verbundenen Vorteile und müssen die personenbezogenen Daten zurückgeben oder löschen, die sie im Rahmen des Datenschutzschilds erhalten haben.

4. Das Ministerium wird ferner ein verbindliches Verzeichnis der US-Organisationen führen und der Öffentlichkeit zugänglich machen, die ehemals eine Selbstzertifizierung gegenüber dem Ministerium abgegeben haben, aber von der Datenschutzschild-Liste gestrichen wurden. Das Ministerium wird deutlich auf Folgendes hinweisen: diese Organisationen nehmen nicht am Datenschutzschild teil; die Streichung von der Datenschutzschild-Liste bedeutet, dass diese Organisationen nicht geltend machen können, dass sie den Datenschutzschild einhalten, und sie alle

([1]) Unter der Voraussetzung, dass der Beschluss über die Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes für Island, Liechtenstein und Norwegen gilt, wird die Materialsammlung zum Datenschutzschild sowohl die Europäische Union als auch diese drei Länder abdecken. Demzufolge sind bei Bezugnahmen auf die EU und ihre Mitgliedstaaten auch Island, Liechtenstein und Norwegen eingeschlossen.

Aussagen oder irreführende Praktiken vermeiden müssen, die auf eine Teilnahme am Datenschutzschild hindeuten; und diese Organisationen können nicht mehr die sich aus dem Angemessenheitsbeschluss der Europäischen Kommission ergebenden Vorteile in Anspruch nehmen, die ihnen den Empfang personenbezogene Daten aus der EU ermöglichen. Gegen eine Organisation, die nach ihrer Streichung von der Datenschutzschild-Liste weiter eine Teilnahme am Datenschutzschild behauptet oder sonstige falsche Angaben zum Datenschutzschild macht, können von der FTC, vom Verkehrsministerium oder anderen Behörden entsprechende Durchsetzungsmaßnahmen eingeleitet werden.

5. Die Einhaltung dieser Grundsätze kann begrenzt sein: a) insoweit, als Erfordernissen der nationalen Sicherheit, des öffentlichen Interesses oder der Durchführung von Gesetzen Rechnung getragen werden muss, b) durch Gesetzesrecht, staatliche Regulierungsvorschriften oder Fallrecht, aus denen sich widersprüchliche Verpflichtungen oder ausdrückliche Ermächtigungen ergeben, vorausgesetzt, die Organisation kann in Wahrnehmung einer derartigen Ermächtigung nachweisen, dass die Grundsätze nur insoweit nicht eingehalten werden, als die Einhaltung übergeordneter berechtigter Interessen aufgrund eben dieser Ermächtigung dies erfordert, oder c) wenn die Richtlinie oder das nationale Recht Ausnahmeregelungen vorsieht, sofern diese Ausnahmeregelungen unter vergleichbaren Voraussetzungen getroffen werden. Im Hinblick auf das Ziel eines wirksameren Schutzes der Privatsphäre sollen die Organisationen die Grundsätze in vollem Umfang und in transparenter Weise anwenden, unter anderem indem sie angeben, in welchen Fällen Abweichungen von den Grundsätzen, die nach b) zulässig sind, bei ihren Datenschutzmaßnahmen regelmäßig Anwendung finden werden. Aus demselben Grund wird, wenn die Wahlmöglichkeit nach den Grundsätzen und/oder nach dem US-Recht besteht, von den Organisationen erwartet, dass sie sich, sofern möglich, für das höhere Schutzniveau entscheiden.

6. Die Organisationen sind verpflichtet, die Grundsätze nach ihrem Beitritt zum Datenschutzschild auf alle personenbezogenen Daten anzuwenden, die im Vertrauen auf den Datenschutzschild übermittelt werden. Eine Organisation, die sich für eine Ausdehnung der Vorteile des Datenschutzschilds auf Personaldaten entscheidet, die im Rahmen eines Beschäftigungsverhältnisses aus der EU übermittelt werden, muss darauf hinweisen, wenn sie sich dem Ministerium gegenüber auf die Grundsätze verpflichtet, und sie muss die in den Zusatzgrundsätzen zur Selbstzertifizierung beschriebenen Anforderungen erfüllen.

7. Für Fragen der Auslegung und der Einhaltung der Grundsätze sowie der einschlägigen Datenschutzbestimmungen durch Organisationen, die dem Datenschutzschild angehören, gilt das US-Recht; es gilt nicht, wenn sich diese Organisationen zur Zusammenarbeit mit europäischen Datenschutzbehörden verpflichtet haben. Sofern nicht anderweitig festgelegt, finden sämtliche Bestimmungen der Grundsätze in allen Fällen, in denen sie relevant sind, Anwendung.

8. Begriffsbestimmungen:

   a. „Personenbezogene Daten“ sind in beliebiger Form aufgezeichnete Daten über eine identifizierte oder identifizierbare Person, die unter die Richtlinie fallen und aus der Europäischen Union an eine Organisation in den Vereinigten Staaten übermittelt werden.

   b. „Verarbeitung“ personenbezogener Daten bezeichnet jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Speichern, die Organisation, die Aufbewahrung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Benutzung, die Weitergabe oder die Verbreitung sowie das Löschen oder Vernichten.

   c. „Für die Verarbeitung Verantwortlicher“ bezeichnet eine Person oder Organisation, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

9. Der Tag des Wirksamwerdens der Grundsätze ist der Tag, an dem der Angemessenheitsbeschluss der Kommission endgültig genehmigt wird.

II. GRUNDSÄTZE

1. **Informationspflicht**

   a. Die Organisation muss Privatpersonen über Folgendes informieren:

      i. ihre Teilnahme am Datenschutzschild mit einem Link zur Datenschutzschild-Liste oder der Webanschrift der Liste,

      ii. die Arten der erfassten personenbezogenen Daten und gegebenenfalls die Einrichtungen oder Tochterunternehmen der Organisation, die die Grundsätze ebenfalls einhalten,

iii. ihre Verpflichtung, die Grundsätze auf alle aus der EU empfangenen personenbezogenen Daten unter Zugrundelegung des Datenschutzschilds anzuwenden,

iv. zu welchem Zweck sie die personenbezogenen Daten über sie erhebt und verwendet,

v. wie sie die Organisation bei eventuellen Nachfragen oder Beschwerden kontaktieren können, wozu auch Angaben zu einer relevanten Einrichtung in der EU gehören, die auf derartige Nachfragen oder Beschwerden eingehen kann,

vi. die Kategorie und Identität von Dritten, an die die Daten weitergegeben werden, sowie der Zweck der Weitergabe,

vii. das Recht von Privatpersonen auf Zugang zu ihren personenbezogenen Daten,

viii. welche Mittel und Wege sie den Privatpersonen zur Verfügung stellt, um die Verwendung und Weitergabe ihrer personenbezogenen Daten einzuschränken,

ix. das zur Bearbeitung von Beschwerden und für einen kostenlosen Rechtsschutz für die Privatperson benannte unabhängige Streitbeilegungsgremium, und ob es sich 1) um das von Datenschutzbehörden eingerichtete Gremium, 2) um einen in der EU ansässigen Anbieter für alternative Streitbeilegung oder 3) um einen in den Vereinigten Staaten ansässigen Anbieter für alternative Streitbeilegung handelt,

x. die für die Organisation geltenden Ermittlungs- und Durchsetzungsbefugnisse der FTC, des Verkehrsministeriums oder einer anderen bevollmächtigten US-Behörde,

xi. die Möglichkeit, unter bestimmten Bedingungen ein verbindliches Schiedsverfahren anzustrengen,

xii. die Bestimmung, personenbezogene Daten auf rechtmäßige Anfrage von Behörden offenzulegen, um Erfordernissen der nationalen Sicherheit oder der Strafverfolgung nachzukommen, und

xiii. die Haftung der Organisation bei Weitergabe an Dritte.

b. Diese Angaben sind den Betroffenen unmissverständlich und deutlich erkennbar zu machen, wenn sie erstmalig ersucht werden, der Organisation personenbezogene Daten zu liefern, oder so bald wie möglich danach, auf jeden Fall aber bevor die Organisation die Daten zu anderen Zwecken verwendet als denen, für die sie von der übermittelnden Organisation ursprünglich erhoben oder verarbeitet wurden, oder bevor sie die Daten erstmalig an einen Dritten weitergibt.

2. **Wahlmöglichkeit**

a. Die Organisation muss Privatpersonen die Möglichkeit geben zu wählen („Opt-out"), ob ihre personenbezogenen Daten i) an Dritte weitergegeben werden sollen oder ii) für einen Zweck verwendet werden sollen, der sich von dem ursprünglichen oder dem nachträglich von der betreffenden Person genehmigten Erhebungszweck wesentlich unterscheidet. Der betroffenen Person muss die Ausübung ihres Wahlrechts durch leicht erkennbare, verständliche und leicht zugängliche Verfahren ermöglicht werden.

b. Abweichend vom vorstehenden Absatz unterliegt die Übermittlung solcher Daten an einen Dritten nicht dem Grundsatz der Wahlmöglichkeit, wenn dieser im Auftrag oder auf Anweisung der Organisation tätig ist. Die Organisation schließt jedoch stets einen Vertrag mit dem Beauftragten.

c. Bei sensiblen Daten (d. h. Angaben über den Gesundheitszustand, über Rassen- oder ethnische Zugehörigkeit, über politische, religiöse oder weltanschauliche Überzeugungen, über die Mitgliedschaft in einer Gewerkschaft oder über das Sexualleben) benötigen die Organisationen die ausdrückliche Zustimmung („Opt-in") der betroffenen Personen, wenn diese Daten i) an Dritte weitergegeben oder ii) für einen anderen als den ursprünglichen Erhebungszweck oder den Zweck verwendet werden sollen, dem die betroffene Person nachträglich durch Ausübung des Wahlrechts zugestimmt hat. Darüber hinaus sollen die Organisationen alle ihnen von Dritten übermittelten personenbezogenen Daten als sensibel behandeln, die der Übermittler als sensibel einstuft und behandelt.

3. **Verantwortlichkeit für die Weitergabe**

a. Eine Organisation darf personenbezogene Daten nur dann an Dritte, die als für die Verarbeitung Verantwortliche tätig sind, weitergeben, wenn sie die Grundsätze der Informationspflicht und der Wahlmöglichkeit anwendet. Die Organisation muss auch einen Vertrag mit dem als für die Verarbeitung Verantwortlichen tätigen Dritten schließen, in dem festgelegt ist, dass diese Daten nur in begrenztem Rahmen für bestimmte Zwecke im Einklang mit der von der betroffenen Person erteilten Zustimmung verarbeitet werden dürfen und dass der Empfänger das gleiche Schutzniveau vorsieht wie die Grundsätze und er die Organisation entsprechend unterrichten muss, wenn er feststellt, dass er diese Verpflichtung nicht mehr erfüllen kann. Der Vertrag muss festlegen, dass im Falle einer derartigen Festlegung der als Verantwortlicher tätige Dritte die Verarbeitung einstellt oder mit anderen sinnvollen und geeigneten Maßnahmen Abhilfe schafft.

b. Bei der Weitergabe von personenbezogenen Daten an einen Dritten, der in ihrem Auftrag und auf ihre Anweisung tätig ist, gilt für eine Organisation Folgendes: i) sie darf diese Daten nur in begrenztem Rahmen für bestimmte Zwecke weitergeben; ii) sie muss sich vergewissern, dass der Beauftragte verpflichtet ist, zumindest das Maß an Schutz personenbezogener Daten zu gewährleisten, das in den Grundsätzen gefordert wird; iii) sie muss mit angemessenen und geeigneten Schritten sicherstellen, dass der Beauftragte die weitergegebenen personenbezogenen Daten in einer den Verpflichtungen der Organisation im Rahmen der Grundsätze konformen Weise verarbeitet; iv) sie muss vom Beauftragten verlangen, dass er sie unterrichtet, wenn er feststellt, dass er seine Verpflichtung, das gleiche Schutzniveau vorzusehen wie in den Grundsätzen gefordert, nicht mehr erfüllen kann, v) sie muss auf entsprechenden Hinweis, einschließlich nach iv), sinnvolle und geeignete Schritte unternehmen, um eine unbefugte Verarbeitung zu unterbinden; vi) sie muss dem Ministerium auf Verlangen eine Zusammenfassung oder ein Exemplar der einschlägigen Datenschutzbestimmungen ihres Vertrags mit diesem Beauftragten vorlegen.

4. **Sicherheit**

a. Organisationen, die personenbezogene Daten erstellen, verwalten, verwenden oder verbreiten, müssen angemessene und geeignete Maßnahmen ergreifen, um sie vor Verlust, Missbrauch und unbefugtem Zugriff, Weitergabe, Änderung und Zerstörung zu schützen; dabei sind insbesondere die Risiken bei der Verarbeitung und die Art der personenbezogenen Daten zu berücksichtigen.

5. **Datenintegrität und Zweckbindung**

a. In Übereinstimmung mit den Grundsätzen müssen personenbezogene Daten auf die Informationen beschränkt sein, die für den Verarbeitungszweck erheblich sind ([1]). 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. In dem für diese Zwecke notwendigen Umfang muss die Organisation durch angemessene Maßnahmen gewährleisten, dass die personenbezogenen Daten für den vorgesehenen Zweck hinreichend zuverlässig, genau, vollständig und aktuell sind. Die Organisation muss die Grundsätze so lange einhalten, wie sie diese Informationen aufbewahrt.

b. Die Daten dürfen nur so lange in einer Form aufbewahrt werden, die eine Person identifiziert oder identifizierbar macht ([2]), wie damit ein Verarbeitungszweck im Sinne von 5a erfüllt wird. Diese Verpflichtung hindert Organisationen nicht daran, personengebundene Informationen über längere Zeiträume zu verarbeiten, solange und soweit diese Verarbeitung hinreichend den Zwecken einer Archivierung im öffentlichen Interesse, des Journalismus, der Literatur und Kunst, der wissenschaftlichen oder historischen Forschung und der statistischen Analyse dient. In diesen Fällen unterliegt die Verarbeitung den anderen Grundsätzen und Bestimmungen der Regelung. Die Organisationen sollen zur Einhaltung dieser Bestimmung angemessene und geeignete Maßnahmen ergreifen.

6. **Auskunftsrecht**

a. Privatpersonen müssen Zugang zu den personenbezogenen Daten haben, die eine Organisation über sie besitzt, und sie müssen die Möglichkeit haben, diese zu korrigieren, zu ändern oder zu löschen, wenn sie falsch sind oder unter Missachtung der Grundsätze verarbeitet wurden, es sei denn, die Belastung oder die Kosten für die Gewährung des Zugangs würden in dem jeweiligen Fall in einem Missverhältnis zu den Nachteilen für den Betroffenen stehen, oder Rechte anderer Personen als des Betroffenen würden verletzt.

([1]) Je nach Sachlage kommt als zulässiger Zweck für die Verarbeitung beispielsweise Folgendes in Frage: Pflege von Kundenbeziehungen, Compliance-Erwägungen und rechtliche Erwägungen, Wirtschaftsprüfung, Sicherheit und Betrugsprävention, Erhaltung oder Wahrung der Rechte der Organisation oder andere Zwecke, die nach vernünftigem Ermessen den Erwartungen im Zusammenhang mit der Erhebung entsprechen.

([2]) In diesem Zusammenhang gilt eine Person als „identifizierbar", wenn sie in Anbetracht der mit hinreichender Wahrscheinlichkeit genutzten Mittel der Identifizierung (z. B. unter Berücksichtigung des Kosten- und Zeitaufwands für die Identifizierung und der zum Zeitpunkt der Verarbeitung verfügbaren Technik) und der Aufbewahrungsform der Daten nach vernünftigem Ermessen von der Organisation oder von einem Dritten mit Zugriff auf die Daten identifiziert werden kann.

7. **Rechtsschutz, Durchsetzung und Haftung**

a. Für einen effektiven Schutz der Privatsphäre müssen belastbare Mechanismen geschaffen werden, die die Einhaltung der Grundsätze gewährleisten, Rechtsbehelfe für Betroffene vorsehen, bei deren Daten die Grundsätze nicht eingehalten wurden, sowie Sanktionen für die Organisation, die die Grundsätze nicht befolgt. Diese Mechanismen müssen mindestens Folgendes umfassen:

i. leicht zugängliche, von unabhängigen Stellen durchgeführte Verfahren, nach denen Beschwerden, die betroffene Personen unter Berufung auf die Grundsätze erhoben haben, ohne Kosten für den Betroffenen untersucht und zügig behandelt werden und nach denen Schadenersatz geleistet wird, wenn das geltende Recht oder private Regelungen dies vorsehen;

ii. Kontrollmaßnahmen, um zu überprüfen, ob die Bescheinigungen und Behauptungen der Organisationen über ihre Datenschutzmaßnahmen der Wahrheit entsprechen und ob diese Maßnahmen wie angegeben durchgeführt werden, und insbesondere in Bezug auf Verstöße;

iii. Verpflichtungen zur Lösung von Problemen, die daraus resultieren, dass Organisationen die Einhaltung der Grundsätze zwar erklärt, sich aber trotzdem nicht daran gehalten haben, sowie entsprechende Sanktionen für diese Organisationen. Die Sanktionen müssen hinreichend streng sein, um sicherzustellen, dass die Organisationen die Grundsätze einhalten.

b. Organisationen und die von ihnen gewählten unabhängigen Beschwerdestellen werden rasch auf Anfragen und Auskunftsbegehren des Ministeriums reagieren, die mit dem Datenschutzschild im Zusammenhang stehen. Alle Organisationen müssen zügig auf von Behörden der EU-Mitgliedstaaten über das Ministerium weitergeleitete Beschwerden bezüglich der Einhaltung der Grundsätze reagieren. Organisationen, die sich für eine Zusammenarbeit mit Datenschutzbehörden entschieden haben, einschließlich Organisationen, die Personaldaten verarbeiten, müssen im Zusammenhang mit der Untersuchung und Bearbeitung von Beschwerden unmittelbar auf diese Behörden eingehen.

c. Organisationen sind verpflichtet, Ansprüche im Schiedsverfahren zu regeln und die in Anlage I aufgeführten Bedingungen einzuhalten, sofern eine Privatperson durch Benachrichtigung der betreffenden Organisation und entsprechend den Verfahren und Bedingungen nach Anlage I ein verbindliches Schiedsverfahren beantragt hat.

d. Im Zusammenhang mit einer Weitergabe ist eine dem Datenschutzschild angehörende Organisation für die Verarbeitung der personenbezogenen Daten, die sie im Rahmen des Datenschutzschilds erhält und anschließend an einen Dritten weitergibt, der in ihrem Auftrag und auf ihre Anweisung tätig ist, verantwortlich. Die dem Datenschutzschild angehörende Organisation bleibt nach den Grundsätzen haftbar, wenn ihr Beauftragter diese personenbezogenen Daten auf eine Art und Weise verarbeitet, die nicht im Einklang mit den Grundsätzen steht, es sei denn, sie weist nach, dass sie für das Ereignis, das den Schaden bewirkt hat, nicht verantwortlich ist.

e. Ist gegen eine Organisation eine Anordnung der FTC oder ein Gerichtsbeschluss wegen eines Verstoßes ergangen, macht die Organisation jene Teile eines der FTC vorgelegten Compliance- oder Sachstandsberichts, die den Datenschutzschild betreffen, öffentlich, soweit dies mit den Verpflichtungen zur Geheimhaltung im Einklang steht. Das Ministerium hat eine spezielle Kontaktstelle eingerichtet, an die sich Datenschutzbehörden bei Compliance-Problemen von dem Datenschutzschild angehörenden Organisationen wenden können. Die FTC wird Fälle der Missachtung der Grundsätze, die ihr vom Ministerium und Behörden der EU-Mitgliedstaaten zugeleitet wurden, vorrangig behandeln und vorbehaltlich der geltenden Geheimhaltungsvorschriften zeitnah mit den vorlegenden staatlichen Behörden Informationen zu diesen Fällen austauschen.

III. ZUSATZGRUNDSÄTZE

1. **Sensible Daten**

a. Eine Organisation muss keine ausdrückliche Zustimmung (Opt-in) für die Verarbeitung sensibler Daten einholen, wenn die Verarbeitung

i. im lebenswichtigen Interesse der betroffenen Person oder einer anderen Person liegt;

ii. zur Geltendmachung von Rechtsansprüchen oder für die Rechtsverteidigung notwendig ist;

iii. für eine medizinische Behandlung oder Diagnose erforderlich ist;

iv. durch eine politisch, weltanschaulich, religiös oder gewerkschaftlich ausgerichtete Stiftung, Vereinigung oder sonstige Körperschaft, die keinen Erwerbszweck verfolgt, im Rahmen rechtmäßiger Tätigkeiten und unter der Voraussetzung, dass sich die Verarbeitung ausschließlich auf die Mitglieder der Organisation oder Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßige Kontakte mit ihr unterhalten, beziehen und die Daten nicht ohne Einwilligung der betroffenen Person an Dritte weitergegeben werden;

v. zur Erfüllung der arbeitsrechtlichen Pflichten der Organisation notwendig ist;

vi. sich auf Daten bezieht, die von der Person nachweislich veröffentlicht worden sind.

2. **Ausnahmen für den journalistischen Bereich**

a. Da die Pressefreiheit durch die amerikanische Verfassung geschützt ist und die Richtlinie Ausnahmen für den Fall vorsieht, dass personenbezogene Daten zu journalistischen Zwecken verarbeitet werden, ist für die Interessenabwägung, wenn die im ersten Zusatzartikel zur Verfassung der Vereinigten Staaten verankerte Pressefreiheit mit dem Recht auf Schutz der Privatsphäre kollidiert, der erste Zusatzartikel maßgeblich, soweit es um die Tätigkeit natürlicher oder juristischer Personen in den USA geht.

b. Die Grundsätze des Datenschutzschilds gelten nicht für personenbezogene Daten, die zur Veröffentlichung, zur Verbreitung über Rundfunk und Fernsehen oder für andere Formen öffentlicher Kommunikation gesammelt werden, unabhängig davon, ob sie tatsächlich genutzt werden oder nicht, ebenso nicht für früher veröffentlichtes Material, das aus Medienarchiven stammt.

3. **Hilfsweise Haftung**

a. Internetdienstanbieter (Internet Service Providers, „ISP"), Telekommunikationsunternehmen und andere Organisationen sind nicht nach den Grundsätzen haftbar, wenn sie im Namen einer anderen Organisation Daten lediglich übermitteln, weiterleiten oder zwischenspeichern. Wie auch die Richtlinie selbst begründet der Datenschutzschild keine hilfsweise Haftung. Soweit eine Organisation personenbezogene Daten Dritter nur weiterleitet und weder Mittel noch Zweck ihrer Verarbeitung bestimmt, ist sie nicht haftbar.

4. **Due-Diligence-Prüfung und Wirtschaftsprüfung**

a. Bei der Tätigkeit von Investmentbanken und Wirtschaftsprüfern kann es vorkommen, dass personenbezogene Daten ohne Wissen und Einwilligung des Betroffenen verarbeitet werden. Dies ist unter den nachfolgend aufgeführten Voraussetzungen mit den Grundsätzen der Informationspflicht, des Wahlrechts und des Auskunftsrechts vereinbar.

b. Aktiengesellschaften und personenbezogene Aktiengesellschaften, einschließlich dem Datenschutzschild angehörende Organisationen, werden regelmäßig einer Wirtschaftsprüfung unterzogen. Diese Prüfungen, vor allem wenn damit ein potenzielles Fehlverhalten untersucht wird, können in Gefahr geraten, wenn sie vorzeitig bekannt werden. Eine dem Datenschutzschild angehörende Organisation, bei der eine Fusion oder Übernahme ansteht, muss zudem eine Due-Diligence-Prüfung durchführen oder ist Gegenstand einer derartigen Prüfung. Dabei werden oft personenbezogene Daten erhoben und verarbeitet, wie z. B. Informationen über Führungskräfte und andere Leistungsträger. Eine vorzeitige Bekanntgabe könnte den Abschluss behindern oder gegen geltende Wertpapiervorschriften verstoßen. Investmentbanken und Rechtsanwälte, die eine Due-Diligence-Prüfung durchführen, oder Wirtschaftsprüfer können personenbezogene Daten ohne Wissen des Betroffenen nur verarbeiten, soweit und solange das aufgrund gesetzlicher oder im öffentlichen Interesse liegender Erfordernisse notwendig ist, und können das auch in anderen Fällen, wenn die Anwendung der Grundsätze ihren legitimen Interessen zuwiderlaufen würde. Legitim sind u. a. die Kontrolle von Organisationen auf Erfüllung ihrer gesetzlichen Pflichten, die Prüfung ihrer Rechnungslegung und die Wahrung der Vertraulichkeit von Informationen betreffend mögliche Übernahmen, Fusionen und Joint Ventures sowie ähnliche Vorgänge, die von Investmentbanken oder Wirtschaftsprüfern abgewickelt werden.

5. **Die Rolle der Datenschutzbehörden**

a. Die Organisationen werden ihre Verpflichtung zur Zusammenarbeit mit Datenschutzbehörden der Europäischen Union wie nachfolgend dargelegt umsetzen. Nach den Grundsätzen des Datenschutzschilds müssen in den USA ansässige Organisationen, die personenbezogene Daten aus der EU erhalten, mit geeigneten Mitteln dafür sorgen, dass diese Grundsätze gewahrt werden. Wie im Grundsatz des Rechtsschutzes, der Durchsetzung und der Haftung beschrieben, gehören zu diesen Mitteln a)i) Rechtsbehelfe für Personen, über die die Organisationen Daten besitzen, a)ii) Verfahren, mit denen sie überprüfen, ob ihre Aussagen und Zusicherungen betreffend ihre Datenschutzpraxis den Tatsachen entsprechen; a)iii) die Pflicht der Organisationen, Abhilfe zu schaffen, falls es zu Problemen kommt, weil die Grundsätze bei ihnen nicht gewahrt werden, sowie Sanktionen für Verstöße gegen diese Grundsätze. Den Punkten a)i) und a)iii) des Grundsatzes des Rechtsschutzes, der Durchsetzung und der Haftung können Organisationen dadurch entsprechen, dass sie die hier festgelegten Anforderungen zur Zusammenarbeit mit den Datenschutzbehörden einhalten.

b. Eine Organisation verpflichtet sich zur Zusammenarbeit mit den Datenschutzbehörden, indem sie in der Mitteilung über die Selbstzertifizierung gegenüber dem Handelsministerium (*siehe* Zusatzgrundsatz „Selbstzertifizierung") Folgendes erklärt:

i. dass sie den Bestimmungen der Punkte a)i) und a)iii) des Datenschutzschild-Grundsatzes des Rechtsschutzes, der Durchsetzung und der Haftung entsprechen will, indem sie sich zur Zusammenarbeit mit den entsprechenden Datenschutzbehörden verpflichtet;

ii. dass sie mit den entsprechenden Datenschutzbehörden bei der Untersuchung und Behandlung von Beschwerden zusammenarbeiten will, die unter Berufung auf die Grundsätze des Datenschutzschilds erhoben werden;

iii. dass sie sich an die Empfehlung der entsprechenden Datenschutzbehörden hält, wenn diese der Organisation aufgeben, spezifische Maßnahmen zu treffen, um den Grundsätzen des Datenschutzschilds zu entsprechen; hierzu gehören auch Rechtsmittel und Entschädigungsleistungen zugunsten von Personen, die infolge Nichteinhaltung der Grundsätze Nachteile erlitten haben; ferner, dass sie den entsprechenden Datenschutzbehörden schriftlich die Durchführung dieser Maßnahmen bestätigt.

c. Tätigkeit von Gremien der Datenschutzbehörden

i. Die Kooperation der Datenschutzbehörden erfolgt über Information und Beratung:

1. Die Beratung übernimmt ein informelles Gremium, in dem europäische Datenschutzbehörden vertreten sind, so dass u. a. ein einheitlicher schlüssiger Ansatz gewährleistet wird.

2. Das Gremium berät die betreffenden US-amerikanischen Organisationen bei ungeklärten Beschwerden von Einzelpersonen über den Umgang mit personenbezogenen Daten, die aus der EU im Rahmen des Datenschutzschilds übermittelt wurden. Diese Beratung soll gewährleisten, dass die Grundsätze des Datenschutzschilds korrekt angewendet werden; sie schließt die Rechtsmittel für die betroffene(n) Einzelperson(en) ein, die die Datenschutzbehörden für angemessen erachten.

3. Das Gremium erbringt derartige Beratungsleistungen auf Anfrage der betreffenden US-Organisationen und/oder auf direkt eingegangene Beschwerden von Einzelpersonen gegen Organisationen, die sich auf die Grundsätze des Datenschutzschilds und zur Zusammenarbeit mit den Datenschutzbehörden verpflichtet haben. Dabei ermutigt es die betroffenen Einzelpersonen zunächst, die verfügbaren internen Verfahren zur Behandlung von Beschwerden, die die Organisation bereitstellt, zu nutzen, und unterstützt sie erforderlichenfalls dabei.

4. 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. Grundsätzlich wird das Gremium sich bemühen, die Beratung binnen sechzig Tagen nach Eingang einer Beschwerde oder dem Ersuchen einer Organisation anzubieten, und falls möglich noch rascher.

5. Soweit es ihm angemessen erscheint, veröffentlicht das Gremium die Ergebnisse der Beschwerdeprüfungen.

6. Die Beratung ist weder für das Gremium selbst noch für eine der beteiligten Datenschutzbehörden mit irgendeiner Form der Haftung verbunden.

ii. Organisationen, die sich für diese Form der Streitbeilegung entscheiden, müssen sich verpflichten, den Empfehlungen der Datenschutzbehörden zu folgen. 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 Federal Trade Commission, das Verkehrsministerium oder eine andere Stelle zu verweisen, die Zuständigkeit bzw. Durchsetzungsgewalt in Fällen von Irreführung oder unrichtiger Erklärung besitzt. Oder es teilt mit, dass es zu dem Schluss gelangt ist, dass eine gravierende Verletzung der Kooperationsvereinbarung vorliegt und diese mithin null und nichtig ist. In diesem Fall unterrichtet das Gremium das Handelsministerium, so dass die Datenschutzschild-Liste entsprechend geändert werden kann. Jede Unterlassung der Zusammenarbeit und jeder Verstoß gegen die Grundsätze des Datenschutzschilds können als Irreführung gemäß § 5 des FTC Act oder anderen vergleichbaren Gesetzen rechtlich verfolgt werden.

d. Wünscht eine Organisation, dass ihr die Vorteile des Datenschutzschilds auch bei Personaldaten zuteilwerden, die zur Verwendung im Rahmen von Beschäftigungsverhältnissen aus der EU übermittelt werden, muss es sich in Bezug auf diese Daten zur Zusammenarbeit mit den Datenschutzbehörden verpflichten (*siehe* Zusatzgrundsatz „Personaldaten").

e. Organisationen, die sich für diese Option entscheiden, zahlen eine Jahresgebühr, die dazu bestimmt ist, die laufenden Kosten des Gremiums der Datenschutzbehörden zu decken; ferner können sie zur Begleichung der Kosten für alle erforderlichen Übersetzungen herangezogen werden, die sich aus der Beratungstätigkeit des Gremiums im Zusammenhang mit Beschwerden gegenüber den Organisationen ergeben. Die Jahresgebühr beträgt höchstens 500 USD und ist für kleinere Organisationen geringer.

6. **Selbstzertifizierung**

a. In den Genuss der Vorteile des Datenschutzschilds kommt eine Organisation ab dem Tag, an dem das Ministerium ihren Selbstzertifizierungsantrag nach Feststellung der Vollständigkeit in die Datenschutzschild-Liste aufgenommen hat.

b. Um sich für den Datenschutzschild selbst zu zertifizieren, muss die Organisation dem Ministerium einen von einem leitenden Mitarbeiter im Namen der Organisation unterzeichneten Selbstzertifizierungsantrag einreichen, der mindestens folgende Angaben enthält:

i. Name der Organisation, Postanschrift, E-Mail-Adresse, Telefon- und Faxnummer;

ii. Beschreibung der Tätigkeit der Organisation im Zusammenhang mit personenbezogenen Daten aus der EU;

iii. Beschreibung der Datenschutzbestimmungen der Organisation, die folgende Angaben umfassen muss:

1. ob die Organisation über eine öffentliche Website verfügt, die entsprechende Webadresse, unter der diese Beschreibung eingesehen kann, oder, wenn die Organisation nicht über eine öffentliche Website verfügt, der Ort, an dem diese Beschreibung von der Öffentlichkeit eingesehen werden kann;

2. Tag, an dem diese Vorkehrungen in Kraft gesetzt wurden;

3. Kontaktstelle, die für die Bearbeitung von Beschwerden, Auskunftsersuchen und anderen Angelegenheiten des Datenschutzschilds zuständig ist;

4. die gesetzliche Aufsichtsbehörde, die über Beschwerden gegen die Organisation wegen unlauteren oder irreführenden Geschäftsgebarens und wegen Verletzung von datenschutzrechtlichen Vorschriften entscheidungsbefugt ist (und in den Grundsätzen oder in einem künftigen Anhang zu den Grundsätzen aufgeführt ist);

5. die Bezeichnungen aller Datenschutzprogramme, an denen die Organisation teilnimmt;

6. die Art der anlassunabhängigen Kontrolle (z. B. intern oder extern) (*siehe* Zusatzgrundsatz „Anlassunabhängige Kontrolle“);

7. die unabhängige Beschwerdestelle zur Behandlung ungeklärter Beschwerdefälle.

c. Wenn die Organisation wünscht, dass ihr die Vorteile des Datenschutzschilds auch bei Personaldaten zuteilwerden, die zur Verwendung im Rahmen von Beschäftigungsverhältnissen aus der EU übermittelt werden, so ist dies möglich, wenn eine in den Grundsätzen oder in einem künftigen Anhang zu den Grundsätzen aufgeführte gesetzliche Aufsichtsbehörde befugt ist, Beschwerden gegen die Organisation aufgrund der Verarbeitung von Personaldaten entgegenzunehmen. Darüber hinaus muss die Organisation darauf in ihrem Selbstzertifizierungsantrag hinweisen und sich bereit erklären, gemäß den Zusatzgrundsätzen „Personaldaten“ und „Rolle der Datenschutzbehörden“, soweit anwendbar, mit der (den) Datenschutzbehörde(n) in der EU zusammenzuarbeiten und den Empfehlungen dieser Behörden nachzukommen. Außerdem muss die Organisation dem Ministerium ihre Datenschutzbestimmungen für Personaldaten sowie Angaben dazu übermitteln, wo die Datenschutzbestimmungen von den betroffenen Mitarbeitern eingesehen werden können.

d. Das Ministerium führt die Datenschutzschild-Liste der Organisationen, die Selbstzertifizierungsanträge eingereicht haben und denen damit die Vorteile des Datenschutzschilds zustehen; die Liste wird anhand der jährlich eingereichten Selbstzertifizierungsanträge und der Meldungen aktualisiert, die gemäß dem Zusatzgrundsatz „Beschwerdeverfahren und Durchsetzung“ eingehen. Diese Selbstzertifizierungsanträge sind mindestens jährlich neu vorzulegen, andernfalls wird die Organisation von der Datenschutzschild-Liste gestrichen, und die Vorteile des Datenschutzschilds sind nicht mehr garantiert. Die Datenschutzschild-Liste und die von den Organisationen vorgelegten Selbstzertifizierungsanträge werden der Öffentlichkeit zugänglich gemacht. Alle Organisationen, die vom Ministerium auf die Datenschutzschild-Liste gesetzt werden, müssen in ihren relevanten veröffentlichten Datenschutzbestimmungen auch erklären, dass sie sich an die Grundsätze des

Datenschutzschilds halten. Wenn die Datenschutzbestimmungen einer Organisation online verfügbar sind, müssen sie mit einem Hyperlink zur Website des Datenschutzschilds beim Ministerium versehen sein sowie mit einem Hyperlink zur Website oder dem Beschwerdeformular der unabhängigen Beschwerdestelle, die ungeklärte Beschwerden prüft.

e. Die Datenschutzgrundsätze werden bei Zertifizierung unverzüglich wirksam. In Anbetracht der Tatsache, dass sich die Grundsätze auf die Geschäftsbeziehungen zu Dritten auswirken, werden Organisationen, die sich innerhalb der ersten zwei Monate nach Inkrafttreten der Datenschutzschild-Regelung dafür zertifizieren, ihre bestehenden Geschäftsbeziehungen zu Dritten so bald wie möglich, spätestens jedoch neun Monate nach ihrer Zertifizierung gegenüber dem Datenschutzschild, mit dem Grundsatz der Verantwortlichkeit für die Weitergabe in Übereinstimmung bringen. In diesem Übergangszeitraum werden die Organisationen bei der Übermittlung von Daten an einen Dritten i) die Grundsätze der Informationspflicht und der Wahlmöglichkeit anwenden und sich ii) bei Übergabe personenbezogener Daten an einen Dritten, der in ihrem Auftrag und auf ihre Anweisung tätig ist, vergewissern, dass der Beauftragte mindestens das Schutzniveau gewährleistet, das in den Grundsätzen gefordert wird.

f. Eine Organisation muss die Grundsätze des Datenschutzschilds auf alle unter Bezugnahme auf den Datenschutzschild aus der EU empfangenen personenbezogenen Daten anwenden. Die Verpflichtung auf die Grundsätze des Datenschutzschilds gilt ohne zeitliche Begrenzung für personenbezogene Daten, die der Organisation übermittelt wurden, während sie in den Genuss der Vorteile des Datenschutzschilds gelangte. Diese Daten unterliegen den Grundsätzen so lange, wie die Organisation sie speichert, verarbeitet oder weitergibt, und das auch dann noch, wenn sie aus welchem Grund auch immer den Datenschutzschild verlässt. Eine Organisation, die aus dem Datenschutzschild ausscheidet, diese Daten aber behalten möchte, muss sich dem Handelsministerium gegenüber jährlich dazu verpflichten, die Grundsätze weiterhin anzuwenden, oder für den „angemessenen" Schutz der Daten durch andere zulässige Mittel sorgen (z. B. durch einen Vertrag, der den Anforderungen der von der Europäischen Kommission gebilligten einschlägigen Standardklauseln vollauf genügt); andernfalls muss die Organisation die Daten zurückgeben oder löschen. Eine Organisation, die aus dem Datenschutzschild ausscheidet, muss aus den relevanten Datenschutzbestimmungen jede Bezugnahme auf den Datenschutzschild entfernen, die darauf hindeutet, dass sich die Organisationen weiterhin aktiv am Datenschutzschild beteiligt und Anspruch auf die damit verbundenen Vorteile hat.

g. Eine Organisation, die aufgrund einer Fusion oder einer Übernahme ihren Status als selbstständige rechtliche Einheit verliert, muss dies dem Ministerium vorher mitteilen. In dieser Mitteilung sollte auch darauf hingewiesen werden, ob die übernehmende Einheit bzw. die Einheit, die aus der Fusion hervorgeht, i) weiterhin nach dem Gesetz, das für die Fusion oder Übernahme maßgeblich war, an die Grundsätze des Datenschutzschilds gebunden ist oder ii) entscheidet, ihren Beitritt zu den Grundsätzen des Datenschutzschildes selbst zu zertifizieren, bzw. andere Garantien, beispielsweise durch schriftliche Vereinbarungen, schafft, die die Einhaltung der Grundsätze des Datenschutzschilds gewährleisten. Ist weder i) noch ii) der Fall, müssen alle Daten, die im Rahmen des Datenschutzschilds gesammelt wurden, unverzüglich gelöscht werden.

h. Wenn eine Organisation aus welchem Grund auch immer den Datenschutzschild verlässt, muss sie alle Erklärungen entfernen, die darauf hindeuten, dass sie sich weiter am Datenschutzschild beteiligt oder Ansprüche auf die damit verbundenen Vorteile hat. Wurde das Gütesiegel des EU-US-Datenschutzschilds verwendet, ist auch dies zu entfernen. Bei falschen Angaben über die Einhaltung der Datenschutzgrundsätze, die die Organisation gegenüber der Öffentlichkeit macht, können die FTC oder andere zuständige staatliche Stellen gegen sie vorgehen. Falsche Angaben gegenüber dem Ministerium unterliegen dem False Statements Act (18 U.S.C. § 1001).

7. **Anlassunabhängige Kontrolle**

a. Organisationen müssen sich anhand von Kontrollverfahren vergewissern, dass der von ihnen zugesicherte Datenschutz im Rahmen des Datenschutzschilds tatsächlich besteht und dass ihre Datenschutzpolitik tatsächlich umgesetzt worden ist und den Grundsätzen des Datenschutzschilds entspricht.

b. Die nach dem Grundsatz des Rechtschutzes, der Durchsetzung und der Haftung erforderliche anlassunabhängige Kontrolle muss eine Organisation entweder selbst durchführen oder von einer externen Stelle durchführen lassen.

c. Im Falle der Selbstkontrolle muss die Organisation in einer Erklärung feststellen, dass ihre veröffentlichten Datenschutzbestimmungen betreffend personenbezogene Daten aus der EU sachgerecht, umfassend, an auffälliger Stelle bekannt gemacht, vollständig umgesetzt und für jedermann zugänglich sind. Sie muss ferner feststellen, dass ihre Datenschutzbestimmungen den Grundsätzen des Datenschutzschilds entsprechen, dass betroffene Personen über interne Beschwerdeverfahren und Beschwerdeverfahren bei unabhängigen Schiedsstellen informiert werden, dass sie ihre Beschäftigten systematisch in der Praxis des Datenschutzes unterweist und Verstöße gegen die Datenschutzregeln ahndet und dass es bei ihr interne Verfahren gibt, nach

denen die Einhaltung der Datenschutzvorschriften regelmäßig und objektiv überprüft wird. Die Selbstkontrolle muss mindestens einmal jährlich stattfinden, eine Erklärung über ihre Durchführung ist von einem leitenden Angestellten oder einem bevollmächtigten Vertreter der Organisation zu unterzeichnen; sie ist vorzulegen auf Verlangen von Einzelpersonen, im Rahmen einer Untersuchung oder bei einer Beschwerde wegen Nichteinhaltung von Datenschutzvorschriften.

d. Bei externer anlassunabhängiger Kontrolle ist nachzuweisen, dass die Bestimmungen der Organisation für den Schutz personenbezogener Daten aus der EU den Grundsätzen des Datenschutzschilds entsprechen, dass diese Regeln eingehalten werden und dass betroffene Personen über die Beschwerdewege informiert werden, die ihnen offenstehen. Dazu können ohne Einschränkung Buchprüfungen und Zufallskontrollen durchgeführt sowie „Köder" und jede Art von technischen Hilfsmitteln eingesetzt werden. Die externe Kontrolle muss mindestens einmal jährlich stattfinden, eine Erklärung über ihre Durchführung ist entweder vom Prüfer oder von einem leitenden Angestellten bzw. einem bevollmächtigten Vertreter der Organisation zu unterzeichnen; sie ist vorzulegen auf Verlangen von Einzelpersonen, im Rahmen einer Untersuchung oder bei einer Beschwerde wegen Nichteinhaltung von Datenschutzvorschriften.

e. Organisationen müssen die Umsetzung ihrer nach den Grundsätzen des Datenschutzschilds konzipierten Datenschutzbestimmungen dokumentieren und im Fall einer Untersuchung oder einer Beschwerde wegen Verletzung der Datenschutzvorschriften ihre Unterlagen der unabhängigen Schiedsstelle übergeben, die für die Prüfung von Beschwerden zuständig ist, oder der gesetzlichen Aufsichtsbehörde, die bei unlauterem und irreführendem Geschäftsgebaren entscheidungsbefugt ist. Die Organisationen müssen zudem unverzüglich auf Anfragen und andere Auskunftsbegehren des Ministeriums reagieren, die sich auf die Einhaltung der Grundsätze beziehen.

8. **Auskunftsrecht**

a. Das Auskunftsrecht in der Praxis

i. Nach den Grundsätzen des Datenschutzschilds ist das Auskunftsrecht grundlegend für den Schutz der Privatsphäre. Es ermöglicht dem Einzelnen, die Richtigkeit von Daten zu überprüfen, die über ihn gespeichert sind. Das Auskunftsrecht bedeutet, dass Privatpersonen einen Anspruch darauf haben,

1. von einer Organisation bestätigt zu bekommen, ob diese personengebundene Daten der betroffenen Person verarbeitet oder nicht ([1]);

2. dass ihnen diese Daten übermittelt werden, damit sie deren Richtigkeit und die Rechtmäßigkeit der Verarbeitung überprüfen können;

3. die Daten korrigieren, ändern oder löschen zu lassen, wenn sie falsch sind oder unter Verletzung der Grundsätze verarbeitet wurden.

ii. Wer Zugang zu den ihn betreffenden Daten verlangt, muss das nicht begründen. Verlangt jemand Zugang zu den über ihn gespeicherten Daten, sollte sich die angesprochene Organisation zunächst fragen, welche Gründe die Person dazu veranlassen. Ist beispielsweise eine Anfrage vage formuliert oder betrifft sie einen sehr weiten Bereich, so kann die Organisation mit der Person in Dialog treten, um die Gründe für die Anfrage besser zu verstehen und die gewünschten Daten zu ermitteln. Die Organisation kann sich danach erkundigen, mit welchen Teilen der Organisation die Person Kontakt hatte oder um welche Art von Daten bzw. deren Nutzung es geht.

iii. Wegen seines grundlegenden Charakters sollen Organisationen das Auskunftsrecht nie ohne Not beschränken. Müssen z. B. bestimmte Daten geschützt werden und lassen sie sich leicht von den personenbezogenen Daten trennen, zu denen Zugang verlangt wird, sollte die Organisation die geschützten Daten unkenntlich machen und die übrigen zur Verfügung stellen. Beschließt eine Organisation in einem bestimmten Fall, den Zugang einzuschränken, sollte sie der Person, die um Zugang ersucht hat, ihre Entscheidung begründen und ihr eine Kontaktstelle nennen, die weitere Auskünfte erteilt.

b. Aufwand oder Kosten für die Gewährung des Zugangs

i. Das Recht auf Zugang zu personenbezogenen Daten darf nur in Ausnahmefällen eingeschränkt werden, wenn legitime Rechte Dritter verletzt würden oder wenn die Zugangsgewährung mit Kosten oder Aufwand verbunden ist, die im Einzelfall in keinem Verhältnis zum Nachteil für die Privatsphäre des Betroffenen stehen. Zwar sind bei der Beurteilung der Zumutbarkeit die Kosten und der Aufwand zu berücksichtigen, die die Gewährung des Zugangs erfordert, sie sind aber nicht entscheidend.

([1]) Die Organisation sollte Anfragen von Privatpersonen zum Zweck der Verarbeitung, zu den Datenkategorien, die verarbeitet werden, sowie zu den Empfängern oder Kategorien der Empfänger der personenbezogenen Daten beantworten.

ii. Bilden die personenbezogenen Daten etwa die Grundlage für Entscheidungen, die für die Person von großer Tragweite sind (z. B. die Gewährung oder Versagung erheblicher Vorteile wie eine Versicherung, einen Kredit oder einen Arbeitsplatz), dann ist es der Organisation im Einklang mit den anderen Bestimmungen dieser Zusatzgrundsätze zumutbar, über diese Daten Auskunft zu geben, selbst wenn das einen relativ hohen Kosten- und Arbeitsaufwand erfordert. Wenn die angeforderten personenbezogenen Daten nicht sensibel sind oder nicht für Entscheidungen verwendet werden, die für die Person von großer Tragweite sind, die Daten aber leicht zugänglich sind und kostengünstig zur Verfügung gestellt werden können, muss die Organisation Zugang zu diesen Daten gewähren.

c. Vertrauliche Geschäftsdaten

i. Vertrauliche Geschäftsdaten sind Daten, die ihr Inhaber durch besondere Vorkehrungen vor unbefugtem Zugriff geschützt hat, weil ihre Kenntnis Konkurrenten Vorteile verschaffen würde. Eine Organisation kann den Zugang zu personenbezogenen Daten verwehren oder einschränken, wenn durch einen vollständigen Zugang eigene vertrauliche Geschäftsdaten, wie z. B. von der Organisation erarbeitete Marketingkonzepte und Klassifikationen, oder aber Geschäftsdaten anderer, die einer vertraglichen Geheimhaltungspflicht unterliegen, offenbart würden.

ii. Können vertrauliche Geschäftsdaten leicht von den personengebundenen Daten getrennt werden, zu denen Zugang verlangt wird, sollte die Organisation die vertraulichen Daten unkenntlich machen und die nichtvertraulichen zur Verfügung stellen.

d. Datenbanken von Organisationen

i. Es genügt, wenn Organisationen der betreffenden Person mitteilen, welche personenbezogenen Daten über sie gespeichert sind; der Person muss kein Zugang zur Datenbank der Organisation gewährt werden.

ii. Die Organisation muss nur Auskunft über die von ihr gespeicherten personenbezogenen Daten geben. Das Auskunftsrecht begründet keine Pflicht, Dateien mit personenbezogenen Daten aufzubewahren, zu pflegen oder erforderlichenfalls umzustrukturieren.

e. Wann eine Beschränkung des Zugangs möglich ist

i. Da Organisationen sich immer redlich bemühen müssen, Privatpersonen Zugang zu ihren personenbezogenen Daten zu verschaffen, ist eine Beschränkung des Zugangs nur in wenigen Fällen möglich und muss stets konkret begründet werden. Wie entsprechend der Richtlinie kann eine Organisation den Zugang zu personenbezogenen Daten insoweit beschränken, als ihre Bekanntgabe wesentliche öffentliche Belange gefährden würde wie die nationale Sicherheit, die Verteidigung oder die öffentliche Sicherheit. Außerdem kann der Zugang verwehrt werden, wenn personenbezogene Daten ausschließlich für wissenschaftliche oder statistische Zwecke verarbeitet werden sollen. Weitere Gründe für die Verweigerung oder Beschränkung des Zugangs sind:

1. Beeinträchtigung des Rechtsvollzugs oder der Rechtsvollstreckung oder eines zivilrechtlichen Verfahrens, einschließlich der Abwehr, Untersuchung und Verfolgung von Straftaten, oder des Rechts auf einen fairen Prozess;

2. die Bekanntgabe der Daten würde die legitimen Rechte oder wichtigen Interessen anderer verletzen;

3. gesetzliche oder andere berufliche Rechte und Pflichten werden verletzt;

4. die Sicherheitsprüfung von Arbeitnehmern oder ein Beschwerdeverfahren oder die Vertraulichkeit im Zusammenhang mit der Neubesetzung von Stellen oder der Umstrukturierung von Organisationen werden beeinträchtigt; oder

5. die Vertraulichkeit ist gefährdet, die bei der Überwachung, bei der Prüfung und bei sonstigen gesetzlich vorgeschriebenen Ordnungsfunktionen im Zusammenhang mit der ordnungsgemäßen Wirtschaftsführung oder bei künftigen oder laufenden Verhandlungen über die Organisation erforderlich ist.

ii. Eine Organisation, die sich auf einen dieser Ausnahmefälle beruft, muss nachweisen, dass er tatsächlich vorliegt, und der anfragenden Person die Gründe für die Beschränkung des Zugangs sowie eine Anlaufstelle für weitere Fragen mitteilen.

f. Recht auf Erhalt einer Bestätigung sowie Erhebung einer Gebühr zur Deckung der Kosten der Zugangserteilung

i. Personen haben das Recht, eine Bestätigung darüber zu erhalten, ob die Organisation sie betreffende personenbezogene Daten besitzt. Ebenso haben Personen ein Recht darauf, dass ihnen die sie betreffenden personenbezogenen Daten mitgeteilt werden. Eine Organisation kann eine Gebühr erheben, die nicht überhöht sein darf.

ii. Die Erhebung einer Gebühr kann beispielsweise gerechtfertigt sein, wenn das Auskunftsbegehren offenkundig überzogen ist, insbesondere bei ständiger Wiederholung.

iii. Der Zugang darf nicht aus Kostengründen verwehrt werden, wenn die Personen, die den Zugang verlangen, bereit sind, diese Kosten zu übernehmen.

g. Wiederholte oder belästigende Auskunftsbegehren

Eine Organisation kann die Zahl der Anfragen einer Person innerhalb eines bestimmten Zeitraums angemessen begrenzen. Bei der Festlegung dieser Grenze sind Faktoren zu berücksichtigen wie die Häufigkeit, mit der Daten aktualisiert werden, der Zweck, für den die Daten verwendet werden, und die Art der Daten.

h. Auskunftserschleichung

Eine Organisation muss nur Auskunft erteilen, wenn die anfragende Person ihre Identität zweifelsfrei nachweist.

i. Frist für die Auskunftserteilung

Eine Organisation soll innerhalb angemessener Frist auf angemessene und eine für die anfragenden Personen leicht verständliche Weise auf Auskunftsbegehren antworten. Organisationen, die betroffene Personen regelmäßig informieren, können einem einzelnen Auskunftsbegehren im Rahmen ihrer regelmäßigen Auskünfte nachkommen, wenn es dadurch nicht zu einer übermäßigen Verzögerung kommt.

9. **Personaldaten**

a. Abdeckung durch den Datenschutzschild

i. Übermittelt eine in der EU ansässige Organisation im Rahmen des Beschäftigungsverhältnisses erhobene personenbezogene Daten über ihre (früheren oder derzeitigen) Beschäftigten an eine Mutterorganisation, eine verbundene Organisation oder eine nicht verbundene Dienstleistungsorganisation in den USA, die sich auf die Grundsätze des Datenschutzschilds verpflichtet hat, so fällt diese Übermittlung in den Anwendungsbereich der Grundsätze des Datenschutzschilds. In einem solchen Fall gelten für die Erhebung der Daten und ihre Verarbeitung vor der Übermittlung die Rechtsvorschriften des EU-Mitgliedstaats, aus dem sie stammen; sämtliche nach diesen Rechtsvorschriften geltende Bedingungen und Beschränkungen der Übermittlung müssen beachtet werden.

ii. Die Grundsätze des Datenschutzschilds gelten nur für die Übermittlung von und den Zugriff auf Daten über identifizierte oder identifizierbare Einzelpersonen. Die Verwendung von statistischen Informationen, die auf aggregierten Beschäftigungsdaten beruhen und keine personenbezogenen Daten enthalten, oder von anonymisierten Daten ist unter dem Datenschutzaspekt unbedenklich.

b. Anwendung der Grundsätze der Informationspflicht und des Wahlrechts

i. Eine Organisation in den USA, die unter Anwendung der Grundsätze des Datenschutzschilds Personaldaten aus der EU empfangen hat, darf diese Dritten nur offenlegen oder diese nur für andere Zwecke nutzen, wenn das mit den Grundsätzen der Informationspflicht und der Wahlmöglichkeit vereinbar ist. Will beispielsweise eine Organisation in den USA Personaldaten einer Organisation in der EU für Zwecke wie Direktmarketing nutzen, muss sie zuvor den betroffenen Personen die Wahlmöglichkeit geben, es sei denn, diese haben bereits der Nutzung der Daten für die jeweiligen Zwecke zugestimmt. Diese Nutzung darf nicht mit den Zwecken unvereinbar sein, zu denen die personengebundenen Daten erhoben wurden oder denen der Betroffene nachträglich zugestimmt hat. Macht ein Beschäftigter von seinem Recht Gebrauch, die Erlaubnis zu versagen, darf das keine Minderung seiner Berufschancen und keine Sanktionen gegen ihn zur Folge haben.

ii. Es ist darauf hinzuweisen, dass aufgrund einiger allgemeingültiger Bedingungen für die Übermittlung von Daten durch bestimmte EU-Mitgliedstaaten die Nutzung der Daten für andere Zwecke auch nach der Übermittlung in Länder außerhalb der EU ausgeschlossen werden kann; solche Bedingungen müssen eingehalten werden.

iii. Außerdem ist den individuellen Datenschutzbedürfnissen der Arbeitnehmer angemessen Rechnung zu tragen. Auf Wunsch könnte etwa der Zugriff auf bestimmte personenbezogene Daten beschränkt werden oder Daten könnten anonymisiert oder Codes/Pseudonymen zugeordnet werden, wenn der tatsächliche Name für den vorgesehenen Zweck nicht benötigt wird.

iv. Die Organisation ist in dem Maß und so lange von der Pflicht zur Information und zur Beachtung der Wahlmöglichkeit befreit, wie es für Beförderungen, Ernennungen und ähnliche Personalentscheidungen notwendig ist.

c. Anwendung des Auskunftsrechts

Im Zusatzgrundsatz „Auskunftsrecht" wird ausgeführt, aus welchen Gründen der Zugang zu Personaldaten beschränkt oder verwehrt werden kann. Selbstverständlich müssen Arbeitgeber in der Europäischen Union Arbeitnehmern aus der EU nach den Rechtsvorschriften ihres Landes Zugang zu Personaldaten gewähren, unabhängig davon, wo diese Daten verarbeitet oder gespeichert werden. Nach den Grundsätzen des Datenschutzschilds muss eine Organisation, die solche Daten in den USA verarbeitet, diesen Zugang direkt oder unter Einschaltung des EU-Arbeitgebers gewährleisten.

d. Rechtsdurchsetzung

i. Soweit personenbezogene Daten nur im Rahmen des Beschäftigungsverhältnisses verwendet werden, bleibt gegenüber dem Arbeitnehmer in erster Linie die in der EU ansässige Organisation verantwortlich. Folglich ist ein europäischer Arbeitnehmer, der gegen die Verwendung der ihn betreffenden Daten Beschwerde erhoben hat (organisationsintern, bei einer externen Stelle oder nach einem tarifvertraglich vorgesehenen Verfahren) und mit dem Ergebnis nicht zufrieden ist, an den zuständigen Datenschutzbeauftragten oder die für arbeitsrechtliche Fragen zuständige Behörde des Landes zu verweisen, in dem er beschäftigt ist. Das gilt auch, wenn für den als unzulässig betrachteten Umgang mit den personenbezogenen Daten die US-Organisation verantwortlich ist, die die Informationen von dem Arbeitgeber erhalten hat, und somit ein Verstoß gegen die Grundsätze des Datenschutzschilds vorliegt. So lässt sich am ehesten klären, wie die einander überschneidenden Bestimmungen des Arbeitsrechts, der Tarifverträge und des Datenschutzrechts miteinander in Einklang zu bringen sind.

ii. Eine auf die Grundsätze des Datenschutzschilds verpflichtete amerikanische Organisation, die Personaldaten, die im Rahmen eines Beschäftigungsverhältnisses aus der Europäischen Union übermittelt wurden, verwendet und wünscht, dass auf solche Übermittlungen die Grundsätze des Datenschutzschilds angewandt werden, muss sich also verpflichten, gegebenenfalls bei Untersuchungen der in der EU jeweils zuständigen Behörden mitzuwirken und deren Empfehlungen zu befolgen.

e. Anwendung des Grundsatzes der Verantwortlichkeit für die Weitergabe

Bei gelegentlichen beschäftigungsbezogenen operativen Erfordernissen der dem Datenschutzschild angehörenden Organisation im Hinblick auf im Rahmen des Datenschutzschilds übertragene personenbezogene Daten, wie z. B. die Buchung von Flügen, Hotelzimmern oder den Abschluss von Versicherungen, kann die Übertragung personenbezogener Daten einer geringen Zahl von Arbeitnehmern an für die Verarbeitung Verantwortliche ohne Anwendung des Auskunftsrechtgrundsatzes oder Abschluss eines Vertrags mit dem als für die Verarbeitung Verantwortlicher tätigen Dritten erfolgen, wie es ansonsten entsprechend dem Grundsatz der Verantwortlichkeit für die Weitergabe notwendig wäre, vorausgesetzt, die dem Datenschutzschild angehörende Organisation hat die Grundsätze der Informationspflicht und der Wahlmöglichkeit eingehalten.

10. **Obligatorische Verträge bei Weitergabe**

a. Datenverarbeitung im Auftrag

i. Wenn personenbezogene Daten aus der EU in den USA im Auftrag verarbeitet werden sollen, muss dafür ein Vertrag geschlossen werden unabhängig davon, ob der Auftragsverarbeiter der Vereinbarung zum Datenschutzschild beigetreten ist oder nicht.

ii. Werden Daten lediglich zur Verarbeitung im Auftrag übermittelt, muss der in der Europäischen Union für die Verarbeitung Verantwortliche darüber stets einen Vertrag schließen, gleich ob die Verarbeitung in oder außerhalb der EU stattfindet und ob der Auftragsverarbeiter dem Datenschutzschild angehört oder nicht. Mit dem Vertrag soll sichergestellt werden, dass der Auftragsverarbeiter

1. nur auf Weisung des für die Verarbeitung Verantwortlichen handelt;

2. die geeigneten technischen und organisatorischen Mittel bereitstellt, die für den Schutz gegen die zufällige oder unrechtmäßige Zerstörung, den zufälligen Verlust, die unberechtigte Änderung, die unberechtigte Weitergabe oder den unberechtigten Zugang erforderlich sind und weiß, ob eine Weitergabe zulässig ist;

3. unter Berücksichtigung der Art der Verarbeitung den für die Verarbeitung Verantwortlichen dabei unterstützt, auf Privatpersonen einzugehen, die ihre Rechte im Rahmen der Grundsätze wahrnehmen.

iii. Da die dem Datenschutzschild angehörenden Organisationen einen angemessenen Schutz gewähren, ist bei reinen Verarbeitungsverträgen mit diesen Organisationen keine vorherige Genehmigung erforderlich (oder die Genehmigung wird von dem jeweiligen EU-Mitgliedstaat automatisch erteilt), wie sie bei Verträgen mit Empfängern, die sich nicht auf die Grundsätze des Datenschutzschilds verpflichtet haben bzw. nicht auf andere Weise einen angemessenen Schutz bieten, erforderlich wäre.

b. Datenübermittlung innerhalb einer kontrollierten Gruppe von Unternehmen

Werden personengebundene Daten zwischen zwei für die Verarbeitung Verantwortlichen innerhalb einer kontrollierten Gruppe von Unternehmen übermittelt, ist ein Vertrag nach dem Grundsatz der Vertraulichkeit der Weitergabe nicht immer erforderlich. Für die Verarbeitung Verantwortliche innerhalb einer kontrollierten Gruppe von Unternehmen können für diese Übermittlungen andere Instrumente zugrunde legen, wie z. B. verbindliche unternehmensinterne Vorschriften der EU oder andere konzerninterne Instrumente (z. B. Compliance- und Kontrollprogramme), um die Kontinuität des Schutzes personenbezogener Daten im Rahmen der Grundsätze zu sichern. Bei einer derartigen Übermittlung bleibt die dem Datenschutzschild angehörende Organisation für die Einhaltung der Grundsätze verantwortlich.

c. Datenübermittlung zwischen für die Verarbeitung Verantwortlichen

Bei der Übermittlung von Daten zwischen für die Verarbeitung Verantwortlichen muss der Empfänger keine dem Datenschutzschild angehörende Organisation sein oder über eine unabhängige Beschwerdestelle verfügen. Die dem Datenschutz angehörende Organisation muss einen Vertrag mit dem empfangenden externen für die Verarbeitung Verantwortlichen schließen, der das gleiche Schutzniveau wie im Rahmen des Datenschutzschilds vorsieht, wobei es nicht erforderlich ist, dass der als für die Verarbeitung Verantwortlicher tätige Dritte eine dem Datenschutzschild angehörende Organisation ist oder über eine unabhängige Beschwerdestelle verfügen muss, vorausgesetzt, er stellt ein gleichwertiges Beschwerdeverfahren zur Verfügung.

11. **Beschwerdeverfahren und Durchsetzung**

a. Im Grundsatz des Rechtsschutzes, der Durchsetzung und der Haftung ist festgelegt, wie dem Datenschutzschild Geltung zu verschaffen ist. Wie Punkt a)ii) des Grundsatzes zu entsprechen ist, wird im Zusatzgrundsatz „Anlassunabhängige Kontrolle“ ausgeführt. Der vorliegende Zusatzgrundsatz befasst sich mit den Punkten a)i) und a)iii), die beide die Forderung nach unabhängigen Beschwerdestellen enthalten. Das Beschwerdeverfahren kann auf verschiedene Weise ausgestaltet werden, es muss aber die im Grundsatz des Rechtsschutzes, der Durchsetzung und der Haftung genannten Anforderungen erfüllen. Organisationen erfüllen die Anforderungen wie folgt: i) indem sie von der Privatwirtschaft entwickelte Datenschutzprogramme befolgen, in deren Regeln die Grundsätze des Datenschutzschilds integriert sind und die wirksame Durchsetzungsmechanismen vorsehen, wie sie im Grundsatz des Rechtsschutzes, der Durchsetzung und der Haftung beschrieben sind; ii) indem sie sich gesetzlich oder durch Rechtsverordnung vorgesehenen Kontrollorganen unterwerfen, die Beschwerden von Einzelpersonen nachgehen und Streitigkeiten schlichten; iii) indem sie sich verpflichten, mit den Datenschutzbehörden in der Europäischen Union oder mit deren bevollmächtigten Vertretern zusammenzuarbeiten.

b. Die hier angeführten Möglichkeiten sind Beispiele, es handelt sich nicht um eine abschließende Aufzählung. Die Privatwirtschaft kann auch andere Durchsetzungsmechanismen einführen, sie müssen nur die Forderungen erfüllen, die im Grundsatz des Rechtsschutzes, der Durchsetzung und der Haftung und in den Zusatzgrundsätzen

niedergelegt sind. Zu beachten ist, dass die Forderungen des Grundsatzes des Rechtsschutzes, der Durchsetzung und der Haftung die Forderung ergänzen, wonach auch bei freiwilliger Selbstkontrolle Verstöße gegen die Grundsätze gemäß § 5 des Federal Trade Commission Act oder einem ähnlichen Gesetz verfolgbar sein müssen.

c. Um die Einhaltung ihrer Verpflichtungen im Rahmen des Datenschutzschilds zu gewährleisten und die Verwaltung des Programms zu unterstützen, müssen Organisationen sowie deren unabhängige Beschwerdestellen dem Ministerium auf Anfrage Informationen zum Datenschutzschild übermitteln. Darüber hinaus müssen die Organisationen umgehend auf von den Datenschutzbehörden über das Ministerium an sie weitergeleitete Beschwerden bezüglich ihrer Einhaltung der Grundsätze antworten. In der Antwort soll darauf eingegangen werden, ob die Beschwerde begründet ist, und wenn ja, wie die Organisation den Missstand zu beheben gedenkt. Das Ministerium wird die Vertraulichkeit der bei ihm eingegangenen Informationen gemäß dem US-Recht wahren.

d. Anrufung unabhängiger Beschwerdestellen

i. Die Verbraucher sollen dazu angehalten werden, Beschwerden zunächst an die Organisation zu richten, die ihre Daten verarbeitet, ehe sie eine unabhängige Beschwerdestelle anrufen. Organisationen müssen dem Verbraucher innerhalb von 45 Tagen nach Eingang einer Beschwerde antworten. Die Unabhängigkeit einer Beschwerdestelle ist an verschiedenen Merkmalen erkennbar wie Unparteilichkeit, transparente Besetzung und Finanzierung oder nachweisbare einschlägige Tätigkeit. Wie im Grundsatz des Rechtsschutzes, der Durchsetzung und der Haftung gefordert, müssen einem Beschwerdeführer kostenlose Rechtsbehelfe ohne Weiteres zur Verfügung stehen. Eine Beschwerdestelle muss jede von einer Einzelperson vorgetragene Beschwerde prüfen, es sei denn, sie ist offensichtlich unbegründet oder nicht ernsthaft. Der Betreiber der Beschwerdestelle kann allerdings Kriterien für die Zulässigkeit von Beschwerden festlegen. Diese Kriterien sollen transparent und einsichtig sein (z. B. Ausschluss von Beschwerden, die nicht unter das jeweilige Datenschutzprogramm fallen oder die in die Zuständigkeit einer anderen Stelle fallen) und sollen nicht zu einer Lockerung der Pflicht führen, berechtigten Beschwerden nachzugehen. Beschwerdestellen sollen Beschwerdeführer zudem umfassend und in leicht zugänglicher Form über den Ablauf des Verfahrens informieren. Zu diesen Informationen gehören auch Angaben über die Datenschutzpraxis der Beschwerdestelle im Einklang mit den Grundsätzen des Datenschutzschilds. Ferner sind die Stellen gehalten, sich an der Erarbeitung von Hilfsmitteln, die das Verfahren vereinfachen, wie z. B. Standardformularen für Beschwerden, zu beteiligen.

ii. Unabhängige Beschwerdestellen müssen auf ihren öffentlichen Websites Informationen zu den Grundsätzen des Datenschutzschilds und zu den von ihnen in diesem Rahmen erbrachten Dienstleistungen veröffentlichen. Diese Informationen müssen Folgendes umfassen: 1) Angaben über die Anforderungen an unabhängige Beschwerdestellen in den Grundsätzen des Datenschutzschilds oder einen Link zu diesen Anforderungen; 2) einen Link zur Datenschutzschild-Website des Ministeriums; 3) einen Hinweis, dass das Beschwerdeverfahren im Rahmen des Datenschutzschilds für Privatpersonen kostenlos ist; 4) eine Beschreibung, wie eine Beschwerde im Zusammenhang mit dem Datenschutzschild eingereicht werden kann; 5) Bearbeitungsfristen für Beschwerden im Zusammenhang mit dem Datenschutzschild; 6) eine Beschreibung der Palette möglicher Abhilfemaßnahmen.

iii. Die unabhängigen Beschwerdestellen müssen alljährlich einen Bericht vorlegen, der zusammengefasste statistische Angaben zu ihren Dienstleistungen beinhaltet. 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; 4) die Ergebnisse der eingegangenen Beschwerden, namentlich Anzahl und Art der verfügten Abhilfemaßnahmen oder Sanktionen.

iv. Wie in Anlage I ausgeführt, steht Privatpersonen ein Schiedsverfahren offen, anhand dessen bei Restansprüchen festgestellt wird, ob eine dem Datenschutzschild angehörende Organisation ihre Pflichten im Rahmen der Grundsätze gegenüber der betreffenden Person verletzt hat und ob diese Verletzung vollständig oder teilweise ungeahndet bleibt. Diese Option steht nur für diese Zwecke zur Verfügung, nicht jedoch beispielsweise bei den geregelten Abweichungen von den Grundsätzen [1] oder im Hinblick auf eine Behauptung zur Angemessenheit des Datenschutzschilds. Im Rahmen dieses Schiedsverfahrens ist das Datenschutzschild-Panel (bestehend aus einem oder drei von den Parteien ausgewählten Schiedsrichtern) befugt, einzelfallabhängige nichtmonetäre billigkeitsrechtliche Ansprüche (wie z. B. Zugang, Korrektur, Löschung oder Rückgabe der betreffenden Daten der Person) anzuerkennen, um die Verstöße gegen die Grundsätze abzustellen. Privatpersonen und dem Datenschutzschild angehörende Organisationen können eine gerichtliche Überprüfung und Durchsetzung der Schiedsentscheidungen nach US-Recht gemäß Federal Arbitration Act beantragen.

[1] Abschnitt I.5 der Grundsätze.

e. Rechtsbehelfe und Sanktionen

Die Inanspruchnahme eines Rechtsbehelfs soll dazu führen, dass die Organisation, gegen die sich die Beschwerde richtet, die Folgen ihres Verstoßes gegen die Grundsätze soweit möglich abstellt oder rückgängig macht und die den Beschwerdeführer betreffenden Daten künftig entweder im Einklang mit den Grundsätzen schützt oder nicht mehr verarbeitet. Sanktionen müssen so empfindlich sein, dass sie die Einhaltung der Grundsätze gewährleisten. Den Beschwerdestellen stehen Sanktionen von abgestufter Strenge zur Verfügung, mit denen sie gegen Verstöße von unterschiedlicher Schwere angemessen vorgehen können. Als Sanktionen kommen in Frage die öffentliche Bekanntmachung des Verstoßes, in bestimmten Fällen die Anordnung der Löschung der betreffenden Daten ([1]), der vorübergehende oder dauernde Entzug der Zugehörigkeit zur Zuständigkeit einer Beschwerdestelle, Entschädigungen für Personen, denen durch die Nichteinhaltung der Grundsätze ein Schaden entstanden ist, und Auflagen. Beschwerdestellen und Einrichtungen der freiwilligen Selbstkontrolle des privaten Sektors müssen bei Missachtung ihrer Entscheidungen die Gerichte anrufen oder die zuständige entscheidungsbefugte Behörde verständigen und das Ministerium unterrichten.

f. Befassung der FTC

Die FTC will Beschwerden wegen Verletzung der Grundsätze, die an sie verwiesen wurden i) von Einrichtungen der Selbstkontrolle für den Datenschutz und anderen unabhängigen Beschwerdestellen, ii) von EU-Mitgliedstaaten, iii) vom Ministerium, vorrangig behandeln und feststellen, ob gegen § 5 des FTC Act verstoßen wurde, der unlautere und irreführende Geschäftspraktiken verbietet. Hat die FTC Grund zu der Annahme, dass ein solcher Verstoß vorliegt, kann sie eine behördliche Anordnung erwirken, die die beanstandete Praxis untersagt, oder sie kann vor einem Bezirksgericht klagen. Entscheidet das Gericht in ihrem Sinne, kann ein Bundesgericht eine Anordnung mit gleicher Wirkung erlassen. Dazu gehören falsche Angaben zur Einhaltung der Grundsätze des Datenschutzschilds oder zur Beteiligung am Datenschutzschild von Organisationen, die entweder nicht mehr auf der Datenschutzschild-Liste stehen oder nie eine Selbstzertifizierung gegenüber dem Ministerium abgegeben haben. Gegen die Missachtung einer behördlichen Unterlassungsanordnung kann die FTC Geldstrafen verhängen; gegen die Missachtung der Anordnung eines Bundesgerichts kann sie zivil- und strafrechtlich vorgehen. Die FTC unterrichtet das Ministerium über von ihr unternommene Schritte. Andere Behörden sind angehalten, dem Ministerium das abschließende Ergebnis in solchen Fällen und sonstige Entscheidungen über die Beachtung der Grundsätze des Datenschutzschilds mitzuteilen.

g. Fortgesetzte Missachtung der Grundsätze

i. Missachtet eine Organisation fortgesetzt die Grundsätze, verliert sie die mit dem Datenschutzschild verbundenen Vorteile. Organisationen, die fortwährend gegen die Grundsätze verstoßen haben, werden vom Ministerium von der Datenschutzschild-Liste gestrichen und müssen die im Rahmen des Datenschutzschilds empfangenen personenbezogenen Daten zurückgeben oder löschen.

ii. Eine fortgesetzte Missachtung liegt vor, wenn sich eine Organisation, die sich gegenüber dem Ministerium selbst zertifiziert hat, weigert, der endgültigen Entscheidung einer Einrichtung der freiwilligen Selbstkontrolle, einer unabhängigen Beschwerdestelle oder eines staatlichen Kontrollorgans zu folgen, oder wenn von einer solchen Stelle festgestellt wird, dass die Organisation so häufig gegen die Grundsätze verstößt, die es einzuhalten vorgibt, dass diese Behauptung nicht mehr glaubwürdig ist. In diesen Fällen muss die Organisation das dem Ministerium unverzüglich mitteilen. Die Unterlassung dieser Mitteilung kann nach dem False Statements Act strafrechtlich verfolgt werden (18 U.S.C § 1001). Beteiligt sich eine Organisation nicht mehr an einem Programm der freiwilligen Selbstkontrolle für den Datenschutz oder an der unabhängigen Streitbeilegung, liegt eine fortgesetzte Missachtung der Grundsätze vor, da die Verpflichtung zur Einhaltung fortbesteht.

iii. Bei Eingang einer Mitteilung über die fortgesetzte Missachtung der Grundsätze wird das Ministerium die betreffende Organisation von der Datenschutzschild-Liste streichen, unabhängig davon, ob die Mitteilung durch die Organisation selbst, durch eine Einrichtung der freiwilligen Selbstkontrolle für den Datenschutz bzw. eine andere unabhängige Beschwerdestelle oder durch ein staatliches Kontrollorgan erfolgt. Das geschieht jedoch erst, nachdem die 30-tägige Frist abgelaufen ist, in der die betroffene Organisation

([1]) Beschwerdestellen können Sanktionen nach eigenem Ermessen verhängen. Die Sensibilität der Daten ist ein maßgebendes Kriterium, wenn zu entscheiden ist, ob Daten zu löschen sind oder ob eine Organisation mit der Erhebung, Nutzung oder Weitergabe von Daten die Grundsätze des Datenschutzschilds in eklatanter Weise verletzt hat.

Gelegenheit hat zu reagieren. Aus der Datenschutzschild-Liste des Ministeriums lässt sich also ersehen, welche Organisationen als Beteiligte am Datenschutzschild anerkannt sind und welche diese Anerkennung verloren haben.

iv. Eine Organisation, die sich einer Einrichtung der freiwilligen Selbstkontrolle anschließt, um sich erneut für den Datenschutzschild zu qualifizieren, muss dieser Einrichtung ihre frühere Teilnahme am Datenschutzschild vollständig offenbaren.

12. **Wahlmöglichkeit — Zeitpunkt des Widerspruchs**

a. Allgemein soll der Grundsatz der Wahlmöglichkeit gewährleisten, dass personenbezogene Daten in einer Weise genutzt und weitergegeben werden, die mit den Erwartungen und Entscheidungen des Betroffenen übereinstimmt. Dementsprechend sollte der Betroffene zu jeder Zeit entscheiden können, ob seine personenbezogenen Daten für das Direktmarketing verwendet werden dürfen oder nicht; hierfür können die Organisationen aber eine angemessene Frist festlegen, die sie zur effektiven Berücksichtigung eines Widerspruchs („Opt-out") benötigen. Daneben kann die Organisation hinreichende Informationen anfordern, die die Identität der Person bestätigen, die Widerspruch einlegt. In den Vereinigten Staaten können Betroffene von der Wahlmöglichkeit Gebrauch machen, indem sie auf ein zentrales „Widerspruchsprogramm" zurückgreifen, wie dem Mail Preference Service der Direct Marketing Association. Organisationen, die an dem Mail Preference Service teilnehmen, sollten Verbraucher, die keine kommerziellen Informationen erhalten möchten, auf diesen Dienst hinweisen. Auf jeden Fall sollte den Betroffenen ein leicht zugänglicher und erschwinglicher Mechanismus zur Verfügung gestellt werden, um diese Möglichkeit nutzen zu können.

b. Gleichermaßen kann eine Organisation Daten für bestimmte Zwecke des Direktmarketing verwenden, wenn es unmöglich ist, dem Betroffenen vor Nutzung der Daten eine Widerspruchsmöglichkeit einzuräumen, sofern die Organisation dem Betroffenen unmittelbar danach (und auf Verlangen jederzeit) die Möglichkeit einräumt, den Erhalt weiterer Direktwerbung (ohne Kosten für den Verbraucher) abzulehnen, und die Organisation den Wünschen des Betroffenen nachkommt.

13. **Reisedaten**

a. Flugreservierungsdaten und andere Reisedaten wie Daten über Vielflieger, über Hotelreservierungen und über spezielle Bedürfnisse wie religiös begründete besondere Speisewünsche oder die Notwendigkeit pflegerischer Betreuung dürfen in bestimmten Fällen an Organisationen außerhalb der EU weitergegeben werden. Nach Artikel 26 der Richtlinie dürfen personenbezogene Daten in ein Drittland übermittelt werden, das kein angemessenes Schutzniveau im Sinne des Artikels 25 Absatz 2 gewährleistet, wenn i) die Übermittlung für die Erfüllung eines Vertrags wie der Vielflieger-Vereinbarung notwendig ist oder ii) die betroffene Person ohne jeden Zweifel ihre Einwilligung gegeben hat. US-Organisationen, die sich den Grundsätzen des Datenschutzschilds angeschlossen haben, gewährleisten einen angemessenen Schutz personenbezogener Daten und können deshalb solche Daten aus der EU empfangen, ohne dass diese Voraussetzungen oder die in Artikel 26 der Datenschutzrichtlinie genannten Voraussetzungen erfüllt sein müssen. Da das Konzept des Datenschutzschilds besondere Regeln für den Umgang mit sensiblen Daten vorsieht, können auch solche Daten (die etwa für die pflegerische Betreuung eines Kunden benötigt werden) an Organisationen übermittelt werden, die am Datenschutzschild teilnehmen. Allerdings ist die übermittelnde Organisation stets dem Recht des EU-Mitgliedstaats unterworfen, in dem sie tätig ist, und das kann unter anderem bedeuten, dass sie im Umgang mit sensiblen Daten besondere Vorschriften zu beachten hat.

14. **Arzneimittel und Medizinprodukte**

a. Anwendung des Rechts der EU-Mitgliedstaaten oder der Grundsätze des Datenschutzschilds

Das Recht der EU-Mitgliedstaaten gilt für die Erhebung der personenbezogenen Daten und für ihre Verarbeitung vor der Übermittlung in die USA. Die Grundsätze des Datenschutzschilds gelten, nachdem die Daten in die USA übermittelt worden sind. Daten, die für die pharmazeutische Forschung oder sonstige Zwecke benutzt werden, sollten gegebenenfalls anonymisiert werden.

b. Künftige Forschungsarbeiten

i. In medizinischen und pharmazeutischen Studien gewonnene personenbezogene Daten sind oft sehr wertvoll für künftige Forschungsarbeiten. Wenn für ein Forschungsvorhaben erhobene personenbezogene Daten an eine dem Datenschutzschild beigetretene US-Organisation übermittelt werden, darf die Organisation diese Daten für ein anderes Forschungsvorhaben verwenden, wenn das dem Betroffenen schon zu Anfang ordnungsgemäß mitgeteilt und wenn ihm eine Wahlmöglichkeit eingeräumt wurde. Eine Mitteilung muss Angaben über die künftige Verwendung der Daten enthalten wie Angaben über regelmäßige Folgeuntersuchungen, ähnliche Forschungsvorhaben, für die sie verwendet werden sollen, oder ihre kommerzielle Nutzung.

ii. Es versteht sich, dass dabei nicht jede künftige Verwendung der Daten angegeben werden kann. Die Verwendung für einen anderen Forschungszweck kann sich aus neuen Erkenntnissen über die ursprünglichen Daten, aus neuen medizinischen Entdeckungen und Fortschritten sowie aus Entwicklungen im Gesundheitswesen und in der Gesetzgebung ergeben. Gegebenenfalls ist in der Mitteilung darauf hinzuweisen, dass personenbezogene Daten für künftige medizinische und pharmazeutische Forschungsarbeiten verwendet werden können, die nicht vorauszusehen sind. Entspricht die neue Verwendung nicht dem allgemeinen Forschungszweck, für den die personenbezogenen Daten ursprünglich erhoben wurden oder in den der Betroffene später eingewilligt hat, muss erneut seine Einwilligung eingeholt werden.

c. Rückzug aus einem klinischen Versuch

Ein Teilnehmer kann sich jederzeit aus einem klinischen Versuch zurückziehen oder dazu aufgefordert werden. Personenbezogene Daten, die vor seinem Rückzug erhoben wurden, können jedoch weiterhin verarbeitet werden wie die übrigen im Rahmen des Versuchs erhobenen Daten, wenn er darauf hingewiesen wurde, als er seine Bereitschaft zur Teilnahme erklärte.

d. Übermittlung von Daten an Aufsichtsbehörden zur Überprüfung

Hersteller von Arzneimitteln und Medizinprodukten dürfen in klinischen Versuchen in der EU gewonnene personenbezogene Daten zur Überprüfung an Aufsichtsbehörden in den USA übermitteln. Unter Beachtung der Grundsätze der Informationspflicht und der Wahlmöglichkeit dürfen sie die Daten auch an andere Stellen wie Organisationen und Wissenschaftler übermitteln.

e. Blindversuche

i. Zur Wahrung der Objektivität dürfen bei klinischen Versuchen die Teilnehmer und oft auch die Forscher selbst nicht erfahren, wer wie behandelt wird, denn das würde die Aussagefähigkeit der Ergebnisse in Frage stellen. Teilnehmern an solchen sogenannten Blindversuchen muss kein Zugang zu Daten über ihre Behandlung während des Versuchs gewährt werden, wenn ihnen diese Beschränkung vor ihrer Teilnahme erklärt wurde und die Offenlegung der Daten den Nutzen der Forschungsarbeit gefährden würde.

ii. Wer sich dennoch zur Teilnahme an dem Versuch entschließt, muss hinnehmen, dass die ihn betreffenden Daten unter Verschluss gehalten werden. Nach Abschluss des Versuchs und Auswertung der Ergebnisse müssen die Teilnehmer allerdings auf Verlangen Zugang zu ihren Daten erhalten. Dafür sollten sie sich in erster Linie an den Arzt oder an anderes medizinisches Personal wenden, von dem sie während des Versuchs behandelt wurden, hilfsweise an die Organisation, in deren Auftrag der Versuch durchgeführt wurde.

f. Überwachung der Sicherheit und Wirksamkeit von Produkten

Wenn ein Hersteller von Arzneimitteln oder Medizinprodukten Maßnahmen zur Überwachung der Sicherheit und Wirksamkeit seiner Produkte trifft und u. a. über Zwischenfälle berichtet und laufend Daten über Patienten/Versuchspersonen erhebt, die bestimmte Arzneimittel oder Medizinprodukte nutzen, muss er die im Datenschutzschild verankerten Grundsätze der Informationspflicht, der Wahlmöglichkeit, der Weiterübermittlung und des Auskunftsrechts nicht beachten, soweit die Grundsätze mit gesetzlichen Pflichten kollidieren. Das gilt sowohl für Berichte von Dienstleistern des Gesundheitswesens an Arzneimittel- und Medizinproduktehersteller als

auch für Berichte von Arzneimittel- und Medizinproduktherstellern an Behörden wie die amerikanische Food and Drug Administration.

g. Verschlüsselte Daten

Forschungsdaten werden stets an der Quelle verschlüsselt, damit aus ihnen nicht die Identität einzelner Personen zu ersehen ist. Den Pharmaorganisationen, also den Projektträgern, wird der Schlüssel nicht ausgehändigt, er verbleibt beim Forscher, so dass er unter bestimmten Umständen (z. B. wenn eine nachträgliche Überwachung notwendig ist) einzelne Versuchspersonen identifizieren kann. Die Übermittlung derart verschlüsselter Daten von der EU in die USA ist nicht als Übermittlung personenbezogener Daten anzusehen, die den Grundsätzen des Datenschutzschilds unterliegt.

15. **Daten aus öffentlichen Registern und öffentlich zugängliche Daten**

a. Eine Organisation muss die im Datenschutzschild verankerten Grundsätze der Sicherheit, Datenintegrität und Zweckbindung sowie des Rechtschutzes, der Durchsetzung und der Haftung auf personenbezogene Daten aus öffentlich zugänglichen Quellen anwenden. Diese Grundsätze gelten auch für personenbezogene Daten, die aus öffentlichen Datenbeständen erhoben werden, d. h. aus Datenbeständen, die von Ämtern aller Ebenen geführt werden und der Öffentlichkeit zur Einsichtnahme offen stehen.

b. Die Grundsätze der Informationspflicht, der Wahlmöglichkeit und der Verantwortlichkeit für die Weitergabe sind nicht auf Daten in öffentlichen Registern anzuwenden, wenn diese nicht mit nichtöffentlichen Daten kombiniert sind und solange die von der zuständigen Behörde festgelegten Bedingungen für ihre Abfrage beachtet werden. Im Allgemeinen gelten die Grundsätze der Informationspflicht, der Wahlmöglichkeit und der Verantwortlichkeit für die Weitergabe auch nicht für öffentlich verfügbare Daten, es sei denn, der europäische Übermittler weist darauf hin, dass diese Daten Beschränkungen unterliegen, aufgrund derer die Organisation die genannten Grundsätze im Hinblick auf die von ihr geplanten Verwendung anwenden muss. Organisationen haften nicht dafür, wie diese Daten von denen genutzt werden, die sie aus veröffentlichtem Material entnommen haben.

c. Wird festgestellt, dass eine Organisation unter Missachtung der Grundsätze absichtlich personenbezogene Daten offengelegt hat, so dass diese Ausnahme von der Regel für die Organisation selbst oder aber für andere von Nutzen ist, verliert sie ihre Vorteile aufgrund des Datenschutzschilds.

d. Das Auskunftsrecht gilt für Daten in öffentlichen Registern nur, wenn sie mit anderen personenbezogenen Daten kombiniert sind (außer bei kleinen Mengen, die verwendet wurden, um die öffentlichen Daten zu indexieren oder zu ordnen). Die Bestimmungen der einschlägigen Rechtsvorschriften über die Einsichtnahme in Datenbestände sind jedoch einzuhalten. Sind dagegen Daten aus öffentlichen Beständen mit anderen als den genannten Datenmengen aus nichtöffentlichen Quellen kombiniert, muss die Organisation Zugang zu allen personenbezogenen Daten gewähren, sofern nicht einer der genannten Ausnahmefälle vorliegt.

e. Wie bei Daten, die aus öffentlichen Beständen gewonnen wurden, ist das Auskunftsrecht nicht auf Daten anzuwenden, die bereits der Öffentlichkeit zur Verfügung stehen, sofern sie mit nicht öffentlich verfügbaren Daten kombiniert sind. Organisationen, die öffentlich zugängliche Information gegen Entgelt anbieten, können ihre üblichen Gebühren erheben. Alternativ können Personen Zugang zu sie betreffenden Daten von der Organisation verlangen, die sie ursprünglich erhoben hat.

16. **Anträge von Behörden auf Datenzugriff**

a. Um für Transparenz bei rechtmäßige Anträgen von Behörden auf Zugang zu personenbezogenen Daten zu sorgen, können dem Datenschutzschild angehörende Organisationen freiwillig in regelmäßigen Abständen Transparenzberichte über die Anzahl der Anträge von Behörden auf Datenzugriff aus Gründen der Strafverfolgung oder nationalen Sicherheit veröffentlichen, soweit diese Offenlegungen nach geltendem Recht zulässig sind.

b. Die von den Organisationen in diesen Berichten aufgeführten Angaben können zusammen mit veröffentlichten nachrichtendienstlichen sowie mit sonstigen Informationen in die gemeinsame jährliche Überprüfung der Funktionsweise des Datenschutzschilds im Einklang mit den Grundsätzen einfließen.

c. Auch wenn keine Information gemäß Punkt a)xii) des Grundsatzes der Informationspflicht erfolgt ist, behindert oder beeinträchtigt dies nicht die Möglichkeiten einer Organisation, rechtmäßigen Anfragen nachzukommen.

Anlage I

Schiedsmodell

In dieser Anlage I sind die Bedingungen aufgeführt, unter denen dem Datenschutz angehörende Organisationen zur Behandlung von Ansprüchen im Schiedsverfahren nach dem Grundsatz des Rechtsschutzes, der Durchsetzung und der Haftung verpflichtet sind. Die im Folgenden beschriebene Möglichkeit des verbindlichen Schiedsverfahrens bezieht sich auf bestimmte „Restansprüche" in Bezug auf Daten, die unter den EU-US-Datenschutzschild fallen. Damit soll Privatpersonen ein zeitnaher, unabhängiger und fairer Mechanismus bereitgestellt werden, der sich mit geltend gemachten Verstößen gegen die Grundsätze befasst, die nicht von einem der gegebenenfalls in Anspruch genommenen anderen Mechanismen des Datenschutzschilds geklärt werden konnten.

A. **Anwendungsbereich**

Mit dem Schiedsverfahren können Privatpersonen bei Restansprüchen feststellen lassen, ob eine dem Datenschutzschild angehörende Organisation ihre Pflichten im Rahmen der Grundsätze gegenüber der betreffenden Person verletzt hat und ob diese Verletzung vollständig oder teilweise ungeahndet bleibt. Diese Option steht nur für diese Zwecke zur Verfügung, nicht jedoch beispielsweise bei den geregelten Abweichungen von den Grundsätzen ([1]) oder im Hinblick auf eine Behauptung zur Angemessenheit des Datenschutzschilds.

B. **Verfügbare Abhilfemaßnahmen**

Im Rahmen dieses Schiedsverfahrens ist das Datenschutzschild-Panel (bestehend aus einem oder drei von den Parteien ausgewählten Schiedsrichtern) befugt, einzelfallabhängige nichtmonetäre billigkeitsrechtliche Ansprüche (wie z. B. Zugang, Korrektur, Löschung oder Rückgabe der betreffenden Daten der Person) anzuerkennen, um die Verstöße gegen die Grundsätze abzustellen. Dieses sind die einzigen Befugnisse des Schiedsforums in Bezug auf Abhilfemaßnahmen. Bei der Prüfung von Abhilfemaßnahmen muss das Schiedsforum andere bereits von anderen Mechanismen im Rahmen des Datenschutzschilds verhängte Abhilfemaßnahmen berücksichtigen. Schadenersatz, Kosten, Gebühren oder andere derartige Maßnahmen sind nicht verfügbar. Jede Partei muss selbst für die anfallenden Anwaltsgebühren aufkommen.

C. **Voraussetzungen für das Schiedsverfahren**

Wer das Schiedsverfahren in Anspruch nehmen möchte, muss vor der Einleitung einer Schiedsklage 1) den behaupteten Verstoß direkt bei der Organisation geltend machen und der Organisation Gelegenheit geben, die Angelegenheit innerhalb der in Abschnitt III.11 d)i) der Grundsätze aufgeführten Frist zu klären, 2) das kostenlose unabhängige Beschwerdeverfahren im Rahmen der Grundsätze in Anspruch nehmen und 3) die Angelegenheit kostenlos über seine zuständige Datenschutzbehörde dem Handelsministerium zuleiten und dem Handelsministerium die Gelegenheit geben, die Angelegenheit nach Möglichkeit innerhalb der im Schreiben der International Trade Administration des Handelsministeriums gesetzten Frist zu klären.

Das Schiedsverfahren kann nicht in Anspruch genommen werden, wenn der von der Person geltend gemachte Verstoß 1) bereits Gegenstand eines verbindlichen Schiedsverfahrens war, 2) Gegenstand eines rechtskräftigen Urteils in einem Gerichtsverfahren mit der Person als Prozesspartei war oder 3) von den Parteien bereits geregelt wurde. Darüber hinaus kann das Schiedsverfahren nicht in Anspruch genommen werden, wenn eine EU-Datenschutzbehörde 1) gemäß Abschnitt III.5 oder III.9 der Grundsätze zuständig ist oder 2) befugt ist, den geltend gemachten Verstoß direkt mit der Organisation zu klären. Die Befugnis einer Datenschutzbehörde, den gleichen Anspruch gegen einen für die Verarbeitung Verantwortlichen in der EU geltend zu machen, schließt die Inanspruchnahme des Schiedsverfahrens gegen eine nicht an die Befugnis der Datenschutzbehörde gebundene andere rechtliche Einheit allein nicht aus.

D. **Verbindlichkeit von Schiedssprüchen**

Die Entscheidung einer Einzelperson, dieses verbindliche Schiedsverfahren in Anspruch zu nehmen, ist vollkommen freiwillig. Die Schiedssprüche sind für alle beteiligten Parteien verbindlich. Mit der Inanspruchnahme verzichtet die betreffende Person auf die Möglichkeit, ein anderes Forum mit der Klärung des geltend gemachten Verstoßes zu befassen; wenn jedoch diesem Verstoß mit der Anerkennung nichtmonetärer Ansprüche nicht vollständig abgeholfen wird, kann die betreffende Person dennoch Schadensersatzansprüche vor Gericht geltend machen.

([1]) Abschnitt I.5 der Grundsätze.

E. **Überprüfung und Durchsetzung**

Privatpersonen und dem Datenschutzschild angehörende Organisationen können eine gerichtliche Überprüfung und Durchsetzung der Schiedsentscheidungen nach US-Recht gemäß Federal Arbitration Act beantragen ([1]). Derartige Fälle müssen bei dem Bundesbezirksgericht eingereicht werden, dessen territoriale Zuständigkeit sich auf den Hauptgeschäftsort der dem Datenschutzschild angehörenden Organisation erstreckt.

Mit diesem Schiedsverfahren sollen individuelle Streitigkeiten geklärt werden, und die Schiedsentscheidungen sollen nicht als zur Nachahmung empfohlener oder verbindlicher Präzedenzfall bei Angelegenheiten anderer Parteien dienen, einschließlich bei künftigen Schiedsverfahren oder an Gerichten der EU oder der USA oder in Verfahren der FTC.

F. **Das Schiedsforum**

Die Parteien wählen die Schiedsrichter aus dem im Folgenden erörterten Verzeichnis der Schiedsrichter aus.

Nach geltendem Recht erstellen das US-Handelsministerium und die Europäische Kommission ein Verzeichnis mit mindestens 20 Schiedsrichtern, die aufgrund ihrer Unabhängigkeit, Integrität und Sachkenntnis ausgewählt werden. Dafür gilt Folgendes:

Die Schiedsrichter

1) verbleiben für einen Zeitraum von 3 Jahren in dem Verzeichnis, sofern keine außergewöhnlichen Umstände oder wichtigen Gründe vorliegen; dieser Zeitraum kann um weitere drei Jahre verlängert werden;

2) sind gegenüber einer der Parteien oder einer dem Datenschutzschild angehörigen Organisation bzw. gegenüber den USA, der EU oder einem EU-Mitgliedstaat oder einer anderen Regierungsbehörde, öffentlichen Behörde oder Strafverfolgungsbehörde weder weisungsgebunden noch anderweitig verpflichtet;

3) müssen als Rechtsanwalt in den USA zugelassen und im US-Privatrecht bewandert sein und Sachkenntnis im EU-Datenschutzrecht aufweisen.

G. **Schiedsverfahren**

Im Einklang mit dem geltenden Recht vereinbaren das Handelsministerium und die Europäische Kommission innerhalb von 6 Monaten nach Annahme des Angemessenheitsbeschlusses die Übernahme einer Reihe von bestehenden, etablierten US-Schiedsverfahren (wie z. B. AAA oder JAMS) zur Regelung des Verfahrens vor dem Datenschutzschild-Panel, wobei die folgenden Aspekte zugrunde gelegt werden:

1. Eine Person kann vorbehaltlich der vorstehend aufgeführten Voraussetzungen ein verbindliches Schiedsverfahren einleiten, indem sie der Organisation eine Mitteilung zukommen lässt. Die Mitteilung enthält eine Zusammenfassung der gemäß Abschnitt C unternommenen Schritte zur Klärung einer Beschwerde, eine Beschreibung des geltend gemachten Verstoßes und, nach eigener Wahl, Belegunterlagen und -materialien und/oder eine Rechtserörterung mit Bezug zum geltend gemachten Verstoß.

([1]) In Kapitel 2 des Federal Arbitration Act („FAA“) heißt es: „Eine Schiedsvereinbarung oder ein Schiedsspruch aus einem vertraglichen oder nicht vertraglichen Rechtsverhältnis, das als kommerziell gilt, einschließlich einer Transaktion, eines Vertrags oder einer Vereinbarung nach [§ 2 des FAA], fällt unter das Übereinkommen über die Anerkennung und Vollstreckung ausländischer Schiedssprüche vom 10. Juni 1958, 21 U.S.T. 2519, T.I.A.S. No. 6997 („New Yorker Übereinkommen“).“ 9 U.S.C. § 202. Weiter ist im FAA festgelegt: „Eine Schiedsvereinbarung oder ein Schiedsspruch aus einem derartigen Verhältnis, das ausschließlich zwischen Bürgern der Vereinigten Staaten besteht, fällt nur dann unter das [New Yorker] Übereinkommen, wenn dieses Verhältnis im Ausland befindliche Immobilien umfasst, eine Leistung oder Rechtsdurchsetzung im Ausland anstrebt oder in einer anderweitigen hinreichenden Beziehung zu einem oder mehreren anderen Staaten steht.“ Ebenda. Nach Kapitel 2 kann „jede Partei des Schiedsverfahrens einen Antrag bei einem nach diesem Kapitel zuständigen Gericht auf eine Anordnung zur Bestätigung des Schiedspruchs gegen eine andere Partei des Schiedsverfahrens stellen. Das Gericht bestätigt den Schiedsspruch, sofern es keinen der Gründe für eine Verweigerung oder einen Aufschub der Anerkennung oder Durchsetzung des Schiedsspruchs gemäß dem besagten [New Yorker] Übereinkommen findet.“ Ebenda § 207. Weiter heißt es in Kapitel 2: „Die Bezirksgerichte der Vereinigten Staaten … haben ungeachtet des Streitwerts die ursprüngliche Zuständigkeit für … eine Klage oder ein Verfahren [im Rahmen des New Yorker Übereinkommens].“ Ebenda § 203.
Außerdem heißt es in Kapitel 2: „Kapitel 1 gilt für Klagen und Verfahren nach diesem Kapitel, soweit jenes Kapitel nicht mit diesem Kapitel oder dem [New Yorker] Übereinkommen, wie von den Vereinigten Staaten ratifiziert, kollidiert.“ Ebenda § 208. In Kapitel 1 heißt es wiederum: „Eine schriftliche Bestimmung in einem Vertrag über eine geschäftliche Transaktion, wonach ein Streit aufgrund dieses Vertrags oder dieser Transaktion oder die Weigerung, diesen bzw. diese ganz oder teilweise zu erfüllen, im Schiedsverfahren beizulegen ist, oder eine schriftliche Vereinbarung, wonach ein bestehender Streit aufgrund dieses Vertrags, dieser Transaktion oder dieser Weigerung an ein Schiedsgericht zu verweisen ist, ist gültig, unwiderruflich und vollstreckbar, sofern nicht Gründe nach Recht oder Billigkeit für den Rücktritt von einem Vertrag vorliegen.“ Ebenda § 2. Weiter heißt es in Kapitel 1: „Jede Partei im Schiedsverfahren kann bei einem angegebenen Gericht eine Anordnung zur Bestätigung des Schiedsspruchs beantragen, woraufhin das Gericht eine derartige Anordnung erlassen muss, sofern der Schiedsspruch nicht gemäß § 10 und 11 des [FAA] aufgegeben, geändert oder korrigiert wird.“ Ebenda § 9.

2. Es werden Verfahren entwickelt, die sicherstellen, dass für einen geltend gemachten Verstoß nicht mehrere Verfahren geführt oder mehrere Abhilfemaßnahmen getroffen werden.

3. Die FTC kann parallel zum Schiedsverfahren tätig werden.

4. An den Schiedsverfahren dürfen keine Vertreter der USA, der EU oder eines EU-Mitgliedstaats oder einer anderen Regierungsbehörde, staatlichen Behörde oder Strafverfolgungsbehörde teilnehmen, wobei auf Antrag einer Person aus der EU die EU-Datenschutzbehörden Hilfe bei der Erstellung ausschließlich der Mitteilung leisten können, jedoch keinen Zugang zu Offenlegungen und anderen Materialien in Bezug auf diese Schiedsverfahren haben dürfen.

5. Ort des Schiedsverfahrens sind die Vereinigten Staaten, und die betroffene Person kann sich für eine Teilnahme per Video oder Telefonkonferenz entscheiden, die für sie mit keinen Kosten verbunden ist. Eine persönliche Anwesenheit ist nicht erforderlich.

6. Verfahrenssprache ist Englisch, wenn von den Parteien nicht anders vereinbart. Auf einen begründeten Antrag hin und unter Berücksichtigung dessen, ob sich die Person von einem Anwalt vertreten lässt, werden Dolmetscher für die mündliche Verhandlung sowie Übersetzungen der Verfahrensunterlagen bereitgestellt, ohne dass sich daraus Kosten für die Person ergeben, es sei denn, das Panel gelangt in einem konkreten Fall zu dem Schluss, dass eine Kostenübernahme nicht gerechtfertigt oder unverhältnismäßig wäre.

7. Den Schiedsrichtern vorgelegte Unterlagen werden vertraulich behandelt und nur in Verbindung mit dem Schiedsverfahren genutzt.

8. Wenn erforderlich, kann eine die Person betreffende Offenlegung zugelassen werden, wobei diese Offenlegung von den Parteien vertraulich behandelt und nur in Verbindung mit dem Schiedsverfahren genutzt wird.

9. Schiedsverfahren sollen innerhalb von 90 Tagen nach Zustellung der Mitteilung an die betreffende Organisation abgeschlossen werden, sofern von den Parteien nicht anderweitig vereinbart.

H. **Kosten**

Die Schiedsrichter sollen angemessene Maßnahmen zur Minimierung der Kosten oder Gebühren der Schiedsverfahren ergreifen.

Nach Maßgabe des geltenden Rechts wird das Handelsministerium in Abstimmung mit der Europäischen Kommission die Einrichtung eines Fonds ermöglichen, in den die dem Datenschutzschild angehörenden Organisationen einen Jahresbeitrag einzahlen, der sich zum Teil nach der Größe der Organisation richtet und die Schiedskosten, einschließlich Schiedsrichtergebühren, bis zu einer Obergrenze deckt. Der Fonds wird von einem Dritten verwaltet, der regelmäßig über die Tätigkeit des Fonds Bericht erstattet. Bei der jährlichen Überprüfung werden das Handelsministerium und die Europäische Kommission die Tätigkeit des Fonds, einschließlich der Notwendigkeit einer Anpassung des Beitrags oder der Obergrenze, kontrollieren und unter anderem die Anzahl der Schiedsverfahren sowie deren Kosten und Dauer prüfen, und zwar im gegenseitigen Einvernehmen, dass den am Datenschutzschild teilnehmenden Organisationen keine übermäßige finanzielle Belastung auferlegt wird. Rechtsanwaltsgebühren sind von dieser Bestimmung oder einem anderen Fonds im Rahmen dieser Bestimmung nicht erfasst.

ANHANG III

Schreiben des US-Außenministers John Kerry

7. Juli 2016

Sehr geehrte Frau Jourová,

es freut mich sehr, dass wir eine Einigung zum Datenschutzschild zwischen der Europäischen Union und den USA erzielen konnten, die auch eine Ombudsstelle beinhaltet, bei der EU-Behörden Auskunftsbegehren von EU-Bürgern im Zusammenhang mit signalerfassender Aufklärung in den USA einreichen können.

Präsident Barack Obama hat am 17. Januar 2014 in der Presidential Policy Directive 28 (PPD-28) eine grundlegende Reform der Nachrichtendienste angekündigt. Im Rahmen der PPD-28 habe ich Under-Secretary Catherine A. Novelli, die ebenfalls das Amt eines Senior Coordinator für internationale Diplomatie im Bereich der Informationstechnologie bekleidet, zur Ansprechpartnerin für ausländische Regierungen benannt, die Bedenken im Zusammenhang mit der US-Signalaufklärung vorbringen. Ausgehend von dieser Funktion habe ich in Übereinstimmung mit den in Anlage A festgelegten Bestimmungen, die seit meinem Schreiben vom 22. Februar 2016 aktualisiert wurden, eine Ombudsstelle des Datenschutzschilds ins Leben gerufen. Dieses Amt wird von Under-Secretary Novelli bekleidet, die unabhängig von den Nachrichtendiensten in den USA arbeitet und mir direkt unterstellt ist.

Meine Mitarbeiter sind angewiesen, die erforderlichen Ressourcen für die Einrichtung dieser neuen Ombudsstelle einzusetzen, und ich bin überzeugt, dass wir den Bedenken der EU-Bürger auf diese Weise wirksam begegnen können.

Hochachtungsvoll

John F. Kerry

Anlage A

Ombudsstelle des EU-U.S.-Datenschutzschilds für die signalerfassende Aufklärung

In Anerkennung der Bedeutung des EU-U.S.-Datenschutzschilds gibt die vorstehende Absichtserklärung einen Überblick über das Verfahren zur Umsetzung eines neuen Mechanismus für die signalerfassende Aufklärung, der mit der Presidential Policy Directive 28 („PPD-28") im Einklang steht ([1]).

Am 17. Januar 2014 hielt Präsident Obama eine Ansprache, in der er wichtige Reformen im Bereich Nachrichtendienste in Aussicht stellte. Dabei betonte er: „Unsere Bemühungen tragen nicht nur zum Schutz unserer eigenen Nation bei, sondern auch zu dem unserer Freunde und Verbündeten. Wirksam werden unsere Bemühungen aber nur dann sein, wenn die normalen Bürger in anderen Ländern ebenfalls darauf vertrauen, dass die Vereinigten Staaten ihre Privatsphäre respektieren." Präsident Obama kündigte die Veröffentlichung einer neuen Presidential Directive, der „PPD-28", an mit „klaren Vorschriften dazu, was wir unternehmen und was nicht, wenn es um unsere Auslandsaufklärung geht".

In § 4 Buchstabe d der PPD-28 wird der Außenminister beauftragt, einen „Senior Coordinator for International Information Technology Diplomacy" (Senior Coordinator) zu benennen, „der … als Ansprechpartner für ausländische Regierungen fungiert, die Bedenken im Zusammenhang mit der Signalaufklärung der Vereinigten Staaten vorbringen." Seit Januar 2015 nimmt Under Secretary C. Novelli die Aufgaben des Senior Coordinators wahr.

In der vorliegenden Absichtserklärung wird der vom Senior Coordinator befolgte neue Mechanismus beschrieben, der bei Daten, die gemäß dem Datenschutzschild, den Standardklauseln (standard contractual clauses, SCC), den verbindlichen unternehmensinternen Datenschutzregelungen (binding corporate rules, BCR) sowie den „Ausnahmeregelungen" ([2]) oder „etwaigen künftigen Ausnahmeregelungen" ([3]) von der EU unter Einhaltung des dafür bestehenden Weges laut geltendem Recht und bestehender Auslegungspraxis in die Vereinigten Staaten übermittelt werden, die Bearbeitung von Anfragen zum Zugriff auf Daten, die die nationale Sicherheit betreffen, und die Beantwortung solcher Anfragen erleichtern soll.

1. **Die Ombudsperson des Datenschutzschilds:** Der Senior Coordinator fungiert als Ombudsperson des Datenschutzschilds und benennt gegebenenfalls zusätzliche Beamte des Außenministeriums, die ihn bei der Wahrnehmung seiner in dieser Absichtserklärung im Einzelnen dargelegten Pflichten unterstützen (der Koordinator und etwaige weitere Beamte, die diese Aufgaben wahrnehmen, werden nachstehend als „Ombudsstelle des Datenschutzschilds" bezeichnet). Die Einrichtung arbeitet eng mit den jeweiligen Beamten aus anderen Regierungsstellen zusammen, die dem geltendem Recht und der bestehenden Auslegungspraxis der Vereinigten Staaten entsprechend für die Bearbeitung von Anträgen zuständig sind. Die Ombudsstelle untersteht unmittelbar dem Außenminister, der dafür Sorge trägt, dass die Ombudsstelle ihre Aufgabe objektiv und frei von unzulässiger Einflussnahme erfüllt, die sich auf die zu erteilende Antwort auswirken kann.

2. **Wirksame Koordinierung:** Die Ombudsstelle setzt die nachstehend beschriebenen Kontrollstellen wirksam ein, koordiniert sie und stellt auf diese Weise sicher, dass sich die Antwort der Ombudsstelle auf Anträge der EU-Stelle für Individualbeschwerden auf die erforderlichen Informationen stützt. Bezieht sich der Antrag auf die Vereinbarkeit der

([1]) Unter der Voraussetzung, dass der Beschluss über die Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes für Island, Liechtenstein und Norwegen gilt, wird die Materialsammlung zum Datenschutzschild sowohl die Europäische Union als auch diese drei Länder abdecken. Demzufolge sind bei Bezugnahmen auf die EU und ihre Mitgliedstaaten auch Island, Liechtenstein und Norwegen eingeschlossen.

([2]) „Ausnahmeregelungen" steht in diesem Zusammenhang für einen oder mehrere kommerzielle Datenübermittlungen, die unter der Voraussetzung stattfinden, dass:(a) die betroffene Person ihre unmissverständliche Einwilligung zu der vorgeschlagenen Datenübermittlung erteilt hat oder (b) die Übermittlung für die Erfüllung eines Vertrags zwischen der betroffenen Person und dem für die Verarbeitung Verantwortlichen oder zur Durchführung von vorvertraglichen Maßnahmen auf Antrag der betroffenen Person erforderlich ist; oder (c) die Übermittlung zum Abschluss oder zur Erfüllung eines Vertrags erforderlich ist, der im Interesse der betroffenen Person von dem für die Verarbeitung Verantwortlichen mit einem Dritten geschlossen wird; oder (d) die Übermittlung für die Wahrung eines wichtigen öffentlichen Interesses oder zur Feststellung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht erforderlich oder gesetzlich vorgeschrieben ist; oder (e) die Übermittlung für die Wahrung lebenswichtiger Interessen der betroffenen Person erforderlich ist; oder (f) die Übermittlung aus einem Register erfolgt, das gemäß den Rechts- oder Verwaltungsvorschriften zur Information der Öffentlichkeit bestimmt ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offensteht, soweit die gesetzlichen Voraussetzungen für die Einsichtnahme im Einzelfall gegeben sind.

([3]) „Etwaige künftige Ausnahmeregelungen" steht in diesem Zusammenhang für eine oder mehrere kommerzielle Datenübermittlungen, die unter einer der folgenden Voraussetzungen stattfinden, soweit die betreffende Voraussetzung rechtlich zulässige Gründe für die Übermittlung personenbezogener Daten aus der EU in die USA darstellt: (a) die betroffene Person hat ihre unmissverständliche Einwilligung zu der vorgeschlagenen Datenübermittlung erteilt, nachdem sie über die möglichen Risiken einer ohne Vorliegen eines Angemesssenheitsbeschlusses und ohne geeignete Garantien durchgeführten Datenübermittlung informiert wurde; oder (b) die Übermittlung ist zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen Person erforderlich, sofern die betroffene Person aus physischen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben; oder (c) bei einer Übermittlung an einen Drittstaat oder eine internationale Organisation, bei der keine andere bestehende oder künftige Ausnahmeregelung anwendbar ist, nur, wenn es sich dabei um keine Wiederholung handelt, wenn die Übermittlung sich nur auf eine begrenzte Zahl betroffener Personen bezieht, wenn ein zwingendes berechtigtes Interesse des für die Verarbeitung Verantwortlichen vorliegt, das nicht von den berechtigten Interessen oder den Rechten und Freiheiten der betroffenen Person außer Kraft gesetzt wird, und wenn der für die Verarbeitung Verantwortliche alle Umstände beurteilt hat, die bei einer Datenübermittlung eine Rolle spielen, und gegebenenfalls auf der Grundlage dieser Beurteilung geeignete Garantien zum Schutz personenbezogener Daten vorgesehen hat.

Überwachung mit dem US-Recht, kann die Ombudsstelle des Datenschutzschilds mit einer der unabhängigen Kontrollstellen mit Ermittlungsbefugnissen zusammenarbeiten.

a. Die Ombudsstelle des Datenschutzschilds arbeitet eng mit anderen Regierungsbeamten der Vereinigten Staaten, unter anderem auch mit entsprechenden unabhängigen Aufsichtsgremien, zusammen und stellt sicher, dass die eingegangenen Anträge vollständig sind und dem geltenden Recht und der bestehenden Auslegungspraxis entsprechend bearbeitet und geklärt werden. Insbesondere sorgt die Ombudsstelle für eine enge Koordinierung mit dem Amt des Director of National Intelligence, dem Justizministerium und den anderen Regierungsstellen, die entsprechend mit der nationalen Sicherheit der Vereinigten Staaten befasst sind, sowie den Generalinspekteuren, den Beauftragten für den Freedom of Information Act und den Bürgerrechts- und Datenschutzbeauftragten.

b. Damit gewährleistet ist, dass die Ombudsstelle des Datenschutzschilds im Sinne von § 4 Buchstabe e auf die eingegangenen Anträge nach § 3 Buchstabe b zu reagieren vermag, vertraut die Regierung der Vereinigten Staaten auf Mechanismen zur ressortübergreifenden Koordinierung und Überwachung von Angelegenheiten der nationalen Sicherheit.

c. Die Ombudsstelle des Datenschutzschilds kann Anträge betreffende Angelegenheiten dem Privacy and Civil Liberties Oversight Board zur Prüfung vorlegen.

3. **Einreichung von Anträgen:**

a. Ein Antrag wird zunächst bei den für die Überwachung der nationalen Sicherheitsbehörden und/oder die Verarbeitung von personenbezogenen Daten durch Behörden zuständigen Aufsichtsstellen der Mitgliedstaaten eingereicht. Die Einreichung des Antrags bei der Ombudsstelle erfolgt durch eine zentrale EU-Stelle (im Folgenden zusammen „EU-Stelle für Individualbeschwerden“).

b. Die EU-Stelle für Individualbeschwerden stellt mit den nachstehenden Maßnahmen sicher, dass ein Antrag ordnungsgemäß abgefasst ist:

i) Sie überprüft die Identität der betreffenden Privatperson und die Tatsache, dass diese im eigenen Namen und nicht als Vertreter/in einer staatlichen oder zwischenstaatlichen Organisation handelt.

ii) Sie stellt sicher, dass der Antrag schriftlich abgefasst ist und die folgenden grundlegenden Informationen enthält:

— alle Informationen, die dem Antrag zugrunde liegen,

— die Art der Information oder der angestrebten Abhilfe,

— die Regierungsstellen der Vereinigten Staaten, die gegebenenfalls beteiligt sein sollen, und

— sonstige Maßnahmen, die ergriffen wurden, um die erbetenen Informationen bzw. die angestrebte Abhilfe zu erlangen, und das Ergebnis dieser sonstigen Maßnahmen.

iii) Sie prüft, ob der Antrag sich auf Daten bezieht, bei denen begründet davon ausgegangen werden kann, dass sie gemäß Datenschutzschild, SCC, BCR, Ausnahmeregelungen oder etwaigen künftigen Ausnahmeregelungen von der EU in die Vereinigten Staaten übermittelt wurden.

iv) Sie trifft eine erste Feststellung, dass der Antrag nicht schikanös oder missbräuchlich ist bzw. nicht bösgläubig erfolgte.

c. Um für die Zwecke der weiteren Bearbeitung durch die Ombudsstelle des Datenschutzschilds im Sinne dieser Absichtserklärung abgefasst zu sein, muss ein Antrag nicht den Nachweis enthalten, dass tatsächlich im Wege der Signalaufklärung ein Zugriff der US-Regierung auf die Daten des Antragstellers erfolgt ist.

4. **Zusagen zur Kommunikation mit der vorlegenden EU-Stelle für Individualbeschwerden**

a. Die Ombudsstelle des Datenschutzschilds bestätigt den Eingang des Antrags gegenüber der EU-Stelle für Individualbeschwerden, durch die die Übermittlung erfolgte.

b. Die Ombudsstelle des Datenschutzschilds nimmt eine erste Prüfung vor, um festzustellen, ob der Antrag in Übereinstimmung mit Abschnitt 3 Buchstabe b abgefasst wurde. Stellt die Ombudsstelle irgendwelche Unzulänglichkeiten fest oder hat sie Fragen zur Abfassung eines Antrags, so setzt sie sich mit der EU-Stelle für Individualbeschwerden in Verbindung und versucht, die betreffenden Fragen zu klären.

c. Benötigt die Ombudsstelle des Datenschutzschilds zur Erleichterung der angemessenen Bearbeitung eines Antrags weitere Informationen oder müssen von der Privatperson, die den Antrag ursprünglich einreichte, besondere Maßnahmen ergriffen werden, so setzt die Ombudsstelle des Datenschutzschilds die vorlegende EU-Stelle für Individualbeschwerden hiervon in Kenntnis.

d. Die Ombudsstelle des Datenschutzschilds überprüft den Status des Antrags und stellt für die vorlegende EU-Stelle für Individualbeschwerden entsprechende Aktualisierungen bereit.

e. Sobald ein Antrag wie in Abschnitt 3 dieser Absichtserklärung beschrieben abgefasst wurde, sendet die Ombudsstelle des Datenschutzschilds vorbehaltlich der andauernden Informationsschutzverpflichtung nach geltendem Recht und bestehender Auslegungspraxis zeitnah eine angemessene Antwort an die vorlegende EU-Stelle für Individualbeschwerden. Die Ombudsstelle lässt der vorlegenden EU-Stelle eine Antwort zukommen, in der sie bestätigt, dass (i) die Beschwerde ordnungsgemäß geprüft wurde und dass (ii) die US-Gesetze und -Rechtsvorschriften, Executive Orders, Presidential Directives und die Auslegungspraxis der Behörden mit den im ODNI-Schreiben dargelegten Einschränkungen und Garantien eingehalten wurden bzw. dass — im Falle der Nichteinhaltung — diese Nichteinhaltung abgestellt wurde. Durch die Ombudsstelle wird weder bestätigt noch bestritten, dass die betreffende Privatperson Ziel einer Überwachungsmaßnahme war, noch bestätigt die Ombudsstelle die spezielle Abhilfe, die geleistet wurde. Wie in Abschnitt 5 weiter erläutert wird, werden Anträge im Rahmen des Freedom of Information ACTS so bearbeitet, wie in diesem Gesetz und den geltenden Bestimmungen vorgesehen.

f. Die Ombudsstelle des Datenschutzschilds nimmt unmittelbaren Kontakt zur EU-Stelle für Individualbeschwerden auf, die ihrerseits für den Kontakt zu der Privatperson, die den Antrag einreichte, verantwortlich ist. Ist der unmittelbare Kontakt Bestandteil eines der nachstehend beschriebenen Verfahren, so erfolgt dieser Kontakt den vorhandenen Verfahren entsprechend.

g. Die Zusagen in dieser Absichtserklärung gelten nicht für pauschale Aussagen, wonach der EU-U.S.-Datenschutzschild den Datenschutzanforderungen der Europäischen Union nicht entspreche. Sie wurden ausgehend von dem gemeinsamen Verständnis der Europäischen Kommission und der US-Regierung getroffen, dass es in Anbetracht der Bandbreite der im Rahmen dieses Mechanismus erteilten Zusagen möglicherweise zu ressourcenbedingten Einschränkungen kommen könnte, unter anderem bei Anträgen im Zusammenhang mit dem Freedom of Information Act (FOIA). Sollte die Wahrnehmung der Aufgaben der Ombudsstelle des Datenschutzschilds über die vertretbaren ressourcenbedingten Einschränkungen hinausgehen und die Erfüllung dieser Zusagen erschweren, so wird die US-Regierung der Europäischen Kommission gegenüber etwaige Anpassungen zur Sprache bringen, die unter diesen Umständen angebracht sind.

5. **Auskunftsbegehren:** Anträge auf Zugang zu amtlichen Unterlagen der Vereinigten Staaten können im Rahmen des Freedom of Information Act (FOIA) gestellt und bearbeitet werden.

a. Der FOIA bietet jedermann die Möglichkeit, den Zugang zu vorhandenen Unterlagen von Regierungsstellen zu beantragen, und zwar unabhängig von der Nationalität des Antragstellers. Dieses Gesetz ist kodifiziert im United States Code unter 5 U.S.C. § 552. Das Gesetz selbst kann zusammen mit zusätzlichen Informationen zum FOIA unter www.FOIA.gov und http://www.justice.gov/oip/foia-resources abgerufen werden. Jede Regierungsstelle hat einen verantwortlichen FOIA-Beauftragten, und auf ihrer öffentlichen Website finden sich Angaben dazu, wie ein FOIA-Antrag bei der betreffenden Stelle einzureichen ist. Die Behörden verfügen über gegenseitige Konsultationsverfahren zu FOIA-Anträgen, für die Unterlagen erforderlich sind, die von einer anderen Stelle vorgehalten werden.

b. Beispiele:

i) Das Amt des Director of National Intelligence (ODNI) hat für das ODNI das ODNI-FOIA-Portal eingerichtet: http://www.dni.gov/index.php/about-this-site/foia. Dieses Portal enthält Angaben zur Übermittlung von Anträgen, zur Überprüfung des Status laufender Anträge und zum Zugang zu Informationen, die vom ODNI im Rahmen des FOIA freigegeben und veröffentlicht wurden. Auf dem FOIA-Portal des ODNI finden sich Links zu anderen FOIA-Websites für Nachrichtendienste: http://www.dni.gov/index.php/about-this-site/foia/other-ic-foia-sites.

ii) Das Office of Information Policy des Justizministeriums stellt umfassende FOIA-Informationen bereit: http://www.justice.gov/oip. Dazu gehören nicht nur Angaben zur Weiterleitung von FOIA-Anträgen an das Justizministerium, sondern auch Hinweise für die US-Regierung zur Auslegung und Anwendung der FOIA-Anforderungen.

c. Gemäß FOIA gelten für den Zugang zu Regierungsunterlagen bestimmte detailliert aufgeführte Ausnahmeregelungen. Dazu zählen Einschränkungen des Zugriffs auf Informationen, die aus Gründen der nationalen Sicherheit der Geheimhaltung unterliegen, personenbezogene Informationen Dritter und Informationen, die strafrechtliche Ermittlungen betreffen, vergleichbar mit den Einschränkungen, die von den einzelnen EU-Mitgliedstaaten durch deren eigene Gesetze über den Zugang zu Informationen auferlegt werden. Diese Einschränkungen gelten für Amerikaner und für Nicht-Amerikaner gleichermaßen.

d. Bei Streitigkeiten im Zusammenhang mit der Freigabe von Unterlagen, die im Rahmen des FOIA angefordert werden, kann der Verwaltungsgerichtsweg eingeschlagen und anschließend ein Bundesgericht angerufen werden. Das Gericht hat de novo zu bestimmen, ob Unterlagen aus triftigen Gründen zurückgehalten werden (5 U.S.C. § 552 Buchstabe a Ziffer 4 Teil B), und kann die Behörden anweisen, Zugang zu Unterlagen zu gewähren. In einigen Fällen wurden von Gerichten die Behauptungen von Behörden zurückgewiesen, Informationen müssten zurückgehalten werden, weil sie aus Gründen der nationalen Sicherheit der Geheimhaltung unterliegen. Obwohl kein Schadensersatz geltend gemacht werden kann, können die Gerichte die Erstattung der Anwaltsgebühren zuerkennen.

6. **Anträge auf Einleitung weiterer Maßnahmen:** Ein Antrag unter Berufung auf eine Rechtsverletzung oder anderes Fehlverhalten wird den zuständigen Regierungsstellen der Vereinigten Staaten zugeleitet, darunter unabhängigen Überwachungsstellen, die befugt sind, den betreffenden Antrag zu prüfen und bei Verstößen gegen Vorschriften die nachstehend beschriebenen Maßnahmen zu ergreifen.

a. Generalinspekteure sind rechtlich unabhängig und verfügen über weitreichende Befugnisse zur Durchführung von Untersuchungen, Audits und Überprüfungen von Programmen, darunter auch bei Missbrauchsfällen oder Rechtsverstößen, und können Abhilfemaßnahmen empfehlen.

i) In der geänderten Fassung des Inspector General Act von 1978 fungieren die Generalinspekteure (IG) auf Bundesebene als unabhängige und objektive Instanzen innerhalb der meisten Behörden, deren Aufgabe es ist, Verschwendung, Betrug und Missbrauch in den Programmen und Aktivitäten der jeweiligen Behörde zu bekämpfen. Zu diesem Zweck ist jeder IG für die Durchführung von Audits und Untersuchungen im Zusammenhang mit den Programmen und Aktivitäten seiner Behörde verantwortlich. Darüber hinaus sind die Generalinspekteure anleitend und koordinierend tätig, erteilen Empfehlungen für Maßnahmen zur Förderung von Wirtschaftlichkeit, Effizienz und Wirksamkeit, decken Betrug und Amtsmissbrauch in den Programmen und Aktivitäten ihrer Behörde auf und verhindern sie.

ii) Jeder Nachrichtendienst hat ein eigenes Büro des Generalinspekteurs, das unter anderem für die Kontrolle der Auslandsaufklärung zuständig ist. Mehrere Berichte von Generalinspekteuren zu nachrichtendienstlichen Programmen wurden veröffentlicht.

iii) Beispiele:

— Das Büro des Generalinspekteurs der Intelligence Community (IC IG) wurde gemäß § 405des Intelligence Authorization Act of Fiscal Year 2010 eingerichtet. Das IC IG ist zuständig für IC-weite Audits, Untersuchungen, Inspektionen und Überprüfungen, bei denen alle nachrichtendienstliche Missionen betreffenden systemimmanenten Risiken, Schwachstellen und Unzulänglichkeiten ermittelt und aufgegriffen werden, um mit Blick auf IC-weite Einsparungen und Wirkungen Verbesserungen herbeizuführen. Das IC IG ist befugt, Beschwerden oder Informationen nachzugehen, die mutmaßliche Verstöße gegen Gesetze oder Rechtsvorschriften, Fälle von Verschwendung, Betrug und Amtsmissbrauch oder eine erhebliche oder besondere Gefahr für die öffentliche Gesundheit und Sicherheit im Zusammenhang mit nachrichtendienstlichen Programmen und Aktivitäten des ODNI und/oder der Intelligence Community betreffen. Das IC IG stellt Informationen darüber bereit, wie das IC IG unmittelbar kontaktiert werden kann, wenn ein Bericht übermittelt werden soll: http://www.dni.gov/index.php/about-this-site/contact-the-ig.

— Das Büro des Generalinspekteurs (OIG) im U.S. Department of Justice (DOJ, Justizministerium) ist eine auf gesetzlicher Grundlage eingesetzte unabhängige Instanz, deren Aufgabe es ist, Verschwendung, Betrug, Amtsmissbrauch und Fehlverhalten in DOJ-Programmen und durch Bedienstete des Ministeriums aufzudecken und zu unterbinden und zur Wirtschaftlichkeit und Effizienz dieser Programme beizutragen. Das OIG untersucht mutmaßliche Straf- und Zivilrechtsverletzungen durch DOJ-Bedienstete und nimmt darüber hinaus Audits und Inspektionen zu DOJ-Programmen vor. Es ist zuständig für alle Beschwerden über Fehlverhalten von Bediensteten des Justizministeriums, unter anderem auch von Bediensteten des Federal Bureau of Investigation, der Drug Enforcement Administration, des Federal Bureau of Prisons, des U.S. Marshals Service, des Bureau of Alcohol, Tobacco, Firearms, and Explosives, der United States Attorneys Offices und der Bediensteten, die in anderen Bereichen oder Büros des Justizministeriums beschäftigt sind. (Die einzige Ausnahme besteht darin, dass Missbrauchsvorwürfe gegenüber einem

Department Attorney oder Mitarbeiter der Strafverfolgungsbehörden, die sich auf die Wahrnehmung der Befugnisse des Department Attorney zur Durchführung von Ermittlungen, zur Austragung von Rechtsstreitigkeiten oder zur Rechtsberatung beziehen, in die Zuständigkeit des Office of Professional Responsibility des Ministeriums fallen.) Darüber hinaus wird der Generalinspekteur in § 1001 des USA Patriot Act, der am 26. Oktober 2001 Rechtskraft erlangte, angewiesen, Beschwerden gegen mutmaßliche Verletzungen von Bürgerrechten und bürgerlichen Freiheiten durch Bedienstete des Justizministeriums entgegenzunehmen und entsprechenden Informationen nachzugehen. Das OIG unterhält eine öffentliche Website — https://www.oig.justice.gov —, auf der auch eine „Hotline" zur Einreichung von Beschwerden zu finden ist: https://www.oig.justice.gov/hotline/index.htm.

b. Die Datenschutz- und Bürgerrechtsbeauftragten und -gremien innerhalb der US-Regierung sind ebenfalls mit entsprechenden Befugnissen ausgestattet. Beispiele:

i) In § 803 der Durchführungsempfehlungen zum 9/11 Commission Act von 2007, kodifiziert im United States Code unter 42 U.S.C. § 2000-ee1, werden für bestimmte Ministerien und Behörden (darunter das Außenministerium, das Justizministerium und das ODNI) Datenschutz- und Bürgerrechtsbeauftragte eingeführt. § 803 besagt, dass diese Datenschutz- und Bürgerrechtsbeauftragten als Hauptratgeber fungieren, die unter anderem sicherstellen sollen, dass das betreffende Ministerium, die Behörde oder der Dienst über angemessene Verfahren verfügt, um sich mit Beschwerden von Privatpersonen auseinanderzusetzen, die dem Ministerium, der Behörde oder dem Dienst vorwerfen, gegen ihre Datenschutz- oder Bürgerrechte verstoßen zu haben.

ii) Das Büro des ODNI für Bürgerrechte und Datenschutz (ODNI's Civil Liberties and Privacy Office, ODNI CLPO) wird geleitet vom Bürgerrechtsbeauftragten des ODNI, eines Amtes, das durch den National Security Act von 1948 in der geänderten Fassung eingeführt wurde. Zu den Pflichten des ODNI CLPO gehört die Schaffung der notwendigen Vorausetzungen dafür, dass die Strategien und Verfahren der Nachrichtendienste einen angemessenen Schutz der Privatsphäre und der bürgerlichen Freiheiten vorsehen, sowie die Prüfung und Untersuchung von Beschwerden wegen mutmaßlichen Amtsmissbrauchs oder Verstößen gegen die Bürgerrechte und den Datenschutz in Programmen und Aktivitäten des ODNI. Das ODNI CLPO stellt auf seiner Website Informationen für die Öffentlichkeit bereit, darunter auch Hinweise dazu, wie Beschwerden einzureichen sind: www.dni.gov/clpo. Geht beim ODNI CLPO eine Beschwerde wegen eines Verstoßes gegen den Datenschutz oder die Bürgerrechte ein, bei der IC-Programme und -Aktivitäten eine Rolle spielen, so spricht es mit den anderen Nachrichtendiensten ab, wie mit dieser Beschwerde innerhalb der Intelligence Community weiter verfahren werden soll. Hierzu sei angemerkt, dass die National Security Agency (NSA) ebenfalls über ein Büro für Bürgerrechte und Datenschutz verfügt, das auf seiner Website — https://www.nsa.gov/civil_liberties/ — Angaben zu seinen Zuständigkeiten bereitstellt. Liegen Informationen vor, dass eine Behörde gegen die Datenschutzbestimmungen verstößt (als Beispiel sei § 4 der PPD-28 genannt), dann verfügen die Behörden über Compliance-Mechanismen, mit denen ein solcher Vorfall geprüft und ausgeräumt wird. Nach PPD-28 sind die Behörden gehalten, Fälle von Nichteinhaltung der Vorschriften an das ODNI zu melden.

iii) Das Büro für Datenschutz und Bürgerrechte (Office of Privacy and Civil Liberties, OPCL) des Justizministeriums unterstützt den Leitenden Datenschutz- und Bürgerrechtsbeauftragten (Chief Privacy and Civil Liberties Officer, CPCLO) des Ministeriums bei der Wahrnehmung seiner Pflichten und Zuständigkeiten. Hauptaufgabe des OPCL ist der Schutz der Privatsphäre und der Bürgerrechte der amerikanischen Bürger durch Überprüfung, Kontrolle und Koordinierung der Datenschutzaktivitäten des Ministeriums. Das OPCL sorgt für die juristische Beratung und Anleitung der Struktureinheiten des Ministeriums und stellt sicher, dass das Ministerium sich an die geltenden Datenschutzbestimmungen hält, unter anderem an den Privacy Act von 1974, die Datenschutzbestimmungen des E-Government Act von 2002 und auch den Federal Information Security Management Act sowie an die verwaltungspolitischen Richtlinien, die im Nachgang zu diesen Gesetzen erlassen wurden; darüber hinaus konzipiert das Büro Datenschutzschulungen des Ministeriums und führt diese durch, unterstützt den CPCLO bei der Weiterentwicklung der Datenschutzstrategie des Ministeriums, verfasst Datenschutzberichte für den Präsidenten und den Kongress und überprüft den praktischen Umgang des Ministeriums mit Informationen, damit sichergestellt ist, dass dabei der Datenschutz und die Bürgerrechte respektiert werden. Das OPCL informiert die Öffentlichkeit unter http://www.justice.gov/opcl über seine Aufgaben.

iv) Damit der Datenschutz und die Bürgerrechte gewährleistet sind, überprüft das Privacy and Civil Liberties Oversight Board gemäß 42 U.S.C. § 2000ee ff. kontinuierlich (i) die Strategien und Verfahren der Ministerien, der Behörden und der Exekutive im Zusammenhang mit den Bemühungen zum Schutz der Nation vor Terrorismus und deren Umsetzung sowie (ii) andere Aktivitäten der Exekutive in Verbindung mit diesen Maßnahmen, um festzustellen, ob bei diesen Aktivitäten Datenschutz und Bürgerrechte angemessen geschützt werden und mit den für diesen Bereich geltenden Gesetzen, Rechtsvorschriften und Strategien konform gehen. Es nimmt Berichte und andere Informationen von Datenschutz- und Bürgerrechtsbeauftragten entgegen, prüft diese und erteilt den Betreffenden gegebenenfalls Empfehlungen zu ihrer Tätigkeit. In § 803 der Durchführungsempfehlungen zum 9/11 Commission Act von 2007, kodifiziert unter 42 U.S.C. § 2000ee-1, werden die Datenschutz- und Bürgerrechtsbeauftragten von acht Bundesbehörden (darunter der Verteidigungsminister, der

Minister für innere Sicherheit, der Director of National Intelligence und der CIA-Direktor) und etwaige zusätzliche Behörden, die vom Board benannt werden, angewiesen, dem PCLOB in regelmäßigen Abständen Berichte vorzulegen, unter anderem auch zu Anzahl, Art und Grundstimmung der Beschwerden, die bei der jeweiligen Behörde wegen mutmaßlicher Verstöße eingegangen sind. Nach dem Gesetz, das die Befugnisse des PCLOB regelt, ist das Board gehalten, diese Berichte entgegenzunehmen und gegebenenfalls den Datenschutz- und Bürgerrechtsbeauftragten Empfehlungen zu ihrer Tätigkeit zu erteilen.

ANHANG IV

Schreiben der Vorsitzenden der Federal Trade Commission Edith Ramirez

7. Juli 2016

PER E-MAIL

Věra Jourová
Kommissionsmitglied für Justiz, Verbraucherschutz und Gleichstellungsfragen
Europäische Kommission
Rue de la Loi/Wetstraat 200
1049 Brüssel
Belgien

Sehr geehrte Frau Jourová:

Die Federal Trade Commission der Vereinigten Staaten („FTC") nimmt gern diese Gelegenheit wahr, um darzulegen, wie sie die neue EU-US-Datenschutzschild-Regelung (die „Datenschutzschild-Regelung" oder „Regelung") durchzusetzen gedenkt. Nach unserer Auffassung wird die Regelung maßgeblich dazu beitragen, den datenschutzfreundlichen Geschäftsverkehr in einer zunehmend vernetzten Welt zu erleichtern. Sie wird Unternehmen in die Lage versetzen, in der globalen Wirtschaft wichtige Transaktionen durchzuführen, und zugleich sicherstellen, dass die Verbraucher in der EU ein hohes Maß an Datenschutz genießen.Die FTC bekennt sich schon seit Langem zum grenzüberschreitenden Datenschutz und wird der Durchsetzung der neuen Regelung eine hohe Priorität einräumen. Im Folgenden geben wir einen allgemeinen Überblick über die bisherigen Bemühungen der FTC um die konsequente Handhabung des Datenschutzes, namentlich der ursprünglich geltenden SAFE-Harbor-Regelung, und über die Vorstellungen der FTC zur Durchsetzung der neuen Regelung.

Zum ersten Mal verpflichtete sich die FTC im Jahr 2000 öffentlich dazu, die SAFE-Harbor-Regelung durchzusetzen. Der damalige FTC-Vorsitzende Robert Pitofsky sandte der Europäischen Kommission ein Schreiben, in dem er die Entschlossenheit der FTC unterstrich, den SAFE-Harbor-Datenschutzgrundsätzen mit Nachdruck Geltung zu verschaffen. Wie fast 40 Durchsetzungsmaßnahmen, zahlreiche zusätzliche Ermittlungen und die Zusammenarbeit mit einzelnen europäischen Datenschutzbehörden zu Fragen von gegenseitigem Interesse deutlich machen, hat die FTC ihre Zusage eingehalten.

Nachdem die Europäische Kommission im November 2013 Bedenken zur Verwaltung und Durchsetzung des SAFE-Harbor-Programms anmeldete, leiteten wir und das US-Handelsministerium Konsultationen mit Vertretern der Europäischen Kommission ein, um Möglichkeiten zur Stärkung des Programms zu erkunden. Während die Konsultationen noch im Gange waren, verkündete der Europäische Gerichtshof am 6. Oktober 2015 ein Urteil in der Rechtssache *Schrems*, das unter anderem die Entscheidung der Europäischen Kommission über die Angemessenheit des SAFE-Harbor-Programms für ungültig erklärte. Danach arbeiteten wir weiter eng mit dem Handelsministerium und der Europäischen Kommission zusammen, um den Datenschutz für Einzelpersonen in der EU effektiver zu gestalten. Die Datenschutzschild-Regelung ist ein Ergebnis dieser weiter andauernden Konsultationen. Wie beim SAFE-Harbor-Programm verpflichtet sich die FTC hiermit zur konsequenten Durchsetzung der neuen Regelung. Dieses Schreiben soll diese Verpflichtung dokumentieren.

Im Mittelpunkt unseres Engagements stehen vier Kernbereiche: (1) die vorrangige Behandlung von überwiesenen Fällen und Ermittlungen; (2) die Unterbindung falscher oder irreführender Angaben zur Mitgliedschaft im Datenschutzschild; (3) die Kontrolle der Befolgung von Verfügungen; und (4) verstärkte Kontakte zu Datenschutzbehörden der EU und engere Zusammenarbeit mit ihnen bei der Durchsetzung. Nachstehend machen wir zu jedem dieser Punkte detaillierte Angaben und geben Hintergrundinformationen zu dem Beitrag, den die FTC bisher zum Schutz von Verbraucherdaten und zur Durchsetzung des SAFE-Harbor-Programms leistete, sowie zur Gesamtsituation des Datenschutzes in den Vereinigten Staaten ([1]).

I. HINTERGRUND

A. **Durchsetzung des Datenschutzrechts durch die FTC und konzeptionelle Fragen**

Die FTC genießt umfassende zivilrechtliche Befugnisse zur Förderung des Verbraucherschutzes und des Wettbewerbs im Wirtschaftsleben. Im Rahmen ihres Auftrags zum Verbraucherschutz verschafft sie einem breiten Spektrum von

([1]) Zusätzliche Angaben über das US-Datenschutzrecht auf Bundesebene und in den Einzelstaaten finden Sie im Anhang A und einen Überblick über unsere neuesten Durchsetzungsmaßnahmen im Bereich Datenschutz und -sicherheit in Anhang B. Dieser Überblick ist auch auf der Website der FTC abrufbar unter https://www.ftc.gov/reports/privacy-data-security-update-2015.

Rechtsvorschriften Geltung und sorgt damit für den Schutz und die Sicherheit von Verbraucherdaten. Das wichtigste von ihr durchzusetzende Gesetz, der FTC Act, untersagt „unlautere" und „irreführende" Handlungen oder Praktiken, die den Geschäftsverkehr betreffen oder sich darauf auswirken ([1]). Eine Darstellung, Unterlassung oder Praxis ist irreführend, wenn sie rechtserheblich und geeignet ist, Verbraucher zu täuschen, die sich unter den gegebenen Umständen angemessen verhalten ([2]). Eine Handlung oder Praxis ist unlauter, wenn sie tatsächlich oder vermutlich einen erheblichen Schaden bewirkt, der von Verbrauchern unter normalen Umständen nicht zu vermeiden ist oder nicht durch ausgleichende Vorteile für die Verbraucher oder den Wettbewerb aufgewogen wird ([3]). Die FTC setzt auch Gesetze durch, die gezielt dem Schutz von Informationen über die Gesundheit, Kredite und andere finanzielle Daten dienen, sowie dem Schutz von Online-Informationen zu Kindern. Zu jedem dieser Gesetze hat sie Durchführungsverordnungen erlassen.

Nach dem FTC Act ist die FTC für Sachen zuständig, die „den Geschäftsverkehr betreffen oder sich darauf auswirken". Sie ist nicht befugt, strafrechtliche Maßnahmen zu ergreifen oder in Fragen der nationalen Sicherheit zu entscheiden. Auch liegen die meisten anderen hoheitlichen Maßnahmen außerhalb ihres Zuständigkeitsbereichs. Hinzu kommen Einschränkungen ihrer Kompetenzen im wirtschaftlichen Bereich, die den Bankensektor, den Luftverkehr, das Versicherungsgewerbe und die Betreiber öffentlicher Telekommunikationsnetze betreffen. Auch ist die FTC nicht zuständig für die meisten gemeinnützigen Organisationen, wohl aber für nur scheinbar karitative oder gemeinnützige Einrichtungen, die in Wirklichkeit gewinnorientiert sind. In ihren Aufgabenbereich fallen auch gemeinnützige Organisationen, die zugunsten gewinnorientierter Mitglieder kommerzielle Zwecke verfolgen, indem sie ihnen beispielsweise erhebliche wirtschaftliche Vorteile verschaffen ([4]). In manchen Fällen überschneiden sich die Kompetenzen der FTC mit denen anderer Strafverfolgungsbehörden.

Wir haben stabile Arbeitsbeziehungen zu Behörden des Bundes und der Einzelstaaten aufgebaut und arbeiten mit ihnen eng zusammen, um die Ermittlungen zu koordinieren oder gegebenenfalls Fälle an eine andere Stelle zu verweisen.

Die Durchsetzung ist der Dreh- und Angelpunkt des Datenschutzkonzepts der FTC. Die FTC ist bisher in über 500 Fällen Verstößen gegen den Schutz und die Sicherheit von Verbraucherdaten nachgegangen. Dabei geht es sowohl um Offline- als auch um Online-Daten und um Durchsetzungsmaßnahmen gegen große wie kleine Unternehmen, denen vorgeworfen wurde, dass sie nicht richtig mit sensiblen Verbraucherdaten umgingen, personenbezogene Daten von Verbrauchern nicht schützten, das Verhalten von Verbrauchern unter Vorspiegelung falscher Tatsachen online verfolgten, unerbetene Werbung an Verbraucher versendeten, Spyware oder andere Schadsoftware auf den PCs von Verbrauchern installierten, gegen das Anrufverbot und andere Regeln des Telemarketing verstießen und missbräuchlich Verbraucherdaten zu Mobilgeräten erfassten und weitergaben. Die Durchsetzungsmaßnahmen der FTC betrafen sowohl realwirtschaftliche als auch digitale Vorgänge und waren eine klare Ansage an die Unternehmen, dass sie die Privatsphäre von Verbrauchern zu respektieren haben.

Die FTC hat auch zahlreiche politische Initiativen zur wirksameren Gestaltung des Verbraucherschutzes verfolgt, die das Ziel all seiner Durchsetzungsmaßnahmen ist. Sie hat Workshops veranstaltet und Berichte mit Empfehlungen zu bewährten Verfahren herausgegeben, die auf folgende Ziele gerichtet sind: besserer Schutz der Privatsphäre im Mobile-Ökosystem; größere Transparenz in der Datenmaklerbranche; Ausschöpfung des Potenzials von Big Data bei gleichzeitiger Minderung der Risiken, insbesondere für Geringverdiener und unterversorgte Verbraucher; und Verdeutlichung der datenschutzrechtlichen und sicherheitstechnischen Probleme, die sich aus der Gesichtserkennung, dem „Internet der Dinge" und anderen Entwicklungen ergeben.

Die FTC bemüht sich auch um die Aufklärung von Verbrauchern und Unternehmen, damit ihre Initiativen zur Durchsetzung der Regeln und zur Politikgestaltung stärker zum Tragen kommen. Sie nutzte ein breites Instrumentarium — Veröffentlichungen, Online-Ressourcen, Workshops und soziale Medien —, um Informationsmaterial zu einem breiten Spektrum von Themen, darunter mobile Apps, Schutz der Privatsphäre von Kindern und Datensicherheit, zur Verfügung zu stellen. Unlängst brachte die Kommission ihre Initiative „Start With Security" mit neuen Leitlinien für Unternehmen auf den Weg, die auf den Erfahrungen mit Datenschutzfällen der Behörde sowie einer Reihe von Workshops in verschiedenen Teilen des Landes aufbauen. Überdies spielt die FTC seit Langem eine führende Rolle bei der Aufklärung der Verbraucher über Grundfragen der Computersicherheit. Im letzten Jahr verzeichneten unsere Website OnGuard Online und ihr spanischsprachiges Pendant Alerta en Línea über fünf Millionen Aufrufe.

B. **US-Rechtsschutz kommt EU-Verbrauchern zugute**

Die Regelung ist im Gesamtzusammenhang des US-Datenschutzes zu sehen, der EU-Verbraucher auf verschiedene Weise schützt.

([1]) 15 U.S.C. § 45(a).

([2]) *Siehe* FTC Policy Statement on Deception, *appended to Cliffdale Assocs., Inc.*, 103 F.T.C. 110, 174 (1984), *abrufbar unter* https://www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception.

([3]) *Siehe* 15 U.S.C § 45(n); FTC Policy Statement on Unfairness, *appended to Int'l Harvester Co.*, 104 F.T.C. 949, 1070 (1984), *abrufbar unter* https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness.

([4]) *Siehe California Dental Ass'n v. FTC*, 526 U, S. 756 (1999).

Das im FTC Act verankerte Verbot unlauterer oder irreführender Handlungen oder Praktiken ist nicht darauf beschränkt, US-Verbraucher vor US-Unternehmen zu schützen, da es Praktiken einschließt, die (1) tatsächlich oder wahrscheinlich einen nach vernünftigem Ermessen vorhersehbaren Schaden in den Vereinigten Staaten bewirken oder (2) entscheidungserhebliches Verhalten in den Vereinigten Staaten dabei eine Rolle spielt. Zudem kann die FTC beim Schutz ausländischer Verbraucher alle Rechtsbehelfe in Anspruch nehmen, darunter eine Wiederherstellungsklage, die zum Schutz inländischer Verbraucher zur Verfügung stehen.

Die Durchsetzungsmaßnahmen der FTC zahlen sich sowohl für amerikanische als auch für ausländische Verbraucher deutlich aus. Beispielsweise galten die Klagen zur Durchsetzung von § 5 des FTC Act dem Schutz der Privatsphäre sowohl amerikanischer als auch ausländischer Verbraucher. In einem Fall, der den Informationsbroker Accusearch betraf, vertrat die FTC den Standpunkt, dass der Verkauf vertraulicher Telefondaten an Dritte ohne Wissen oder Zustimmung des Verbrauchers unlauteres Handeln darstellte und gegen § 5 des FTC verstieß. Accusearch verkaufte Daten, die sowohl US-Bürger als auch ausländische Verbraucher betrafen ([1]). Das Gericht erließ eine einstweilige Verfügung, die Accusearch unter anderem die Vermarktung oder den Verkauf personenbezogener Daten von Verbrauchern ohne schriftliche Einwilligung untersagte, sofern sie nicht rechtmäßig aus öffentlich zugänglichen Informationen beschafft wurden, und verhängte eine Geldbuße von fast 200 000 USD ([2]).

Ein weiteres Beispiel ist der Vergleich, den die FTC mit TRUSTe geschlossen hat. Er stellt sicher, dass sich Verbraucher — auch in der Europäischen Union — auf Erklärungen verlassen können, die eine zur Selbstkontrolle verpflichtete globale Organisation zur Überprüfung und Zertifizierung von inländischen und ausländischen Online-Diensten abgibt ([3]). Hervorzuheben ist dabei, dass unser Vorgehen gegen TRUSTe auch das Selbstkontrollsystem im Bereich des Datenschutzes insgesamt stärkt, denn es gewährleistet die Rechenschaftspflicht von Einrichtungen, die in Systemen der freiwilligen Selbstkontrolle eine wichtige Rolle spielen, wozu auch grenzüberschreitende Datenschutzregelungen gehören.

Die FTC setzt darüber hinaus weitere zielgerichtete Rechtsvorschriften durch, deren Schutzwirkung sich auch auf Nicht-US-Verbraucher erstreckt, beispielsweise den Children's Online Privacy Protection Act („COPPA"). Dieses Gesetz schreibt vor, dass Betreiber von Websites und Online-Diensten, die für Kinder bestimmt sind, sowie von allgemeinen Websites, die wissentlich personenbezogene Daten von Kinder unter 13 Jahren erfassen, die Eltern davon in Kenntnis setzen und deren nachprüfbare Zustimmung einholen müssen. In den USA beheimatete Websites und Dienste, die dem COPPA unterliegen und personenbezogene Daten ausländischer Kinder erfassen, müssen das Gesetz einhalten. Es gilt auch für ausländische Websites und Online-Dienste, wenn sie für Kinder in den Vereinigten Staaten bestimmt sind oder wenn wissentlich personenbezogene Daten von Kindern in den USA erfasst werden. Neben den von der FTC durchgesetzten Bundesgesetzen können sich noch weitere Verbraucherschutz- und Datenschutzregelungen des Bundes und der Einzelstaaten als vorteilhaft für EU-Verbraucher erweisen.

C. **Durchsetzung der SAFE-Harbor-Regelung**

Im Rahmen ihres Programms zur Durchsetzung des Datenschutzes und der Datensicherheit bemühte sich die FTC zudem um den Schutz der EU-Verbraucher, indem sie bei Verstößen gegen die SAFE-Harbor-Regelung Durchsetzungsmaßnahmen einleitete. Die FTC hat im Rahmen von SAFE Harbor 39 Durchsetzungsmaßnahmen eingeleitet: In 36 Fällen ging es um falsche Angaben zur Zertifizierung und in drei Fällen — Google, Facebook und Myspace — um mutmaßliche Verstöße gegen Datenschutzgrundsätze von SAFE Harbor ([4]). Diese Verfahren belegen, dass korrekte Angaben zur Zertifizierung durchgesetzt werden können und welche Folgen Verstöße nach sich ziehen. Mit Zustimmung der Gegenseite erlassene „Consent orders" mit einer Geltungsdauer von zwanzig Jahren verpflichten Google, Facebook und Myspace dazu, umfassende Datenschutzprogramme zu erstellen, die nach menschlichem Ermessen so konzipiert sind, dass sie Datenschutzrisiken abdecken, die sich aus der Entwicklung bzw. Verwaltung neuer und bestehender Produkte und Dienstleistungen ergeben, und die Privatsphäre und die Vertraulichkeit personenbezogener Daten schützen. Die aufgrund dieser Verfügungen erstellten umfassenden Datenschutzprogramme müssen wesentliche vorhersehbare Risiken benennen und Kontrollen zur Ausräumung dieser Risiken vorsehen. Zudem müssen sich die Unternehmen kontinuierlichen unabhängigen Einschätzungen ihrer Datenschutzprogramme unterziehen, die der FTC vorzulegen sind. In den Verfügungen wird diesen Unternehmen auch untersagt, falsche Angaben zu ihrer Datenschutzpraxis und zur Beteiligung an einem Datenschutz- oder Sicherheitsprogramm zu machen. Dieses Verbot würde auch für die Handlungen und Praktiken von Unternehmen im Rahmen der neuen Datenschutzschild-Regelung gelten. Die FTC kann diese Verfügungen durch zivilrechtliche Klagen durchsetzen. So hat Google 2012 ein Bußgeld in Rekordhöhe, nämlich

([1]) Siehe Office of the Privacy Commissioner of Canada, Complaint under PIPEDA against Accusearch, Inc., doing business as Abika.com, https://www.priv.gc.ca/cf-dc/2009/2009_009_0731_e.asp. Das Büro des kanadischen Datenschutzbeauftragten legte im Rechtsmittelverfahren gegen die FTC-Maßnahme einen Amicus-curiae-Schriftsatz vor und führte eigene Ermittlungen durch, die zu dem Schluss führten, dass die Praktiken von Accusearch auch gegen kanadisches Recht verstießen.

([2]) *Siehe FTC v. Accusearch, Inc.*, No. 06CV015D (D. Wyo. Dec. 20, 2007), *aff'd* 570 F.3d 1187 (10th Cir. 2009).

([3]) *Siehe In the Matter of True Ultimate Standards Everywhere, Inc.*, No. C-4512 (F.T.C. Mar. 12, 2015) (Entscheidung und Verfügung), *abrufbar unter* https://www ftc.gov/system/files/documents/cases/150318trust-edo.pdf.

([4]) *Siehe In the Matter of Google, Inc.*, No. C-4336 (F.T.C. Oct. 13 2011) (Entscheidung und Verfügung), *abrufbar unter* https://www.ftc.gov/news-events/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz; *In the Matter of Facebook, Inc.*, No. C-4365 (F.T.C. July 27, 2012) (Entscheidung und Verfügung), *abrufbar unter* https://www.ftc.gov/news-events/press-releases/2012/08/ftc-approves-final-settlement-facebook; *In the Matter of Myspace LLC*, No. C-4369 (F.T.C. Aug. 30, 2012) (Entscheidung und Verfügung), *abrufbar unter* https://www.ftc.gov/news-events/press-releases/2012/09/ftc-finalizes-privacy-settlement-myspace.

22,5 Mio. USD, gezahlt, weil ihm Verstöße gegen die Verfügung vorgeworfen wurden. Die Maßnahmen der FTC tragen also zum Schutz von über einer Milliarde Verbraucher in der Welt bei, von denen Hunderte von Millionen in Europa beheimatet sind.

Einen weiteren Schwerpunkt der FTC bildeten falsche oder irreführende Behauptungen über eine Beteiligung an der SAFE-Harbor-Regelung. Die FTC nimmt derartige falsche Angaben sehr ernst. Beispielsweise erhob die FTC 2011 in der Rechtssache *FTC/Karnani* Klage gegen einen Internet-Anbieter in den Vereinigten Staaten, dem vorgeworfen wurde, dass er und sein Unternehmen britischen Verbrauchern vortäuschte, der Sitz der Firma befände sich im Vereinigten Königreich, indem er unter anderem Webadressen mit der Endung.uk verwendete und auf die britische Währung und das britische Postsystem Bezug nahm ([1]). Als aber die Ware eintraf, stellten die Käufer fest, dass darauf wider Erwarten Einfuhrzölle erhoben wurden, die Garantiezusagen im Vereinigten Königreich nichts galten und Kosten für die Erstattung der Zollgebühren anfielen. Die FTC machte zudem geltend, dass die Beklagten die Verbraucher über ihre Beteiligung am SAFE-Harbor-Programm getäuscht hatten. Im Übrigen waren alle Opfer des Betrugs Briten.

Bei vielen anderen Verfahren zur Durchsetzung der SAFE-Harbor-Regelung ging es um Organisationen, die dem Programm beitraten, ohne ihre Zertifizierung jährlich zu erneuern, sich aber weiterhin als aktuelle Mitglieder ausgaben. Wie weiter unten dargelegt, verpflichtet sich die FTC auch dazu, gegen falsche Angaben über die Beteiligung an der Datenschutzschild-Regelung vorzugehen. Diese strategischen Durchsetzungsmaßnahmen ergänzen die verstärkten Bemühungen des Handelsministeriums, die Einhaltung der Anforderungen an die Zertifizierung und Rezertifizierung zu überprüfen, die tatsächliche Einhaltung zu überwachen, unter anderem durch Fragebogenaktionen bei den Teilnehmern, und falsche Angaben zur Mitgliedschaft im Datenschutzschild und Fälle des Missbrauchs von Zertifizierungsmarken aufzudecken ([2]).

II. DIE VORRANGIGE BEHANDLUNG VON ÜBERWIESENEN FÄLLEN UND ERMITTLUNGEN

Wie schon beim SAFE-Harbor-Programm verpflichtet sich die FTC, die ihr von EU-Mitgliedstaaten im Rahmen des Datenschutzschilds zugeleiteten Fälle vorrangig zu behandeln. Priorität haben auch Fälle, die Verstöße gegen die für den Datenschutzschild geltenden Leitlinien der freiwilligen Selbstkontrolle betreffen und mit denen wir von Einrichtungen der Selbstkontrolle und anderen unabhängigen Beschwerdestellen befasst werden.

Um im Rahmen der Regelung die Zuleitung von Fällen aus den EU-Mitgliedstaaten zu erleichtern, richtet die FTC ein standardisiertes Verweisungsverfahren ein und gibt den EU-Mitgliedstaaten eine Anleitung dazu, welche Art von Informationen für die FTC bei den Ermittlungen zu einem ihr zugeleiteten Fall besonders hilfreich ist. Zu diesem Zweck benennt die FTC innerhalb der Behörde eine Kontaktstelle für aus den EU-Mitgliedstaaten weitergeleitete Fälle. Es ist zweifellos von Vorteil, wenn die vorlegende Behörde bereits eine Voruntersuchung des mutmaßlichen Verstoßes eingeleitet hat und bei den Ermittlungen mit der FTC zusammenarbeiten kann.

Wenn ein EU-Mitgliedstaat oder eine der Selbstkontrolle unterliegende Organisation die FTC mit einer Sache befasst, kann diese eine Reihe von Maßnahmen ergreifen, um die aufgeworfenen Fragen zu klären. Beispielsweise können wir die Datenschutzpolitik des Unternehmens überprüfen; zusätzliche Informationen direkt beim Unternehmen oder bei Dritten einholen; die vorlegende Stelle dazu befragen; untersuchen, ob die Verstöße systematisch erfolgen oder eine größere Anzahl von Verbrauchern betreffen; in Erfahrung bringen, ob der uns zugeleitete Fall Fragen berührt, die in den Zuständigkeitsbereich des Handelsministeriums fallen; prüfen, ob Aufklärungsmaßnahmen für Verbraucher und Unternehmen hilfreich wären; und gegebenenfalls ein Verfahren einleiten.

Die FTC verpflichtet sich auch dazu, mit den vorlegenden Durchsetzungsinstanzen Informationen über die ihr zugeleiteten Sachen auszutauschen, unter anderem zu deren Status im Hinblick auf Geheimhaltungsvorschriften und Einschränkungen. In dem Maße, wie es Anzahl und Art der überwiesenen Fälle erlauben, enthalten die Informationen eine Beurteilung der Fälle, einschließlich einer Beschreibung der aufgeworfenen Kernfragen und der Maßnahmen, die gegen Verstöße im Zuständigkeitsbereich der FTC ergriffen wurden. Die FTC unterrichtet die vorlegende Behörde auch über die Art der ihr zugeleiteten Fälle, um die Wirksamkeit der Bemühungen um die Ahndung gesetzwidrigen Verhaltens zu erhöhen. Wenn eine vorlegende Durchsetzungsinstanz um Informationen zum Status eines bestimmten Falles ersucht,

([1]) *Siehe FTC v. Karnani*, No. 2:09-cv-05276 (C.D. Cal. May 20, 2011) (abschließende Verfügung), *abrufbar unter* https://www ftc.gov/sites/default/files/documents/cases/2011/06/110609karnanistip.pdf; *siehe auch* Lesley Fair, FTC Business Center Blog, *Around the World in Shady Ways*, https://www.ftc.gov/blog/2011/06/around-world-shady-ways (9. Juni 2011).

([2]) Schreiben von Ken Hyatt, geschäftsführender Staatssekretär für internationalen Handel im Handelsministerium, Leiter der International Trade Administration, an Věra Jourová, Kommissionsmitglied für Justiz, Verbraucherschutz und Gleichstellungsfragen.

um eigene Durchsetzungsmaßnahmen zu verfolgen, wird die FTC diesem Wunsch nachkommen, wobei sie die Anzahl der jeweils zu prüfenden Sachen ebenso berücksichtigt wie Geheimhaltungsvorschriften sowie andere rechtliche Vorgaben.

Die FTC wird auch eng mit den Datenschutzbehörden der EU zusammenarbeiten, um die Durchsetzung der Regelung zu unterstützen. In bestimmten Fällen könnten ein Informationsaustausch und Amtshilfe bei Ermittlungen gemäß U.S. SAFE WEB Act dazugehören, denn dieses Gesetz gestattet der FTC, ausländischen Strafverfolgungsbehörden Amtshilfe zu leisten, wenn die betreffende ausländische Behörde Vorschriften zur Unterbindung von Praktiken durchsetzt, die im Wesentlichen denen entsprechen, die auch nach den von der FTC durchgesetzten Vorschriften strafbar sind ([1]). Im Rahmen dieser Amtshilfe kann die FTC Informationen weitergeben, die sie im Zusammenhang mit eigenen Ermittlungen erlangt hat, Zwangsmaßnahmen zur Beweissicherung im Auftrag von Datenschutzbehörden der EU anordnen, die eigene Ermittlungen durchführen, und Zeugen oder Beschuldigte im Zusammenhang mit Durchsetzungsmaßnahmen der Datenschutzbehörden anhören, wobei die Bestimmungen des U.S. SAFE WEB Act einzuhalten sind. Die FTC macht regelmäßig von diesem Recht Gebrauch, um anderen Behörden weltweit bei Daten- und Verbraucherschutzsachen zur Seite zu stehen ([2]).

Die FTC räumt nicht nur im Rahmen des Datenschutzschilds den Fällen, die ihr von EU-Mitgliedstaaten und der Selbstkontrolle unterliegenden Organisationen zugeleitet werden, Priorität ein ([3]), sondern verpflichtet sich auch dazu, mögliche Verstöße gegen die Regelung gegebenenfalls aus eigener Initiative zu untersuchen und dazu verschiedene Instrumente einzusetzen.

Seit gut einem Jahrzehnt verfolgt die FTC ein tragfähiges Programm zur Untersuchung von Datenschutz- und Sicherheitsproblemen, die in Unternehmen auftreten. Im Rahmen dieser Ermittlungen prüfte die FTC routinemäßig, ob sich die Unternehmen öffentlich zu den SAFE-Harbor-Grundsätzen bekannten. Wenn dies der Fall war, die Ermittlungen aber offensichtliche Verstöße gegen diese Grundsätze erkennen ließen, berücksichtigte die FTC das mutmaßliche Fehlverhalten bei ihren Durchsetzungsmaßnahmen. Wir werden bei der neuen Regelung an diesem offensiven Vorgehen festhalten. Anzumerken ist, dass die Zahl der Untersuchungen, die von der FTC eingeleitet werden, wesentlich höher ist als die Zahl der Untersuchungen, die letztendlich zu öffentlichen Durchsetzungsmaßnahmen führen. Vielfach werden Ermittlungen der FTC eingestellt, weil keine offensichtlichen Rechtsverstöße erkennbar sind. Da die Untersuchungen vertraulich und nicht öffentlich zugänglich sind, wird häufig auch die Einstellung nicht publik gemacht.

Die fast 40 Durchsetzungsmaßnahmen, die von der FTC im Zusammenhang mit dem SAFE-Harbor-Programm ergriffen wurden, belegen den Einsatz der Behörde für eine offensive Durchsetzung grenzüberschreitender Datenschutzregelungen. Die FTC wird bei ihren regelmäßigen Untersuchungen im Bereich des Datenschutzes und der Sicherheit auf mögliche Verstöße gegen die neue Regelung achten.

III. UNTERBINDUNG FALSCHER ODER IRREFÜHRENDER ANGABEN ZUR MITGLIEDSCHAFT IM DATENSCHUTZSCHILD

Wie bereits ausgeführt, wird die FTC gegen Unternehmen vorgehen, die falsche Angaben zu ihrer Beteiligung an der Regelung machen. Priorität erhalten dabei die Fälle, die ihr vom Handelsministerium zugeleitet werden und Organisationen betreffen, die wahrheitswidrig behaupten, aktuelle Mitglieder der Regelung zu sein, oder unbefugt Zertifizierungsmarken der Regelung verwenden.

Wenn im Übrigen eine Organisation in ihren Datenschutzbestimmungen zusichert, dass sie sich an die Grundsätze des Datenschutzschilds hält, reicht die bloße Tatsache, dass sie sich beim Handelsministerium nicht registrieren lässt oder ihre Registrierung nicht verlängert, nicht aus, um sich der Durchsetzung dieser Zusicherungen durch die FTC zu entziehen.

([1]) Zur Beantwortung der Frage, ob sie ihre Befugnisse nach dem U.S. SAFE WEB Act ausüben sollte, prüft die FTC unter anderem, „(A) ob die vorlegende Behörde sich dazu bereit erklärt hat, ihrerseits der Kommission Amtshilfe zu leisten; (B) ob die Befürwortung des Antrags dem öffentlichen Interesse der Vereinigten Staaten zuwiderlaufen würde; und (C) ob die Ermittlungen oder Durchsetzungsmaßnahmen der vorlegenden Behörde Handlungen oder Praktiken zum Gegenstand haben, die einer größeren Zahl von Personen tatsächlich oder voraussichtlich zum Schaden gereichen." 15 U.S.C. § 46(j)(3). Die Befugnisse erstrecken sich nicht auf die Durchsetzung von Wettbewerbsvorschriften.

([2]) In den Haushaltsjahren 2012-2015 beispielsweise machte die FTC Gebrauch von ihren Befugnissen gemäß U.S. SAFE WEB Act, um auf fast 60 Anträge ausländischer Behörden hin Informationen weiterzugeben, und erließ fast 60 „civil investigative demands" (Auskunftsersuchen zur Beweissicherung) und leistete damit Amtshilfe in 25 ausländischen Ermittlungsverfahren.

([3]) Auch wenn die FTC keinen Beschwerden einzelner Verbraucher nachgeht oder dabei vermittelt, wird sie Fälle, die ihr von Datenschutzbehörden der EU im Rahmen des Datenschutzschilds zugeleitet werden, vorrangig behandeln. Zudem wertet die FTC Beschwerden für ihre Datenbank Consumer Sentinel aus, die vielen Strafverfolgungsbehörden zugänglich ist, um Trends zu erkennen, Schwerpunkte der Durchsetzung festzulegen und mögliche Ziele von Ermittlungen auszumachen. EU-Bürger können dasselbe Beschwerdesystem, das US-Bürgern zur Verfügung steht, für eine Beschwerde an die FTC unter www.ftc.gov/complaint nutzen. Bei Individualbeschwerden, die den Datenschutzschild betreffen, ist es aber für EU-Bürger am zweckmäßigsten, wenn sie ihre Beschwerde bei einer Datenschutzbehörde ihres Mitgliedstaats oder einer Schiedsstelle einreichen.

IV. KONTROLLE DER BEFOLGUNG VON VERFÜGUNGEN

Die FTC bekräftigt zudem die von ihr eingegangene Verpflichtung, die Befolgung von Verfügungen zu überwachen, um die Einhaltung der Datenschutzschild-Regelung zu gewährleisten.

Wir werden bei künftigen die Regelung betreffenden FTC-Verfügungen durch eine Vielzahl geeigneter vorläufiger Anordnungen auf die Einhaltung der Grundsätze hinwirken. Dazu gehört die Untersagung von falschen Angaben zur neuen Regelung oder anderen Datenschutzprogrammen, wenn diese die Grundlage für das Vorgehen der FTC bilden.

Die bisherigen Verfahren der FTC zur Durchsetzung des SAFE-Harbor-Programms sind sehr aufschlussreich. In den 36 Fällen, die falsche oder irreführende Angaben zur SAFE-Habor-Zertifizierung betrafen, untersagt die jeweilige Verfügung den Beklagten, falsche Angaben zur Beteiligung an SAFE Harbor oder anderen Datenschutz- bzw. Sicherheitsprogrammen zu machen, und verpflichtet das Unternehmen dazu, der FTC Compliance-Berichte vorzulegen. Wenn es in den Verfahren um Verstöße gegen die Datenschutzgrundsätze von SAFE Harbor ging, wurde es den Unternehmen zur Auflage gemacht, umfassende Datenschutzprogramme einzurichten und zwanzig Jahre lang alle zwei Jahre für unabhängige externe Einschätzungen dieser Programme zu sorgen, die der FTC vorzulegen sind.

Die Nichtbefolgung von Verfügungen der FTC kann zur Folge haben, dass je Verstoß ein Bußgeld von bis zu 16 000 USD und bei anhaltenden Verstößen von 16 000 USD je Tag verhängt wird ([1]). Wenn sich die Praktiken auf zahlreiche Verbraucher auswirken, kann sich die Summe schnell auf Millionen von Dollar belaufen. Jeder „Consent order" ist auch mit Berichts- und Einhaltungspflichten verbunden. Die betroffenen Unternehmen müssen über einen festgelegten Zeitraum die Belege für regelkonformes Verhalten aufbewahren. Auch sind sie gehalten, die Verfügungen an die Mitarbeiter weiterzuleiten, die für die Befolgung zuständig sind.

Wie bei all ihren Verfügungen kontrolliert die FTC auch bei SAFE Harbor systematisch die Einhaltung der Auflagen. Sie nimmt die Durchsetzung ihrer Verfügungen in den Bereichen Datenschutz und -sicherheit sehr ernst und leitet erforderlichenfalls dazu juristische Schritte ein. Wie schon erwähnt, zahlte Google aufgrund der Anschuldigung, es habe gegen eine FTC-Verfügung verstoßen, ein Bußgeld von 22,5 Mio. USD. Die Verfügungen der FTC werden auch künftig alle Verbraucher weltweit schützen, die Kunden eines Unternehmens sind, und nicht nur jene unter ihnen, die Beschwerden eingereicht haben.

Abschließend dazu sei betont, dass die FTC weiterhin eine Online-Liste von Unternehmen führen wird, die Auflagen im Zusammenhang mit der Durchsetzung des SAFE-Harbor-Programms und der neuen Datenschutzschild-Regelung unterliegen ([2]). Überdies sind nach den Grundsätzen des Datenschutzschilds alle Unternehmen, die aufgrund von Verstößen gegen die Grundsätze Auflagen der FTC oder eines Gerichts erfüllen müssen, jetzt dazu verpflichtet, sämtliche die Regelung betreffenden Abschnitte eines der FTC vorgelegten Compliance- oder Prüfberichts publik zu machen, soweit die Geheimhaltungsvorschriften und -regeln dies gestatten.

V. VERSTÄRKTE KONTAKTE ZU DATENSCHUTZBEHÖRDEN DER EU UND ENGERE ZUSAMMENARBEIT MIT IHNEN BEI DER DURCHSETZUNG

Die FTC erkennt die wichtige Rolle an, die Datenschutzbehörden der EU bei der Einhaltung der Regelung spielen, und befürwortet verstärkte Konsultationen und eine engere Zusammenarbeit bei der Durchsetzung. Über Rücksprachen mit vorlegenden Datenschutzbehörden zu fallspezifischen Fragen hinaus verpflichtet sich die FTC, an regelmäßigen Zusammenkünften mit dazu benannten Vertretern der Artikel-29-Datenschutzgruppe teilzunehmen, um in allgemeiner Form darüber zu diskutieren, wie sich die Zusammenarbeit bei der Durchsetzung der Regelung verbessern lässt. Die FTC wird sich zudem gemeinsam mit dem Handelsministerium, der Europäischen Kommission und Vertretern der Artikel-20-Datenschutzgruppe an der jährlichen Überprüfung der Regelung beteiligen, um die praktische Umsetzung zu erörtern.

Die FTC wirkt auch auf die Entwicklung von Instrumenten hin, die eine verstärkte Zusammenarbeit mit Datenschutzbehörden der EU sowie ähnlichen Einrichtungen in der ganzen Welt bei Durchsetzungsmaßnahmen ermöglichen. Vor allem hat die FTC zusammen mit Partnern in der Europäischen Union und der übrigen Welt im letzten Jahr ein Warnsystem innerhalb des Global Privacy Enforcement Network („GPEN") ins Leben gerufen, um Informationen über Ermittlungen auszutauschen und die Koordinierung der Durchsetzungsmaßnahmen zu fördern. Dieses als „GPEN Alert" bezeichnete Instrument könnte sich bei der Datenschutzschild-Regelung als besonders nützlich erweisen. Die FTC und die Datenschutzbehörden der EU könnten es für diesbezügliche und andere datenschutzrechtliche Ermittlungen nutzen, auch als Ausgangspunkt für den Informationsaustausch, um für einen besser koordinierten und effektiveren Verbraucherschutz zu sorgen. Wir sehen erwartungsvoll der weiteren Zusammenarbeit mit den beteiligten EU-Behörden

([1]) 15 U.S.C. § 45(m); 16 C.F.R. § 1.98.
([2]) *Siehe* FTC, Business Center, Legal Resources, https://www.ftc.gov/tips-advice/business-center/legal-resources?type=case&field-consumer-protection-topics-tid=251.

entgegen, damit wir das GPEN-Alert-System auf noch breiterer Grundlage einsetzen und weitere Instrumente entwickeln können, die zur Verbesserung der Zusammenarbeit bei der Durchsetzung des Datenschutzes, auch im Rahmen der neuen Regelung, beitragen.

Die FTC bekennt sich hiermit zu ihrer Verpflichtung, der neuen Datenschutzschild-Regelung zum Erfolg zu verhelfen. Wir freuen uns darauf, weiterhin im Zusammenwirken mit unseren Kollegen in der EU den Verbraucherschutz beiderseits des Atlantiks zu befördern.

Hochachtungsvoll

Edith Ramirez

Vorsitzende

Anlage A

Der EU-US-Datenschutzschild in der Praxis: Ein Überblick über das Datenschutz- und -sicherheitsumfeld in den USA

Das durch die Regelung zum EU-US-Datenschutzschild („die Regelung") gebotene Sicherheitsniveau ist in die umfassenderen Datenschutzvorschriften des US-Rechtssystems eingebettet. Erstens wacht die Federal Trade Commission („FTC") der USA mithilfe eines wirksamen Datenschutz- und -sicherheitsprogramms für US-Geschäftspraktiken über den weltweiten Verbraucherschutz. Zweitens hat sich das Umfeld für Verbraucherdatenschutz und -sicherheit in den USA seit dem Jahre 2000, als die ursprüngliche SAFE-Harbor-Regelung zwischen den USA und der EU angenommen wurde, merklich gewandelt. In der Zwischenzeit wurden auf Bundesebene und in den Einzelstaaten zahlreiche Gesetze zum Datenschutz und zur Datensicherheit erlassen, und es war ein deutlicher Anstieg bei der Zahl der Verwaltungs- und Zivilprozesse zur Durchsetzung der Datenschutzrechte zu vermelden. Ergänzt wird der für Einzelpersonen in der EU mit der neuen Regelung verbundene Rechtsschutz durch ein breites Spektrum an US-Rechtsvorschriften für den Schutz und die Sicherheit von Verbraucherdaten, die für den Umgang mit Geschäftsdaten gelten.

I. DAS ALLGEMEINE PROGRAMM DES FTC ZUR DURCHSETZUNG DES DATENSCHUTZES UND DER DATENSICHERHEIT

Die FTC ist die führende Verbraucherschutzbehörde in den USA und vorrangig im Bereich des Datenschutzes im Geschäftsverkehr aktiv. Sie ist befugt, unlautere und irreführende Handlungen oder Praktiken, die gegen den Verbraucherdatenschutz verstoßen, zu verfolgen und zielgenauere Datenschutzregelungen durchzusetzen, um bestimmte Finanz- und Gesundheitsdaten, Daten von Kindern sowie Daten, auf deren Grundlage bestimmte Entscheidungen über Anspruchsberechtigungen von Verbrauchern getroffen werden, zu schützen.

Die FTC verfügt über einzigartige Erfahrungen im Bereich der Durchsetzung des Verbraucherdatenschutzes. Die bisherigen Durchsetzungsmaßnahmen der FTC betrafen gesetzwidrige Praktiken im Offline- und Online-Umfeld. So hat die FTC beispielsweise Durchsetzungsmaßnahmen gegen bekannte Unternehmen wie Google, Facebook, Twitter, Microsoft, Wyndham, Oracle, HTC und Snapchat sowie gegen weniger bekannte Unternehmen eingeleitet. Sie hat Unternehmen verklagt, denen vorgeworfen wurde, unerbetene Werbung an Verbraucher zu senden, Spyware auf PCs zu installieren, personenbezogene Daten von Verbrauchern nicht zu schützen, das Verhalten von Verbrauchern unter Vorspiegelung falscher Tatsachen online zu verfolgen, die Privatsphäre von Kindern zu verletzen, missbräuchlich Verbraucherdaten über Mobilgeräte zu erfassen und Endgeräte mit Internet-Zugang, die zur Speicherung personenbezogener Daten genutzt werden, nicht zu sichern. In der Regel wurde in diesen Fällen für einen Zeitraum von zwanzig Jahren eine kontinuierliche Überwachung durch die FTC angeordnet, weitere Gesetzesverstöße wurden untersagt und hohe Geldstraßen für den Fall angekündigt, dass die Unternehmen gegen diese Verfügungen verstoßen ([1]). Die Verfügungen der FTC schützen nicht nur jene Verbraucher, die Beschwerde eingereicht haben, sondern alle Verbraucher, die Kunde eines Unternehmens sind. Auf grenzüberschreitender Ebene ist die FTC für den weltweiten Verbraucherschutz im Zusammenhang mit allen in den USA stattfindenden Praktiken zuständig ([2]).

Bisher ist die FTC Verstößen in mehr als 130 Spam- und Spyware-Fällen nachgegangen, hat über 120 Anrufsverbote im Telemarketing verhängt, mehr als 100 Maßnahmen im Bereich des Fair Credit Reporting Act (Gesetz zur Regelung des Datenschutzes bei Konsumentenkrediten) ergriffen, ist in nahezu 60 Datensicherheitsfällen und mehr als 50 allgemeinen Datenschutzfällen sowie in etwa 30 Fällen einer Verletzung des Gramm-Leach-Bliley Act tätig geworden und hat mehr als 20 Maßnahmen zur Durchsetzung des Children's Online Privacy Protection Act („COPPA") eingeleitet ([3]). Neben den genannten Fällen hat die FTC auch Warnschreiben verfasst und herausgegeben ([4]).

([1]) Gegen ein Unternehmen, das gegen eine Verfügung der FTC verstößt, kann ein Bußgeld von bis zu 16 000 USD und bei anhaltenden Verstößen von 16 000 USD je Tag verhängt werden. Siehe 15 U.S.C. § 45(l); 16 C.F.R. § 1.98(c).

([2]) Der Kongress hat ausdrücklich die Befugnis der FTC bekräftigt, Rechtsbehelfe, darunter auch eine Wiederherstellungsklage, in Anspruch zu nehmen bei allen für den Außenhandel bedeutenden Handlungen oder Praktiken, die 1. tatsächlich oder wahrscheinlich einen nach vernünftigem Ermessen vorhersehbaren Schaden in den Vereinigten Staaten bewirken oder (2) bei denen entscheidungserhebliches Verhalten in den Vereinigten Staaten eine Rolle spielt. *Siehe* 15 U.S.C. § 45(a)(4).

([3]) In einigen der von ihr behandelten Datenschutz- und -sicherheitsfälle geht die FTC davon aus, dass ein Unternehmen, das sich sowohl irreführender als auch unlauterer Praktiken bedient hat, bisweilen auch gegen mehrere Gesetze verstoßen hat, darunter gegen den Fair Credit Reporting Act, den Gramm-Leach-Bliley Act und den COPPA.

([4]) *Siehe beispielsweise* Pressemitteilung, FTC, FTC Warns Children's App Maker BabyBus About Potential COPPA Violations (22. Dez. 2014), https://www.ftc.gov/news-events/press-releases/2014/12/ftc-warns-childrens-app-maker-babybus-about-potential-coppa; Pressemitteilung, FTC, FTC Warns Data Broker Operations of Possible Privacy Violations (7. Mai 2013), https://www.ftc.gov/news-events/press-releases/2013/05/ftc-warns-data-broker-operations-possible-privacy-violations; Pressemitteilung, FTC, FTC Warns Data Brokers That Provide Tenant Rental Histories They May Be Subject to Fair Credit Reporting Act (3. Apr. 2013), https://www.ftc.gov/news-events/press-releases/2013/04/ftc-warns-data-brokers-provide-tenant-rental-histories-they-may.

Darüber hinaus hat die FTC im Rahmen ihrer bisherigen Bemühungen um eine konsequente Handhabung des Datenschutzes kontinuierlich über mögliche Verstöße gegen die SAFE-Harbor-Regelung gewacht. Seit Annahme der SAFE-Harbor-Regelung hat die FTC auf eigene Initiative zahlreiche Ermittlungen im Zusammenhang mit der Einhaltung der SAFE-Harbor-Verfahren geführt und 39 Verfahren gegen US-Unternehmen wegen Verstößen gegen die SAFE-Harbor-Regelung eingeleitet. Diese proaktive Herangehensweise will die FTC auch weiterhin fortsetzen und dabei der Durchsetzung der neuen Regelung eine hohe Priorität einräumen.

II. VERBRAUCHERDATENSCHUTZ AUF BUNDESEBENE UND IN DEN EINZELSTAATEN

Der Überblick über die Möglichkeiten der Durchsetzung der Grundsätzes des sicheren Hafens im Anhang zur Entscheidung der Kommission über die Angemessenenheit des von den Grundsätzen des sicheren Hafens gewährleisteten Schutzes enthält eine Zusammenfassung vieler der zum Zeitpunkt der Annahme der SAFE-Harbor-Regelung im Jahr 2000 auf Bundesebene und in den Einzelstaaten geltenden Datenschutzgesetze ([1]). Zu diesem Zeitpunkt wurde die gewerbliche Erfassung und Verwendung personenbezogener Daten durch zahlreiche Bundesgesetze — neben §5 des FTC Act — geregelt, darunter der Cable Communications Policy Act, der Driver's Privacy Protection Act, der Electronic Communications Privacy Act, der Electronic Funds Transfer Act, der Fair Credit Reporting Act, der Gramm-Leach-Bliley Act, der Right to Financial Privacy Act, der Telephone Consumer Protection Act und der Video Privacy Protection Act. Viele Bundesstaaten hatten in diesen Bereichen eine analoge Rechtsprechung.

Seit dem Jahr 2000 hat es auf Bundesebene und in den Einzelstaaten grundlegende Veränderungen gegeben, die zu einem zusätzlichen Verbraucherdatenschutz beitragen ([2]). So hat die FTC im Jahr 2013 auf Bundesebene beispielsweise den COPPA überarbeitet, um einige zusätzliche Schutzmechanismen für die personenbezogenen Angaben von Kindern einzuführen. Darüber hinaus hat sie mit der Datenschutz- und der Garantiebestimmung zwei Bestimmungen zur Umsetzung des Gramm- Leach-Bliley Act eingeführt, die Finanzinstitutionen dazu verpflichten ([3]) ihre Praktiken beim Austausch von Informationen offenzulegen und ein umfassendes Informationssicherheitsprogramm zum Schutz von Verbraucherdaten zu erarbeiten ([4]). Der im Jahr 2003 eingeführte Fair and Accurate Credit Transactions Act („FACTA") dient ebenfalls der Ergänzung altbewährter US-Kreditgesetze und enthält Bestimmungen zur Unkenntlichmachung, gemeinsamen Nutzung und Vernichtung sensibler Finanzdaten. Im Rahmen des FACTA hat die FTC eine Reihe von Regeln eingeführt, die sich unter anderem auf das Recht der Verbraucher auf einen kostenfreien jährlichen Kreditbericht, auf Bestimmungen zur sicheren Vernichtung von gemeldeten Verbraucherdaten, auf das Recht der Verbraucher, den Erhalt bestimmter Informationen zu Krediten und Versicherungen abzubestellen, auf das Recht der Verbraucher, der Verwendung von durch ein Tochterunternehmen bereitgestellten Angaben für die Vermarktung seiner Produkte und Dienstleistungen zu widersprechen sowie auf Anforderungen an Institutionen und Kreditgeber zur Durchführung von Programmen zur Ermittlung und Prävention von Identitätsdiebstahl beziehen ([5]). Darüber hinaus wurden die im Rahmen des Health Insurance Portability and Accountability Act eingeführten Regeln im Jahr 2013 überarbeitet und um zusätzliche Garantien für den Schutz und die Sicherheit personenbezogener Gesundheitsdaten ergänzt ([6]). Dank neuer Vorschriften werden Verbraucher zudem vor unerbetener Telefonwerbung, computergesteuerten Werbeanrufen und Spam geschützt. Der Kongress hat ferner Gesetze erlassen, die Gesundheitsinformationen erfassende Unternehmen dazu verpflichten, Verbraucher über einen möglichen Verstoß zu unterrichten ([7]).

Auch in den Bundestaaten wurden zahlreiche Gesetze im Bereich Datenschutz und -sicherheit erlassen. Seit dem Jahre 2000 haben 47 Bundesstaaten, der District of Columbia, Guam, Puerto Rico und die Virgin Islands Gesetze eingeführt,

---

([1]) *Siehe* U.S.-Handelministerium, SAFE Harbor Enforcement Overview (Überblick über die Möglichkeiten der Durchsetzung der Grundsätzes des sicheren Hafens), https://build.export.gov/main/safeharbor/eu/eg_main_018476.

([2]) Für einen umfassenderen Überblick über den Rechtsschutz in den USA siehe Daniel J. Solove & Paul Schwartz, *Information Privacy Law* (5th ed. 2015).

([3]) Gemäß dem Gramm-Leach-Bliley Act sind Finanzinstitutionen alle Unternehmen, die vornehmlich mit der Bereitstellung von Finanzprodukten und -dienstleistungen befasst sind. Dazu gehören beispielsweise Scheckeinlösestellen, Kurzzeitkreditgeber, Hypothekenmakler, nichtinstitutionelle Kreditgeber, Sachverständige für persönliche Vermögens- und Immobilienbewertung und professionelle Steuerberater.

([4]) Im Rahmen des Consumer Financial Protection Act von 2010 („CFPA"), Titel X der Pub. L. 111-203, 124 Stat. 1955 (21. Juli 2010) (auch bekannt unter der Bezeichnung „Dodd-Frank Wall Street Reform and Consumer Protection Act") wurde der Großteil der Gesetzgebungsbefugnisse der FTC gemäß dem Gramm-Leach-Bliley Act an das Consumer Financial Protection Bureau („CFPB") übertragen. Die FTC behält ihre Durchsetzungsbefugnisse im Rahmen des Gramm-Leach- Bliley Act sowie die Regelungsbefugnisse in Bezug auf Garantieregeln sowie eingeschränkte Regulierungsbefugnisse gemäß den Datenschutzregeln in Bezug auf Kraftfahrzeughändler.

([5]) Im Rahmen des CFPA verfügt die FTC über eine gemeinsame Zuständigkeit mit der CFPB bei der Durchsetzung des FCRA, während die Regulierungsbefugnis größtenteils auf die CFPB übertragen wurde (mit Ausnahme der „Roten Flaggen" und der Vorschriften zur Datenvernichtung).

([6]) *Siehe* 45 C.F.R. pts. 160, 162, 164.

([7]) *Siehe beispielsweise* American Recovery & Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115 (2009) sowie einschlägige Regelungen, 45 C.F.R. §§ 164.404-164.414; 16 C.F.R. pt. 318.

die Unternehmen dazu verpflichten, Einzelpersonen über Verstöße gegen die Sicherheit personenbezogener Angaben zu unterrichten ([1]). In mindestens 32 Staaten sowie in Puerto Rico gibt es Gesetze zur Datenvernichtung mit Vorschriften zur Zerstörung oder Vernichtung personbezogener Daten ([2]). In einer Reihe von Bundesstaaten wurden zudem allgemeine Datensicherheitsgesetze erlassen. Darüber hinaus wurden in Kalifornien unterschiedliche Datenschutzgesetze eingeführt, darunter ein Gesetz, das Unternehmen zur Festlegung von Datenschutzbestimmungen und zur Offenlegung ihrer „do-not-track"-Verfahren verpflichtet ([3]) sowie ein „Shine the Light"-Gesetz mit höheren Transparenzanforderungen an Datenvermittler ([4]) und ein Gesetz, das die Einführung einer Schaltfläche vorsieht, mit der Minderjährige die Löschung bestimmter Daten in sozialen Medien auslösen können ([5]). Mit Hilfe dieser Gesetze sowie weiterer Befugnisse konnten die Regierungen auf Bundesebene und in den Einzelstaaten hohe Geldbußen gegen Unternehmen verhängen, die den Schutz und die Sicherheit der personenbezogenen Daten von Verbrauchern nicht gewährleistet haben ([6]).

Auch zivilrechtliche Verfahren hatten erfolgreiche gerichtliche Entscheidungen und Vergleiche zum Ergebnis, die zu mehr Datenschutz und -sicherheit für Verbraucher beitragen. So hat beispielsweise Target im Jahr 2015 zugestimmt, im Rahmen eines Vergleichs 10 Mio. USD an Kunden zu zahlen, die Klage wegen Missbrauchs ihrer personenbezogenen Finanzdaten im Zuge einer umfassenden Datenschutzverletzung eingereicht hatten. AOL hat sich 2013 bereit erklärt, im Rahmen eines Vergleichs 5 Mio. USD zu zahlen, um eine Sammelklage wegen unzureichender Anonymisierung im Zusammenhang mit der Veröffentlichung von Suchanfragen von Hunderttausenden AOL-Nutzern abzuwehren. Darüber hinaus hat ein Bundesgericht einer Zahlung in Höhe von 9 Mio. USD durch Netflix zugestimmt. Gegen das Unternehmen war Beschwerde eingereicht worden, weil es entgegen den Bestimmungen aus dem Video Privacy Protection Act von 1988 die Verleihhistorien seiner Nutzer gespeichert hatte. Bundesgerichte in Kalifornien haben zwei separate Vergleiche mit Facebook über 20 bzw. 9,5 Mio. USD genehmigt, in denen es um die Erfassung, die Verwendung und den Austausch personenbezogener Daten der Nutzer durch das Unternehmen ging. Ferner hat ein Gericht des Bundestaats Kalifornien im Jahr 2008 einem Vergleich in Höhe von 20 Mio. USD in einem Verfahren gegen LensCrafters wegen unrechtmäßige Offenlegung medizinischer Verbraucherinformationen zugestimmt.

Alles in allem zeigt dieser Überblick, dass in den USA ein umfassender Rechtsschutz im Bereich Verbraucherdatenschutz und -sicherheit besteht. Auf dieser soliden Rechtsgrundlage, die Verbraucherdatenschutz und -sicherheit nach wie vor oberste Priorität einräumt, kann die neue Datenschutzschild-Regelung zur Anwendung kommen, mit der wirksame Garantien für Einzelpersonen in der EU verbunden sind.

([1]) *Siehe beispielsweise* National Conference of State Legislatures („NCSL"), *State Security Breach Notification Laws* (Jan. 4, 2016), einzusehen unter http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

([2]) NCSL, *Data Disposal Laws* (12. Januar 2016), *einzusehen unter* http://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx.

([3]) Cal. Bus. & Professional Code §§ 22575-22579.

([4]) Cal. Civ. Code §§ 1798.80-1798.84.

([5]) Cal. Bus. & Professional Code § 22580-22582.

([6]) *Siehe* Jay Cline, *U.S. Takes the Gold in Doling Out Privacy Fines*, Computerworld (17 Feb. 2014), einzusehen unter http://www.computerworld.com/s/article/9246393/Jay-Cline-U.S.-takes-the-gold-in-doling-out-privacy-fines?taxonomyId=17&pageNumber=1.

ANHANG V

Schreiben von US-Verkehrsminister Anthony Foxx

19. Februar 2016

Kommissionsmitglied Vera Jourová
Europäische Kommission
Rue de la Loi/Wetstraat 200
1049 Brüssel
Belgien

Re: EU-US-Datenschutzschild

Sehr geehrte Frau Jourová,

das US-Verkehrsministerium („Ministerium" oder „DOT") freut sich über diese Gelegenheit, näher auf seine Rolle bei der Umsetzung des EU-US-Datenschutzschilds eingehen zu können. Der Datenschutzschild leistet einen wesentlichen Beitrag zum Schutz personenbezogener Daten, die im Geschäftsverkehr in einer zunehmend vernetzten Welt zur Verfügung gestellt werden. Er ermöglicht Unternehmen die Durchführung wichtiger Transaktionen in der Weltwirtschaft und stellt gleichzeitig sicher, dass EU-Verbraucher weiterhin durch grundlegende Datenschutzbestimmungen geschützt werden.

Bereits vor mehr als 15 Jahren hat das Verkehrsministerium in einem an die Europäische Kommission gerichteten Schreiben erstmals sein Engagement für die Durchsetzung der SAFE-Harbor-Regelung zum Ausdruck gebracht. In diesem Schreiben hat sich das Ministerium dazu verpflichtet, die Grundsätze der SAFE-Harbor-Regelung mit Nachdruck geltend zu machen. An dieser Verpflichtung hält das Ministerium unverändert fest, woran mit dem vorliegenden Schreiben erinnert werden soll.

Das erneuerte Engagement des Ministeriums bezieht sich insbesondere auf die folgenden Schlüsselbereiche: 1) vorrangige Ermittlung bei mutmaßlichen Verstößen gegen die Grundsätze des Datenschutzschilds, 2) angemessene Durchsetzungsmaßnahmen gegen Organisationen, die falsche oder irreführende Angaben zur Beteiligung am Datenschutzschild machen und 3) Kontrolltätigkeit und Unterrichtung der Öffentlichkeit über behördliche Durchsetzungsmaßnahmen. Auf jede dieser Verpflichtungen wollen wir im Folgenden näher eingehen und relevante Hintergrundinformationen zur Rolle des Ministeriums beim Schutz von Verbraucherdaten und bei der Durchsetzung der Datenschutzschild-Regelung liefern, um den notwendigen Kontext herzustellen.

I. HINTERGRUND

A. **Die Datenschutzabteilung im Ministerium**

Das Ministerium setzt sich konsequent dafür ein, die Geheimhaltung personenbezogener Daten, die Verbraucher den Luftverkehrsgesellschaften oder den Inhabern von Kartenverkaufsstellen überlassen werden, zu gewährleisten. Die Handlungsbefugnisse des Ministeriums auf diesem Gebiet ergeben sich aus 49 U.S.C. 41712. Diese Vorschrift verbietet Luftverkehrsgesellschaften oder Inhabern von Kartenverkaufsstellen, unlautere und irreführende Praktiken beim Verkauf von Flugtickets anzuwenden, die den Verbraucher schädigen bzw. schädigen könnten. § 41712 ist nach dem Vorbild von § 5 des Federal Trade Commission Act (15 U.S.C. 45) aufgebaut. Nach unserer Auslegung ist es einer Luftverkehrsgesellschaft oder einem Inhaber einer Kartenverkaufsstelle gemäß dem Gesetz über unlautere und irreführende Praktiken untersagt: 1) gegen die eigenen Datenschutzbestimmungen zu verstoßen oder 2) personenbezogene Daten in einer Art und Weise zu erfassen oder offenzulegen, die der öffentlichen Ordnung zuwiderläuft, gegen moralische Grundsätze verstößt oder dem Verbraucher einen erheblichen Schaden zufügt, der nicht durch geldwerte Vorteile aufgehoben wird. Gemäß § 41712 ist es Luftverkehrsgesellschaften oder Inhabern einer Kartenverkaufsstelle nach unserer Auslegung ebenfalls verboten: 1) gegen eine vom Ministerium verabschiedete Regel zu verstoßen, wonach bestimmte Datenschutzpraktiken als unlauter oder irreführend eingestuft werden oder 2) den Children's Online Privacy Protection Act (COPPA) oder FTC-Bestimmungen zu seiner Umsetzung zu verletzen. Gemäß Bundesgesetz verfügt das Ministerium über die alleinige Befugnis, die Datenschutzpraxis von Luftverkehrsgesellschaften zu regulieren, und mit der FTC über die gemeinsame Befugnis, die Datenschutzpraxis der Inhaber von Verkaufsstellen für Flugtickets zu regeln.

Sobald sich eine Luftverkehrsgesellschaft oder der Inhaber einer Verkaufsstelle für Flugtickets öffentlich zu den Rahmengrundsätzen des Datenschutzschilds bekennt, kann das Ministerium daher von den rechtlichen Befugnissen gemäß § 41712 Gebrauch machen und die Einhaltung dieser Grundsätze sicherstellen. Gibt also ein Passagier Informationen an eine Luftverkehrsgesellschaft oder den Inhaber einer Verkaufsstelle, die sich zur Einhaltung der Rahmengrundsätze des Datenschutzschilds verpflichtet haben, dann würde ein Verstoß gegen diese Grundsätze eine Verletzung der Bestimmungen des § 41712 darstellen.

B. **Durchsetzungsmaßnahmen**

Die Dienststelle des Ministeriums für Rechtsdurchsetzung und Verfahren im Luftverkehr (Office of Aviation Enforcement and Proceedings/Aviation Enforcement Office) untersucht und verfolgt Fälle, die 49 U.S.C. 41712 betreffen. Sie setzt das gesetzliche Verbot unlauterer und irreführender Praktiken gemäß § 41712 durch, insbesondere auf dem Verhandlungswege sowie durch den Erlass von Unterlassungsanordnungen und Anordnungen zur Festsetzung zivilrechtlicher Sanktionen. Die Dienststelle wird auf mögliche Verstöße insbesondere durch Beschwerden von Privatpersonen, Reisebüros, Luftverkehrsgesellschaften sowie US-amerikanischen und ausländischen staatlichen Stellen aufmerksam. Verbraucher haben die Möglichkeit, über die Website des Ministeriums Beschwerden wegen Verletzung der Datenschutzbestimmungen durch Luftverkehrsgesellschaften und Inhaber von Kartenverkaufsstellen einzureichen ([1]).

Sollte in einem Fall keine angemessene und geeignete Vereinbarung erzielt werden können, ist die Dienststelle befugt, zur Rechtsdurchsetzung ein Verfahren einzuleiten, das eine Beweisverhandlung vor einem Verwaltungsrichter des Ministeriums vorsieht. Der Verwaltungsrichter ist befugt, Unterlassungsanordnungen sowie zivilrechtliche Sanktionen festzulegen. Eine Verletzung der Bestimmungen des § 41712 kann Unterlassungsanordnungen nach sich ziehen; der Verstoß gegen diese Anordnungen kann zivilrechtliche Sanktionen in Höhe von bis zu 27 500 USD für jeden Verstoß gegen § 41712 zur Folge haben.

Das Ministerium hat nicht das Recht, beschwerdeführenden Privatpersonen Schadenersatz oder finanzielle Entschädigungen zuzuerkennen. Es kann allerdings Vereinbarungen genehmigen, die sich aus von seiner Dienststelle eingebrachten Untersuchungen ergeben und dem Verbraucher als Ausgleich für andernfalls an die US-Regierung zu entrichtende Geldbußen einen unmittelbaren Vorteil (z. B. in Form von Bargeld, Gutscheinen) verschaffen. Dies wurde in der Vergangenheit so gehandhabt und kann auch im Zusammenhang mit den Rahmengrundsätzen des Datenschutzschilds weiterhin so gehandhabt werden, falls die Umstände dies erfordern. Sollte eine Luftverkehrsgesellschaft die Bestimmungen des § 41712 wiederholt verletzen, würden Zweifel an der Bereitschaft der Gesellschaft zur Einhaltung der Grundsätze aufkommen, was in gravierenden Fällen dazu führen könnte, dass die Gesellschaft als nicht mehr betriebstauglich angesehen und ihr somit die wirtschaftliche Betriebsgenehmigung entzogen würde.

Bisher sind beim Ministerium relativ wenige Beschwerden wegen mutmaßlicher Verstöße gegen die Datenschutzbestimmungen durch Inhaber von Kartenverkaufsstellen und Luftverkehrsgesellschaften eingegangen. Bei Vorliegen einer Beschwerde wird diese gemäß den im Vorangehenden ausgeführten Grundsätzen geprüft.

C. **Der durch das Ministerium gewährte Rechtsschutz kommt EU-Verbrauchern zugute**

Gemäß § 41712 gilt das Verbot unlauterer und irreführender Praktiken im Luftverkehr oder beim Verkauf von Flugtickets für amerikanische oder ausländische Luftverkehrsunternehmen oder Inhaber von Kartenverkaufsstellen. Das Ministerium geht häufig gegen amerikanische und ausländische Luftverkehrsunternehmen wegen Praktiken vor, die sich sowohl auf ausländische als auch auf amerikanische Verbraucher nachteilig auswirken, sofern diese bei der Erbringung von Verkehrsdienstleistungen mit Ziel oder Ausgangspunkt in den USA stattgefunden haben. Das Ministerium nutzt alle ihm zur Verfügung stehenden Rechtsbehelfe und wird dies auch weiterhin tun, um ausländische wie amerikanische Verbraucher vor unlauteren und irreführenden Praktiken im Luftverkehr vonseiten beaufsichtigter Unternehmen zu schützen.

Im Zusammenhang mit Luftverkehrsunternehmen setzt das Ministerium darüber hinaus weitere zielgerichtete Gesetze durch, die Bestimmungen zum Schutz von Verbrauchern außerhalb der USA beinhalten, darunter das COPPA. Dieses Gesetz verlangt unter anderem von Betreibern von Websites und Online-Diensten, die an Kinder gerichtet sind, sowie von für die Allgemeinheit bestimmten Websites, die wissentlich personenbezogene Daten von Kindern unter 13 erheben, dass sie die Eltern darüber in Kenntnis setzen und die nachweisliche Zustimmung der Eltern einholen. In den USA betriebene Websites und Dienste, die dem COPPA unterliegen und personenbezogene Daten von ausländischen Kindern erheben, sind an die Bestimmungen des COPPA gebunden. Im Ausland betriebene Websites und Dienste müssen sich ebenfalls daran halten, wenn sie sich an Kinder in den USA richten oder wissentlich personenbezogene Daten von Kindern in den USA erheben. Für den Fall, dass amerikanische oder ausländische Luftverkehrsunternehmen, die in den USA geschäftlich tätig sind, gegen das COPPA verstoßen, ist das Ministerium zur Einleitung von Durchsetzungsmaßnahmen befugt.

II. DURCHSETZUNG DES DATENSCHUTZSCHILDS

Sobald sich eine Luftverkehrsgesellschaft oder der Inhaber einer Kartenverkaufsstelle für eine Beteiligung am Datenschutzschild entscheidet und beim Ministerium eine Beschwerde eingeht, wonach diese Luftverkehrsgesellschaft bzw. dieser Inhaber einer Kartenverkaufsstelle gegen die Grundsätze verstoßen hat, kann das Ministerium folgende Schritte einleiten, um dem Datenschutzschild mit Nachdruck Geltung zu verschaffen.

([1]) http://www.transportation.gov/airconsumer/privacy-complaints.

A. **Vorrangige Ermittlung bei mutmaßlichen Verstößen**

Die Dienststelle des Ministeriums für Rechtsdurchsetzung und Verfahren im Luftverkehr prüft alle Beschwerden wegen mutmaßlicher Verstöße gegen den Datenschutzschild (dazu gehören auch Beschwerden von EU-Datenschutzbehörden) und leitet Durchsetzungsmaßnahmen ein, sofern es Anzeichen für einen Verstoß gibt. Darüber hinaus arbeitet die Dienststelle mit der FTC und dem Handelsministerium zusammen und befasst sich vorrangig mit Beschwerden über den Verstoß beaufsichtigter Unternehmen gegen im Rahmen des Datenschutzschilds eingegangene Datenschutzverpflichtungen.

Nach Eingang einer Beschwerde über einen mutmaßlichen Verstoß gegen den Datenschutzschild kann die Dienststelle im Rahmen ihrer Ermittlungen eine Reihe von Maßnahmen ergreifen. So kann sie beispielsweise die Datenschutzbestimmungen des Inhabers einer Kartenverkaufsstelle oder der Luftverkehrsgesellschaft überprüfen, beim Inhaber der Kartenverkaufsstelle, bei der Luftverkehrsgesellschaft oder bei Dritten zusätzliche Informationen einholen, die vorlegende Stelle dazu befragen und untersuchen, ob die Verstöße systematisch erfolgen oder eine größere Anzahl von Verbrauchern betreffen. Darüber hinaus stellt die Dienststelle fest, ob in dem vorliegenden Fall Sachverhalte berührt werden, die in den Zuständigkeitsbereich des Handelsministeriums oder der FTC fallen, sie prüft, ob Aufklärungsmaßnahmen für Verbraucher und Unternehmen hilfreich wären und leitet gegebenenfalls ein Verfahren ein.

Sollte das Ministerium Kenntnis von möglichen Verstößen gegen den Datenschutzschild durch die Inhaber von Kartenverkaufsstellen erhalten, stimmt es sein weiteres Vorgehen mit der FTC ab. Darüber hinaus unterrichten wir die FTC und das Handelsministerium über die Ergebnisse von Durchsetzungsmaßnahmen im Rahmen des Datenschutzschilds.

B. **Vorgehen bei falschen oder irreführenden Angaben zur Beteiligung**

Das Ministerium bekräftigt seine Zusage, im Falle von Verstößen gegen den Datenschutzschild, die auch falsche oder irreführende Angaben zur Beteiligung am Datenschutzschild-Programm einschließen, Ermittlungen einzuleiten. Wir behandeln vorrangig Fälle, die uns durch das Handelsministerium übermittelt werden und Organisationen betreffen, die sich seinen Nachforschungen zufolge unrechtmäßig als Mitglied des Datenschutzschilds bezeichnen oder das Gütesiegel des Datenschutzschilds ohne Genehmigung verwenden.

Wenn im Übrigen eine Organisation in ihren Datenschutzbestimmungen zusichert, dass sie sich an die Grundsätze des Datenschutzschilds hält, reicht die bloße Tatsache, dass sie sich beim Handelsministerium nicht registrieren lässt oder ihre Registrierung nicht verlängert, nicht aus, um sich der Durchsetzung dieser Zusicherungen durch das Handelsministerium zu entziehen.

C. **Überwachung von Durchsetzungsmassnahmen bei Verstössen gegen den Datenschutzschild und Unterrichtung der Öffentlichkeit darüber**

Darüber hinaus bekräftigt die Dienststelle des Ministeriums ihr Engagement für die Überwachung möglicher Durchsetzungsmaßnahmen, die zur Gewährleistung der Einhaltung der Grundsätze des Datenschutzschilds erforderlich sein können. Insbesondere wenn die Dienststelle eine Anordnung an eine Luftverkehrsgesellschaft oder einen Inhaber einer Kartenverkaufsstelle erlässt, in der künftige Verstöße gegen den Datenschutzschild und gegen § 41712 untersagt werden, überwacht sie in der Folge die Einhaltung der Vorgaben in der Unterlassungsanordnung durch die jeweilige Organisation. Die Dienststelle stellt zudem sicher, dass Anordnungen im Zusammenhang mit den Datenschutzschild betreffenden Fällen auf ihrer Website eingesehen werden können.

Einer weiteren Zusammenarbeit mit unseren Partnern in den USA und mit den verantwortlichen Akteuren in der EU in allen den Datenschutzschild betreffenden Angelegenheiten sehen wir erwartungsvoll entgegen.

Ich hoffe, dass Ihnen diese Ausführungen weiterhelfen. Falls Sie noch Fragen haben oder weitere Auskünfte benötigen, wenden Sie sich bitte vertrauensvoll an mich.

Hochachtungsvoll

Anthony R. Foxx

Verkehrsminister

ANHANG VI

Schreiben von General Counsel Robert Litt
Amt des Director of National Intelligence

22. Februar 2016

Justin S. Antonipillai
Counselor
U.S. Department of Commerce
1401 Constitution Ave., NWt
Washington, DC 20230

Ted Dean
Deputy Assistant Secretary
International Trade Administration
1401 Constitution Ave., NW
Washington, DC 20230

Sehr geehrter Herr Antonipillai, sehr geehrter Herr Dean,

im Verlaufe der letzten zweieinhalb Jahre stellten die Vereinigten Staaten im Zusammenhang mit den Verhandlungen zum EU-US-Datenschutzschild umfangreiche Informationen über die Erhebungstätigkeit der US Intelligence Community im Wege der signalerfassenden Aufklärung bereit. Dazu gehören Auskünfte zum geltenden rechtlichen Rahmen, zu der auf verschiedenen Ebenen durchgeführten Überwachung dieser Tätigkeiten, zu deren weitreichender Transparenz und zu den allgemeinen Maßnahmen für den Schutz der Privatsphäre und der bürgerlichen Freiheiten, die der Europäischen Kommission die Entscheidung über die Angemessenheit dieser Schutzmaßnahmen erleichtern sollten, soweit sie sich auf die aus Gründen der nationalen Sicherheit gewährten Ausnahmen von den Grundsätzen des Datenschutzschilds beziehen. Dieses Dokument enthält eine Zusammenfassung der übermittelten Informationen.

I. DIE PPD-28 UND DIE DURCHFÜHRUNG DER SIGNALERFASSENDEN AUFKLÄRUNG IN DEN USA

Die Vorgehensweise der Intelligence Community der USA bei der Beschaffung ihrer Auslandsaufklärungsdaten unterliegt einer sorgfältigen Kontrolle, steht voll und ganz im Einklang mit den Rechtsvorschriften der USA und wird auf verschiedenen Ebenen überwacht, wobei das Hauptaugenmerk auf wichtigen Daten der Auslandsaufklärung und Schwerpunkten der nationalen Sicherheit liegt. Ein Mosaik aus Gesetzen und Maßnahmen regelt die Signalaufklärung in den USA, darunter die Verfassung der USA, der Foreign Intelligence Surveillance Act (50 U.S.C., § 1801 ff.) (FISA), Executive Order 12333 und damit zusammenhängende Durchführungsverfahren, Direktiven des Präsidenten sowie zahlreiche durch das FISA-Gericht und den Justizminister gebilligte Verfahren und Leitlinien, mit denen zusätzliche Regeln zur Einschränkung der Erhebung, Speicherung, Nutzung und Weitergabe von Auslandsaufklärungsdaten festgelegt werden ([1]).

a. **Die PPD-28 im Überblick**

Im Januar 2014 erläuterte Präsident Obama in einer Rede verschiedene Reformen in der signalerfassenden Aufklärung der USA und unterzeichnete hierzu die Presidential Policy Directive 28 (PPD-28) ([2]). Der Präsident betonte, dass die US-Signalaufklärung nicht nur dazu dient, unser Land und unsere Freiheiten zu schützen, sondern auch zum Schutz der Sicherheit und der Freiheiten anderer Länder beiträgt, einschließlich der EU-Mitgliedstaaten, die zum Schutz ihrer eigenen Bürger auf Erkenntnisse von US-Nachrichtendiensten zugreifen.

Die PPD-28 enthält eine Reihe von Grundsätzen und Anforderungen, die für sämtliche Aktivitäten der US-Signalaufklärung und für alle Personen unabhängig von Nationalität oder Standort gelten. Insbesondere werden Anforderungen an Verfahren im Zusammenhang mit der Erhebung, Speicherung und Weitergabe von personenbezogenen Daten zu Nicht-US-Bürgern festgelegt, die im Rahmen der US-Signalaufklärung gesammelt wurden. Diese Anforderungen werden nachstehend detaillierter, aber dennoch zusammenfassend, dargelegt:

— In der PPD wird bekräftigt, dass die Vereinigten Staaten Signalaufklärungsdaten nur in dem Umfang erheben, wie dies per Gesetz, Executive Order oder Presidential Directive zulässig ist.

([1]) Weitere Informationen zur US-Auslandsaufklärung werden online veröffentlicht und sind über „IC on the Record" (www.icontherecord.tumblr.com) abrufbar, der öffentlichen Website des ODNI, mit der die nachrichtendienstlichen Aktivitäten der Regierung für die Öffentlichkeit transparenter gemacht werden sollen.

([2]) *Abrufbar unter* https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

— In der PPD sind Verfahren festgelegt, mit denen sichergestellt wird, dass signalerfassende Aufklärung nur zur Förderung von legitimen und autorisierten Zielsetzungen der nationalen Sicherheit erfolgt.

— In der PPD wird zudem gefordert, dass bei der Planung der signalerfassenden Aufklärung die Privatsphäre und die bürgerlichen Freiheiten integraler Bestandteil aller Überlegungen sind. Insbesondere sammeln die Vereinigten Staaten keine Geheimdienstinformationen, um Kritik oder abweichende Meinungen zu unterdrücken oder zu belasten, um Menschen aufgrund ihrer ethnischen Zugehörigkeit, ihrer Rasse, ihres Geschlechts, ihrer sexuellen Orientierung oder ihres Glaubens zu diskriminieren oder um amerikanischen Firmen oder bestimmten amerikanischen Branchen einen Wettbewerbsvorteil zu verschaffen.

— In der PPD ist festgelegt, dass die Datenerhebung im Rahmen der signalerfassenden Aufklärung immer so „passgerecht wie möglich" erfolgen muss und dass Daten als Ergebnis von Sammelerhebungen nur für bestimmte, explizit aufgeführte Zwecke genutzt werden dürfen.

— In der PPD ist festgelegt, dass die Intelligence Community Verfahren anwendet, die so sinnvoll konzipiert sind, dass sie die Weitergabe und Speicherung von personenbezogenen Daten aus der signalerfassenden Aufklärung auf ein Mindestmaß beschränken und vor allem bestimmte Schutzmaßnahmen, die für personenbezogene Daten von US-Bürgern gelten, auch auf Daten von Nicht-US-Bürger erweitern.

— Es wurden behördliche Verfahren zur Umsetzung der PPD-28 festgelegt und publik gemacht.

Die Anwendbarkeit der darin festgelegten Verfahren und Schutzmaßnahmen auf den Datenschutzschild steht außer Frage. Nach der Übermittlung von Daten an Unternehmen in den Vereinigten Staaten im Rahmen des Datenschutzschilds — oder auch auf jede andere Art und Weise — dürfen die amerikanischen Nachrichtendienste diese Daten von den Unternehmen nur abfragen, wenn ihr Antrag mit dem FISA im Einklang steht oder über einen National Security Letter erfolgt, die an anderer Stelle erläutert werden ([1]). Ohne dass Medienberichte bestätigt oder dementiert werden, wonach die US Intelligence Community Daten aus transatlantischen Kabeln sammelt, während sie in die Vereinigten Staaten übertragen werden, würde eine solche Datensammlung vorbehaltlich der hierin dargelegten Beschränkungen und Garantien erfolgen, einschließlich der Anforderungen der PPD-28.

b. **Beschränkungen der Datenerhebung**

Die PPD-28 legt eine Reihe wichtiger allgemeiner Grundsätze für die Erhebung von Signalaufklärungsdaten fest:

— Die signalerfassende Aufklärung muss gesetzlich zulässig oder vom Präsidenten autorisiert sein und muss im Einklang mit der Verfassung der USA und dem amerikanischen Recht stehen.

— Die Privatsphäre und die bürgerlichen Freiheiten sind integraler Bestandteil aller Überlegungen bei der Planung der signalerfassenden Aufklärung.

— Die signalerfassende Aufklärung kommt ausschließlich dann zum Einsatz, wenn dies der Auslandsaufklärung oder der Spionageabwehr dient.

— Die Vereinigten Staaten sammeln keine Signalaufklärungsdaten, um Kritik oder abweichende Meinungen zu unterdrücken oder zu belasten.

— Die Vereinigten Staaten sammeln keine Signalaufklärungsdaten, um Menschen aufgrund ihrer ethnischen Zugehörigkeit, ihrer Rasse, ihres Geschlechts, ihrer sexuellen Orientierung oder ihres Glaubens zu diskriminieren.

— Die Vereinigten Staaten sammeln keine Signalaufklärungsdaten, um amerikanischen Firmen oder bestimmten amerikanischen Branchen einen Wettbewerbsvorteil zu verschaffen.

— Die signalerfassende Aufklärung der USA muss *immer* so „passgerecht wie möglich" erfolgen und dabei die Verfügbarkeit anderer Informationsquellen berücksichtigen. Das bedeutet unter anderem, dass — wann immer dies machbar ist — eine gezielte Datenerhebung und keine Sammelerhebung erfolgt.

Die Anforderung, dass die signalerfassende Aufklärung so „passgerecht wie möglich" erfolgen sollte, gilt sowohl für die Art und Weise, in der Signalaufklärungsdaten erhoben werden, als auch für die Daten selbst. Bei der Entscheidung

([1]) Strafverfolgungs- oder Aufsichtsbehörden können von Unternehmen die Herausgabe von Daten für Ermittlungszwecke in den USA nach Maßgabe anderer Justiz- und Aufsichtsbehörden verlangen, die nicht in den Anwendungsbereich dieses Dokuments fallen, der auf die nationalen Sicherheitsbehörden beschränkt ist.

darüber, ob Daten dieser Art erhoben werden sollen, muss die Intelligence Community die Verfügbarkeit anderer Informationen prüfen, einschließlich diplomatische oder öffentliche Quellen, und bei der Erhebung vorrangig auf diese Alternativen zurückgreifen, sofern diese geeignet und machbar sind. Darüber hinaus 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.

Die der Kommission bereitgestellten Informationen müssen unbedingt in ihrer Gesamtheit gesehen werden. Die Entscheidungen darüber, was „machbar" oder „praktikabel" ist, bleiben nicht dem Ermessen Einzelner überlassen, sondern sind Gegenstand der Strategien, die die Nachrichtendienste zur Umsetzung der PPD-28 erlassen haben — und die öffentlich zugänglich gemacht wurden — sowie der anderen darin beschriebenen Verfahren ([1]). Wie es in der PPD-28 heißt, erfolgt bei einer Sammelerhebung von Signalaufklärungsdaten die Erhebung „aufgrund technischer oder operativer Erwägungen" ohne die Heranziehung von Selektoren (z. B. konkrete Objekte, Suchkriterien und Identifikatoren). In diesem Zusammenhang wird in der PPD-28 anerkannt, dass Nachrichtendienste unter bestimmten Umständen auf die Sammelerhebung zurückgreifen müssen, um neue oder sich abzeichnende Bedrohungen zu erkennen oder andere für die nationale Sicherheit hochwichtige Informationen zu erlangen, die oftmals innerhalb des großen und komplexen Systems der modernen globalen Kommunikation verborgen sind. Auch die im Zusammenhang mit der Sammelerhebung vorgebrachten Bedenken, was den Schutz der Privatsphäre und der bürgerlichen Freiheiten betrifft, werden in der PPD-28 nicht von der Hand gewiesen. Folglich orientiert sie die Intelligence Community dahingehend, Alternativen den Vorzug zu geben, die eine gezielte Signalaufklärung ermöglichen. Nachrichtendienste sollten — wann immer dies möglich ist — die Sammelerhebung durch gezielte Informationsgewinnung ersetzen ([2]). Diese Grundsätze gewährleisten, dass ungeachtet der Ausnahme der Sammelerhebung die allgemeine Regel bestehen bleibt.

Was das Konzept der Verhältnismäßigkeit betrifft, so handelt es sich um einen fundamentalen Grundsatz des US-Rechts. Die Nachrichtendienste sollen demnach nicht theoretisch mögliche Maßnahmen ergreifen, sondern müssen ihre Bemühungen um den Schutz der legitimen Interessen auf dem Gebiet des Datenschutzes und der bürgerlichen Freiheiten mit den praktischen Erfordernissen der signalerfassenden Aufklärung in Einklang bringen. Auch in diesem Zusammenhang haben die Nachrichtendienste ihre Strategien vorgelegt, mit denen gesichert werden kann, dass die allgemeine Regel nicht untergraben wird, wenn Maßnahmen „so sinnvoll konzipiert sind, dass sie die Weitergabe und Speicherung von personenbezogenen Daten auf ein Mindestmaß beschränken".

Die PPD-28 beschränkt außerdem die Nutzung der durch Sammelerhebung gewonnenen Signalaufklärungsdaten auf eine Liste von sechs spezifischen Zielsetzungen, und zwar die Ermittlung und Abwehr bestimmter Aktivitäten ausländischer Mächte, Terrorismusbekämpfung, Nichtverbreitung von Massenvernichtungswaffen, Cybersecurity, Aufdeckung und Abwehr von Bedrohungen für die amerikanischen oder mit ihnen verbündeten Streitkräfte und Abwehr länderübergreifender krimineller Bedrohungen, einschließlich Umgehung von Sanktionen. Der Nationale Sicherheitsberater des Präsidenten wird in Absprache mit dem Director for National Intelligence (DNI) jährlich Überprüfungen zu diesen zulässigen Nutzungszwecken durchführen und feststellen, ob Änderungen erforderlich sind. Der DNI macht diese Liste unter Berücksichtigung der Interessen der nationalen Sicherheit in größtmöglichem Umfang publik. Dadurch wird die Nutzung von Signalaufklärungsdaten aus Sammelerhebungen ganz wesentlich und gleichzeitig auf transparente Art und Weise eingeschränkt.

Abgesehen davon haben die mit der Umsetzung der PPD-28 befassten Nachrichtendienste vorhandene Analysemethoden und -standards für die Abfrage ungeprüfter Signalaufklärungsdaten verschärft ([3]). Die Analysten müssen ihre Anfragen oder Suchbegriffe und -methoden so strukturieren, dass sie mit Sicherheit Aufklärungsdaten bezeichnen können, die für einen begründeten Zweck der Auslandsaufklärung oder Strafverfolgung von Belang sind. Zu diesem Zweck müssen die Nachrichtendienste bei Anfragen zu Personen die Kategorien der Signalaufklärungsdaten in den Mittelpunkt stellen, die den Erfordernissen der Auslandsaufklärung oder Strafverfolgung entsprechen, um so die Verwendung von personenbezogenen Informationen zu verhindern, die für den Zweck der Auslandsaufklärung oder Strafverfolgung nicht relevant sind.

Es ist wichtig zu betonen, dass die Sammelerhebung von Internetdaten, die von der Intelligence Community der USA im Wege der signalerfassenden Aufklärung durchgeführt wird, nur einen kleinen Teil des Internets berührt. Gezielte Abfragen, wie sie an anderer Stelle beschrieben wurden, stellen zudem sicher, dass den Analysten nur Objekte vorgelegt werden, die einen potenziellen Erkenntniswert aufweisen. Ziel dieser Einschränkungen ist es, die Privatsphäre und die bürgerlichen Freiheiten aller Personen unabhängig von ihrer Nationalität und ihrem Wohnort zu schützen.

([1]) *Abrufbar unter* www.icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties#ppd-28. Mit diesen Verfahren werden die in diesem Schreiben erörterten Konzepte der Zielgenauigkeit und Passgerechtigkeit in einer für die einzelnen Nachrichtendienste spezifischen Form umgesetzt.

([2]) In den Durchführungsbestimmungen der NSA zur PPD-28 — um nur ein Beispiel zu nennen — heißt es, dass nach Möglichkeit bei der Erhebung ein Selektor oder mehrere Selektoren angewandt werden, um die Erhebung auf spezifische Aufklärungsziele (z. *B*. einen konkreten, bekannten internationalen Terroristen oder eine Terroristengruppe) oder Aufklärungsthemen (z *B*. die Verbreitung von Massenvernichtungswaffen durch eine ausländische Macht oder deren Vertreter) im Ausland zu konzentrieren.

([3]) *Abrufbar unter* http://www.dni.gov/files/documents/1017/PPD-28_Status_Report_Oct_2014.pdf.

Die Vereinigten Staaten bedienen sich aufwändiger Verfahren, um zu gewährleisten, dass signalerfassende Aufklärung nur zur Förderung von angemessenen Zielsetzungen der nationalen Sicherheit erfolgt. Jedes Jahr legt der Präsident nach einem umfassenden formellen Verfahren unter Einbeziehung aller Nachrichtendienste die höchsten Prioritäten des Landes in der Auslandsaufklärung fest. Der DNI ist für die Umsetzung dieser nachrichtendienstlichen Schwerpunkte im „National Intelligence Priorities Framework", oder NIPF, zuständig. Durch die PPD-28 wurde das behördenübergreifende Verfahren gestärkt und weiter ausgestaltet, damit gesichert ist, dass alle Schwerpunkte der nachrichtendienstlichen Tätigkeit auf hoher politischer Ebene überprüft und bestätigt werden. Die Intelligence Community Directive (ICD) 204 gibt weiterführende Orientierung zum NIPF und wurde im Januar 2015 zur Aufnahme der Anforderungen der PPD-28 aktualisiert ([1]). Der NIPF selbst unterliegt der Geheimhaltung, jedoch finden Informationen zu den spezifischen Schwerpunkten der Auslandsaufklärung der USA jährlich Eingang in die nicht geheime *„Worldwide Threat Assessment"* des DNI, die auf der ODNI-Website leicht zugänglich ist.

Die Schwerpunkte im NIPF tragen in recht hohem Maße allgemeinen Charakter. Sie beinhalten Themen wie die Bestrebungen feindlicher ausländischer Akteure im Bereich nuklearer und ballistischer Raketen, die Auswirkungen von Drogenkartellen und Korruption sowie Menschenrechtsverletzungen in bestimmten Ländern. Und sie gelten nicht nur für die signalerfassende Aufklärung, sondern für alle nachrichtendienstlichen Tätigkeiten. Zuständig für die Umsetzung der NIPF-Schwerpunkte bei der tatsächlichen Erhebung von Signalaufklärungsdaten ist das National Signals Intelligence Committee, oder SIGCOM. Es agiert unter der Leitung des Direktors der National Security Agency (NSA), der gemäß Executive Order 12333 die Aufgaben eines „operativen Leiters der signalerfassenden Aufklärung" wahrnimmt und für die Überwachung und Koordinierung der Signalaufklärung der gesamten Intelligence Community zuständig ist und dabei sowohl vom Verteidigungsminister als auch vom DNI beaufsichtigt wird. Im SIGCOM sind alle Nachrichtendienste vertreten, und da die USA die PPD-28 vollständig umsetzen, werden auch andere Regierungsstellen, die ein politisches Interesse an der signalerfassenden Aufklärung haben, umfassend repräsentiert sein.

Alle Ministerien und Regierungsstellen der USA, die die Auslandsaufklärung für sich in Anspruch nehmen, richten ihre Auskunftsersuchen an das SIGCOM. Dieses prüft die Ersuchen, stellt sicher, dass sie mit dem NIPF in Einklang stehen und versieht sie mit Schwerpunkten, wobei unter anderem folgende Kriterien zur Anwendung kommen:

— Kann die signalerfassende Aufklärung in diesem Fall nützliche Informationen liefern oder gibt es bessere oder kostengünstigere Informationsquellen zur Erfüllung der Anfrage, wie etwa Bildmaterial oder öffentliche Informationsquellen?

— Wie wichtig ist dieser Informationsbedarf? Wenn er im NIPF mit hoher Priorität eingestuft ist, kommt ihm größtenteils bei der Signalaufklärung hohe Priorität zu.

— Welche Art der signalerfassenden Aufklärung könnte eingesetzt werden?

— Ist die Erhebung so passgerecht wie möglich? Sollte es zeitliche, geografische oder sonstige Beschränkungen geben?

Beim amerikanischen Verfahren zur Prüfung der Erfordernisse einer Signalaufklärung sind ausdrücklich auch andere Faktoren zu berücksichtigen, nämlich:

— Ist das Ziel der Erhebung oder die verwendete Erhebungsmethode besonders sensibel? Wenn ja, ist eine Überprüfung durch ranghohe Entscheidungsträger erforderlich.

— Ist mit der Erhebung ein ungerechtfertigtes Risiko für den Schutz der Privatsphäre und die bürgerlichen Freiheiten unabhängig von der Nationalität verbunden?

— Sind zusätzliche Garantien bezüglich Weitergabe und Speicherung erforderlich, um die Privatsphäre oder nationale Sicherheitsinteressen zu schützen?

Zum Abschluss des Verfahrens schließlich untersuchen und benennen ausgebildete NSA-Mitarbeiter auf der Grundlage der vom SIGCOM validierten Schwerpunkte konkrete Suchkriterien wie etwa Telefonnummern oder E-Mail-Adressen, anhand derer Erkenntnisse aus dem Ausland gewonnen werden können, die den Schwerpunkten entsprechen. Jeder Selektor muss überprüft und bestätigt werden, bevor er in die Erhebungssysteme der NSA aufgenommen wird. Aber

([1]) *Abrufbar unter* http://www.dni.gov/files/documents/ICD/ICD%20204%20National%20Intelligence%20Priorities%20Framework.pdf.

selbst dann werden zum Teil noch zusätzliche Kriterien wie die Verfügbarkeit von geeigneten Erhebungsressourcen herangezogen, um zu entscheiden, ob und wann die tatsächliche Erhebung stattfindet. Durch dieses Verfahren wird gewährleistet, dass die Ziele der US-Signalaufklärung einen begründeten und wichtigen Bedarf an Auslandsaufklärungsdaten widerspiegeln. Und natürlich müssen die NSA und andere Nachrichtendienste bei Durchführung der Erhebung gemäß FISA weitere Einschränkungen nach Maßgabe des Foreign Intelligence Surveillance Court beachten. Kurz gesagt, weder die NASA noch ein anderer amerikanischer Nachrichtendienst entscheidet selbst darüber, was erhoben wird.

Generell ist dieses Verfahren Gewähr dafür, dass die Schwerpunkte der nachrichtendienstlichen Tätigkeit der USA allesamt von ranghohen politischen Entscheidungsträgern festgelegt werden, die die Erfordernisse im Bereich der Auslandsaufklärung am besten bestimmen können, und dass diese Entscheidungsträger nicht nur den potenziellen Wert der geheimdienstlichen Datenerhebung im Auge haben, sondern auch die damit verbundenen Risiken, einschließlich der Gefahren für den Datenschutz, die nationalen wirtschaftlichen Interessen und die Außenbeziehungen.

Wenngleich die Vereinigten Staaten konkrete nachrichtendienstliche Methoden oder Operationen nicht bestätigen oder dementieren können, so gelten doch in Bezug auf die im Rahmen des Datenschutzschilds in die Vereinigten Staaten übermittelten Daten die Anforderungen der PPD-28 für alle von den Vereinigten Staaten durchgeführten Operationen der signalerfassenden Aufklärung, unabhängig von Art oder Quelle der erhobenen Daten. Zudem gelten die auf die signalerfassende Aufklärung anzuwendenden Einschränkungen und Garantien für alle Signalaufklärungsdaten, die für einen autorisierten Zweck erhoben wurden, was sowohl die Außenbeziehungen als auch die Belange der nationalen Sicherheit einschließt.

Die hier erörterten Verfahren lassen das deutliche Bemühen erkennen, die willkürliche und anlassunabhängige Erhebung signalerfassender Aufklärungsdaten zu verhindern und — ausgehend von den höchsten Ebenen staatlicher Verwaltung — dem Grundsatz der Verhältnismäßigkeit Geltung zu verschaffen. Mit der PPD-28 und den Durchführungsverfahren der Nachrichtendienste werden neue und bestehende Einschränkungen bei der Signalaufklärung eindeutig geregelt, und es wird konkreter festgelegt, für welchen Zweck die Vereinigten Staaten Signalaufklärungsdaten erheben und verwenden. Dadurch sollte gesichert sein, dass Aktivitäten der signalerfassenden Aufklärung jetzt und in Zukunft nur zur Verfolgung berechtigter Ziele der Auslandsaufklärung durchgeführt werden.

c. **Einschränkungen der Speicherung und Weitergabe**

§ 4 der PPD-28 schreibt für die gesamte Intelligence Community Grenzen für die Speicherung und Weitergabe von personenbezogenen Daten betreffend Nicht-US-Bürger vor, die im Wege der signalerfassenden Aufklärung erhoben wurden, und diese Grenzen sind mit den für US-Bürger geltenden Grenzen vergleichbar. Diese Regelungen sind Bestandteil der für die einzelnen Nachrichtendienste geltenden Verfahren, die im Februar 2015 herausgegeben wurden und öffentlich zugänglich sind. Um für eine Speicherung oder Weitergabe als Auslandsaufklärungsdaten in Frage zu kommen, müssen sich die personenbezogenen Daten auf einen autorisierten Zweck der nachrichtendienstlichen Tätigkeit beziehen, wie er entsprechend dem weiter oben beschriebenen NIPF-Verfahren bestimmt wurde, müssen mit hinreichender Bestimmtheit Anhaltspunkte für eine Straftat liefern oder einem der anderen Standards für die Speicherung von Daten zu US-Bürgern gemäß Executive Order 12333, Abschnitt 2.3., entsprechen.

Daten, für die keine derartigen Festlegungen gelten, dürfen nicht länger als fünf Jahre gespeichert werden, sofern nicht der DNI ausdrücklich bestimmt, dass eine weitere Speicherung im Interesse der nationalen Sicherheit der Vereinigten Staaten liegt. Die Nachrichtendienste müssen daher Informationen zu Nicht-US-Bürgern, die per Signalaufklärung erhoben wurden, fünf Jahre nach der Erhebung löschen, wenn nicht beispielsweise festgestellt wurde, dass die Daten für ein autorisiertes Ziel der Auslandsaufklärung von Belang sind oder der DNI unter Berücksichtigung der Auffassung des ODNI Civil Liberties Protection Officer sowie der Datenschutz- und Bürgerrechtsbeauftragten der Behörde zu der Entscheidung gelangt, dass eine weitere Speicherung dem nationalen Sicherheitsinteresse entspricht.

Darüber hinaus ist mittlerweile bei allen nachrichtendienstlichen Maßnahmen zur Umsetzung der PPD-28 ausdrücklich vorgeschrieben, dass personenbezogene Daten nicht einfach weitergegeben werden dürfen, weil die betreffende Person kein US-Bürger ist, und das ODNI hat im Sinne dieser Anforderung eine Direktive an alle Nachrichtendienste gerichtet ([1]). Geheimdienstmitarbeiter sind ausdrücklich aufgefordert, bei der Erarbeitung und Weitergabe von Aufklärungsberichten den Schutz der Privatsphäre von Nicht-US-Bürgern zu berücksichtigen. Insbesondere wird signalerfassende Aufklärung 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 autorisiertem Zweck der Auslandsaufklärung dient. Damit wird eine wichtige Einschränkung anerkannt und den Bedenken der Europäischen Kommission bezüglich der Breite der Definition der Auslandsaufklärung gemäß Executive Order 12333 Rechnung getragen.

([1]) Intelligence Community Directive (ICD) 203, *abrufbar unter* http://www.dni.gov/files/documents/ICD/ICD%20203%20Analytic%20Standards.pdf.

d. **Compliance und Überwachung**

Das US-System zur Überwachung der Auslandsaufklärung sieht eine gründliche und mehrstufige Kontrolle vor, um die Einhaltung der geltenden Gesetze und Verfahren zu gewährleisten, auch was die Erhebung, Speicherung und Weitergabe von Daten zu Nicht-US-Bürgern betrifft, die per Signalaufklärung gemäß PPD-28 erhoben wurden. Das beinhaltet Folgendes:

— Die Intelligence Community beschäftigt Hunderte von Mitarbeitern für die Überwachung. Bei der NSA allein befassen sich 300 Mitarbeiter mit der Compliance, und andere Nachrichtendienste haben ebenfalls Überwachungsbüros. Darüber hinaus werden die nachrichtendienstlichen Tätigkeiten vom Justizministerium umfassend beaufsichtigt, und ebenso nimmt das Vereidigungsministerium eine Aufsichtsfunktion wahr.

— Jeder Nachrichtendienst verfügt über ein eigenes Büro des Generalinspekteurs, das unter anderem für die Überwachung der Auslandsaufklärung zuständig ist. Generalinspekteure sind rechtlich unabhängig, haben umfassende Befugnisse zur Durchführung von Untersuchungen, Audits und Überprüfungen im Zusammenhang mit den Programmen, darunter auch in Bezug auf Betrug sowie Missbrauchsfälle oder Rechtsverstöße, und können Korrekturmaßnahmen empfehlen. Zwar sind derartige Empfehlungen nicht bindend, doch werden die Berichte der Generalinspekteure oftmals publik gemacht und in jedem Fall dem Kongress übermittelt, was Folgeberichte einschließt, wenn in vorangegangenen Berichten empfohlene Korrekturmaßnahmen noch nicht abgeschlossen sind. Der Kongress wird daher über jede Nichteinhaltung informiert und kann durch entsprechenden Druck, nicht zuletzt über die Haushaltsmittel, auf die Durchsetzung der Korrekturmaßnahme hinarbeiten. Mehrere Berichte von Generalinspekteuren zu Aufklärungsprogrammen wurden veröffentlicht ([1]).

— Das ODNI Civil Liberties and Privacy Office (CLPO) hat die Aufgabe sicherzustellen, dass die Nachrichtendienste durch die Art ihrer Vorgehensweise dem Schutz der nationalen Sicherheit dienen und gleichzeitig die bürgerlichen Freiheiten und das Recht auf Privatsphäre geschützt werden ([2]). Andere Nachrichtendienste haben ihre eigenen Datenschutzbeauftragten.

— Dem Privacy and Civil Liberties Oversight Board (PCLOB), einem unabhängigen, gesetzlich festgelegten Gremium, obliegt die Analyse und Überprüfung von Programmen und Maßnahmen zur Terrorismusbekämpfung, einschließlich des Einsatzes signalerfassender Aufklärung, um in diesem Zusammenhang den Schutz der Privatsphäre und der bürgerlichen Freiheiten zu gewährleisten. Er hat mehrere öffentliche Berichte zu nachrichtendienstlichen Aktivitäten herausgegeben.

— Wie an anderer Stelle noch ausführlicher dargelegt wird, ist das FISA-Gericht (Foreign Intelligence Surveillance Court), das aus einem Gremium unabhängiger Bundesrichter besteht, für die Überwachung aller Signalaufklärungsaktivitäten gemäß FISA und die damit zusammenhängenden Compliance-Fragen zuständig.

— Und schließlich nimmt auch der Kongress der USA, vor allem über die Ausschüsse des Repräsentantenhauses und des Senats für Nachrichtendienste und Justiz, wichtige Kontrollaufgaben wahr, die alle Formen der Auslandsaufklärung, darunter die US-Signalaufklärung, betreffen.

Abgesehen von diesen formellen Überwachungsmechanismen verfügen auch die Nachrichtendienste selbst über verschiedene Mechanismen, um die Einhaltung der bereits beschriebenen Einschränkungen bei der Erhebung zu sichern. Hier einige Beispiele:

— Von Kabinettsbeamten wird gefordert, dass sie ihre Anforderungen an die Signalaufklärung jährlich validieren.

— Die NSA kontrolliert die Ziele der Signalaufklärung während der gesamten Erhebung, um festzustellen, ob damit tatsächlich wertvolle Erkenntnisse aus dem Ausland gewonnen werden, die den Schwerpunkten entsprechen. Für Ziele, bei denen dies nicht der Fall ist, wird die Erhebung eingestellt. Durch zusätzliche Verfahren ist eine regelmäßige Überprüfung der Suchkriterien gewährleistet.

([1]) *Siehe z. B.* U.S. Department of Justice, Inspector General Report „A Review of the Federal Bureau of Investigation's Activities Under Section 702 of the Foreign Intelligence Surveillance Act of 2008" (September 2012), *abrufbar unter* https://oig.justice.gov/reports/2016/o1601a.pdf.

([2]) *Siehe* www.dni.gov/clpo.

— Ausgehend von der Empfehlung einer von Präsident Obama benannten unabhängigen Review Group hat der DNI einen neuen Mechanismus zur Überwachung der Erhebung und Weitergabe von Signalaufklärungsdaten eingerichtet, der bedingt durch die Art des Zieles bzw. das Mittel der Erhebung besonders sensibel ist, um auf diese Weise eine vollständige Übereinstimmung mit den auf politischer Ebene getroffenen Festlegungen sicherzustellen.

— Schließlich prüft das ODNI jährlich die von den Nachrichtendiensten vorgenommene Ressourcenverteilung nach Schwerpunkten und die nachrichtendienstliche Tätigkeit insgesamt. Im Rahmen dieser Prüfung erfolgt eine Beurteilung des Nutzens aller Arten der geheimdienstlichen Datenerhebung, einschließlich der signalerfassenden Aufklärung, und es wird sowohl ein Resümee gezogen — wie erfolgreich hat die Intelligence Community ihre Ziele umgesetzt? — als auch nach vorn geschaut — wie sieht der künftige Bedarf der Intelligence Community aus? So wird sichergestellt, dass die Ressourcen der Signalaufklärung für die wichtigsten nationalen Schwerpunkte zum Einsatz kommen.

Aus diesen umfassenden Darlegungen geht hervor, dass die Intelligence Community nicht allein entscheidet, welche Gespräche abgehört werden, dass sie keine lückenlose Erfassung anstrebt und nicht frei von Kontrolle operiert. Sie richtet ihre Aktivitäten auf die von den politischen Entscheidungsträgern festgelegten Schwerpunkt aus, was insgesamt mit einem Prozess verbunden ist, in den sich die verschiedensten staatlichen Stellen einbringen und der sowohl innerhalb der NSA als auch durch das ODNI, das Justizministerium und das Verteidigungsministerium überwacht wird.

Die PPD-28 enthält zahlreiche weitere Bestimmungen zur Sicherung des Schutzes von personenbezogenen Signalaufklärungsdaten, unabhängig von der Nationalität. Beispielsweise trifft sie mit Blick auf den Schutz dieser Daten Regelungen zur Datensicherheit, zum Zugang und zu Qualitätsverfahren und sieht obligatorische Schulungen vor, damit sich die Mitarbeiter jederzeit der Verantwortung für den Schutz personenbezogener Daten unabhängig von der Nationalität bewusst sind. Die PPD orientiert zudem auf zusätzliche Überwachungs- und Compliance-Mechanismen. Dazu gehört, dass die Verfahren zum Schutz der personenbezogenen Informationen, die bei der Signalaufklärung anfallen, regelmäßig von kompetenten Überwachungs- und Compliance-Mitarbeitern überprüft und begutachtet werden. Bei den Prüfungen muss zudem die Einhaltung der Verfahren zum Schutz solcher Daten seitens der Nachrichtendienste untersucht werden.

Darüber hinaus wird in der PPD-28 geregelt, dass wichtige Compliance-Probleme in Bezug auf Nicht-US-Bürger an höhere Regierungsebenen weitergeleitet werden. Im Falle eines wichtigen Compliance-Problems, bei dem es um personenbezogene Daten geht, die per Signalaufklärung erhoben wurden, muss das Problem ungeachtet sonstiger bestehender Berichtspflichten unverzüglich dem DNI gemeldet werden. Sind hierbei die personenbezogenen Daten einer Nicht-US-Person betroffen, entscheidet der DNI in Abstimmung mit dem Außenminister und dem Leiter des betreffenden Nachrichtendienstes darüber, ob Schritte einzuleiten sind, um die betreffende ausländische Regierung in einer Weise davon in Kenntnis zu setzen, die mit dem Schutz der Quellen und Methoden und der US-Mitarbeiter vereinbar ist. Darüber hinaus hat der Außenminister gemäß PPD-28 als Ansprechpartner für ausländische Regierungen, die Bedenken im Zusammenhang mit der US-Signalaufklärung vorbringen, eine hochrangige Beamtin eingesetzt, Under Secretary Catherine Novelli. Dieses Bekenntnis zu einem Engagement auf höchster Ebene ist beispielhaft für die Bemühungen der US-Regierung in den letzten Jahren, Vertrauen in die zahlreichen bestehenden und sich überschneidenden Bestimmungen zum Schutz der Daten von US-Bürgern und Nicht-US-Bürgern zu schaffen.

e. **Zusammenfassung**

Die Verfahren der Vereinigten Staaten für die Erhebung, Speicherung und Weitergabe von Daten aus der Auslandsaufklärung schließen wichtige Vorkehrungen zum Schutz der personenbezogenen Daten aller Personen unabhängig von der Nationalität ein. Insbesondere wird durch diese Verfahren sichergestellt, dass sich unsere Intelligence Community in der nach Gesetz, Executive Order oder Presidential Directive zulässigen Form auf den Schutz der nationalen Sicherheit konzentriert, dass sie die Daten vor unbefugtem Zugriff, unbefugter Nutzung und Weitergabe schützt und dass ihre Aktivitäten einer mehrstufigen Kontrolle und Überwachung unterliegen, einschließlich durch Kontrollausschüsse des Kongresses. Die PPD-28 und die Verfahren zu ihrer Durchführung machen unsere Bemühungen deutlich, bestimmte Minimierungsverfahren und andere wesentliche Grundsätze des Datenschutzes auf die personenbezogenen Daten aller Personen unabhängig der Nationalität auszuweiten. Personenbezogene Informationen, die durch die signalerfassende Aufklärung der USA erhoben wurden, unterliegen den Grundsätzen und Anforderungen des amerikanischen Rechts und den Anweisungen des Präsidenten, einschließlich der in der PPD-28 festgelegten Schutzbestimmungen. Diese Grundsätze und Anforderungen sind die Gewähr dafür, dass alle Personen unabhängig von ihrer Nationalität oder ihrem Wohnort würde- und respektvoll behandelt werden, und sie erkennen an, dass alle Personen berechtigte Datenschutzinteressen beim Umgang mit ihren personenbezogenen Informationen haben.

II. FOREIGN INTELLIGENCE SURVEILLANCE ACT — § 702

Die Erhebung gemäß § 702 des Foreign Intelligence Surveillance Act ([1]) erfolgt nicht „massenhaft und anlassunabhängig", sondern ist strikt auf die Erhebung ausländischer Aufklärungsdaten einzeln benannter legitimer Ziele gerichtet; ist eindeutig durch ausdrückliche gesetzliche Ermächtigung autorisiert und unterliegt sowohl der unabhängigen richterlichen Aufsicht als auch einer umfassenden Überprüfung und Überwachung innerhalb der Exekutive und im Kongress. Die Erhebung gemäß § 702 gilt als signalerfassende Aufklärung nach Maßgabe der Anforderungen der PPD-28 ([2]).

Die Erhebung gemäß § 702 stellt eine der wertvollsten Quellen für Aufklärungsdaten dar, da sowohl die Vereinigten Staaten als auch unsere europäischen Partner geschützt werden. Umfassende Informationen zur Funktionsweise und Überwachung von § 702 sind öffentlich zugänglich. Zahlreiche Gerichtsunterlagen, richterliche Entscheidungen und Überwachungsberichte im Zusammenhang mit dem Programm wurden freigegeben und auf der Website des ODNI öffentlich bekannt gemacht (www.icontherecord.tumblr.com.). Außerdem führte das PCLOB eine umfassende Analyse zu § 702 durch; der entsprechende Bericht ist abrufbar unter https://www.pclob.gov/library/702-Report.pdf ([3]).

Der § 702 wurde nach einer breiten öffentlichen Debatte als Teil des FISA Amendments Act von 2008 ([4]) im Kongress verabschiedet. Er genehmigt die Sammlung von Auslandsaufklärungsdaten durch die gezielte Überwachung von Nicht-US-Bürgern, die sich außerhalb der Vereinigten Staaten aufhalten, wobei amerikanische Anbieter elektronischer Kommunikationsdienste zur Unterstützung verpflichtet sind. § 702 autorisiert den Justizminister und den DNI — zwei vom Präsidenten ernannte und vom Senat bestätigte Beamte auf Kabinettsebene —, dem FISA Court jährliche Zertifizierungen vorzulegen ([5]). Diese beziehen sich auf spezifische Kategorien von zu erhebenden Auslandsaufklärungsdaten, wie etwa Erkenntnisse in Bezug auf Terrorismusbekämpfung oder Massenvernichtungswaffen, die unter die im FISA-Gesetz festgelegten Kategorien von Auslandsaufklärungsdaten fallen müssen ([6]). Wie das PCLOB feststellte, „ist aufgrund dieser Einschränkungen eine unbeschränkte Erhebung von Daten über Ausländer *nicht* möglich" ([7]).

Zudem müssen die Zertifizierungen Verfahren zur „zielgenauen Erfassung" und „Minimierung" vorsehen, die vom FISA-Gericht zu überprüfen und zu bestätigen sind ([8]). Die Verfahren für eine zielgenaue Erfassung sollen sicherstellen, dass die Erhebung nur in der gesetzlich zulässigen Form stattfindet und der Anwendungsbereich der Zertifizierungen eingehalten wird; durch die Verfahren zur Minimierung sollen die Gewinnung, Weitergabe und Speicherung von Informationen über US-Bürger eingeschränkt werden, sie sehen jedoch auch einen umfassenden Schutz für Informationen über Nicht-US-Bürger vor, wie an anderer Stelle noch erläutert wird. Zudem hat der Präsident, wie bereits dargelegt, in der PPD-28 angewiesen, dass die Intelligence Community zusätzliche Schutzvorkehrungen für personenbezogene Daten von Nicht-US-Bürgern treffen, und diese Vorkehrungen gelten für Daten, die gemäß § 702 erhoben werden.

Bestätigt das Gericht die Verfahren zur zielgenauen Erfassung und Minimierung, erfolgt die Erhebung gemäß § 702 nicht als Sammelerhebung oder anlassunabhängig, sondern es geht ausschließlich um konkrete Zielpersonen, zu denen individualisierte Merkmale festgelegt worden sind, wie das PCLOB anmerkt ([9]). Zur zielgenauen Ausrichtung der Erhebung werden individuelle Selektoren verwendet, wie etwa E-Mail-Adressen oder Telefonnummern, die nach

([1]) 50 U.S.C., § 1881a.

([2]) Die Vereinigten Staaten können aufgrund anderer Bestimmungen des FISA auch gerichtliche Anordnungen erwirken, um Daten zu erlangen, wozu auch im Rahmen des Datenschutzschilds übermittelte Daten gehören. *Siehe* 50 U.S.C., § 1801 ff.. Nach Titel I und III des FISA, durch die elektronische Überwachung und Durchsuchung genehmigt werden, ist (außer in Notfällen) eine gerichtliche Anordnung erforderlich und muss in jedem Falle hinreichend Anlass zu der Vermutung bestehen, dass das Ziel eine ausländische Macht oder ein Vertreter einer ausländischen Macht ist. Titel IV des FISA genehmigt die Verwendung von Geräten zur Rufnummernerfassung von ausgehenden und eingehenden Anrufen gemäß gerichtlicher Anordnung (außer in Notfällen) bei autorisierten Untersuchungen in den Bereichen Auslandsaufklärung, Spionageabwehr oder Terrorismusbekämpfung. Titel V des FISA gestattet dem FBI, gemäß gerichtlicher Anordnung (außer in Notfällen) Geschäftsunterlagen einzuholen, die für autorisierte Untersuchungen in den Bereichen Auslandsaufklärung, Spionageabwehr oder Terrorismusbekämpfung von Belang sind. Wie weiter unten erörtert wird, untersagt der USA FREEDOM Act ausdrücklich die Verwendung von Rufnummernerfassung oder abgeforderten Geschäftsunterlagen auf der Grundlage von FISA für die Sammelerhebung und schreibt einen „konkreten Suchbegriff" vor, um eine zielgerichtete Autorisierung zu gewährleisten.

([3]) Privacy and Civil Liberties Board, „Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act" (2. Juli 2014) („PCLOB Report").

([4]) *Siehe* Pub. L. No. 110-261, 122 Stat. 2436 (2008).

([5]) *Siehe* 50 U.S.C., § 1881a(a) und (b).

([6]) *Siehe ebenda* § 1801(e).

([7]) *Siehe* PCLOB Report unter 99.

([8]) *Siehe* 50 U.S.C., § 1881a(d) und (e).

([9]) *Siehe* PCLOB Report unter 111.

Erkenntnissen der Mitarbeiter der US-Nachrichtendienste vermutlich dazu verwendet werden, um Auslandsaufklärungsdaten der Art zu übermitteln, die unter die dem Gericht vorgelegte Zertifizierung fällt ([1]). Die Grundlage für die Auswahl des Ziels muss dokumentiert werden, und die Dokumentation für die einzelnen Selektoren wird nachfolgend vom Justizministerium überprüft ([2]). Nach Informationen der Regierung der USA wurden 2014 zu etwa 90 000 Personen gezielte Erhebungen nach § 702 durchgeführt, was einem winzigen Bruchteil der weltweit mehr als drei Milliarden Internetnutzer entspricht ([3]).

Nach § 702 erhobene Daten sind Gegenstand der vom Gericht bestätigten Minimierungsverfahren, die Schutzmaßnahmen für Nicht-US-Bürger wie auch für US-Bürger vorsehen und die der Öffentlichkeit bekanntgegeben wurden ([4]). Beispielsweise werden nach § 702 gesammelte Kommunikationsinhalte — sei es von US-Bürgern oder von Nicht-US-Bürgern — in Datenbanken mit strengen Zugangskontrollen gespeichert. Sie dürfen nur von nachrichtendienstlichem Personal überprüft werden, die in den auf den Datenschutz abgestellten Minimierungsverfahren geschult und für diesen Zugang speziell bestätigt wurden, damit sie ihre autorisierten Aufgaben wahrnehmen können ([5]). Verwendet werden dürfen die Daten nur für die Ermittlung von Auslandsaufklärungsdaten oder den Nachweis einer Straftat ([6]). Die Weitergabe darf gemäß PPD-28 nur dann erfolgen, wenn dies einem begründeten Ziel der Auslandsaufklärung oder der Strafverfolgung dient; die alleinige Tatsache, dass es sich bei einer der Kommunikationsparteien nicht um eine US-Person handelt, ist nicht ausreichend ([7]). Außerdem wird durch die Minimierungsverfahren und die PPD-28 die mögliche Speicherdauer der nach § 702 gewonnenen Daten begrenzt ([8]).

Der § 702 unterliegt einer umfassenden Überwachung, an der alle drei Gewalten des Staates beteiligt sind. Bei den Nachrichtendiensten, die das Gesetz umsetzen, erfolgen interne Überprüfungen auf mehreren Ebenen, einschließlich durch unabhängige Generalinspekteure, sowie technische Kontrollen des Datenzugriffs. Seitens des Justizministeriums und des ODNI wird die Anwendung von § 702 genau überprüft und untersucht, um die Einhaltung der rechtlichen Bestimmungen zu verifizieren. Unabhängig davon sind auch die Nachrichtendienste verpflichtet, potenzielle Verstöße zu melden. Hierzu erfolgt eine Untersuchung, und über alle Verstöße wird dem Foreign Intelligence Surveillance Court, dem Intelligence Oversight Board des Präsidenten und dem Kongress Bericht erstattet, und es wird gegebenenfalls Abhilfe geschaffen ([9]). Bislang gibt es keine Fälle, in denen vorsätzlich versucht wurde, gegen das Gesetz zu verstoßen oder rechtliche Vorgaben zu umgehen ([10]).

Das FISA-Gericht spielt bei der Umsetzung von § 702 eine wichtige Rolle. Es besteht aus einem Gremium unabhängiger Bundesrichter, die ihm sieben Jahre angehören, jedoch wie alle Bundesrichter auf Lebenszeit als Richter ernannt werden. Wie bereits an anderer Stelle ausgeführt, ist es Aufgabe des Gerichts, die jährlichen Zertifizierungen und die Verfahren zur zielgenauen Erfassung und Minimierung auf die Einhaltung der Rechtsvorschriften zu überprüfen. Darüber hinaus muss die Regierung, wie ebenfalls schon festgestellt, das Gericht bei Compliance-Problemen unverzüglich in Kenntnis setzen ([11]), und es wurden mehrere Stellungnahmen des Gerichts freigegeben und veröffentlicht, um deutlich zu machen, mit welch außerordentlich hohem Maße an richterlicher Kontrolle und Unabhängigkeit derartige Fälle überprüft werden.

Die anspruchsvollen Prozesse des Gerichts wurden von dessen ehemaligem vorsitzenden Richter in einem Schreiben an den Kongress erläutert, das öffentlich zur Verfügung gestellt wurde ([12]). Als eine Auswirkung des USA FREEDOM Act, auf den weiter unten genauer eingegangen wird, ist das Gericht nunmehr ausdrücklich autorisiert, in Fällen neuer oder bedeutender rechtlicher Fragen einen externen Anwalt als unabhängigen Vertreter des Datenschutzes zu benennen ([13]). Dieser Grad der Beteiligung der unabhängigen Gerichte an Aktivitäten der Auslandsaufklärung in Bezug auf Personen, die weder Bürger dieses Landes sind noch sich in diesem Land aufhalten, ist ungewöhnlich, wenn nicht sogar beispiellos, und trägt dazu bei, dass bei Erhebungen gemäß § 702 die entsprechenden rechtlichen Beschränkungen eingehalten werden.

([1]) *Ebenda*.

([2]) *Ebenda*, unter 8; 50 U.S.C. § 1881a(l); *siehe auch* Bericht des NSA Director of Civil Liberties and Privacy „NSA's Implementation of Foreign Intelligence Surveillance Act Section 702" (im Folgenden „NSA-Bericht") unter 4, *abrufbar unter* http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties.

([3]) Director of National Intelligence 2014 Transparency Report, *abrufbar unter* http://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2014.

([4]) Minimierungsverfahren abrufbar unter: http://www.dni.gov/files/documents/ppd-28/2014%20NSA%20702%20Minimization%20Procedures.pdf („NSA-Minimierungsverfahren"); http://www.dni.gov/files/documents/ppd-28/2014%20FBI%20702%20Minimization%20Procedures.pdf; and http://www.dni.gov/files/documents/ppd-28/2014%20CIA%20702%20Minimization%20Procedures.pdf.

([5]) *Siehe* NSA-Bericht unter 4.

([6]) *Siehe z. B.* NSA-Minimierungsverfahren unter 6.

([7]) Nachrichtendienstliche PPD-28-Verfahren abrufbar unter http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties.

([8]) *Siehe* NSA-Minimierungsverfahren; PPD-28 Section 4.

([9]) *Siehe* 50 U.S.C. § 1881(l); *siehe auch* PCLOB Report unter 66-76.

([10]) *Siehe* Semiannual Assessment of Compliance with Procedures and Guidelines Issues Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, vorgelegt vom Justizminister und dem Director of National Intelligence unter 2–3, abrufbar unter http://www.dni.gov/files/documents/Semiannual%20Assessment%20of%20Compliance%20with%20procedures%20and%20guidelines%20issued%20pursuant%20to%20Sect%20702%20of%20FISA.pdf.

([11]) Rule 13 der Rules of Procedures des Foreign Intelligence Surveillance Court, abrufbar unter http://www.fisc.uscourts.gov/sites/default/files/FISC%20Rules%20of%20Procedure.pdf.

([12]) 29. Juli 2013, Letter from The Honorable Reggie B. Walton to The Honorable Patrick J. Leahy, *abrufbar unter* http://fas.org/irp/news/2013/07/fisc-leahy.pdf.

([13]) *Siehe* § 401 des USA FREEDOM Act, P.L. 114-23.

Die Überwachung durch den Kongress erfolgt mittels gesetzlich vorgeschriebener Berichte an die Ausschüsse für Nachrichtendienste und Justiz sowie häufiger Informationsgespräche und Anhörungen. Dazu gehören ein halbjährlicher Bericht des Justizministers über die Anwendung von § 702 und alle aufgetretenen Verstöße ([1]); eine gesonderte halbjährliche Einschätzung des Justizministers und des DNI, der die Einhaltung der Verfahren zur zielgenauen Erfassung und Minimierung dokumentiert, darunter auch die Einhaltung der Verfahren, die sicherstellen sollen, dass die Erhebung einem begründeten Ziel der Auslandsaufklärung dient ([2]); und ein jährlicher Bericht der Leiter der Nachrichtendienste einschließlich einer Bestätigung, dass mit der Erhebung gemäß § 702 auch weiterhin Auslandsaufklärungsdaten erlangt werden ([3]).

Zusammenfassend ist festzustellen, dass die Erhebung gemäß § 702 gesetzlich zulässig ist, Überprüfungen auf mehreren Ebenen sowie richterlicher Aufsicht und Überwachung unterliegt und, wie das FISA-Gericht in einer jüngst freigegebenen Stellungnahme feststellte, „nicht als Sammelerhebung oder anlassunabhängig durchgeführt wird", sondern „durch separate Entscheidungen über eine zielgenaue Erfassung für einzelne [kommunikationstechnische] Möglichkeiten" ([4]).

III. USA FREEDOM ACT

Der USA FREEDOM Act, der im Juni 2015 unterzeichnet und in Kraft gesetzt wurde, brachte erhebliche Veränderungen für die Überwachungsbehörden der USA und andere nationale Sicherheitsbehörden und stellte in Bezug auf den Einsatz dieser Behörden und die Entscheidungen des FISA-Gerichts mehr Transparenz für die Öffentlichkeit her, wie weiter unten dargelegt wird ([5]). Der Act gewährleistet, dass die in den Bereichen der Nachrichtendienste und der Strafverfolgung tätigen Berufsgruppen über die für den Schutz der Nation notwendigen Befugnisse verfügen, während ein angemessener Schutz der Privatsphäre bei Wahrnehmung dieser Befugnisse auch weiterhin gewahrt bleibt. Er bedeutet folglich eine Verstärkung des Datenschutzes und des Schutzes der bürgerlichen Freiheiten und eine Erhöhung der Transparenz.

Der Act verbietet die Sammelerhebung von Aufzeichnungen, sowohl von US- als auch von Nicht-US-Bürgern, unter Berufung auf verschiedene Bestimmungen des FISA oder durch den Einsatz von National Security Letters, einer Form von gesetzlich zulässigen behördlichen Anordnungen ([6]). Dieses Verbot bezieht sich speziell auf Telefon-Metadaten zu Gesprächen zwischen Personen innerhalb der USA und Personen außerhalb der USA und würde auch die Erhebung von Informationen im Rahmen des Datenschutzschilds gemäß dieser Rechtsgrundlagen einschließen. Der Act fordert, dass die Behörden bei allen dementsprechend geregelten Anforderungen von Aufzeichnungen einen „konkreten Suchbegriff" verwenden, d. h. einen Begriff, der eine Person, ein Konto, eine Adresse oder ein persönliches Gerät so präzise bezeichnet, dass der Suchbereich in einem nach vernünftigem Ermessen möglichen Maße eingeschränkt wird ([7]). Damit wird einmal mehr gewährleistet, dass die Erhebung von Informationen für nachrichtendienstliche Zwecke eng gefasst und zielgenau ausgerichtet ist.

Der Act bewirkte auch erhebliche Änderungen bei den Verfahren vor dem FISA-Gericht, was sowohl mit einer Erhöhung der Transparenz als auch mit einer zusätzlichen Gewähr für den Datenschutz verbunden ist. Wie bereits festgestellt, ermöglicht er die Einsetzung einer ständigen Gruppe von sicherheitsüberprüften Anwälten mit Fachkenntnissen in solchen Bereichen wie Datenschutz und bürgerliche Freiheiten, nachrichtendienstliche Datenerhebung und Kommunikationstechnologie, die benannt werden können, um in Fällen mit bedeutenden oder neuen Rechtsauffassungen vor dem Gericht als „Amicus curiae" aufzutreten. Diese Anwälte sind ermächtigt, juristische Argumente zur Wahrung des Schutzes der Privatsphäre und der bürgerlichen Freiheiten vorzubringen, und sie haben Zugang zu allen Informationen, einschließlich der Geheimhaltung unterliegenden Informationen, die sie nach Feststellung des Gerichts für die Erfüllung ihrer Aufgaben benötigen ([8]).

Aufbauend auf der bisher einmaligen Transparenz der US-Regierung in Bezug auf nachrichtendienstliche Tätigkeiten wird der DNI durch den Act verpflichtet, in Abstimmung mit dem Justizminister jegliche Entscheidung, Anordnung oder Stellungnahme des Foreign Intelligence Surveillance Court bzw. des Foreign Intelligence Surveillance Court of Review, die eine bedeutsame Auslegung oder Interpretation einer gesetzlichen Bestimmung enthält, entweder freizugeben oder eine nicht der Geheimhaltung unterliegende Zusammenfassung davon zu veröffentlichen.

([1]) *Siehe* 50 U.S.C. § 1881f.
([2]) *Siehe ebenda*, § 1881a(l)(1).
([3]) *Siehe ebenda*, § 1881a(l)(3). Einige dieser Berichte unterliegen der Geheimhaltung.
([4]) Mem. Opinion and Order unter 26 (FISC 2014), abrufbar unter http://www.dni.gov/files/documents/0928/FISC%20Memorandum%20Opinion%20and%20Order%2026%20August%202014.pdf.
([5]) *Siehe* USA FREEDOM Act von 2015, Pub. L. No. 114-23, § 401, 129 Stat. 268.
([6]) *Siehe ebenda*, §§ 103, 201, 501. National Security Letters sind durch verschiedene Gesetze zugelassen und ermöglichen dem FBI die Einholung von Informationen aus Kreditauskünften, von Finanzdaten sowie von Daten aus elektronischen Nutzer- und Transaktionsaufzeichnungen ausschließlich zum Zweck des Schutzes vor internationalem Terrorismus und verdeckten nachrichtendienstlichen Aktivitäten. *Siehe* 12 U.S.C. § 3414; 15 U.S.C. §§ 1681u-1681v; 18 U.S.C. § 2709. National Security Letters werden normalerweise vom FBI verwendet, um in den frühen Phasen von Ermittlungen zur Terrorismusbekämpfung und Spionageabwehr wichtige nichtinhaltliche Informationen zu sammeln — wie etwa die Identität eines Kontonutzers, der möglicherweise mit Agenten einer Terroristengruppe wie ISIL kommuniziert. Empfänger eines National Security Letter haben das Recht, diesen vor Gericht anzufechten. *Siehe* 18 U.S.C. § 3511.
([7]) *Siehe ebenda*.
([8]) *Siehe ebenda*, § 401.

Darüber hinaus sieht der Act umfangreiche Offenlegungen vor, was Erhebungen gemäß FISA und Anfragen auf der Grundlage von National Security Letters betrifft. So müssen die Vereinigten Staaten alljährlich gegenüber dem Kongress und der Öffentlichkeit unter anderem die Anzahl der beantragten und genehmigten FISA-Anordnungen und -Zertifizierungen, die geschätzte Anzahl der von Überwachungsmaßnahmen betroffenen US-Bürger und Nicht-US-Bürger und die Anzahl der Zulassungen als „Amicus curiae" offenlegen ([1]). Das Gesetz verlangt zudem, die Öffentlichkeit zusätzlich über die Anzahl der Anfragen auf der Grundlage von National Security Letters sowohl zu US- als auch zu Nicht-US-Bürgern zu unterrichten ([2]).

In Bezug auf die Unternehmenstransparenz bietet der Act den Unternehmen eine Reihe von Optionen, wie sie die Gesamtzahl der FISA-Anordnungen und -Direktiven oder der von Behörden übermittelten National Security Letters sowie die Anzahl der von diesen Anordnungen betroffenen Kundenkonten öffentlich bekanntmachen können ([3]). Einige Unternehmen haben diese Zahlen bereits offengelegt, wobei deutlich wurde, dass nur von wenigen Kunden Daten angefordert wurden.

Diese Berichte zur Unternehmenstransparenz zeigen auf, dass von den Anfragen der US-Nachrichtendienste nur ein winziger Bruchteil der Daten betroffen ist. In einem kürzlich erschienen Transparenzbericht eines großen Unternehmens beispielsweise heißt es, dass die bei ihm eingegangenen Anfragen zur nationalen Sicherheit (gemäß FISA oder durch National Security Letters) weniger als 20 000 seiner Konten betreffen, und zwar zu einer Zeit, da er mindestens 400 Mio. Nutzer verzeichnete. Mit anderen Worten, alle von diesem Unternehmen gemeldeten Anfragen zur nationalen Sicherheit betrafen weniger als 0,005 % seiner Nutzer. Selbst wenn sich jede dieser Anfragen auf Daten im Rahmen der SAFE-Harbor-Regelung bezogen hätten, was natürlich nicht der Fall ist, lässt sich doch zweifelsohne erkennen, dass die Anfragen zielgenau sind und einen angemessenen Umfang haben und die Erhebung weder massenhaft noch anlassunabhängig erfolgt.

Die Umstände, unter denen Empfängern von National Security Letters deren Offenlegung untersagt werden kann, wurden bereits in den Rechtsvorschriften zu deren Genehmigung entsprechend eingeschränkt. Der Act sieht darüber hinaus vor, dass solche Verpflichtungen zur Geheimhaltung regelmäßig überprüft werden müssen und Empfänger von National Security Letters darüber zu unterrichten sind, wenn die Faktenlage die Verpflichtung zur Geheimhaltung nicht länger rechtfertigt, und er kodifiziert Verfahren, mit denen Empfänger Verpflichtungen zur Geheimhaltung anfechten können ([4]).

Zusammenfassend lässt sich feststellen, dass die wichtigen Änderungen bei den Nachrichtendiensten der USA als Folge des USA FREEDOM Act ein deutlicher Beleg dafür sind, dass sich die Vereinigten Staaten umfassend darum bemühen, bei allen nachrichtendienstlichen Praktiken dem Schutz von personenbezogenen Daten, Privatsphäre und bürgerlichen Freiheiten sowie der Transparenz einen vorrangigen Stellenwert einzuräumen.

IV. TRANSPARENZ

Abgesehen von den Transparenzverpflichtungen gemäß dem USA FREEDOM Act stellt die Intelligence Community der USA der Öffentlichkeit umfangreiche zusätzliche Informationen bereit und setzt damit ein deutliches Zeichen, was die Transparenz in ihrer Aufklärungsarbeit betrifft. Die Intelligence Community hat zahlreiche ihrer Strategien und Verfahren, viele Entscheidungen des Foreign Intelligence Surveillance Court und andere freigegebene Materialien publik gemacht und damit ein außerordentlich hohes Maß an Transparenz bewiesen. Zudem veröffentlicht sie in viel größerem Umfang als zuvor statistische Angaben zur Einbeziehung der für Erhebungen zuständigen nationalen Sicherheitsbehörden seitens der Regierung. In ihrem am 22. April 2015 herausgegebenen zweiten Jahresbericht präsentiert sie Statistiken dazu, wie oft diese wichtigen Behörden an der Arbeit der Regierung beteiligt wurden. Das ODNI hat ebenfalls auf seiner Website und auf *IC On the Record* eine Anzahl konkreter Transparenzgrundsätze ([5]) und einen Plan zur Umsetzung dieser Grundsätze in konkrete messbare Initiativen veröffentlicht ([6]). Im Oktober 2015 hat der Director of National Intelligence verfügt, dass im Interesse der Förderung der Transparenz und der Durchführung von Transparenzinitiativen jeder Nachrichtendienst in den Reihen seiner Führungskräfte einen Intelligence Transparency Officer benennt ([7]). Dieser wird eng mit dem jeweiligen Privacy and Civil Liberties Officer zusammenarbeiten, damit Transparenz, Privatsphäre und bürgerliche Freiheiten auch weiterhin oberste Priorität genießen.

([1]) *Siehe ebenda*, § 602.
([2]) *Siehe ebenda*.
([3]) *Siehe ebenda*, § 603.
([4]) *Siehe ebenda*, §§ 502(f)–503.
([5]) *Abrufbar unter* http://www.dni.gov/index.php/intelligence-community/intelligence-transparency-principles.
([6]) *Abrufbar unter* http://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/Principles%20of%20Intelligence%20Transparency%20Implementation%20Plan.pdf.
([7]) *Siehe ebenda*.

Beispielhaft für diese Bemühungen ist die Veröffentlichung von mehreren nicht der Geheimhaltung unterliegenden Berichten durch den Chief Privacy and Civil Liberties Officer der NSA während der letzten Jahre, namentlich von Berichten zu den Aktivitäten gemäß § 702, Executive Order 12333 und dem USA FREEDOM Act ([1]). Darüber hinaus besteht eine enge Zusammenarbeit der Intelligence Community mit dem PCLOB, dem Kongress und den Datenschutzorganisationen in den USA (U.S. privacy advocacy community), um die Tätigkeit der US-Nachrichtendienste noch transparenter zu gestalten, wann immer dies machbar und mit dem Schutz sensibler nachrichtendienstlicher Quellen und Methoden vereinbar ist. Insgesamt gesehen ist die nachrichtendienstliche Tätigkeit der USA mindestens genauso transparent wie die eines jeden anderen Staates in der Welt und weist den höchstmöglichen Grad an Transparenz auf, bei dem der Notwendigkeit des Schutzes von sensiblen Quellen und Methoden noch entsprochen werden kann

Zusammenfassende Angaben zur umfassenden Transparenz nachrichtendienstlicher Aktivitäten der USA:

— Die Intelligence Community hat Tausende von Seiten mit gerichtlichen Stellungnahmen und behördlichen Verfahren herausgegeben und online gestellt, in denen die spezifischen Verfahren und Anforderungen unserer nachrichtendienstlichen Tätigkeit dargelegt werden. Außerdem haben wir Berichte über die Einhaltung der geltenden Beschränkungen durch die Nachrichtendienste veröffentlicht.

— Hochrangige Beamte des Nachrichtendienstes äußern sich regelmäßig öffentlich über die Aufgaben und Aktivitäten ihrer Organisationen, wobei sie auch die für ihre Arbeit maßgeblichen Compliance-Regelungen und -Sicherungsmaßnahmen erläutern.

— Die Intelligence Community veröffentlichte zahlreiche zusätzliche Dokumente zu den nachrichtendienstlichen Aktivitäten gemäß unserem Freedom of Information Act.

— Der Präsident erließ die PPD-28 und legte damit öffentlich zusätzliche Einschränkungen für unsere nachrichtendienstliche Tätigkeit fest, und das ODNI gab zwei öffentlich zugängliche Berichte über die Umsetzung dieser Einschränkungen heraus.

— Die Intelligence Community ist nunmehr gesetzlich verpflichtet, wichtige Rechtsgutachten des FISA-Gerichts oder Zusammenfassungen dieser Gutachten zu veröffentlichen.

— Die staatlichen Behörden sind verpflichtet, jährlich darüber Bericht zu erstatten, in welchem Umfang sie bestimmte nationale Sicherheitsbehörden einbeziehen, und für Unternehmen ist dies ebenfalls möglich.

— Das PCLOB hat mehrere ausführliche öffentliche Berichte zu nachrichtendienstlichen Aktivitäten herausgegeben und wird künftig auch weiterhin so verfahren.

— Die Intelligence Community stellt Kontrollausschüssen des Kongresses umfangreiche Informationen zur Verfügung, die der Geheimhaltung unterliegen.

— Der DNI hat Transparenzgrundsätze herausgegeben, die für die Tätigkeit der Intelligence Community maßgebend sind.

Dieses hohe Maß an Transparenz wird künftig noch weiter ausgebaut. Alle für die Öffentlichkeit zugänglich gemachten Informationen werden selbstverständlich sowohl dem Handelsministerium als auch der Europäischen Kommission zur Verfügung stehen. Die jährliche Überprüfung der Umsetzung des Datenschutzschilds durch diese beiden Seiten wird der Europäischen Kommission Gelegenheit geben, alle Fragen im Zusammenhang mit neu herausgegebenen Informationen wie auch andere Aspekte bezüglich des Datenschutzschilds und seiner Handhabung anzusprechen und zu erörtern, und wir gehen davon aus, dass das Ministerium möglicherweise nach eigenem Ermessen Vertreter anderer Stellen, einschließlich der Intelligence Community, zur Teilnahme an dieser Überprüfung einlädt. Das geht natürlich über den in der PPD-28 vorgesehenen Mechanismus hinaus, mit dem geregelt wird, in welcher Form EU-Mitgliedstaaten Bedenken im Zusammenhang mit der Überwachung an einen speziell benannten Beamten im Außenministerium herantragen können.

V. RECHTSBEHELFE

Das amerikanische Recht sieht eine Reihe von Rechtsschutzinstrumenten für Personen vor, die aus Gründen der nationalen Sicherheit rechtswidrig elektronisch überwacht wurden. Gemäß FISA ist das Recht, ein amerikanisches Gericht um Unterstützung anzurufen, nicht auf US-Bürger beschränkt. Jeder Person, die über eine entsprechende

([1]) *Abrufbar unter* https://www.nsa.gov/civil_liberties/_files/nsa_report_on_section_702_program.pdf; https://www.nsa.gov/civil_liberties/_files/UFA_Civil_Liberties_and_Privacy_Report.pdf; https://www.nsa.gov/civil_liberties/_files/UFA_Civil_Liberties_and_Privacy_Report.pdf.

Klagebefugnis verfügt, würden Rechtsbehelfe zur Verfügung stehen, um auf der Grundlage des FISA gegen rechtswidrige elektronische Überwachung vorzugehen. So haben Personen, die von rechtswidriger elektronischer Überwachung betroffen sind, gemäß FISA die Möglichkeit, US-Regierungsbeamte in persönlicher Eigenschaft auf Schadenersatz zu verklagen, was pönalen Schadensersatz und Anwaltsgebühren einschließt. *Siehe* 50 U.S.C. § 1810. Klagebefugte Personen haben auch die Möglichkeit, eine Zivilklage auf Schadensersatz einschließlich Prozesskostenerstattung gegen die Vereinigten Staaten anzustrengen, wenn die durch elektronische Überwachung im Rahmen des FISA erlangten Informationen, die sie betreffen, gesetzwidrig und vorsätzlich genutzt oder offengelegt wurden. *Siehe* 18 U.S.C. § 2712. Sofern die US-Regierung beabsichtigt, Erkenntnisse über einen Geschädigten, die direkt oder mittelbar aus der elektronischen Überwachung gemäß FISA gewonnen wurden, in einem Gerichts- oder Verwaltungsverfahren in den Vereinigten Staaten gegen die betroffene Person zu verwenden oder offenzulegen, muss sie dem Gericht und der betroffenen Person ihre Absicht mitteilen, die daraufhin die Rechtmäßigkeit der Überwachung anfechten und auf die Unterdrückung der Informationen hinwirken kann. *Siehe* 50 U.S.C. § 1806. Das FISA sieht letztlich auch Strafen für Personen vor, die vorsätzlich und unter Vortäuschung rechtlicher Kompetenz eine gesetzwidrige elektronische Überwachung vornehmen oder vorsätzlich Informationen nutzen oder offenlegen, die durch gesetzwidrige Überwachung gewonnen wurden. *Siehe* 50 U.S.C. § 1809.

EU-Bürgern stehen andere Möglichkeiten zur Verfügung, um gegen US-Regierungsbeamte wegen der rechtswidrigen Verarbeitung oder Abfrage von Daten rechtlich vorzugehen, d. h. auch gegen Regierungsbeamte, die im Zusammenhang mit der rechtswidrigen Abfrage oder Verarbeitung von Informationen für vorgebliche Ziele der nationalen Sicherheit gegen das Gesetz verstoßen. Der Computer Fraud and Abuse Act verbietet vorsätzlichen nicht autorisierten Zugang (oder eine Ausweitung des autorisierten Zugangs) zur Einholung von Daten von einem Finanzinstitut, einem Computersystem der US-Regierung oder einem Computer, auf den über das Internet zugegriffen wird, wie auch zum Zweck der Erpressung oder des Betrugs vorgebrachte Drohungen, geschützten Computern Schaden zuzufügen. *Siehe* 18 U.S.C. § 1030. Jede Person, ganz gleich welcher Nationalität, die infolge einer Verletzung dieses Gesetzes einen Schaden oder einen Verlust erleidet, kann die Person, die gegen das Gesetz verstoßen hat (einschließlich Regierungsbeamte), nach § 1030(g) auf kompensatorischen Schadenersatz und Unterlassung verklagen oder einen anderen billigkeitsrechtlichen Rechtsbehelf erwirken, was von der Durchführung eines Strafverfahrens unabhängig ist, allerdings das Vorhandensein von mindestens einer der im Gesetz festgelegten Bedingungen voraussetzt. Der Electronic Communications Privacy Act (ECPA) regelt den Zugang der staatlichen Behörden zu gespeicherter elektronischer Kommunikation und Transaktionsaufzeichnungen sowie zu Nutzerdaten, die sich im Besitz von Drittanbietern im Bereich Kommunikation befinden. *Siehe* 18 U.S.C. §§ 2701-2712. Gemäß ECPA ist ein Geschädigter berechtigt, Regierungsbeamte wegen vorsätzlichen gesetzwidrigen Zugriffs auf gespeicherte Daten zu verklagen. Der ECPA gilt für alle Personen unabhängig von der Staatsbürgerschaft, und Geschädigte haben Anrecht auf Schadensersatz und die Anwaltsgebühren. Der Right to Financial Privacy Act (RFPA) beschränkt den Zugriff der US-Regierung auf Bank- und Brokerunterlagen einzelner Kunden. *Siehe* 12 U.S.C. §§ 3401-3422. Gemäß RFPA kann ein Bank- oder Brokerkunde die US-Regierung wegen unrechtmäßigen Zugangs zu Kundenunterlagen auf gesetzlichen, eigentlichen und pönalen Schadensersatz verklagen, und wenn sich zeigt, dass ein solcher unrechtmäßiger Zugang vorsätzlich erfolgte, wird automatisch eine Untersuchung über mögliche disziplinarische Maßnahmen gegen die betreffenden Regierungsmitarbeiter eingeleitet. *Siehe* 12 U.S.C. § 3417.

Der Freedom of Information Act (FOIA) schließlich ist ein Mittel, mit dem alle Personen zu jedem beliebigen Thema Zugang zu vorhandenen Unterlagen von Bundesbehörden erlangen können, vorbehaltlich einiger Kategorien von Ausnahmen. *Siehe* 5 U.S.C. § 552(b). Dazu gehören Zugangsbegrenzungen bei Informationen, die aus Gründen der nationalen Sicherheit der Geheimhaltung unterliegen, bei personenbezogenen Daten anderer Personen sowie bei Informationen, die strafrechtliche Ermittlungen betreffen. Diese Einschränkungen sind mit denen vergleichbar, die andere Länder in ihren Datenzugangsgesetzen festgelegt haben, und gelten gleichermaßen für Amerikaner und Nicht-Amerikaner. Bei Streitigkeiten über die Freigabe von Unterlagen, die gemäß FOIA angefordert wurden, können auf dem Verwaltungsweg Rechtsbehelfe eingelegt werden, danach ist das Bundesgericht anzurufen. Das Gericht muss eine De-novo-Entscheidung dazu treffen, ob die Unterlagen ordnungsgemäß zurückgehalten werden, 5 U.S.C. § 552(a)(4)(B), und kann die Regierung zwingen, Zugang zu den Unterlagen zu gewähren. In einigen Fällen haben die Gerichte die Behauptungen der Regierung zurückgewiesen, dass die Information als der Geheimhaltung unterliegend zurückgehalten werden sollte ([1]). Obwohl kein Schadensersatz geleistet wird, können die Gerichte die Anwaltskosten erstatten.

VI. FAZIT

Die Vereinigten Staaten erkennen an, dass bei ihrer signalerfassenden Aufklärung und anderen nachrichtendienstlichen Tätigkeiten zu berücksichtigen ist, dass alle Personen unabhängig von ihrer Nationalität oder ihrem Wohnort würde- und respektvoll zu behandeln sind und dass alle Personen berechtigte Datenschutzinteressen beim Umgang mit ihren personenbezogenen Daten haben. Die Vereinigten Staaten nutzen die signalerfassende Aufklärung ausschließlich zur Gewährleistung ihrer nationalen Sicherheit und ihrer außenpolitischen Interessen sowie zum Schutz ihrer Bürger und der Bürger von mit ihnen verbündeten oder befreundeten Staaten. Die Intelligence Community der USA betreibt keine systematische anlassunabhängige Überwachung von Personen, was normale europäische Bürger einschließt. Die Erhebung von Signalaufklärungsdaten erfolgt nur bei ordnungsgemäßer Ermächtigung und unter strenger Einhaltung der

([1]) *Siehe z. B. New York Times v. Department of Justice*, 756 F.3d 100 (2d Cir. 2014); *American Civil Liberties Union v. CIA*, 710 F.3d 422 (D.C. Cir. 2014).

geltenden Einschränkungen; sie erfolgt erst nach Prüfung der Verfügbarkeit alternativer Quellen, einschließlich diplomatischer und öffentlicher Quellen, und in einer Weise, bei der vorrangig auf geeignete und machbare Alternativen zurückgegriffen wird. Und wann immer es praktikabel erscheint, wird die Erhebung unter Verwendung von Selektoren auf spezifische Aufklärungsziele oder -themen im Ausland konzentriert.

Die Politik der USA in diesem Bereich wurde in der PPD-28 bekräftigt. Innerhalb dieser Rahmenbedingungen verfügen die US-Nachrichtendienste nicht über die rechtliche Befugnis, die Ressourcen, die technischen Voraussetzungen oder den Wunsch, weltweit die gesamte Kommunikation zu überwachen. Die Nachrichtendienste lesen nicht die E-Mails einer jeden Person in den Vereinigten Staaten oder alle weltweit verschickten E-Mails. Entsprechend der PPD-28 gibt es in den Vereinigten Staaten wirksame Schutzvorkehrungen für die personenbezogenen Daten von Nicht-US-Bürgern, die per Signalaufklärung erhoben wurden. Dazu gehören Regeln und Verfahren, um — vergleichbar mit den Schutzmaßnahmen für US-Bürger — die Speicherung und Weitergabe von sie betreffenden personenbezogenen Daten auf ein Mindestmaß zu beschränken, soweit es die Gewährleistung der nationalen Sicherheit zulässt. Zudem besteht, wie oben dargelegt, ein umfassendes Überwachungsregime für die zielgenaue Autorisierung nach § 702 FISA, das seinesgleichen sucht. Und schließlich bewirken die wesentlichen Änderungen an den rechtlichen Grundlagen für die nachrichtendienstliche Tätigkeit, wie sie im USA FREEDOM Act festgelegt wurden, und auch die vom ODNI geleiteten Initiativen zur Förderung der Transparenz innerhalb der Intelligence Community eine deutliche Verbesserung des Schutzes der Privatsphäre und der bürgerlichen Freiheiten für alle Personen unabhängig von ihrer Nationalität.

Hochachtungsvoll

Robert S. Litt

21. Juni 2016

Herrn Justin S. Antonipillai
Counselor
U.S. Department of Commerce
1401 Constitution Avenue, N.W.
Washington, DC 20230

Herrn Ted Dean
Deputy Assistant Secretary
International Trade Administration
1401 Constitution Avenue, N.W.
Washington, DC 20230

Sehr geehrter Herr Antonipillai, sehr geehrter Herr Dean,

ich möchte Ihnen weitere Informationen über die Art und Weise übermitteln, in der die Vereinigten Staaten die Sammelerhebung von Signalaufklärungsdaten durchführen. Wie in der Fußnote 5 der Presidential Policy Directive 28 (PPD-28) erläutert, bezieht sich der Begriff „Sammelerhebung" auf den Erwerb einer relativ großen Menge von signalerfassenden Aufklärungsdaten unter Bedingungen, in denen die Intelligence Community keinen mit einer bestimmten Zielperson verbundenen Identifikator (wie z. B. die E-Mail-Adresse oder Telefonnummer) für eine zielgerichtete Erhebung verwenden kann. Das bedeutet jedoch nicht, dass diese Art der Erhebung „massenhaft" oder „anlassunabhängig" erfolgt. So wird in der PPD-28 auch gefordert, dass die signalerfassende Aufklärung „so passgerecht wir möglich" sein sollte. Gemäß diesem Auftrag stellt die Intelligence Community mit entsprechenden Maßnahmen sicher, dass auch in Fällen, in denen keine konkreten Suchkriterien für eine gezielte Erhebung verfügbar sind, die zu erhebenden Daten wahrscheinlich Informationen der Auslandsaufklärung enthalten, die den Anforderungen entsprechen, wie sie anhand des in meinem früheren Schreiben erläuterten Prozesses formuliert wurden, und so die Menge erhobener nicht relevanter Daten minimiert wird.

Zum Beispiel kann die Intelligence Community den Auftrag erhalten, Signalaufklärungsdaten zu den Aktivitäten einer Terroristengruppe zu erlangen, die in einer Region eines Nahoststaates operiert und von der vermutet wird, dass sie Anschläge gegen westeuropäische Länder plant. Dabei sind möglicherweise die Namen, Telefonnummern, E-Mail-Adressen oder andere konkrete Identifikatoren von mit dieser Terroristengruppe in Verbindung gebrachten Personen nicht bekannt. Wir könnten uns dafür entscheiden, diese Gruppe ins Visier zu nehmen, indem wir Kommunikationsvorgänge aus dieser und in diese Region überwachen und dann weitere Auswertungen und Analysen vornehmen, um jene Vorgänge zu ermitteln, die sich auf die Gruppe beziehen. Dabei würden sich die Nachrichtendienste bemühen, die Erhebung so weit wie möglich einzugrenzen. Es würde sich also um eine „Sammelerhebung" handeln, da eine Verwendung von Selektoren nicht möglich ist. Sie ist weder „massenhaft" noch „anlassunabhängig", sondern erfolgt so zielgerichtet wie möglich.

Somit erheben die Vereinigten Staaten auch dann, wenn eine zielgenaue Ausrichtung der Erhebung durch Verwendung konkreter Selektoren nicht möglich ist, nicht sämtliche Kommunikationsdaten sämtlicher Kommunikationseinrichtungen der ganzen Welt, sondern konzentrieren ihre Erhebung mithilfe von Filtern und anderen technischen Hilfsmitteln auf jene Einrichtungen, die wahrscheinlich für die Auslandsaufklärung wertvolle Kommunikationsdaten enthalten. Somit erstreckt sich die signalerfassende Aufklärung der Vereinigten Staaten nur auf einen Bruchteil des Datenverkehrs im Internet.

Da, wie in meinem früheren Schreiben angeführt, bei einer „Sammelerhebung" eher die Gefahr besteht, dass nicht relevante Kommunikationsdaten erhoben werden, beschränkt die PPD-28 die zulässige Verwendung von durch Sammelerhebung gewonnenen Signalaufklärungsdaten auf sechs konkrete Zielsetzungen. In der PPD-28 und bei nachrichtendienstlichen Maßnahmen zur Umsetzung der PPD-28 sind zudem Grenzen für die Speicherung und Weitergabe durch Signalaufklärung erlangter personenbezogener Daten festgelegt, und zwar ungeachtet dessen, ob die Daten durch Sammelerhebung oder gezielte Erhebung gewonnen wurden, und unabhängig von der Staatsangehörigkeit der betreffenden Person.

Daher handelt es sich bei der „Sammelerhebung" der Intelligence Community nicht um eine „massenhafte" oder „anlassunabhängige" Erhebung, sondern sie umfasst vielmehr die Anwendung von Verfahren und Hilfsmitteln zum Filtern, um die Erhebung auf Material zu konzentrieren, das die Anforderungen der von den Entscheidungsträgern

formulierten Anforderungen an die Auslandsaufklärung erfüllt, und zugleich die Erhebung nicht relevanter Daten zu minimieren; dabei kommen strenge Regeln für den Schutz möglicherweise erhobener nicht relevanter Informationen zur Anwendung. Die in diesem Schreiben geschilderten Strategien und Verfahren gelten für die gesamte Sammelerhebung von Signalaufklärungsdaten, einschließlich der Sammelerhebung des Datenverkehrs von und nach Europa, ohne dass hier bestätigt oder dementiert wird, ob eine derartige Erhebung erfolgt.

Sie haben zudem weitere Informationen über das Privacy and Civil Liberties Oversight Board (PCLOB) und die Generalinspekteure sowie über deren Rechtsgrundlagen angefragt. Das PCLOB ist ein unabhängiges Gremium in der Exekutive ([1]). Die fünf Mitglieder dieses parteienübergreifenden Gremiums werden vom Präsidenten ernannt und vom Senat bestätigt; ihre Amtszeit beträgt sechs Jahre. Die Mitglieder des PCLOB und deren Mitarbeiter erhalten entsprechende Zugangsberechtigungen, damit sie ihren gesetzlichen Pflichten und Aufgaben uneingeschränkt nachkommen können ([2]).

Der Auftrag des PCLOB besteht darin zu gewährleisten, dass die Anstrengungen der Bundesregierung zur Terrorismusprävention mit dem notwendigen Schutz der Privatsphäre und der bürgerlichen Freiheiten in Einklang gebracht werden. Das Gremium hat zwei grundlegende Aufgaben — Überwachung und Beratung. Dabei steckt das PCLOB sein Arbeitsgebiet selbst ab und legt fest, welche Tätigkeiten der Überwachung und Beratung es durchzuführen wünscht.

In seiner Rolle als *Überwachungsgremium* überprüft und analysiert das PCLOB die Maßnahmen der Exekutive zum Schutz der Nation vor Terrorismus, die mit dem notwendigen Schutz der Privatsphäre und der bürgerlichen Freiheiten in Einklang gebracht werden müssen ([3]). Die jüngste abgeschlossene Kontrollarbeit des PCLOB konzentrierte sich auf Überwachungsprogramme nach § 702 des FISA ([4]). Zurzeit überprüft das Gremium die nachrichtendienstlichen Tätigkeiten gemäß Executive Order 12333 ([5]).

In seiner Rolle als *Beratungsgremium* sorgt das PCLOB dafür, dass bei der Entwicklung und Umsetzung von Gesetzen, Regelungen und Maßnahmen zum Schutz der Nation vor Terrorismus die individuellen Freiheitsrechte hinreichend berücksichtigt werden ([6]).

Zur Erfüllung seines Auftrags hat das Gremium per Gesetz Zugriff auf alle einschlägigen Unterlagen von Behörden wie Berichte, Audits, Überprüfungen, Dokumente, Schriftstücke, Empfehlungen und sonstige einschlägige Materialien, einschließlich gesetzlich der Geheimhaltung unterliegender Informationen ([7]). Darüber hinaus kann das PCLOB alle Beamten oder Mitarbeiter der Exekutive befragen sowie Aussagen und Zeugenaussagen einholen ([8]). Außerdem kann das Gremium schriftlich beantragen, dass der Justizminister im Namen des PCLOB Anordnungen ausstellt, mit der Parteien außerhalb der Exekutive gezwungen werden, entsprechende Informationen bereitzustellen ([9]).

Nicht zuletzt muss das PCLOB gesetzlichen Anforderungen zur Transparenz gegenüber der Öffentlichkeit nachkommen. Dazu gehört, dass es die Öffentlichkeit über seine Tätigkeit auf dem Laufenden hält, indem es Anhörungen öffentlich durchführt und seine Berichte, soweit es der notwendige Schutz der Geheimhaltung unterliegender Informationen zulässt, in größtmöglichem Umfang publik macht ([10]). Zudem muss das PCLOB melden, wenn eine Regierungsstelle sich weigert, seinem Rat zu folgen.

Die Generalinspekteure in der Intelligence Community führen Audits, Inspektionen und Überprüfungen der Programme und Tätigkeiten der Nachrichtendienste durch, um systemimmanente Risiken, Schwachstellen und Unzulänglichkeiten zu ermitteln und anzusprechen. Darüber hinaus gehen die Generalinspekteure Beschwerden oder Informationen nach, die

([1]) 42 U.S.C. 2000ee(a), (h).
([2]) 42 U.S.C. 2000ee(k).
([3]) 42 U.S.C. 2000ee(d)(2).
([4]) *Siehe allgemein* https://www.pclob.gov/library.html#oversightreports.
([5]) *Siehe allgemein* https://www.pclob.gov/events/2015/may13.html.
([6]) 42 U.S.C. 2000ee(d)(1); *siehe auch* PCLOB Advisory Function Policy and Procedure, Policy 2015-004, *abrufbar unter* https://www.pclob.gov/library/Policy-Advisory_Function_Policy_Procedure.pdf.
([7]) 42 U.S.C. 2000ee(g)(1)(A).
([8]) 42 U.S.C. 2000ee(g)(1)(B).
([9]) 42 U.S.C. 2000ee(g)(1)(D).
([10]) 42 U.S.C. 2000eee(f).

mutmaßliche Verstöße gegen Gesetze oder Rechtsvorschriften bzw. Misswirtschaft, die grobe Verschwendung von Mitteln, Amtsmissbrauch oder eine erhebliche oder besondere Gefahr für die öffentliche Gesundheit und Sicherheit im Zusammenhang mit nachrichtendienstlichen Programmen und Aktivitäten betreffen. Die Unabhängigkeit der Generalinspekteure ist ein maßgeblicher Faktor für die Objektivität und Integrität aller von ihnen vorgelegten Berichte, Erkenntnisse und Empfehlungen. Zu den wichtigsten Aspekten der Aufrechterhaltung der Unabhängigkeit der Generalinspekteure gehören das Verfahren der Ernennung und Abberufung von Inspekteuren, gesonderte Stellen für die operative Tätigkeit, Haushalt und Personalfragen sowie doppelte Rechenschaftspflichten gegenüber den Leitern von Regierungsbehörden sowie gegenüber dem Kongress.

Vom Kongress wurde in jeder Regierungsbehörde, darunter bei allen Nachrichtendiensten, ein unabhängiges Büro des Generalinspekteurs eingerichtet ([1]). Im Zuge der Annahme des Intelligence Authorization Act for Fiscal Year 2015 werden nahezu alle Generalinspekteure mit Überwachungsaufgaben für eine Stelle der Intelligence Community vom Präsidenten ernannt und vom Senat bestätigt, einschließlich Justizministerium, Central Intelligence Agency (CIA), National Security Agency (NSA) und Intelligence Community ([2]). Bei diesen Generalinspekteuren handelt es sich zudem um parteienunabhängige Beamte, die nur vom Präsidenten abberufen werden können. Obgleich die Befugnis des Präsidenten zur Abberufung der Inspekteure in der US-Verfassung verankert ist, wird sie kaum wahrgenommen und erfordert, dass der Präsident dem Kongress 30 Tage vor der Abberufung eines Generalinspekteurs eine schriftliche Begründung zukommen lässt ([3]). Mit diesem Ernennungsverfahren wird gewährleistet, dass Beamte der Exekutive keinen ungebührlichen Einfluss auf die Auswahl, Ernennung oder Abberufung eines Generalinspekteurs ausüben.

Zweitens verfügen die Generalinspekteure über erhebliche gesetzliche Befugnisse zur Durchführung von Audits, Untersuchungen und Überprüfungen von Programmen und Maßnahmen der Exekutive. Neben den gesetzlich vorgeschriebenen Kontrolluntersuchungen und -überprüfungen haben die Generalinspekteure weitreichende Ermessensfreiheit zur Ausübung von Kontrollbefugnissen bei der Überprüfung der von ihnen selbst ausgewählten Programme und Aktivitäten ([4]). Dabei stellt das Gesetz sicher, dass den Inspekteuren bei der Wahrnehmung dieser Befugnisse unabhängige Mittel zur Erfüllung ihrer Aufgaben zur Verfügung stehen, einschließlich der Möglichkeit, eigene Mitarbeiter einzustellen und ihre Haushaltsanträge an den Kongress gesondert zu dokumentieren ([5]). Es ist gesetzlich sichergestellt, dass die Generalinspekteure Zugang zu den für die Erfüllung ihrer Aufgaben benötigten Informationen erhalten. Dazu gehört der direkte Zugriff auf sämtliche behördlichen Unterlagen und Informationen mit ausführlichen Angaben zu den Programmen und Aktivitäten der Behörde ungeachtet der Geheimhaltungsstufe; die Befugnis zur Einholung von Informationen und Dokumenten per Anordnung sowie die Befugnis zur Vereidigung ([6]). In wenigen Fällen kann der Leiter einer Regierungsbehörde die Tätigkeit eines Generalinspekteurs untersagen, wenn z. B. ein Audit oder eine Untersuchung des Inspekteurs die nationalen Sicherheitsinteressen der Vereinigten Staaten erheblich beeinträchtigen würde. Auch die Wahrnehmung dieser Befugnis ist äußerst ungewöhnlich und macht es erforderlich, dass der Leiter der Behörde den Kongress binnen 30 Tagen über die Gründe in Kenntnis setzt ([7]). Der Director of National Intelligence hat diese Amtsbefugnis zur Einschränkung der Tätigkeiten von Generalinspekteuren noch nie eingesetzt.

Drittens haben die Generalinspekteure die Aufgabe, sowohl die Leiter der Regierungsbehörden als auch den Kongress mithilfe von Berichten umfassend und zeitnah über Betrugsfälle und andere schwerwiegende Probleme, Missstände und Mängel bei Programmen und Aktivitäten der Exekutive zu informieren ([8]). Die doppelte Berichterstattung stützt die Unabhängigkeit der Inspekteure, indem die Überwachung durch sie transparent wird und die Behördenleiter Gelegenheit erhalten, Empfehlungen der Inspekteure umzusetzen, bevor der Kongress gesetzgeberische Maßnahmen einleiten kann. Beispielsweise sind die Generalinspekteure gesetzlich verpflichtet, diese Probleme sowie bislang eingeleitete Abhilfemaßnahmen in halbjährlichen Berichten darzulegen ([9]). Die Regierungsbehörden nehmen die Feststellungen und Empfehlungen der Inspekteure ernst, und Letztere können oftmals die Akzeptanz und Umsetzung ihrer Empfehlungen in

([1]) § 2 und 4 des Inspektor General Act von 1978 in der geltenden Fassung (im Folgenden „IG Act"); § 103H(b) und (e) des National Security Act von 1947 in der geltenden Fassung; § 17(a) des Central Intelligence Act (im Folgenden „CIA Act").

([2]) *Siehe* Pub. L. No. 113-293, 128 Stat. 3990, (19. Dezember 2014). Nur die Generalinspekteure der Defense Intelligence Agency und der National Geospatial-Intelligence Agency werden nicht vom Präsidenten ernannt; allerdings haben der Generalinspekteur des Vereidigungsministeriums und der Generalinspekteur der Intelligence Community konkurrierende Zuständigkeit für diese Behörden.

([3]) § 3 des the IG Act von 1978 in der geltenden Fassung; § 103H(c) des National Security Act; und § 17(b) des CIA Act.

([4]) *Siehe* §§ 4(a) und 6(a)(2) des IG Act von 1947; § 103H(e) und (g)(2)(A) des National Security Act; § 17(a) und (c) des CIA Act.

([5]) §§ 3(d), 6(a)(7) ud 6(f) des IG Act; § 103H(d), (i), (j) und (m) des National Security Act; § 17(e)(7) und (f) des CIA Act.

([6]) § 6(a)(1), (3), (4), (5), und (6) des IG Act; § 103H(g)(2) des National Security Act; § 17(e)(1), (2), (4), und (5) des CIA Act.

([7]) *Siehe z. B.* §§ 8(b) und 8E(a) des IG Act; § 103H(f) des National Security Act; § 17(b) des CIA Act.

([8]) § 4(a)(5) des IG Act; § 103H(a)(b)(3) und (4) des National Security Act; § 17(a)(2) und (4) des CIA Act.

([9]) § 2(3), 4(a), und 5 des IG Act; § 103H(k) des National Security Act; § 17(d) des CIA Act. Der Generalinspekteur des Justizministeriums stellt seine für die Öffentlichkeit bestimmten Berichte im Internet unter folgendem Link bereit: http://oig.justice.gov/reports/all.htm. Ebenso veröffentlich der Generalinspekteur für die Intelligence Community seine halbjährlichen Berichte unter https://www.dni.gov/index.php/intelligence-community/ic-policies-reports/records-requested-under-foia#icig.

diese und andere Berichte an den Kongress und mitunter an die Öffentlichkeit aufnehmen ([1]). Neben der doppelten Berichterstattung sind die Generalinspekteure auch dafür verantwortlich, Whistleblowern der Exekutive den Weg zu den zuständigen Kontrollgremien des Kongresses zu weisen, wo sie mutmaßliche Betrugsfälle, Verschwendung oder Missstände bei Programmen und Aktivitäten der Exekutive melden können. Die Identität der Hinweisgeber ist vor einer Preisgabe gegenüber der Exekutive geschützt, so dass sie vor möglichen unzulässigen Disziplinarmaßnahmen oder Sicherheitsüberprüfungen als Vergeltung dafür, dass sie sich an den Inspekteur gewandt haben, bewahrt bleiben ([2]). Da Whistleblower oftmals die Informationsquelle für Untersuchungen der Generalinspekteure darstellen, erhöht die Möglichkeit, dass sie ihr Anliegen ohne Einflussnahme der Exekutive dem Kongress vortragen können, die Wirksamkeit der Überwachung durch die Inspekteure. Aufgrund dieser Unabhängigkeit können die Generalinspekteure Wirtschaftlichkeit, Effizienz und Rechenschaftspflicht in den Regierungsbehörden mit Objektivität und Integrität fördern.

Abschließend sei erwähnt, dass der Kongress den Rat der Generalinspekteure für Integrität und Effizienz eingerichtet hat. Dieser Rat entwickelt u. a. Standards der Generalinspekteure für Audits, Untersuchungen und Überprüfungen, fördert Schulungen und ist befugt, ein angebliches Fehlverhalten von Generalinspekteuren zu überprüfen; somit dient er als kritisches Auge gegenüber den Generalinspekteuren, die damit betraut sind, alle anderen zu überwachen ([3]).

Ich hoffe, dass Ihnen diese Ausführungen weiterhelfen.

Mit freundlichen Grüßen,
Robert S. Litt
General Counsel

([1]) §§ 2(3), 4(a), und 5 des IG Act; § 103H(k) des National Security Act; § 17(d) des CIA Act. Der Generalinspekteur des Justizministeriums stellt seine für die Öffentlichkeit bestimmten Berichte im Internet unter folgendem Link bereit: http://oig.justice.gov/reports/all.htm. Ebenso veröffentlich der Generalinspekteur für die Intelligence Community seine halbjährlichen Berichte unter https://www.dni.gov/index.php/intelligence-community/ic-policies-reports/records-requested-under-foia#icig.

([2]) § 7 des IG Act; § 103H(g)(3) des National Security Act; § 17(e)(3) des CIA Act.

([3]) § 11 des IG Act.

ANHANG VII

Schreiben von Bruce Swartz, stellvertretender Generalstaatsanwalt des Justizministeriums und Berater für internationale Angelegenheiten, US-Justizministerium

19. Februar 2016

Herrn Justin S. Antonipillai
Counselor
U.S. Department of Commerce
1401 Constitution Ave., NW
Washington, DC 20230

Herrn Ted Dean
Deputy Assistant Secretary
International Trade Administration
1401 Constitution Ave., NW
Washington, DC 20230

Sehr geehrter Herr Antonipillai, sehr geehrter Herr Dean,

dieses Schreiben gibt einen kurzen Überblick über die wichtigsten Ermittlungsinstrumente, mit denen aus Gründen der Strafverfolgung oder des öffentlichen (zivil- und aufsichtsrechtlichen) Interesses Geschäfts- und andere Daten von amerikanischen Unternehmen eingeholt werden können, und über die in diesen Behörden bestehenden Zugriffsbeschränkungen ([1]). Die erlassenen Anordnungen sind insofern nicht diskriminierend, als sie dazu dienen, sowohl Informationen von US-amerikanischen Unternehmen einzuholen als auch solche von Unternehmen, die eine Selbstzertifizierung unter dem US-EU-Datenschutzschild vornehmen, unabhängig von der Staatsangehörigkeit der betroffenen Person. Darüber hinaus können Unternehmen, gegen die in den Vereinigten Staaten rechtliche Schritte eingeleitet werden, dieses Einholen von Informationen wie im Folgenden dargestellt anfechten ([2]).

Von besonderer Bedeutung in Bezug auf die Beschlagnahme von Daten durch öffentliche Behörden ist der vierte Zusatzartikel zur Verfassung der Vereinigten Staaten, der folgendermaßen lautet: „Das Recht des Volkes auf Sicherheit der Person und der Wohnung, der Urkunden und des Eigentums vor willkürlicher Durchsuchung, Festnahme 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." Wie das Oberste Gericht der Vereinigten Staaten in der Rechtssache *Berger v. State of New York* urteilte „besteht der Hauptzweck dieses Zusatzartikels, wie in zahlreichen Urteilen dieses Gerichts bestätigt wird, im Schutz der Privatsphäre und der Sicherheit von Einzelpersonen vor willkürlichem Eingriffen durch Regierungsbeamte", siehe 388 U, S. 41, 53 (1967) (unter Berufung auf die Rechtssache *Camara vs. Mun. Court of San Francisco*, 387 U, S. 523, 528 (1967)). Für strafrechtliche Ermittlungen im Inland ist im vierten Zusatzartikel generell vorgeschrieben, dass den Strafverfolgungsbeamten vor der Durchführung einer Haussuchung ein gerichtlicher Hausdurchsuchungsbefehl vorliegen muss. Siehe Rechtssache *Katz v. United States*, 389 U, S. 347, 357 (1967). In Fällen, in denen diese Vorschrift nicht gilt, unterliegt das Eingreifen des Staates einer Prüfung der „Zumutbarkeit". Somit gewährleistet also die Verfassung selbst, dass die Regierung der Vereinigten Staaten nicht uneingeschränkt oder willkürlich private Informationen beschlagnahmen darf.

Strafverfolgungsbehörden:

Bundesanwälte, die Beamte des Justizministeriums sind, und Ermittler des Bundes einschließlich Ermittler des Federal Bureau of Investigation (FBI), einer Strafverfolgungsbehörde innerhalb des Justizministeriums, können von Unternehmen in den USA die Herausgabe von Unterlagen und anderen Aufzeichnungen zu strafrechtlichen Ermittlungszwecken

([1]) In diesem Überblick geht es nicht um die Instrumente, die die Strafverfolgungsbehörden beispielsweise bei Ermittlungen im Zusammenhang mit dem Terrorismus oder Fragen der nationalen Sicherheit nutzen, z. B. National Security Letters (NSLs) für bestimmte Aufzeichnungen zu Kreditdaten, Finanzdaten und elektronischen Teilnehmer- und Transaktionsdaten, siehe 12 U.S.C. § 3414; 15 U.S.C. § 1681u; 15 U.S.C. § 1681v; 18 U.S.C. § 2709, und nicht um die elektronische Überwachung, Durchsuchungsbefehle, Geschäftsunterlagen und die anderweitige Erfassung von Kommunikation gemäß dem Foreign Intelligence Surveillance Act, siehe 50 U.S.C. § 1801 ff.

([2]) Hier geht es um die Strafverfolgungs- und Aufsichtsbehörden des Bundes; Verstöße gegen das Recht der Bundesstaaten werden von diesen selbst untersucht und vor deren Gerichten verhandelt. Die Strafverfolgungsbehörden der Bundesstaaten wenden die gemäß ihrem Recht erteilten Befehle und Anordnungen an, wie sie hier dargestellt sind, wobei die Möglichkeit besteht, dass die Verfassungen der Bundesstaaten ein Rechtsschutzniveau vorsehen, das über jenes der Verfassung der USA hinausgeht. Der von den Bundesstaaten gewährte Rechtsschutz muss mindestens dem der US-Verfassung — insbesondere Zusatzartikel 4, aber nicht darauf beschränkt — entsprechen.

mithilfe mehrerer Arten von Zwangsmaßnahmen — wie Anordnungen einer Grand Jury oder Behörde und Durchsuchungsbefehlen — erzwingen und auch sonstige Kommunikation gemäß den für das Abhören und für die Rufnummernerfassung zuständigen Bundesbehörden einholen.

Anordnungen einer Grand Jury oder eines Gerichts: Mit strafrechtlichen Anordnungen sollen konkrete strafrechtliche Ermittlungen unterstützt werden. Bei einer Anordnung einer Grand Jury handelt es sich um einen offiziellen Antrag einer Grand Jury (üblicherweise auf Verlangen eines Bundesanwalts), Ermittlungen zu einem konkreten mutmaßlichen Verdacht auf einen Verstoß gegen das Strafrecht durchzuführen. Grand Juries sind eine Anklagekammer eines Gerichts, deren Mitglieder von einem Richter oder Magistrate ausgewählt werden. Bei einer Anordnung kann von der betroffenen Person verlangt werden, in einem Gerichtsverfahren auszusagen oder Geschäftsunterlagen, elektronisch gespeicherte Informationen oder sonstige materielle Beweismittel vorzulegen bzw. zur Verfügung zu stellen. Hierbei muss es sich um für die Ermittlungen relevante Informationen handeln, und die Anordnung darf nicht unverhältnismäßig sein, weil sie überzogen, repressiv oder belastend ist — denn aus diesen Gründen kann ein Empfänger die Anfechtung der Anordnung beantragen. Siehe dazu die Federal Rules of Criminal Procedure [Strafprozessordnung], S. 17. In einigen wenigen Fällen kann ein Gericht nach Anklage durch die Grand Jury die Vorlage von Unterlagen anordnen.

Behördliche Anordnungen: Bei straf- oder zivilrechtlichen Ermittlungen können behördliche Anordnungen ergehen. Im Zuge der Strafverfolgung ist es in mehreren Bundesstaaten gesetzlich zulässig, behördliche Anordnungen zu erlassen, um Geschäftsunterlagen, elektronisch gespeicherte Informationen oder sonstige materielle Beweismittel, die für Ermittlungen zu Betrug im Gesundheitswesen, zum Kindesmissbrauch, zum Schutz durch den Geheimdienst, zu Verstößen gegen das Betäubungsmittelgesetz und Ermittlungen eines Generalinspekteurs, die sich auf Regierungsbehörden auswirken, relevant sind, vorzulegen bzw. zur Verfügung zu stellen. Möchte die Regierung eine behördliche Anordnung gerichtlich durchsetzen, kann der Empfänger der behördlichen Anordnung — wie der Empfänger einer Anordnung einer Grand Jury — die Unverhältnismäßigkeit der Anordnung geltend machen, weil sie überzogen, repressiv oder belastend ist.

Gerichtlich angeordnete Rufnummernerfassung: Gemäß den strafrechtlichen Vorschriften zur Rufnummernerfassung können die Strafverfolgungsbehörden eine gerichtliche Anordnung erlangen, um in Echtzeit nichtinhaltliche Wähl-, Routing-, Anschluss- und Signalinformationen zu einer Telefonnummer oder E-Mail-Adresse zu erfassen, sofern bestätigt wird, dass die gelieferten Informationen für laufende strafrechtliche Ermittlungen relevant sind. Siehe 18 U.S.C. §§ 3121-3127. Dem Bundesgesetz zufolge ist die gesetzwidrige Nutzung bzw. der gesetzwidrige Einbau eines einschlägigen Geräts strafbar.

Electronic Communications Privacy Act (ECPA): Gemäß Titel II des ECPA (Gesetz zum Datenschutz in der elektronischen Kommunikation), das auch als Stored Communications Act (SCA, Gesetz zur Speicherung von Kommunikation) bezeichnet wird (18 U.S.C. §§ 2701–2712), regeln zusätzliche Vorschriften den Zugriff des Staates auf Teilnehmerdaten, Verkehrsdaten und bei Internetdienstanbietern von Telefongesellschaften und anderen dritten Dienstanbietern gespeicherte Kommunikationsinhalte. Im SCA ist ein System gesetzlich vorgeschriebener Datenschutzrechte festgelegt, die den Datenzugriff zu Zwecken der Strafverfolgung einschränken und ihn nur in dem Maße gestatten, wie es verfassungsrechtlich für die Kunden und Abonnenten von Internetdienstanbietern erforderlich ist. Durch das SCA wird die Privatsphäre in Abhängigkeit vom Ausmaß der Datenerfassung stärker geschützt. Um Informationen über die registrierten Abonnenten, IP-Adressen und dazugehörigen Zeitstempel und Rechnungsinformationen einholen zu können, müssen die Strafverfolgungsbehörden eine entsprechende Anordnung erhalten. Für die meisten anderen gespeicherten, nichtinhaltlichen Informationen wie E-Mail-Header ohne Betreffzeile müssen die Strafverfolgungsbehörden einem Richter konkrete Fakten vorlegen, aus denen hervorgeht, dass die beantragten Informationen für laufende strafrechtliche Ermittlungen relevant sind. Um an die gespeicherten Inhalte elektronischer Kommunikation zu gelangen, benötigen die Strafverfolgungsbehörden generell eine entsprechende richterliche Anordnung, die auf dem hinreichenden Verdacht basiert, dass das betreffende Konto Nachweise für eine Straftat enthält. Im SCA sind darüber hinaus auch die Privathaftpflicht und die strafrechtlichen Sanktionen geregelt.

Gerichtlich angeordnete Überwachung nach dem Federal Wiretap Law (Bundesabhörgesetz): Nach dem Bundesabhörgesetz kann die Strafverfolgung darüber hinaus zu strafrechtlichen Ermittlungszwecken in Echtzeit drahtgebundene, mündliche oder elektronische Kommunikation abhören bzw. abfangen. Siehe 18 U.S.C. §§ 2510-2522. Dies kann nur auf gerichtliche Anordnung geschehen, wenn durch einen Richter unter anderem festgestellt wird, dass das Abhören

oder elektronische Abfangen vermutlich Beweise für einen Verstoß gegen das Bundesgesetz erbringen oder Hinweise auf den Aufenthaltsort einer sich der Strafverfolgung entziehenden Person liefern wird. In diesem Gesetz sind darüber hinaus auch die Privathaftpflicht und die strafrechtlichen Sanktionen bei Verstoß gegen die Abhörvorschriften geregelt.

Durchsuchungsbefehl — Artikel 41: Nach richterlicher Anordnung können Gebäude in den USA von den Strafverfolgungsbehörden durchsucht werden. Letztere müssen dem Richter anhand eines „hinreichenden Verdachts" glaubhaft darlegen, dass eine Straftat begangen wurde bzw. begangen werden soll und dass an dem im Durchsuchungsbefehl genannten Ort vermutlich mit der Straftat zusammenhängende Gegenstände gefunden werden. Von dieser Befugnis wird häufig Gebrauch gemacht, wenn eine polizeiliche Durchsuchung eines Gebäudes erforderlich wird, weil die Gefahr besteht, dass möglicherweise Beweismittel vernichtet werden, wenn eine Anordnung zur Herausgabe gegen das betreffende Unternehmen ergeht. *Siehe* vierter Zusatzartikel zur Verfassung der Vereinigten Staaten (auf den oben bereits eingegangen wurde), Federal Rules of Criminal Procedure, S. 41. Die Person, gegen die der Durchsuchungsbefehl ergeht, kann gegen diesen vorgehen, weil er überzogen und schikanös ist oder auf unberechtigte Weise erlangt wurde, und Geschädigte mit Klageberechtigung können bei rechtswidrigen Durchsuchungen erlangte Beweise unterdrücken. Siehe Rechtssache *Mapp v. Ohio*, 367 U, S. 643 (1961).

Leitlinien und Strategien des Justizministeriums: Neben diesen verfassungsrechtlichen, gesetzlich vorgeschriebenen und auf Regelungen beruhenden Einschränkungen des staatlichen Zugriffs auf Daten hat der Justizminister Leitlinien veröffentlicht, die den Datenzugriff zu Zwecken der Strafverfolgung weiter einschränken und auch die Privatsphäre und die Bürgerrechte schützen. So wird beispielsweise in den Leitlinien des Justizministers für Inlandseinsätze des FBI von September 2008 (im Folgenden FBI-Leitlinien des Justizministers), abrufbar unter http://www.justice.gov/archive/opa/docs/guidelines.pdf, die Anwendung von Ermittlungstechniken zur Einholung von Informationen für Ermittlungen im Rahmen von Verstößen gegen das Bundesgesetz eingeschränkt. Diese Leitlinien verpflichten das FBI, die mit den geringsten Eingriffen verbundenen Ermittlungsmethoden anzuwenden und die Auswirkungen auf die Privatsphäre und die Bürgerrechte und die potenzielle Rufschädigung zu berücksichtigen. Darüber hinaus wird darauf hingewiesen, dass „das FBI seine Ermittlungen und sonstigen Aktivitäten selbstverständlich rechtmäßig und angemessen unter Einhaltung von Bürgerrechten und Privatsphäre so durchführen muss, dass ein unnötiges Eindringen in das Privatleben gesetzestreuer Personen vermieden wird." Siehe FBI-Leitlinien des Justizministers, Seite 5. Umgesetzt hat das FBI diese Leitlinien mithilfe des FBI Domestic Investigations and Operations Guide (abrufbar unter https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20(DIOG), eines umfassenden Handbuchs mit detaillierten Erläuterungen zu den Grenzen der Anwendung von Ermittlungsinstrumenten und entsprechenden Hilfestellungen zur Gewährleistung des Schutzes von Bürgerrechten und Privatsphäre bei sämtlichen Ermittlungen. Weitere Vorschriften und Strategien, die die Ermittlungstätigkeit der Bundesanwälte einschränken, sind im **United States Attorneys' Manual** (USAM, Anwaltshandbuch der Vereinigten Staaten), aufgeführt, das ebenfalls online abrufbar ist unter http://www.justice.gov/usam/united-states-attorneys-manual.

Zivil- und Aufsichtsbehörden (öffentliches Interesse):

Auch die Zivil- oder Aufsichtsbehörden (die im öffentlichen Interesse handeln) erhalten nur sehr eingeschränkt Zugriff auf Daten von Unternehmen in den Vereinigten Staaten. Behörden mit zivilen und aufsichtsrechtlichen Aufgaben können von Unternehmen die Herausgabe von Geschäftsunterlagen, elektronisch gespeicherten Informationen oder sonstigen materiellen Beweismitteln verlangen. Diese Behörden unterliegen in der Ausübung ihrer administrativen oder zivilen Anordnungsbefugnis Einschränkungen, und zwar nicht nur durch ihre jeweiligen Gründungsgesetze, sondern auch, weil die Anordnungen vor ihrer potenziellen gerichtlichen Umsetzung einer unabhängigen gerichtlichen Überprüfung unterzogen werden. Siehe z. B. die Federal Rules of Civil Procedure [Zivilprozessordnung], S. 45. Die Behörden können nur den Zugriff auf Daten beantragen, die für Sachen innerhalb ihres Verantwortungsbereichs von Belang sind. Darüber hinaus kann ein Empfänger einer behördlichen Anordnung deren Umsetzung vor Gericht anfechten, indem er nachweist, dass die Behörde den Grundsatz der Zumutbarkeit missachtet hat, wie bereits oben dargelegt wurde.

Unternehmen, die sich Datenabfragen von Verwaltungsbehörden widersetzen möchten, können sich je nach Branche und Datenart auf weitere Rechtsgrundlagen stützen. So können Finanzinstitute beispielsweise behördliche Anordnungen anfechten, bei denen bestimmte Arten von Informationen abgerufen werden sollen, wodurch gegen das Bank Secrecy Act (Gesetz über das Bankgeheimnis) und dessen Durchführungsbestimmungen verstoßen wird. Siehe 31 U.S.C. § 5318, 31 C.F.R. Part X. Andere Unternehmen wiederum können sich auf das Fair Credit Reporting Act (Gesetz zur Regelung des Datenschutzes bei Konsumentenkrediten), siehe 15 U.S.C. § 1681b, oder andere branchenspezifische Gesetze berufen. Der Missbrauch einer Anordnungsbefugnis einer Behörde kann deren Haftung bzw. eine persönliche Haftung ihrer Beamten nach sich ziehen. Siehe z. B. das Right to Financial Privacy Act (Gesetz zum Schutz von Finanzdaten), 12 U.S.C. §§ 3401–3422. Somit schützen die Gerichte in den Vereinigten Staaten vor unangemessenen Anträgen der Regulierungsbehörden und vermitteln einen unabhängigen Überblick über die Maßnahmen der Bundesbehörden.

Jegliche gesetzliche Befugnis der Verwaltungsbehörden, Unterlagen eines Unternehmens in den Vereinigten Staaten nach einer behördlichen Durchsuchung zu beschlagnahmen, muss die Anforderungen des vierten Zusatzartikels erfüllen. *Siehe See v. City of Seattle*, 387 U, S. 541 (1967).

Fazit

Sämtliche Strafverfolgungsmaßnahmen und Aufsichtstätigkeiten in den Vereinigten Staaten müssen nach geltendem Recht erfolgen und im Einklang mit der Verfassung der USA sowie den Gesetzen, Regelungen und Vorschriften stehen. Außerdem müssen einschlägige Strategien wie die Leitlinien des Justizministers zur Regelung der Strafverfolgung auf Bundesebene befolgt werden. Mit dem oben beschriebenen Rechtsrahmen wird die Möglichkeit der amerikanischen Strafverfolgungs- und Aufsichtsbehörden eingeschränkt, Informationen von Unternehmen in den USA einzuholen — unabhängig davon, ob es sich dabei um Informationen über US-Bürger oder Drittstaatsangehörige handelt —, und die gerichtliche Überprüfung jeglicher Datenanfragen, die über diese Behörden erfolgen, ermöglicht.

Hochachtungsvoll

Bruce C. Swartz

Stellvertretender Generalstaatsanwalt des Justizministeriums und Berater für internationale Angelegenheiten

DURCHFÜHRUNGSBESCHLUSS (EU) 2016/1251 DER KOMMISSION

vom 12. Juli 2016

zur Annahme eines mehrjährigen Unionsprogramms für die Erhebung, Verwaltung und Nutzung von Daten im Fischerei- und Aquakultursektor für den Zeitraum 2017-2019

(Bekannt gegeben unter Aktenzeichen C(2016) 4329)

DIE EUROPÄISCHE KOMMISSION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union,

gestützt auf die Verordnung (EG) Nr. 199/2008 des Rates vom 25. Februar 2008 zur Einführung einer gemeinschaftlichen Rahmenregelung für die Erhebung, Verwaltung und Nutzung von Daten im Fischereisektor und Unterstützung wissenschaftlicher Beratung zur Durchführung der Gemeinsamen Fischereipolitik ([1]), insbesondere auf Artikel 3,

in Erwägung nachstehender Gründe:

(1) Gemäß Artikel 3 der Verordnung (EG) Nr. 199/2008 soll ein mehrjähriges Unionsprogramm für die Erhebung, Verwaltung und Nutzung von Daten im Fischereisektor für einen Zeitraum von drei Jahren angenommen werden, um die einheitliche Anwendung der Verpflichtung zur Erhebung und Verwaltung von Daten zu gewährleisten.

(2) Das derzeitige mehrjährige Unionsprogramm basiert auf dem mehrjährigen Programm für den Zeitraum 2011-2013, das mit dem Durchführungsbeschluss C(2013) 5243 der Kommission verlängert wurde, um den Zeitraum zwischen dem Erlass der Verordnung (EU) Nr. 1380/2013 des Europäischen Parlaments und des Rates ([2]) und dem 31. Dezember 2016 zu überbrücken. Daher sollte ein mehrjähriges Unionsprogramm für den Zeitraum ab dem 1. Januar 2017 erstellt werden.

(3) Gemäß Artikel 25 der Verordnung (EU) Nr. 1380/2013 erheben die Mitgliedstaaten biologische, ökologische, technische und sozioökonomische Daten für das Fischereimanagement. Das mehrjährige Unionsprogramm ist notwendig, damit die Mitgliedstaaten ihre Datenerhebungstätigkeiten in ihren nationalen Arbeitsplänen spezifizieren und planen können. Im Einklang mit Artikel 21 der Verordnung (EU) Nr. 508/2014 des Europäischen Parlaments und des Rates ([3]) werden diese nationalen Arbeitspläne der Kommission bis zum 31. Oktober des Jahres vorgelegt, das dem Jahr vorausgeht, ab dem der Arbeitsplan Anwendung finden soll.

(4) Im mehrjährigen Unionsprogramm sollten die Anforderungen in Bezug auf die Datenerhebung gemäß Artikel 1 der Verordnung (EG) Nr. 199/2008 festgelegt werden. Dieses sollte die für die Umsetzung der Gemeinsamen Fischereipolitik notwendigen Elemente enthalten, soweit sie nicht bereits im Rahmen anderer Rechtsvorschriften erforderlich sind.

(5) Im Hinblick auf die Verwirklichung der Ziele der reformierten Gemeinsamen Fischereipolitik gemäß Artikel 2 der Verordnung (EU) Nr. 1380/2013 ist es erforderlich, die Datenanforderungen der Union für fundierte wissenschaftliche Gutachten für den Zeitraum ab dem 1. Januar 2017 zu aktualisieren.

(6) Darüber hinaus erfordern neue internationale Verpflichtungen und Auflagen, denen die Mitgliedstaaten und die Union durch multilaterale und bilaterale Abkommen im Bereich Fischerei unterliegen, die Aufnahme bestimmter Anforderungen in Bezug auf die Datenerhebung in das mehrjährige Unionsprogramm. Dies gilt insbesondere für die Anforderungen, die sich aus den partnerschaftlichen Abkommen über nachhaltige Fischerei ergeben.

([1]) ABl. L 60 vom 5.3.2008, S. 1.

([2]) Verordnung (EU) Nr. 1380/2013 des Europäischen Parlaments und des Rates vom 11. Dezember 2013 über die Gemeinsame Fischereipolitik und zur Änderung der Verordnungen (EG) Nr. 1954/2003 und (EG) Nr. 1224/2009 des Rates sowie zur Aufhebung der Verordnungen (EG) Nr. 2371/2002 und (EG) Nr. 639/2004 des Rates und des Beschlusses 2004/585/EG des Rates (ABl. L 354 vom 28.12.2013, S. 22).

([3]) Verordnung (EU) Nr. 508/2014 des Europäischen Parlaments und des Rates vom 15. Mai 2014 über den Europäischen Meeres- und Fischereifonds und zur Aufhebung der Verordnungen (EG) Nr. 2328/2003, (EG) Nr. 861/2006, (EG) Nr. 1198/2006 und (EG) Nr. 791/2007 des Rates und der Verordnung (EU) Nr. 1255/2011 des Europäischen Parlaments und des Rates (ABl. L 149 vom 20.5.2014, S. 1).

(7) Eine Bewertung des geltenden Rahmens für die Erhebung, Verwaltung und Nutzung von Daten im Fischereisektor und anschließende Konsultationen von Interessenträgern haben gezeigt, dass das mehrjährige Unionsprogramm sich darauf konzentrieren sollte, welche Daten der Mitgliedstaaten notwendig sind, und nicht auf die Verfahren zu ihrer Erhebung. Methodische Anforderungen werden in den Arbeitsplänen der Mitgliedstaaten dargelegt, die von der Kommission vor dem Hintergrund einer engen Zusammenarbeit zwischen den Mitgliedstaaten auf Ebene der Meeresregionen genehmigt werden.

(8) Das Unionsprogramm für den Zeitraum 2017-2019 sollte daher alle diese Aspekte berücksichtigen und den Zielen der Verordnung (EU) Nr. 1380/2013, insbesondere der Artikel 2 und 25, so weit wie möglich innerhalb des durch die Verordnung (EG) Nr. 199/2008 geschaffenen Rechtsrahmens Rechnung tragen. Gehen neue Datenanforderungen über den derzeitigen Rechtsrahmen hinaus, so sollten sie fakultativ sein. Sobald ein neuer Rechtsrahmen zur Änderung der Verordnung (EG) Nr. 199/2008 in Kraft treten wird, kann die Kommission das mehrjährige Unionsprogramm ändern und, soweit erforderlich, die neuen Anforderungen in Bezug auf die Datenerhebung einfließen lassen.

(9) Die Kommission hat die Empfehlungen berücksichtigt, die sich aus der Konsultation im Rahmen der regionalen Koordinierungstreffen gemäß Artikel 5 der Verordnung (EG) Nr. 199/2008 und mit dem Wissenschafts-, Technik- und Wirtschaftsausschuss für die Fischerei (STECF) ergeben haben. Andere geeignete beratende wissenschaftliche Einrichtungen wie der Internationale Rat für Meeresforschung (ICES) wurden ebenfalls konsultiert, ebenso Vertreter der Mitgliedstaaten in spezialisierten Sachverständigengruppen.

(10) Aus Gründen der Rechtssicherheit sollte der Durchführungsbeschluss C(2013) 5243 aufgehoben werden.

(11) Die in diesem Beschluss vorgesehenen Maßnahmen entsprechen der Stellungnahme des Verwaltungsausschusses für Fischerei und Aquakultur —

HAT FOLGENDEN BESCHLUSS ERLASSEN:

Artikel 1

Das in Artikel 3 der Verordnung (EG) Nr. 199/2008 genannte mehrjährige Unionsprogramm für die Erhebung, Verwaltung und Nutzung von Daten im Fischereisektor für den Zeitraum 2017-2019 ist im Anhang dieses Beschlusses enthalten.

Artikel 2

Der Durchführungsbeschluss C(2013) 5243 wird mit Wirkung vom 1. Januar 2017 aufgehoben.

Artikel 3

Dieser Beschluss ist an die Mitgliedstaaten gerichtet.

Brüssel, den 12. Juli 2016

Für die Kommission
Karmenu VELLA
Mitglied der Kommission

ANHANG

KAPITEL I

Begriffsbestimmungen

Für die Zwecke dieses Anhangs finden die Begriffsbestimmungen in der Verordnung (EG) Nr. 1224/2009 des Rates ([1]), der Durchführungsverordnung (EU) Nr. 404/2011 der Kommission ([2]) und der Verordnung (EU) Nr. 1380/2013 des Europäischen Parlaments und des Rates ([3]) Anwendung. Ferner gelten die folgenden Begriffsbestimmungen:

1. **Aktive Fischereifahrzeuge**: Fischereifahrzeuge, die im Verlauf eines Kalenderjahres (einen Tag oder mehr) einer Fangtätigkeit nachgegangen sind. Ein Fischereifahrzeug, das in einem Jahr keiner Fangtätigkeit nachgegangen ist, gilt als inaktiv.

2. **Anadrome Arten**: lebende aquatische Ressourcen mit einem Lebenszyklus, der mit dem Schlüpfen in Süßwasser beginnt, gefolgt von einer Migration ins Salzwasser, der Rückkehr und schließlich dem Laichen in Süßwasser.

3. **Katadrome Arten**: lebende aquatische Ressourcen mit einem Lebenszyklus, der mit dem Schlüpfen in Salzwasser beginnt, gefolgt von einer Migration ins Süßwasser, der Rückkehr und schließlich dem Laichen in Salzwasser.

4. **Fanganteil**: ein Teil der Gesamtfänge. Beispiele sind der Anteil der oberhalb der Mindestreferenzgröße für die Bestandserhaltung angelandeten Fänge, der Anteil der unterhalb der Mindestreferenzgröße für die Bestandserhaltung angelandeten Fänge, der Anteil der Rückwürfe, die unterhalb der Mindestreferenzgröße für die Bestandserhaltung liegen, „De-minimis-Rückwürfe“ oder Rückwürfe.

5. **Tag auf See**: ein fortlaufender Zeitabschnitt von 24 Stunden (oder einem Teil von 24 Stunden), während dessen ein Fischereifahrzeug in einem Gebiet anwesend ist und sich nicht in einem Hafen befindet.

6. **Fangtage**: jeder Tag auf See, an dem eine Fangtätigkeit erfolgt, unbeschadet der internationalen Verpflichtungen der Union und ihrer Mitgliedstaaten. Eine Fangreise kann sowohl zu der Summe der Fangtage für stationäre Fanggeräte als auch zu der Summe der Fangtage für bewegliche Fanggeräte beitragen

7. **Fanggrund**: (Gruppe) geografische(r) Einheiten, in denen Fischerei stattfindet. Diese Einheiten müssen auf Ebene der Meeresregion auf der Grundlage bestehender, von regionalen Fischereiorganisationen oder wissenschaftlichen Gremien definierter Gebiete vereinbart werden.

8. **Flottensegment**: eine Gruppe von Fischereifahrzeugen der gleichen Längenklasse (Lüa, Länge über alles) mit im Jahresverlauf gleichem vorherrschendem Fanggerät.

9. **Metier**: eine Einheit von Fangvorgängen, die ähnliche Arten oder eine ähnliche Gruppe von Arten betreffen, mit ähnlichem Fanggerät ([4]) während desselben Zeitraums im Jahr und/oder im gleichen Gebiet stattfinden und durch eine ähnliche Art der fischereilichen Nutzung eines Bestands gekennzeichnet sind.

10. **Wissenschaftliche Forschungsreisen auf See**: Reisen auf einem Forschungsschiff oder einem Schiff für die wissenschaftliche Forschung zur Überwachung von Beständen und Ökosystemen, das von der für die Durchführung des nationalen Arbeitsplans gemäß Artikel 21 der Verordnung (EU) Nr. 508/2014 verantwortlichen Stelle mit dieser Aufgabe betraut wurde.

([1]) Verordnung (EG) Nr. 1224/2009 des Rates vom 20. November 2009 zur Einführung einer gemeinschaftlichen Kontrollregelung zur Sicherstellung der Einhaltung der Vorschriften der Gemeinsamen Fischereipolitik und zur Änderung der Verordnungen (EG) Nr. 847/96, (EG) Nr. 2371/2002, (EG) Nr. 811/2004, (EG) Nr. 768/2005, (EG) Nr. 2115/2005, (EG) Nr. 2166/2005, (EG) Nr. 388/2006, (EG) Nr. 509/2007, (EG) Nr. 676/2007, (EG) Nr. 1098/2007, (EG) Nr. 1300/2008, (EG) Nr. 1342/2008 sowie zur Aufhebung der Verordnungen (EWG) Nr. 2847/93, (EG) Nr. 1627/94 und (EG) Nr. 1966/2006 (ABl. L 343 vom 22.12.2009, S. 1).

([2]) Durchführungsverordnung (EU) Nr. 404/2011 der Kommission vom 8. April 2011 mit Durchführungsbestimmungen zu der Verordnung (EG) Nr. 1224/2009 des Rates zur Einführung einer gemeinschaftlichen Kontrollregelung zur Sicherstellung der Einhaltung der Vorschriften der Gemeinsamen Fischereipolitik (ABl. L 112 vom 30.4.2011, S. 1).

([3]) Verordnung (EU) Nr. 1380/2013 des Europäischen Parlaments und des Rates vom 11. Dezember 2013 über die Gemeinsame Fischereipolitik und zur Änderung der Verordnungen (EG) Nr. 1954/2003 und (EG) Nr. 1224/2009 des Rates sowie zur Aufhebung der Verordnungen (EG) Nr. 2371/2002 und (EG) Nr. 639/2004 des Rates und des Beschlusses 2004/585/EG des Rates (ABl. L 354 vom 28.12.2013, S. 22).

([4]) Gemäß Anhang XI der Verordnung (EU) Nr. 404/2011.

KAPITEL II

Verfahren der Datenerhebung

Methoden zur Datenerfassung und Qualität müssen den in Artikel 25 der Verordnung (EU) Nr. 1380/2013 definierten Zwecken angemessen sein und sich an den von den einschlägigen wissenschaftlichen Gremien empfohlenen bewährten Verfahren und Methoden orientieren. Zu diesem Zweck sind die Methoden und das Ergebnis ihrer Anwendung in regelmäßigen Abständen von unabhängigen wissenschaftlichen Gremien daraufhin zu prüfen, ob sie für die Verwaltung der Gemeinsamen Fischereipolitik geeignet sind.

KAPITEL III

Datenanforderungen

1. **Datensätze**

1.1. Die Mitgliedstaaten legen im Rahmen der Arbeitspläne gemäß Artikel 21 der Verordnung (EU) Nr. 508/2014 die zu erhebenden Daten unter den folgenden Datensätzen nach Maßgabe der Nummern 2 bis 7 dieses Kapitels fest:

a) biologische Daten je Fanganteil, über Bestände, die im Rahmen der gewerblichen Fischerei der Union in Unionsgewässern und Gewässern außerhalb der Union sowie durch die Freizeitfischerei in Unionsgewässern gefangen werden;

b) Daten zur Bewertung der Auswirkungen der Unionsfischerei auf das Meeresökosystem in Unionsgewässern und Gewässern außerhalb der Union;

c) ausführliche Daten über die Tätigkeiten der Fischereifahrzeuge der Union in Unionsgewässern und Gewässern außerhalb der Union, gemeldet gemäß der Verordnung (EG) Nr. 1224/2009;

d) soziale und wirtschaftliche Daten zur Fischerei ([1]);

e) soziale, wirtschaftliche und umweltbezogene Daten zur Aquakultur.

1.2. Die Daten werden in Übereinstimmung mit den Artikeln 3, 4 und 5 der Verordnung (EG) Nr. 199/2008 und unter Berücksichtigung der Schwellenwerte gemäß Kapitel V dieses Anhangs erhoben.

1.3. Es sind Daten zu erheben, um gültige Schätzungen für die Art der Fischereien, Zeiträume und Gebiete zu ermöglichen, die auf Ebene der Meeresregion entsprechend den Bedürfnissen der Endnutzer vereinbart werden. Die Häufigkeit der Datenerhebungen wird auf Ebene der Meeresregion koordiniert, sofern in diesem Anhang und den entsprechenden Tabellen nichts anderes bestimmt ist.

2. **Biologische Daten über Bestände, die im Rahmen der gewerblichen Fischerei der Union in Unionsgewässern und Gewässern außerhalb der Union sowie durch die Freizeitfischerei in Unionsgewässern gefangen werden**

Diese Daten umfassen Folgendes:

a) Fangmengen nach Arten und biologische Daten von einzelnen Exemplaren, die folgende Schätzungen ermöglichen:

i) für gewerbliche Fischereien Umfang und Längen aller Fanganteile (einschließlich Rückwürfe und unerwünschte Fänge) für die Bestände, die in den Tabellen 1A, 1B und 1C aufgeführt sind und auf Aggregationsebene 6 gemäß Tabelle 2 gemeldet werden. Die zeitliche Auflösung wird auf der Grundlage der Bedürfnisse der Endnutzer auf Ebene der Meeresregion abgestimmt;

ii) für gewerbliche Fischereien Durchschnittsgewicht und Altersverteilung bei Fängen der in den Tabellen 1A, 1B und 1C aufgeführten Bestände. Die Auswahl der Bestände, aus denen diese Variablen zu erheben sind, und die zeitliche Auflösung werden auf der Grundlage der Bedürfnisse der Endnutzer auf Ebene der Meeresregion koordiniert;

([1]) Daten über die Verarbeitungsindustrie können auf freiwilliger Basis erhoben werden. In diesem Fall können die Unterteilung und die Variablen der Tabelle 11 verwendet werden.

iii) für gewerbliche Fischereien Geschlechterverhältnis, Reife und Fruchtbarkeitsdaten für die in den Tabellen 1A, 1B und 1C aufgeführten Bestände bei Fängen in für wissenschaftliche Gutachten erforderlicher Häufigkeit. Die Auswahl der Bestände, aus denen diese Variablen zu erheben sind, und die zeitliche Auflösung werden auf der Grundlage der Bedürfnisse der Endnutzer auf Ebene der Meeresregion koordiniert;

iv) für die Freizeitfischerei jährliche Menge (Anzahl und Gewichte oder Länge) der Fänge und Freisetzungen für die in Tabelle 3 aufgeführten Arten und/oder die je nach Bedarf auf Ebene der Meeresregion als für das Fischereimanagement erforderlich eingestuften Arten. Die Bedürfnisse der Endnutzer in Bezug auf Alter oder andere biologische Daten gemäß den Ziffern i bis iii werden für die Freizeitfischerei auf Ebene der Meeresregion bewertet.

b) Zusätzlich zu den Daten gemäß Buchstabe a Daten über anadrome und katadrome Arten gemäß Tabelle 1E, die während der Süßwasserphase ihres Lebenszyklus im Rahmen der gewerblichen Fischerei gefangen werden, und zwar unabhängig von der Art dieser Fischereien:

i) bestandsbezogene Variablen (für einzelne Exemplare, Alter, Länge, Gewicht, Geschlecht, Reife und Fruchtbarkeit, nach Entwicklungsstadium, jedoch näher aufgeschlüsselt nach Art und auf regionaler Ebene) und

ii) jährliche Fangmengen nach Altersklasse oder Entwicklungsstadium.

c) Darüber hinaus

in Bezug auf Aal Informationen (z. B. Daten, Schätzungen, Trends usw.), die jährlich in mindestens einem Flusseinzugsgebiet pro Aal-Bewirtschaftungseinheit gesammelt werden über

i) die Abundanz der Zugänge,

ii) die Abundanz des ständigen Bestands (Gelbaal) und

iii) Anzahl oder Gewicht und Geschlechterverhältnis abwandernder Blankaale;

in Bezug auf alle Wildlachse jährlich erhobene Informationen — sofern nicht auf regionaler Ebene anders vereinbart — über die Abundanz von Sälmling und Junglachs und die Anzahl flussaufwärts wandernder Individuen.

Die für Aal und Lachs zu überwachenden Flüsse werden auf regionaler Ebene festgelegt. Die Auswahl der Bestände, aus denen diese Variablen zu erheben sind, wird auf der Grundlage der Bedürfnisse der Endnutzer auf regionaler Ebene koordiniert.

3. **Daten zur Bewertung der Auswirkungen der Unionsfischerei auf Meeresökosysteme in Unionsgewässern und Gewässern außerhalb der Union**

Diese Daten umfassen Folgendes:

a) für alle Arten der Fischerei ungewollte Beifänge von Vögeln, Säugetieren, Reptilien und Fischen, die gemäß den Rechtsvorschriften der Union und internationalen Vereinbarungen geschützt sind, einschließlich der in der Tabelle 1D aufgeführten Arten, einschließlich nicht erfolgter Beifänge, während wissenschaftlicher Beobachterfahrten an Bord von Fischereifahrzeugen oder durch die Fischer selbst in Logbüchern erfasst.

Werden Daten zu Beifängen aus Beobachterfahrten als nicht hinreichend für die Bedürfnisse der Endnutzer betrachtet, wenden die Mitgliedstaaten andere Verfahren an. Die Auswahl dieser Verfahren wird auf der Grundlage der Bedürfnisse der Endnutzer auf Ebene der Meeresregion abgestimmt.

b) Daten zur Unterstützung der Abschätzung der Auswirkungen der Fischereien in den Unionsgewässern und außerhalb der Gewässer der Union auf marine Lebensräume.

Zur Bewertung der Auswirkungen der Fischerei auf marine Lebensräume werden die Variablen gemäß der Verordnung (EG) Nr. 1224/2009 verwendet. Die Daten werden auf Ebene 3 der Fischereitätigkeit aufgeschlüsselt ([1]), außer wenn auf regionaler Ebene, insbesondere im Fall von Meeresschutzgebieten, eine niedrigere Aggregationsebene notwendig ist.

([1]) Siehe Tabelle 2.

Wenn gemäß der Verordnung (EG) Nr. 1224/2009 erhobene Daten nicht ordnungsgemäß aufgeschlüsselt oder nicht von ausreichender Qualität oder Deckung für die vorgesehene wissenschaftliche Verwendung sind, werden sie auf andere Weise mit geeigneten Stichprobenverfahren erhoben. Gemäß der Verordnung (EG) Nr. 1224/2009 erhobene Daten werden den nationalen Stellen, die die Arbeitspläne umsetzen, auf der geeigneten Aggregationsebene zur Verfügung gestellt.

c) Daten für die Schätzung des fischereilichen Umfangs und der Auswirkungen der Fischereitätigkeiten auf die biologischen Meeresschätze und die marinen Ökosysteme, wie Auswirkungen auf nichtkommerzielle Arten, Räuber-Beute-Beziehungen und natürliche Sterblichkeit von Fischarten in jeder Meeresregion.

Diese Daten werden zunächst im Rahmen von Pilotstudien untersucht. Auf der Grundlage der Ergebnisse dieser Pilotstudien entscheiden die Mitgliedstaaten über die künftige Datenerhebung für jede einzelne Meeresregion, abgestimmt auf Ebene der Meeresregion und auf der Grundlage der Bedürfnisse der Endnutzer.

4. **Ausführliche Daten über die Tätigkeiten der Fischereifahrzeuge der Union** [1] **in Unionsgewässern und Gewässern außerhalb der Union, gemeldet gemäß der Verordnung (EG) Nr. 1224/2009**

Daten zur Bewertung der Tätigkeiten der Fischereifahrzeuge der Union in Unionsgewässern und außerhalb der Gewässer der Union bestehen aus den in Tabelle 4 aufgeführten Variablen. Gemäß der Verordnung (EG) Nr. 1224/2009 erhobene, erfasste und übermittelte Daten werden den nationalen Stellen, die die Arbeitspläne umsetzten, in Form von Primärdaten zur Verfügung gestellt. Wenn diese Daten im Rahmen der Verordnung (EG) Nr. 1224/2009 nicht erhoben werden sollen oder im Rahmen der genannten Verordnung erhobene Daten nicht richtig aufgeschlüsselt sind oder nicht die angemessene Qualität oder ausreichende Abdeckungsbreite für die vorgesehene wissenschaftliche Verwendung aufweisen, werden sie auf andere Weise mit geeigneten Stichprobenverfahren erhoben. Diese Verfahren ermöglichen die Schätzung der in Tabelle 4 aufgeführten Variablen auf der untersten relevanten geografischen Ebene je Flottensegment (Tabelle 5A) und Metier auf Ebene 6 (Tabelle 2).

5. **Soziale und wirtschaftliche Daten über die Fischerei, um die soziale und wirtschaftliche Leistung des Fischereisektors der Union bewerten zu können**

Diese Daten umfassen Folgendes:

a) Wirtschaftliche Variablen gemäß Tabelle 5A nach Sektoraufteilung gemäß Tabelle 5B und Supraregionen gemäß Tabelle 5C.

Die Grundgesamtheit umfasst alle aktiven und inaktiven Schiffe im Fischereiflottenregister der Union nach Maßgabe der Verordnung (EG) Nr. 26/2004 der Kommission [2] am 31. Dezember des Berichtsjahres und Schiffe, die zu diesem Zeitpunkt nicht im Register geführt werden, aber im Berichtsjahr mindestens einen Tag gefischt haben.

Für inaktive Schiffe werden lediglich der Kapitalwert und die Kapitalkosten erhoben.

In den Fällen, in denen auf die Identität einzelner natürlicher und/oder juristischer Personen geschlossen werden könnte, kann bei der Meldung wirtschaftlicher Variablen Clustering angewendet werden, um die statistische Vertraulichkeit sicherzustellen. Clustering kann gegebenenfalls auch für die Erstellung eines statistisch fundierten Beprobungsplans angewandt werden. Ein solches Clustering-Verfahren wird im Zeitverlauf konsistent gehandhabt.

Wirtschaftliche Daten werden jährlich erhoben.

b) Soziale Variablen gemäß Tabelle 6.

Soziale Daten werden ab 2018 alle drei Jahre erhoben.

Daten über die Beschäftigung nach Bildungsstand und Beschäftigung nach Staatsangehörigkeit können auf der Grundlage von Pilotstudien erhoben werden.

---

[1] Einschließlich besonderer Anforderungen für RFO im Sinne der Verordnung (EU) Nr. 1343/2011 des Europäischen Parlaments und des Rates vom 13. Dezember 2011 mit Vorschriften für die Fischerei im Übereinkommensgebiet der GFCM (Allgemeine Kommission für die Fischerei im Mittelmeer) und zur Änderung der Verordnung (EG) Nr. 1967/2006 des Rates betreffend die Maßnahmen für die nachhaltige Bewirtschaftung der Fischereiressourcen im Mittelmeer (ABl. L 347 vom 30.12.2011, S. 44).

[2] Verordnung (EG) Nr. 26/2004 der Kommission vom 30. Dezember 2003 über das Fischereiflottenregister der Gemeinschaft (ABl. L 5 vom 9.1.2004, S. 25).

6. **Soziale, wirtschaftliche und umweltbezogene Daten über marine Aquakultur und wahlweise zur Süßwasseraquakultur, um die soziale, wirtschaftliche und umweltbezogene Leistung des Aquakultursektors der Union zu bewerten**

Diese Daten umfassen Folgendes:

a) Wirtschaftliche Variablen gemäß Tabelle 7, nach Sektoraufteilung gemäß Tabelle 9.

Die Grundgesamtheit umfasst alle Unternehmen, deren Haupttätigkeit gemäß der Europäischen Klassifikation der Wirtschaftszweige NACE ([1]) unter die Codes 03.21 und 03.22 fällt und die einen Erwerbszweck verfolgen.

Wirtschaftliche Daten werden jährlich erhoben.

b) Soziale Variablen gemäß Tabelle 6.

Soziale Daten werden ab 2018 alle drei Jahre erhoben.

Daten über die Beschäftigung nach Bildungsstand und Beschäftigung nach Staatsangehörigkeit können auf der Grundlage von Pilotstudien erhoben werden.

c) Umweltbezogene Daten über die Aquakultur gemäß Tabelle 8, um die Bewertung von Aspekten der Umweltleistung zu ermöglichen.

Umweltbezogene Daten können auf der Grundlage von Pilotstudien erhoben und hochgerechnet werden, um für die Gesamtmenge des in dem Mitgliedstaat erzeugten Fischs relevante Ergebnisse zu erhalten.

Umweltbezogene Daten werden alle zwei Jahre erhoben.

KAPITEL IV

Forschungsreisen auf See

1. Mindestens alle Forschungsreisen auf See gemäß Tabelle 10 sind durchzuführen, es sei denn, eine Bewertung von Forschungsreisen führt zu dem Schluss, dass eine entsprechende Erhebung nicht länger für die Bestandsbewertung und das Fischereimanagement geeignet ist. Auf der Grundlage der gleichen wissenschaftlichen Kriterien können neue Forschungsreisen zu dieser Tabelle hinzugefügt werden.

2. Die Mitgliedstaaten legen im Rahmen der Arbeitspläne gemäß Artikel 21 der Verordnung (EU) Nr. 508/2014 die durchzuführenden Forschungsreisen auf See fest und sind verantwortlich für die Erhebungen.

3. Die jeweiligen Beiträge der Mitgliedstaaten zu internationalen Forschungsreisen werden innerhalb der gleichen Meeresregion abgestimmt.

4. Die Mitgliedstaaten garantieren in ihren nationalen Arbeitsplänen die Kontinuität mit früheren Surveykonzepten.

KAPITEL V

Schwellenwerte

1. Dieses Kapitel gilt für die Fischerei in der Union.

2. Es müssen keine biologischen Daten gesammelt werden, wenn für einen bestimmten Bestand oder eine bestimmte Art:

a) der Anteil eines Mitgliedstaats an der entsprechenden zulässigen Gesamtfangmenge (TAC) weniger als 10 % der Gesamtfangmenge der Union beträgt oder

([1]) Verordnung (EG) Nr. 1893/2006 des Europäischen Parlaments und des Rates vom 20. Dezember 2006 zur Aufstellung der statistischen Systematik der Wirtschaftszweige NACE Revision 2 und zur Änderung der Verordnung (EWG) Nr. 3037/90 des Rates sowie einiger Verordnungen der EG über bestimmte Bereiche der Statistik (ABl. L 393 vom 30.12.2006, S. 1).

b) in Fällen, in denen keine TAC festgesetzt ist, die gesamten Anlandungen eines Bestands oder einer Art durch einen Mitgliedstaat weniger als 10 % des Durchschnitts der Gesamtanlandungen der Union in den letzten drei Jahren betragen oder

c) die gesamten jährlichen Anlandungen einer Art durch einen Mitgliedstaat weniger als 200 Tonnen betragen. Für Arten mit besonderen Bewirtschaftungsbedürfnissen kann auf Ebene der Meeresregion ein niedrigerer Schwellenwert bestimmt werden.

Liegt die Summe der entsprechenden Quoten mehrerer Mitgliedstaaten, deren Anteil an der TAC weniger als 10 % beträgt, für einen bestimmten Bestand bei mehr als 25 % der TAC, findet der Schwellenwert von 10 % gemäß Buchstabe a keine Anwendung, und die Mitgliedstaaten gewährleisten eine Aufgabenteilung auf regionaler Ebene um sicherzustellen, dass der Bestand in Übereinstimmung mit den Bedürfnissen der Endnutzer beprobt wird.

Für große pelagische Arten sowie anadrome und katadrome Arten gilt kein Schwellenwert.

3. Unbeschadet genauerer Bestimmungen im Zusammenhang mit internationalen Verpflichtungen im Rahmen von RFO müssen keine biologische Daten erhoben werden, wenn der Unionsanteil für einen bestimmten international genutzten Fischbestand — mit Ausnahme von Beständen großer pelagischer oder weit wandernder Arten — weniger als 10 % beträgt.

4. Innerhalb von zwei Jahren ab dem Datum, an dem dieser Beschluss wirksam wird, stellen die Mitgliedstaaten Fangschätzungen aus bestehenden Erhebungen über die Freizeitfischerei bereit, einschließlich von Erhebungen der Rahmenregelung für die Datenerhebung oder zusätzlicher Pilotstudien, Diese Erhebungen ermöglichen, den Anteil der Fänge aus der Freizeitfischerei im Verhältnis zu gewerblichen Fängen für alle Arten in einer Meeresregion zu beurteilen, für die Fangschätzungen der Freizeitfischerei im Rahmen dieses Mehrjahresprogramms erforderlich sind. Die spätere Konzeption und der Umfang nationaler Erhebungen über die Freizeitfischerei, einschließlich etwaiger Schwellenwerte für die Datenerhebung, werden auf der Grundlage der Bedürfnisse der Endnutzer auf Ebene der Meeresregion festgelegt.

Kein Schwellenwert gilt für Freizeitfischereifänge bei Beständen, die Wiederauffüllungsplänen oder mehrjährigen Bewirtschaftungsplänen unterliegen, wie dies bei großen pelagischen Arten und weit wandernden Arten der Fall ist.

5. Es müssen keine sozialen und wirtschaftlichen Daten zur Aquakultur erhoben werden, wenn die Gesamterzeugung des Mitgliedstaats weniger als 1 % der gesamten Unionsproduktion (nach Menge und Wert) ausmacht. Es müssen keine Daten zur Aquakultur erhoben werden für Arten, auf die weniger als 10 % der Aquakulturerzeugung des Mitgliedstaats nach Menge und Wert entfallen. Darüber hinaus können die Mitgliedstaaten mit einer Gesamtproduktion von weniger als 2,5 % der Menge und des Werts der gesamten Aquakulturerzeugung der Union ein vereinfachtes Verfahren wie beispielsweise Pilotstudien festlegen, um die Daten für die Arten, die mehr als 10 % der Aquakulturerzeugung des Mitgliedstaats nach Menge und Wert ausmachen, hochzurechnen.

Referenzdaten sind die Daten der letzten Datenübermittlung der Mitgliedstaaten gemäß der Verordnung (EG) Nr. 762/2008 des Europäischen Parlaments und des Rates [1] und die entsprechenden von Eurostat veröffentlichten Daten.

6. Es müssen keine umweltbezogenen Daten über die Aquakultur erfasst werden, wenn die gesamte Aquakulturerzeugung des Mitgliedstaats weniger als 2,5 % der Gesamtproduktion dieses Wirtschaftszweigs der Union nach Menge und Wert ausmacht.

Referenzdaten sind die Daten der letzten Datenübermittlung der Mitgliedstaaten gemäß der Verordnung (EG) Nr. 762/2008 des Europäischen Parlaments und des Rates und die entsprechenden von Eurostat veröffentlichten Daten.

7. Die Beteiligung eines Mitgliedstaats (physisch oder finanziell) an Forschungsreisen auf See gemäß Tabelle 10 ist nicht obligatorisch, wenn sein Anteil an einer TAC der Union der entsprechenden Zielart unter einem Schwellenwert von 3 % liegt. Ist keine TAC festgesetzt, ist die Beteiligung eines Mitgliedstaats (physisch oder finanziell) an Forschungsreisen auf See nicht obligatorisch, wenn sein Anteil an den gesamten Anlandungen der Union in den vorangegangenen drei Jahren für einen Bestand oder eine Art unter einem Schwellenwert von 3 % liegt. Schwellenwerte für Erhebungen über mehrere Arten und Ökosysteme können auf Ebene der Meeresregion festgelegt werden.

8. Unbeschadet der Nummern 2 bis 7 können Mitgliedstaaten innerhalb der gleichen Meeresregion andere Schwellenwerte vereinbaren.

[1] Verordnung (EG) Nr. 762/2008 des Europäischen Parlaments und des Rates vom 9. Juli 2008 über die Vorlage von Aquakulturstatistiken durch die Mitgliedstaaten und zur Aufhebung der Verordnung (EG) Nr. 788/96 des Rates (ABl. L 218 vom 13.8.2008, S. 1).

BIOLOGISCHE DATEN

Tabelle 1A

Bestände in Unionsgewässern

Art (gebräuchliche Bezeichnung)	Art (wissenschaftliche Bezeichnung)	Gebiet (ICES- [1], IBSFC [2]- oder FAO [3]-Gebietscode), in dem sich der Bestand befindet/Bestandscode
Östliche Arktis, Norwegische See und Barentsee		
Aal	*Anguilla anguilla European eel*	I, II
Lumb	*Brosme brosme*	I, II
Atlanto-skandischer Hering	*Clupea harengus*	I, II
Kabeljau	*Gadus morhua*	I, II
Lodde	*Mallotus villosus*	I, II
Schellfisch	*Melanogrammus aeglefinus*	I, II
Blauer Wittling	*Micromesistius poutassou*	I-II
Tiefseegarnele	*Pandalus borealis*	I, II
Seelachs	*Pollachius virens*	I, II
Schwarzer Heilbutt	*Reinhardtius hippoglossoides*	I, II
Lachs	*Salmo salar*	I, II
Makrele	*Scomber scombrus*	II
Rotbarsch	*Sebastes marinus*	I, II
Tiefenbarsch	*Sebastes mentella*	I, II
Bastardmakrele	*Trachurus trachurus*	IIa
Skagerrak und Kattegat		
Sandaal	*Ammodytidae*	IIIa
Aal	*Anguilla anguilla*	IIIa
Hering	*Clupea harengus*	IIIa/22-24, IIIa
Rundnasen-Grenadier	*Coryphaenoides rupestris*	IIIa
Grauer Knurrhahn	*Eutrigla gurnardus*	IIIa
Kuckucks-Knurrhahn	*Aspitrigla cuculus*	IIIa

Art (gebräuchliche Bezeichnung)	Art (wissenschaftliche Bezeichnung)	Gebiet (ICES- (1), IBSFC (2)- oder FAO (3)-Gebietscode), in dem sich der Bestand befindet/Bestandscode
Kabeljau	*Gadus morhua*	IIIaN
Kabeljau	*Gadus morhua*	IIIaS
Rotzunge	*Glyptocephalus cynoglossus*	IIIa
Scharbe	*Limanda limanda*	IIIa
Schellfisch	*Melanogrammus aeglefinus*	IIIa
Wittling	*Merlangius merlangus*	IIIa
Seehecht	*Merluccius merluccius*	IIIa,
Blauer Wittling	*Micromesistius poutassou*	IIIa
Kaisergranat	*Nephrops norvegicus*	Funktionseinheit
Tiefseegarnele	*Pandalus borealis*	IIIa
Scholle	*Pleuronectes platessa*	IIIa
Seelachs	*Pollachius virens*	IIIa
Lachs	*Salmo salar*	IIIa
Steinbutt	*Psetta maxima*	IIIa
Makrele	*Scomber scombrus*	IIIa
Glattbutt	*Scophthalmus rhombus*	IIIa
Seezunge	*Solea solea*	IIIa
Sprotte	*Sprattus sprattus*	IIIa
Stintdorsch	*Trisopterus esmarki*	IIIa
Alle gewerblichen Haie und Rochen (4)	*Selachii, Rajidae*	IIIa
	Ostsee	
Aal	*Anguilla anguilla*	22-32
Hering	*Clupea harengus*	22-24/25-29, 32/30/31/Golf von Riga
Ostseeschnäpel	*Coregonus lavaretus*	IIId
Kleine Maräne	*Coregonus albula*	22-32
Dorsch	*Gadus morhua*	22-24/25-32

Art (gebräuchliche Bezeichnung)	Art (wissenschaftliche Bezeichnung)	Gebiet (ICES- (1), IBSFC (2)- oder FAO (3)-Gebietscode), in dem sich der Bestand befindet/Bestandscode
Scharbe	*Limanda limanda*	22-32
Barsch	*Perca fluviatilis*	IIId
Flunder	*Platichtys flesus*	22-32
Scholle	*Pleuronectes platessa*	22-32
Steinbutt	*Psetta maxima*	22-32
Lachs	*Salmo salar*	22-31/32
Meerforelle	*Salmo trutta*	22-32
Zander	*Sander lucioperca*	IIId
Glattbutt	*Scophthalmus rhombus*	22-32
Seezunge	*Solea solea*	22
Sprotte	*Sprattus sprattus*	22-32
Nordsee und östlicher Ärmelkanal		
Sandaal	*Ammodytidae*	IV
Wels	*Anarhichas* spp.	IV
Aal	*Anguilla anguilla*	IV, VIId
Goldlachs	*Argentina* spp.	IV
Grauer Knurrhahn	*Eutrigla gurnardus*	IV
Lumb	*Brosme brosme*	IV
Hering	*Clupea harengus*	IV, VIId
Sandgarnele	*Crangon crangon*	IV, VIId
Wolfsbarsch	*Dicentrarchus labrax*	IV, VIId
Grauer Knurrhahn	*Eutrigla gurnardus*	IV
Dorsch	*Gadus morhua*	IV, VIId
Rotzunge	*Glyptocephalus cynoglossus*	IV
Blaumaul	*Helicolenus dactylopterus*	IV
Vierfleckbutt	*Lepidorhombus boscii*	IV, VIId

Art (gebräuchliche Bezeichnung)	Art (wissenschaftliche Bezeichnung)	Gebiet (ICES- (1), IBSFC (2)- oder FAO (3)-Gebietscode), in dem sich der Bestand befindet/Bestandscode
Butte	*Lepidorhombus whiffiagonis*	IV, VIId
Scharbe	*Limanda limanda*	IV, VIId
Budegassa-Anglerfisch	*Lophius budegassa*	IV, VIId
Seeteufel	*Lophius piscatorius*	IV
Nordatlantik-Grenadier	*Macrourus berglax*	IV
Schellfisch	*Melanogrammus aeglefinus*	IV
Wittling	*Merlangius merlangus*	IV, VIId
Seehecht	*Merluccius merluccius*	IV, VII
Blauer Wittling	*Micromesistius poutassou*	IV, VIId
Limande	*Microstomus kitt*	IV, VIId
Blauleng	*Molva dypterygia*	IV
Leng	*Molva molva*	IV
Meerbarbe	*Mullus barbatus*	IV, VIId
Streifenbarbe	*Mullus surmuletus*	IV, VIId
Kaisergranat	*Nephrops norvegicus*	alle Funktionseinheiten
Tiefseegarnele	*Pandalus borealis*	IVa Ost/IVa/IV
Große Jakobsmuschel	*Pecten maximus*	VIId
Gabeldorsch	*Phycis blennoides*	IV
Mittelmeer-Gabeldorsch	*Phycis phycis*	IV
Flunder	*Platichthys flesus*	IV
Scholle	*Pleuronectes platessa*	IV
Scholle	*Pleuronectes platessa*	VIId
Seelachs	*Pollachius virens*	IV
Steinbutt	*Psetta maxima*	IV, VIId
Schwarzer Heilbutt	*Reinhardtius hippoglossoides*	IV

Art (gebräuchliche Bezeichnung)	Art (wissenschaftliche Bezeichnung)	Gebiet (ICES- (1), IBSFC (2)- oder FAO (3)-Gebietscode), in dem sich der Bestand befindet/Bestandscode
Lachs	*Salmo salar*	IV, VIId
Makrele	*Scomber scombrus*	IV, VIId
Glattbutt	*Scophthalmus rhombus*	IV, VIId
Rotbarsch	*Sebastes mentella.*	IV
Seezunge	*Solea solea*	IV
Seezunge	*Solea solea*	VIId
Sprotte	*Sprattus sprattus*	IV/VIId
Bastardmakrele	*Trachurus trachurus.*	IV, VIId
Roter Knurrhahn	*Trigla lucerna*	IV
Stintdorsch	*Trisopterus esmarki*	IV
Petersfisch	*Zeus faber*	IV, VIId
Alle gewerblichen Haie und Rochen (4)	*Selachii, Rajidae*	IV, VIId
Nordostatlantik und westlicher Ärmelkanal		
Glattkopf	*Alepocephalus bairdii*	VI, XII
Sandaal	*Ammodytidae*	VIa
Eberfisch	*Capros aper*	V, VI,VII
Jakobsmuschel	*Pecten maximus*	IV, VI, VII
Bunte Kammmuschel	*Aequipecten opercularis*	VII
Seespinne	*Maja squinado*	V, VI,VII
Aal	Anguilla anguilla	Alle Gebiete
Degenfisch	*Aphanopus spp.*	Alle Gebiete
Goldlachs	*Argentina* spp.	Alle Gebiete
Adlerfisch	*Argyrosomus regius*	Alle Gebiete
Kuckucks-Knurrhahn	*Aspitrigla cuculus*	Alle Gebiete
Kaiserbarsch	*Beryx* spp.	Alle Gebiete außer X und IXa
Kaiserbarsch	*Beryx* spp.	IXa und X

Art (gebräuchliche Bezeichnung)	Art (wissenschaftliche Bezeichnung)	Gebiet (ICES- (1), IBSFC (2)- oder FAO (3)-Gebietscode), in dem sich der Bestand befindet/Bestandscode
Taschenkrebs	*Cancer pagurus*	Alle Gebiete
Hering	*Clupea harengus*	VIa/VIaN/ VIa S, VIIbc/VIIa/VIIj
Meeraal	*Conger conger*	Alle Gebiete außer X
Meeraal	*Conger conger*	X
Rundnasen-Grenadier	*Coryphaenoides rupestris*	Alle Gebiete
Schokoladenhai	*Dalatias licha*	Alle Gebiete
Gewöhnlicher Stechrochen	*Dasyatis pastinaca*	VII, VIII
Schnabeldornhai	*Deania calcea*	V, VI, VII, IX, X, XII
Wolfsbarsch	*Dicentrarchus labrax*	Alle Gebiete außer IX
Wolfsbarsch	*Dicentrarchus labrax*	IX
Bastardzunge	*Dicologlossa cuneata*	VIIIc, IX
Sardelle	*Engraulis encrasicolus*	IXa (nur Cadiz)
Sardelle	*Engraulis encrasicolus*	VIII
Kleiner Schwarzer Dornhai	*Etmopterus spinax*	VI, VII, VIII
Grauer Knurrhahn	*Eutrigla gurnardus*	VIId,e
Kabeljau	*Gadus morhua*	Va/Vb/VIa/VIb/VIIa/VIIe-k
Rotzunge	*Glyptocephalus cynoglossus*	VI, VII
Blaumaul	*Helicolenus dactylopterus*	Alle Gebiete
Hummer	*Homarus gammarus*	Alle Gebiete
Granatbarsch	*Hoplostethus atlanticus*	Alle Gebiete
Degenfisch	*Lepidopus caudatus*	IXa
Vierfleckbutt	*Lepidorhombus boscii*	VIIIc, IXa
Butte	*Lepidorhombus whiffiagonis*	VI/VII, VIIIabd/VIIIc, IXa
Scharbe	*Limanda limanda*	VIIe/VIIa,f-h
Kalmar	*Loligo vulgaris*	Alle Gebiete außer VIIIc, IXa
Kalmar	*Loligo vulgaris*	VIIIc, IXa

Art (gebräuchliche Bezeichnung)	Art (wissenschaftliche Bezeichnung)	Gebiet (ICES- (1), IBSFC (2)- oder FAO (3)-Gebietscode), in dem sich der Bestand befindet/Bestandscode
Budegassa-Anglerfisch	*Lophius budegassa*	IV, VI/VIIb-k, VIIIabd
Budegassa-Anglerfisch	*Lophius budegassa*	VIIIc, IXa
Seeteufel	*Lophius piscatorius*	IV, VI/VIIb-k, VIIIabd
Seeteufel	*Lophius piscatorius*	VIIIc, IXa
Lodde	*Mallotus villosus*	XIV
Schellfisch	*Melanogrammus aeglefinus*	Va/Vb
Schellfisch	*Melanogrammus aeglefinus*	VIa/VIb/VIIa/VIIb-k
Wittling	*Merlangius merlangus*	VIII/IX, X
Wittling	*Merlangius merlangus*	Vb/VIa/VIb/VIIa/VIIe-k
Seehecht	*Merluccius merluccius*	IIIa, IV, VI, VII, VIIIab/VIIIc, IXa
Bastardzunge	*Microchirus variegatus*	Alle Gebiete
Blauer Wittling	*Micromesistius poutassou*	I-IX, XII, XIV
Limande	*Microstomus kitt*	Alle Gebiete
Blauleng	*Molva dypterygia*	Alle Gebiete außer X
Mittelmeer-Leng	*Molva macrophthalma*	X
Leng	*Molva molva*	Alle Gebiete
Streifenbarbe	*Mullus surmuletus*	Alle Gebiete
Nördlicher Glatthai	*Mustelus asterias*	VI, VII, VIII, IX
Glatthai	*Mustelus mustelus*	VI, VII, VIII, IX
Schwarzpunkt-Glatthai	*Mustelus punctulatus*	VI, VII, VIII, IX
Kaisergranat	*Nephrops norvegicus*	VI Funktionseinheit
Kaisergranat	*Nephrops norvegicus*	VII Funktionseinheit
Kaisergranat	*Nephrops norvegicus*	VIII, IX Funktionseinheit
Gewöhnlicher Krake	*Octopus vulgaris*	Alle Gebiete außer VIIIc, IXa
Gewöhnlicher Krake	*Octopus vulgaris*	VIIIc, IXa

Art (gebräuchliche Bezeichnung)	Art (wissenschaftliche Bezeichnung)	Gebiet (ICES- (1), IBSFC (2)- oder FAO (3)-Gebietscode), in dem sich der Bestand befindet/Bestandscode
Rote Fleckenbrasse	*Pagellus bogaraveo*	IXa, X
Tiefseegarnelen	*Pandalus* spp.	Alle Gebiete
Rosa Geißelgarnele	*Parapenaeus longirostris*	IXa
Gabeldorsch	*Phycis blennoides*	Alle Gebiete
Mittelmeer-Gabeldorsch	*Phycis phycis*	Alle Gebiete
Scholle	*Pleuronectes platessa*	VIIa/VIIe/VIIfg
Scholle	*Pleuronectes platessa*	VIIbc/VIIh-k/VIII, IX, X
Pollack	*Pollachius pollachius*	Alle Gebiete außer IX, X
Pollack	*Pollachius pollachius*	IX, X
Seelachs	*Pollachius virens*	Va/Vb/IV, IIIa, VI
Seelachs	*Pollachius virens*	VII, VIII
Wrackbarsch	*Polyprion americanus*	X
Steinbutt	*Psetta maxima*	Alle Gebiete
Schwarzer Heilbutt	*Reinhardtius hippoglossoides*	V, XIV/VI
Atlantischer Heilbutt	*Hippoglossus hippoglossus*	V, XIV
Lachs	*Salmo salar*	Alle Gebiete
Sardine	*Sardina pilchardus*	VIIIabd/VIIIc, IXa
Spanische Makrele	*Scomber colias*	VIII, IX, X
Makrele	*Scomber scombrus*	II, IIIa, IV, V, VI, VII, VIII, IX
Glattbutt	*Scophthalmus rhombus*	Alle Gebiete
Rotbarsch	*Sebastes marinus*	ICES-Untergebiete V, VI, XII, XIV & NAFO SA 2 + (Div. 1F + 3K)
Tiefenbarsch	*Sebastes mentella*	ICES-Untergebiete V, VI, XII, XIV & NAFO SA 2 + (Div. 1F + 3K)
Tintenfische	*Sepia officinalis*	Alle Gebiete
Seezunge	*Solea solea*	VIIa/VIIfg
Seezunge	*Solea solea*	VIIbc/VIIhjk/IXa/VIIIc

Art (gebräuchliche Bezeichnung)	Art (wissenschaftliche Bezeichnung)	Gebiet (ICES- (1), IBSFC (2)- oder FAO (3)-Gebietscode), in dem sich der Bestand befindet/Bestandscode
Seezunge	*Solea solea*	VIIe
Seezunge	*Solea solea*	VIIIab
Meerbrassen	*Sparidae*	Alle Gebiete
Mittelmeerstöcker	*Trachurus mediterraneus*	VIII, IX
Blaue Bastardmakrele	*Trachurus picturatus*	VIII, IX, X
Bastardmakrele	*Trachurus trachurus*	IIa, IVa, Vb, VIa, VIIa-c, e-k, VIIIabde/X
Bastardmakrele	*Trachurus trachurus*	VIIIc, IXa
Franzosendorsch	*Trisopterus* spp.	Alle Gebiete
Petersfisch	*Zeus faber*	Alle Gebiete
Alle gewerblichen Haie und Rochen (4)	*Selachii, Rajidae*	IV, VIId
Mittelmeer und Schwarzes Meer		
Aal	*Anguilla anguilla*	Alle Gebiete des Mittelmeers
Rote Tiefseegarnele	*Aristeomorpha foliacea*	Alle Gebiete des Mittelmeers
Rote Riesengarnele	*Aristeus antennatus*	Alle Gebiete des Mittelmeers
Gelbstriemen	*Boops boops*	1.3, 2.1, 2.2, 3.1, 3.2
Goldmakrele	*Coryphaena equiselis*	Alle Gebiete des Mittelmeers
Goldmakrele	*Coryphaena hippurus*	Alle Gebiete des Mittelmeers
Wolfsbarsch	*Dicentrarchus labrax*	Alle Gebiete des Mittelmeers
Zirrenkrake	*Eledone cirrhosa*	1.1, 1.3, 2.1, 2.2, 3.1
Moschuskrake	*Eledone moschata*	1.3, 2.1, 2.2, 3.1
Sardelle	*Engraulis encrasicolus*	Alle Gebiete des Mittelmeers
Sardelle	*Engraulis encrasicolus*	Schwarzes Meer GSA 29
Grauer Knurrhahn	*Eutrigla gurnardus*	2.2, 3.1
Kalmar	*Illex* spp., *Todarodes* spp.	Alle Gebiete des Mittelmeers
Segelfisch	*Istiophoridae*	Alle Gebiete des Mittelmeers

Art (gebräuchliche Bezeichnung)	Art (wissenschaftliche Bezeichnung)	Gebiet (ICES- [1], IBSFC [2]- oder FAO [3]-Gebietscode), in dem sich der Bestand befindet/Bestandscode
Kalmar	*Loligo vulgaris*	Alle Gebiete des Mittelmeers
Budegassa-Anglerfisch	*Lophius budegassa*	1.1, 1.2, 1.3, 2.2, 3.1
Seeteufel	*Lophius piscatorius*	1.1, 1.2, 1.3, 2.2, 3.1
Wittling	*Merlangius merlangus*	Schwarzes Meer GSA 29
Seehecht	*Merluccius merluccius*	Alle Gebiete des Mittelmeers
Blauer Wittling	*Micromesistius poutassou*	1.1, 3.1
Meeräschen	*Mugilidae*	1.3, 2.1, 2.2, 3.1
Meerbarbe	*Mullus barbatus*	Alle Gebiete des Mittelmeers
Meerbarbe	*Mullus barbatus*	Schwarzes Meer GSA 29
Streifenbarbe	*Mullus surmuletus*	Alle Gebiete des Mittelmeers
Gewöhnlicher Krake	*Octopus vulgaris*	Alle Gebiete des Mittelmeers
Kaisergranat	*Nephrops norvegicus*	Alle Gebiete des Mittelmeers
Rotbrasse	*Pagellus erythrinus*	Alle Gebiete des Mittelmeers
Rosa Geißelgarnele	*Parapenaeus longirostris*	Alle Gebiete des Mittelmeers
Furchengarnele	*Penaeus kerathurus*	3.1
Steinbutt	*Psetta maxima*	Schwarzes Meer GSA 29
Sardine	*Sardina pilchardus*	Alle Gebiete des Mittelmeers
Makrele	*Scomber* spp.	Alle Gebiete des Mittelmeers
Tintenfische	*Sepia officinalis*	Alle Gebiete des Mittelmeers
Seezunge	*Solea vulgaris*	1.2, 2.1, 3.1
Goldbrasse	*Sparus aurata*	1.2, 3.1
Schnauzenbrasse	*Spicara smaris*	2.1, 3.1, 3.2
Sprotte	*Sprattus sprattus*	Schwarzes Meer GSA 29
Gemeiner Heuschreckenkrebs	*Squilla mantis*	1.3, 2.1, 2.2
Mittelmeerstöcker	*Trachurus mediterraneus*	Alle Gebiete des Mittelmeers

Art (gebräuchliche Bezeichnung)	Art (wissenschaftliche Bezeichnung)	Gebiet (ICES- (1), IBSFC (2)- oder FAO (3)-Gebietscode), in dem sich der Bestand befindet/Bestandscode
Mittelmeerstöcker	*Trachurus mediterraneus*	Schwarzes Meer GSA 29
Bastardmakrele	*Trachurus trachurus*	Alle Gebiete des Mittelmeers
Bastardmakrele	*Trachurus trachurus*	Schwarzes Meer GSA 29
Roter Knurrhahn	*Trigla lucerna*	1.3, 2.2, 3.1
Venusmuschel	*Veneridae*	2.1, 2.2
Glasgrundel	*Aphia minuta*	GSA 9,10,16 und 19
Großer Ährenfisch	Atherina spp.	GSA 9,10,16 und 19
Zwergdorsch	*Trisopterus minutus*	Alle Regionen
Alle gewerblichen Haie und Rochen (4)	*Selachii, Rajidae*	Alle Regionen

(1) Internationaler Rat für Meeresforschung.
(2) Internationale Ostseefischereikommission.
(3) Ernährungs- und Landwirtschaftsorganisation der Vereinten Nationen.
(4) Auf Ebene der Arten zu melden.

BIOLOGISCHE DATEN

Tabelle 1B

Bestände der Regionen in äußerster Randlage der Union

Art (gebräuchliche Bezeichnung)	Art (wissenschaftliche Bezeichnung)
Französisch-Guayana	
Südlicher Schnapper	*Lutjanus purpureus*
Garnelen	*Farfantepenaeus subtilis*
Cynoscion acoupa	*Cynoscion acoupa*
Cynoscion steindachneri	*Cynoscion steindachneri*
Cynoscion virescens	*Cynoscion virescens*
Kreuzwelse	*Ariidae*
Dreischwanz	*Lobotes surinamensis*
Süßlippe	*Genyatremus luteus*
Snooks	Centropomus spp.

Art (gebräuchliche Bezeichnung)	Art (wissenschaftliche Bezeichnung)
Zackenbarsche	*Serranidae*
Meeräschen	Mugil spp.
Guadeloupe und Martinique	
Schnapper	*Lutjanidae*
Grunzer	*Haemulidae*
Zackenbarsche	*Serranidae*
Pazifischer Rotfeuerfisch	*Pterois volitans*
Thunfischähnliche	*Scombridae*
Atlantischer Blauer Marlin	*Makaira nigricans*
Goldmakrele	*Coryphaena hippurus*
Réunion und Mayotte	
Schnapper	*Lutjanidae*
Zackenbarsche	*Serranidae*
Thunfischähnliche	*Scombridae*
Schwertfisch	*Xiphias gladius*
Andere Segelfische	*Istiophoridae*
Goldmakrele	*Coryphaena hippurus*
Großäugiger Selar	*Selar crumenophthalmus*
Azoren, Madeira und Kanarische Inseln	
Spanische Makrele	*Scomber colias*
Sardinelle	*Sardinella maderensis*
Bastardmakrele	Trachurus spp.
Sardine	*Sardina pilchardus*
Seepapagei	*Sparisoma cretense*
Napfschnecken	*Patellidae*

BIOLOGISCHE DATEN

Tabelle 1C

Bestände in Meeresregionen, die regionalen Fischereiorganisationen (RFO) und partnerschaftlichen Abkommen über nachhaltige Fischerei unterliegen

IATTC (Interamerikanische Kommission für tropischen Thunfisch)

ARTEN Bei der Ausarbeitung der Stichprobenpläne für die Erhebung von biologischen Informationen gemäß Kapitel III dieses Anhangs sind die von den zuständigen regionalen Fischereiorganisationen festgesetzten Bestandsgrenzen zu berücksichtigen und geeignete Beprobungsmaßnahmen für jeden Bestand festzulegen.				Häufigkeit der Erhebung biologischer Variablen
Wissenschaftliche Bezeichnung	Gebräuchliche Bezeichnung	Geografisches Gebiet	Priorität	
Thunnus albacares	Gelbflossenthun	Östlicher Pazifik	hoch	Die Datenerhebung erfolgt jährlich, und die Aktualisierung/Verarbeitung der Daten muss zeitnah erfolgen, um in den Zeitplan für die Bestandsabschätzung zu passen.
Thunnus obesus	Großaugenthun	Östlicher Pazifik	hoch	
Katsuwonus pelamis	Echter Bonito	Östlicher Pazifik	hoch	
Thunnus alalunga	Weißer Thun	Östlicher Pazifik	hoch	
Thunnus orientalis	Nordpazifischer Blauflossenthun	Östlicher Pazifik	hoch	
Xiphias gladius	Schwertfisch	Östlicher Pazifik	hoch	
Makaira nigricans (oder Mazara)	Atlantischer Blauer Marlin	Östlicher Pazifik	hoch	
Makaira indica	Schwarzer Marlin	Östlicher Pazifik	hoch	
Tetrapturus audax	Gestreifter Marlin	Östlicher Pazifik	hoch	

ICCAT (Internationale Kommission für die Erhaltung der Thunfischbestände im Atlantik)

ARTEN Bei der Ausarbeitung der Stichprobenpläne für die Erhebung von biologischen Informationen gemäß Kapitel III dieses Anhangs sind die von den zuständigen regionalen Fischereiorganisationen festgesetzten Bestandsgrenzen zu berücksichtigen und geeignete Beprobungsmaßnahmen für jeden Bestand festzulegen.				Häufigkeit der Erhebung biologischer Variablen
Wissenschaftliche Bezeichnung	Gebräuchliche Bezeichnung	Geografisches Gebiet	Priorität	
Thunnus albacares	Gelbflossenthun	Atlantik und angrenzende Meere	hoch	Die Datenerhebung erfolgt jährlich, und die Aktualisierung/Verarbeitung der Daten muss zeitnah erfolgen, um in den Zeitplan für die Bestandsabschätzung zu passen.
Thunnus obesus	Großaugenthun	Atlantik und angrenzende Meere	hoch	
Katsuwonus pelamis	Echter Bonito	Atlantik und angrenzende Meere	hoch	
Thunnus alalunga	Weißer Thun	Atlantik und angrenzende Meere	hoch	

ARTEN Bei der Ausarbeitung der Stichprobenpläne für die Erhebung von biologischen Informationen gemäß Kapitel III dieses Anhangs sind die von den zuständigen regionalen Fischereiorganisationen festgesetzten Bestandsgrenzen zu berücksichtigen und geeignete Beprobungsmaßnahmen für jeden Bestand festzulegen.				Häufigkeit der Erhebung biologischer Variablen
Thunnus thynnus	Roter Thun	Atlantik und angrenzende Meere	hoch	
Xiphias gladius	Schwertfisch	Atlantik und angrenzende Meere	hoch	
Makaira nigricans (oder Mazara)	Blauer Marlin	Atlantik und angrenzende Meere	hoch	
Istiophorus albicans	Segelfisch	Atlantik und angrenzende Meere	hoch	
Tetrapturus albidus	Weißer Marlin	Atlantik und angrenzende Meere	hoch	
Prionace glauca	Blauhai	Atlantik und angrenzende Meere	hoch	
Auxis rochei	Unechter Bonito	Atlantik und angrenzende Meere	hoch	
Sarda sarda	Pelamide	Atlantik und angrenzende Meere	hoch	
Euthynnus alleteratus	Falscher Bonito	Atlantik und angrenzende Meere	mittel	
Thunnus atlanticus	Schwarzflossenthun	Atlantik und angrenzende Meere	mittel	
Orcynopsis unicolor	Ungestreifte Pelamide	Atlantik und angrenzende Meere	mittel	
Scomberomorus brasiliensis	Serra-Makrele	Atlantik und angrenzende Meere	mittel	
Scomberomorus regalis	Falsche Königsmakrele	Atlantik und angrenzende Meere	mittel	
Auxis thazard	Fregattmakrele	Atlantik und angrenzende Meere	mittel	
Scomberomorus cavalla	Ostatlantische Königsmakrele	Atlantik und angrenzende Meere	mittel	
Scomberomorus tritor	Ostatlantische Königsmakrele	Atlantik und angrenzende Meere	mittel	
Scomberomorus maculatus	Gefleckte Königsmakrele	Atlantik und angrenzende Meere	mittel	

ARTEN Bei der Ausarbeitung der Stichprobenpläne für die Erhebung von biologischen Informationen gemäß Kapitel III dieses Anhangs sind die von den zuständigen regionalen Fischereiorganisationen festgesetzten Bestandsgrenzen zu berücksichtigen und geeignete Beprobungsmaßnahmen für jeden Bestand festzulegen.				Häufigkeit der Erhebung biologischer Variablen
Acanthocybium solandri	Indische Königsmakrele	Atlantik und angrenzende Meere	mittel	
Coryphaena hippurus	Goldmakrele	Atlantik und angrenzende Meere	mittel	

NAFO (Organisation für die Fischerei im Nordwestatlantik)

ARTEN Bei der Ausarbeitung der Stichprobenpläne für die Erhebung von biologischen Informationen gemäß Kapitel III dieses Anhangs sind die von den zuständigen regionalen Fischereiorganisationen festgesetzten Bestandsgrenzen zu berücksichtigen und geeignete Beprobungsmaßnahmen für jeden Bestand festzulegen.				Häufigkeit der Erhebung biologischer Variablen
Wissenschaftliche Bezeichnung	Gebräuchliche Bezeichnung	Bestände gemäß der Definition der RFO	Priorität	
Gadus morhua	Kabeljau	NAFO 2J 3KL	niedrig	
Gadus morhua	Kabeljau	NAFO 3M	hoch	
Gadus morhua	Kabeljau	NAFO 3NO	hoch	
Gadus morhua	Kabeljau	NAFO 3Ps	hoch	
Gadus morhua	Kabeljau	NAFO SA1	hoch	
Glyptocephalus cynoglossus	Rotzunge	NAFO 3NO	hoch	
Glyptocephalus cynoglossus	Rotzunge	NAFO 2J3KL	niedrig	
Hippoglossoides platessoides	Raue Scharbe	NAFO 3LNO	hoch	
Hippoglossoides platessoides	Raue Scharbe	NAFO 3M	hoch	
Limanda ferruginea	Gelbschwanzflunder	NAFO 3LNO	mittel	
Coryphaenoides rupestris	Rundnasen-Grenadier	NAFO SA0 + 1	niedrig	
Macrourus berglax	Nordatlantik-Grenadier	NAFO SA2 + 3	hoch	
Pandalus borealis	Tiefseegarnele	NAFO 3LNO	hoch	
Pandalus borealis	Tiefseegarnele	NAFO 3M	hoch	
Amblyraja radiata	Atlantischer Sternrochen	NAFO 3LNOPs	hoch	
Reinhardtius hippoglossoides	Schwarzer Heilbutt	NAFO 3KLMNO	hoch	

Die Datenerhebung erfolgt jährlich, und die Aktualisierung/Verarbeitung der Daten muss zeitnah erfolgen, um in den Zeitplan für die Bestandsabschätzung zu passen.

ARTEN Bei der Ausarbeitung der Stichprobenpläne für die Erhebung von biologischen Informationen gemäß Kapitel III dieses Anhangs sind die von den zuständigen regionalen Fischereiorganisationen festgesetzten Bestandsgrenzen zu berücksichtigen und geeignete Beprobungsmaßnahmen für jeden Bestand festzulegen.				Häufigkeit der Erhebung biologischer Variablen
Reinhardtius hippoglossoides	Schwarzer Heilbutt	NAFO SA1	hoch	
Hippoglossus hippoglossus	Atlantischer Heilbutt	NAFO SA1	niedrig	
Sebastes mentella	Rotbarsch	NAFO SA1	hoch	
Sebastes spp.	Rotbarsch	NAFO 3LN	hoch	
Sebastes spp.	Rotbarsch	NAFO 3M	hoch	
Sebastes spp.	Rotbarsch	NAFO 3O	hoch	
Urophycis tenuis	Weißer Gabeldorsch	NAFO 3NO	hoch	
Mallotus villosus	Lodde	NAFO 3NO	hoch	
Beryx sp.	Kaiserbarsch	NAFO 6G	hoch	
Illex illecebrosus	Nördlicher Kurzflossen-Kalmar	NAFO-Untergebiete 3 + 4	niedrig	
Salmo salar	Lachs	NAFO S1 + ICES-Untergebiet XIV, NEAF, NASCO	hoch	

FAO Meeresgebiet 34 — Fischereiausschuss für den östlichen Mittelatlantik (CECAF)

ARTEN Bei der Ausarbeitung der Stichprobenpläne für die Erhebung von biologischen Informationen gemäß Kapitel III dieses Anhangs sind die von den zuständigen regionalen Fischereiorganisationen festgesetzten Bestandsgrenzen zu berücksichtigen und geeignete Beprobungsmaßnahmen für jeden Bestand festzulegen.				Häufigkeit der Erhebung biologischer Variablen
Wissenschaftliche Bezeichnung	Gebräuchliche Bezeichnung	Geografisches Gebiet	Priorität	
Brachydeuterus spp.	Süßlippe	34.1.3., 34.3.1., 34.3.3-6.	hoch	
Caranx spp.	Barsch	34.3.1., 34.3.3-6.	hoch	
Cynoglossus spp.	Handszunge	34.1.1., 34.1.3., 34.3.1., 34.3.3-6.	hoch	Die Datenerhebung erfolgt jährlich, und die Aktualisierung/Verarbeitung der Daten muss zeitnah erfolgen, um in den Zeitplan für die Bestandsabschätzung zu passen.
Decapterus spp.	Stöcker	34.3.1., 34.3.3-6.	hoch	
Dentex canariensis	Kanarische Zahnbrasse	34.1.1., 34.1.3., 34.3.1., 34.3.3-6.	mittel	
Dentex congoensis	Kongo-Zahnbrasse	34.1.1., 34.1.3., 34.3.1., 34.3.3-6.	mittel	
Dentex macrophthalmus	Angola-Zahnbrasse	34.1.1., 34.1.3., 34.3.1., 34.3.3-6.	hoch	

ARTEN Bei der Ausarbeitung der Stichprobenpläne für die Erhebung von biologischen Informationen gemäß Kapitel III dieses Anhangs sind die von den zuständigen regionalen Fischereiorganisationen festgesetzten Bestandsgrenzen zu berücksichtigen und geeignete Beprobungsmaßnahmen für jeden Bestand festzulegen.				Häufigkeit der Erhebung biologischer Variablen
Dentex maroccanus	Marokko-Zahnbrasse	34.1.1., 34.1.3., 34.3.1., 34.3.3-6.	mittel	
Dentex spp.	Zahnbrasse	34.1.1., 34.1.3., 34.3.1., 34.3.3-6.	hoch	
Engraulis encrasicolus	Sardelle	34.1.1., 34.1.3., 34.3.1., 34.3.3-6.	hoch	
Epinephelus aeneus	Weißer Zackenbarsch	34.1.3., 34.3.1., 34.3.3-6.	hoch	
Ethmalosa fimbriata	Bonga-Hering	34.3.1., 34.3.3-6.	hoch	
Farfantepenaeus notialis	Südliche Rosa Geißelgarnele	34.1.1., 34.1.3., 34.3.1., 34.3.3-6.	hoch	
Galeoides decadactylus	Pelagische Barschartige	34.1.3., 34.3.1., 34.3.3-6.	hoch	Die Datenerhebung erfolgt jährlich, und die Aktualisierung/Verarbeitung der Daten muss zeitnah erfolgen, um in den Zeitplan für die Bestandsabschätzung zu passen.
Loligo vulgaris	Kalmar	34.1.1., 34.1.3., 34.3.1., 34.3.3-6.	hoch	
Merluccius polli	Benguela Seehecht	34.1.1., 34.1.3., 34.3.1., 34.3.3-6.	hoch	
Merluccius senegalensis	Senegalesischer Seehecht	34.1.1., 34.1.3., 34.3.1., 34.3.3-6.	hoch	
Merluccius spp.	Andere Seehechte	34.1.1., 34.1.3., 34.3.1., 34.3.3-6.	mittel	
Octopus vulgaris	Gewöhnlicher Krake	34.1.1., 34.1.3., 34.3.1., 34.3.3-6.	hoch	
Pagellus acarne	Achselfleckbrasse	34.1.1.	hoch	
Pagellus bellottii	Rote Pandora	34.1.1., 34.1.3., 34.3.1., 34.3.3-6.	hoch	
Pagellus bogaraveo	Rote Fleckenbrasse	34.1.1.	mittel	
Pagellus spp.	Rotbrasse	34.1.1., 34.1.3., 34.3.1., 34.3.3-6.	hoch	
Pagrus caeruleostictus	Pagrus caeruleostictus	34.1.1., 34.1.3., 34.3.1., 34.3.3-6.	hoch	
Parapenaeus longirostris	Rosa Geißelgarnele	34.1.1., 34.1.3., 34.3.1., 34.3.3-6.	hoch	
Pomadasys incisus	Bastard-Süßlippe	34.1.1.	mittel	
Pomadasys spp.	Süßlippe	34.1.1., 34.1.3., 34.3.1., 34.3.3-6.	hoch	

ARTEN Bei der Ausarbeitung der Stichprobenpläne für die Erhebung von biologischen Informationen gemäß Kapitel III dieses Anhangs sind die von den zuständigen regionalen Fischereiorganisationen festgesetzten Bestandsgrenzen zu berücksichtigen und geeignete Beprobungsmaßnahmen für jeden Bestand festzulegen.				Häufigkeit der Erhebung biologischer Variablen
Pseudotolithus spp.	Umberfische	34.1.1.	hoch	
Sardina pilchardus	Sardine	34.1.1., 34.1.3.	hoch	
Sardinella aurita	Ohrensardine	34.1.1., 34.1.3., 34.3.1., 34.3.3-6.	hoch	
Sardinella maderensis	Madeira-Sardinelle	34.1.1., 34.1.3., 34.3.1., 34.3.3-6.	hoch	Die Datenerhebung erfolgt jährlich, und die Aktualisierung/Verarbeitung der Daten muss zeitnah erfolgen, um in den Zeitplan für die Bestandsabschätzung zu passen.
Scomber japonicus	Spanische Makrele	34.1.1., 34.1.3., 34.3.1., 34.3.3-6.	hoch	
Scomber spp.	Andere Makrelen	34.1.1., 34.1.3., 34.3.1., 34.3.3-6.	hoch	
Sepia hierredda	Tintenfische	34.1.1., 34.1.3., 34.3.1., 34.3.3-6.	hoch	
Sepia officinalis	Gemeiner Tintenfisch	34.1.1., 34.1.3., 34.3.1., 34.3.3-6.	hoch	
Sepia spp.	Tintenfische	34.1.1., 34.1.3., 34.3.1., 34.3.3-6.	mittel	
Sparidae	Meerbrasse	34.1.1., 34.1.3., 34.3.1., 34.3.3-6.	hoch	
Sparus spp.	Meerbrasse	34.1.1.	hoch	
Trachurus trachurus	Stöcker	34.1.1., 34.1.3., 34.3.1., 34.3.3-6.	hoch	
Trachurus trecae	Cunene-Bastardmakrele	34.1.1., 34.1.3., 34.3.1., 34.3.3-6.	hoch	
Umbrina canariensis	Umberfische	34.3.3-6.	mittel	

SEAFO (Organisation für die Fischerei im Südostatlantik)

ARTEN Bei der Ausarbeitung der Stichprobenpläne für die Erhebung von biologischen Informationen gemäß Kapitel III dieses Anhangs sind die von den zuständigen regionalen Fischereiorganisationen festgesetzten Bestandsgrenzen zu berücksichtigen und geeignete Beprobungsmaßnahmen für jeden Bestand festzulegen.				Häufigkeit der Erhebung biologischer Variablen
Wissenschaftliche Bezeichnung	Gebräuchliche Bezeichnung	Geografisches Gebiet	Priorität	Die Datenerhebung erfolgt jährlich, und die Aktualisierung/Verarbeitung der Daten muss zeitnah erfolgen, um in den Zeitplan für die Bestandsabschätzung zu passen.
Dissostichus eleginoides	Schwarzer Seehecht	Südostatlantik	*hoch*	
Beryx spp.	Kaiserbarsch	Südostatlantik	*hoch*	

ARTEN Bei der Ausarbeitung der Stichprobenpläne für die Erhebung von biologischen Informationen gemäß Kapitel III dieses Anhangs sind die von den zuständigen regionalen Fischereiorganisationen festgesetzten Bestandsgrenzen zu berücksichtigen und geeignete Beprobungsmaßnahmen für jeden Bestand festzulegen.				Häufigkeit der Erhebung biologischer Variablen
Chaceon spp.	Rot/Goldkabben	Südostatlantik	*hoch*	
Pseudopentaceros richardsoni	Pseudopentaceros spp.	Südostatlantik	*hoch*	
Helicolenus spp.	Blaumaul	Südostatlantik	*hoch*	
Hoplostethus atlanticus	Granatbarsch	Südostatlantik	*hoch*	
Trachurus spp.	Bastardmakrele	Südostatlantik	*hoch*	
Scomber spp.	Makrele	Südostatlantik	*hoch*	
Polyprion americanus	Wrackbarsch	Südostatlantik	*mittel*	
Jasus tristani	Tristans Languste	Südostatlantik	*mittel*	
Lepidopus caudatus	Degenfisch	Südostatlantik	*mittel*	
Schedophilus ovalis	Schedophilus ovalis	Südostatlantik	*niedrig*	
Schedophilus velaini	Schedophilus velaini	Südostatlantik	*niedrig*	
Allocyttus verucossus	Oreos	Südostatlantik	*niedrig*	
Neocyttus romboidales		Südostatlantik		
Allocyttus guineensis		Südostatlantik		
Smaculatus pseudocyttu		Südostatlantik		
Emmelichthys nitidus	Emmelichthys nitidus	Südostatlantik	*niedrig*	
Ruvettus pretiosus	Ölfisch	Südostatlantik	*niedrig*	
Prometheus promethichthys	Silber-Escolar	Südostatlantik	*niedrig*	
Macrourus spp.	Grenadierfische	Südostatlantik	*niedrig*	
Antimora rostrata	Blauhecht	Südostatlantik	*niedrig*	
Epigonus spp.	Kardinalfisch	Südostatlantik	*niedrig*	
Merluccius spp.	Seehecht	Südostatlantik	*niedrig*	

ARTEN Bei der Ausarbeitung der Stichprobenpläne für die Erhebung von biologischen Informationen gemäß Kapitel III dieses Anhangs sind die von den zuständigen regionalen Fischereiorganisationen festgesetzten Bestandsgrenzen zu berücksichtigen und geeignete Beprobungsmaßnahmen für jeden Bestand festzulegen.				Häufigkeit der Erhebung biologischer Variablen
Notopogon fernandezianus	Notopogon fernandezianus	Südostatlantik	*niedrig*	
Octopodidae und Loliginidae	Tintenfische und Kalmare	Südostatlantik	*niedrig*	

WCPFC (Fischereikommission für den westlichen und mittleren Pazifik)

ARTEN Bei der Ausarbeitung der Stichprobenpläne für die Erhebung von biologischen Informationen gemäß Kapitel III dieses Anhangs sind die von den zuständigen regionalen Fischereiorganisationen festgesetzten Bestandsgrenzen zu berücksichtigen und geeignete Beprobungsmaßnahmen für jeden Bestand festzulegen.				Häufigkeit der Erhebung biologischer Variablen
Wissenschaftliche Bezeichnung	Gebräuchliche Bezeichnung	Geografisches Gebiet	Priorität	
Thunnus albacares	Gelbflossenthun	Westlicher und mittlerer Pazifik	hoch	
Thunnus obesus	Großaugenthun	Westlicher und mittlerer Pazifik	hoch	
Katsuwonus pelamis	Echter Bonito	Westlicher und mittlerer Pazifik	hoch	
Thunnus alalunga	Weißer Thun	Westlicher und mittlerer Pazifik	hoch	
Thunnus orientalis	Nordpazifischer Blauflossenthun	Westlicher und mittlerer Pazifik	hoch	
Xiphias gladius	Schwertfisch	Westlicher und mittlerer Pazifik	hoch	Die Datenerhebung erfolgt jährlich, und die Aktualisierung/Verarbeitung der Daten muss zeitnah erfolgen, um in den Zeitplan für die Bestandsabschätzung zu passen.
Makaira nigricans (oder Mazara)	Blauer Marlin	Westlicher und mittlerer Pazifik	hoch	
Makaira indica	Schwarzer Marlin	Westlicher und mittlerer Pazifik	hoch	
Tetrapturus audax	Gestreifter Marlin	Westlicher und mittlerer Pazifik	hoch	
Acanthocybium solandri	Indische Königsmakrele	Westlicher und mittlerer Pazifik	mittel	
Coryphaena hippurus	Goldmakrele	Westlicher und mittlerer Pazifik	mittel	
Elagatis bipinnulata	Regenbogen-Stachelmakrele	Westlicher und mittlerer Pazifik	mittel	
Lepidocybium flavobrunneum	Escolar	Westlicher und mittlerer Pazifik	mittel	
Lampris regius	Fleckenmondfisch	Westlicher und mittlerer Pazifik	mittel	

ARTEN Bei der Ausarbeitung der Stichprobenpläne für die Erhebung von biologischen Informationen gemäß Kapitel III dieses Anhangs sind die von den zuständigen regionalen Fischereiorganisationen festgesetzten Bestandsgrenzen zu berücksichtigen und geeignete Beprobungsmaßnahmen für jeden Bestand festzulegen.				Häufigkeit der Erhebung biologischer Variablen
Mola mola	Mondfisch	Westlicher und mittlerer Pazifik	mittel	
Istiophorus platypterus	Segelfisch	Westlicher und mittlerer Pazifik	mittel	
Tetrapturus angustirostris	Speerfisch	Westlicher und mittlerer Pazifik	mittel	
Ruvettus pretiosus	Ölfisch	Westlicher und mittlerer Pazifik	mittel	
Prionace glauca	Blauhai	Westlicher und mittlerer Pazifik	hoch	
Carcharhinus longimanus	Weißspitzen-Hochseehai	Westlicher und mittlerer Pazifik	hoch	
Carcharhinus falciformis	Seidenhai	Westlicher und mittlerer Pazifik	hoch	
Alopias superciliosus	Drescher	Westlicher und mittlerer Pazifik	hoch	
Alopias vulpinus	Gemeiner Drescher	Westlicher und mittlerer Pazifik	hoch	
Alopias pelagicus	Pelagischer Drescher	Westlicher und mittlerer Pazifik	hoch	

NB: Für die WCPF werden folgende Meldepflichten für Langleiner angefügt:

1. Anzahl der Mundschnüre zwischen den Schwimmern: Die Anzahl der Mundschnüre zwischen den Schwimmern wird für jeden Hol gemeldet.
2. Anzahl der gefangenen Fische je Hol für die folgenden Arten: Weißer Thun (*Thunnus alalunga*), Großaugenthun (*Thunnus obesus*), Echter Bonito (*Katsuwonus pelamis*), Gelbflossen-Thun (*Thunnus albacares*), Gestreifter Marlin (*Tetrapturus audax*), Blauer Marlin (*Makaira mazara*), Schwarzer Marlin (*Makaira indica*) und Schwertfisch (*Xiphias gladius*), Blauhai, Seidenhai, Weißspitzen-Hochseehai, Makrelenhai, Fuchshai, Heringshai (südlich von 20°S, bis biologische Daten zeigen, dass diese oder eine andere geografische Grenze angemessen ist), Hammerhaie (Flügelkopf-Hammerhai, Bogenstirn-Hammerhai, Großer Hammerhai und Glatter Hammerhai), Walhai, und andere Arten, wie von der Kommission festgelegt.

Wenn das Gesamtgewicht oder Durchschnittsgewicht der gefangenen Fische je Hol erfasst wurde, wird auch das Gesamtgewicht oder Durchschnittsgewicht der gefangenen Fische je Hol nach Arten gemeldet. Wenn das Gesamtgewicht oder Durchschnittsgewicht der gefangenen Fische je Hol nicht erfasst wurde, wird das Gesamtgewicht oder Durchschnittsgewicht der gefangenen Fische je Hol nach Arten geschätzt und die Schätzungen werden gemeldet. Das Gesamtgewicht oder Durchschnittsgewicht bezieht sich auf ganze und nicht auf verarbeitete Mengen.

WECAFC (Fischereikommission für den westlichen Mittelatlantik)

ARTEN Bei der Ausarbeitung der Stichprobenpläne für die Erhebung von biologischen Informationen gemäß Kapitel III dieses Anhangs sind die von den zuständigen regionalen Fischereiorganisationen festgesetzten Bestandsgrenzen zu berücksichtigen und geeignete Beprobungsmaßnahmen für jeden Bestand festzulegen.				Häufigkeit der Erhebung biologischer Variablen
Wissenschaftliche Bezeichnung	Gebräuchliche Bezeichnung	Geografisches Gebiet	Priorität	Die Datenerhebung erfolgt jährlich, und die Aktualisierung/Verarbeitung der Daten muss zeitnah erfolgen, um in den Zeitplan für die Bestandsabschätzung zu passen.
Panulirus argus	Karibik-Languste	Westlicher Mittelatlantik	hoch	
Strombus gigas	Riesen-Flügelschnecke	Westlicher Mittelatlantik	hoch	

ARTEN Bei der Ausarbeitung der Stichprobenpläne für die Erhebung von biologischen Informationen gemäß Kapitel III dieses Anhangs sind die von den zuständigen regionalen Fischereiorganisationen festgesetzten Bestandsgrenzen zu berücksichtigen und geeignete Beprobungsmaßnahmen für jeden Bestand festzulegen.				Häufigkeit der Erhebung biologischer Variablen
Haiähnliche Selachii, Rajidae	Haie und Rochen	Westlicher Mittelatlantik	hoch	
Coryphaena hippurus	Goldmakrele	Westlicher Mittelatlantik	hoch	
Acanthocybium solandri	Indische Königsmakrele	Westlicher Mittelatlantik	hoch	
Epinephelus guttatus	Roter Zackenbarsch	Westlicher Mittelatlantik	hoch	
Lutjanus vivanus	Seidenschnapper	Westlicher Mittelatlantik	hoch	
Lutjanus buccanella	Schwarzflossenschnapper	Westlicher Mittelatlantik	hoch	
Lutjanus campechanus	Südlicher Schnapper	Westlicher Mittelatlantik	hoch	
Penaeus subtilis	Geißelgarnele	AWZ Französisch-Guayana	hoch	

IOTC (Thunfischkommission für den Indischen Ozean)

ARTEN Bei der Ausarbeitung der Stichprobenpläne für die Erhebung von biologischen Informationen gemäß Kapitel III dieses Anhangs sind die von den zuständigen regionalen Fischereiorganisationen festgesetzten Bestandsgrenzen zu berücksichtigen und geeignete Beprobungsmaßnahmen für jeden Bestand festzulegen.				Häufigkeit der Erhebung biologischer Variablen
Wissenschaftliche Bezeichnung	Gebräuchliche Bezeichnung	Geografisches Gebiet	Priorität	
Thunnus albacares	Gelbflossenthun	Westlicher und östlicher Indischer Ozean	hoch	
Thunnus obesus	Großaugenthun	Westlicher und östlicher Indischer Ozean	hoch	
Katsuwonus pelamis	Echter Bonito	Westlicher und östlicher Indischer Ozean	hoch	
Thunnus alalunga	Weißer Thun	Westlicher und östlicher Indischer Ozean	hoch	
Xiphias gladius	Schwertfisch	Westlicher und östlicher Indischer Ozean	hoch	
Makaira nigricans (oder Mazara)	Blauer Marlin	Westlicher und östlicher Indischer Ozean	hoch	
Makaira indica	Schwarzer Marlin	Westlicher und östlicher Indischer Ozean	hoch	
Tetrapturus audax	Gestreifter Marlin	Westlicher und östlicher Indischer Ozean	hoch	
Istiophorus platypterus	Fächerfisch	Westlicher und östlicher Indischer Ozean	hoch	

Die Datenerhebung erfolgt jährlich, und die Aktualisierung/Verarbeitung der Daten muss zeitnah erfolgen, um in den Zeitplan für die Bestandsabschätzung zu passen.

ARTEN Bei der Ausarbeitung der Stichprobenpläne für die Erhebung von biologischen Informationen gemäß Kapitel III dieses Anhangs sind die von den zuständigen regionalen Fischereiorganisationen festgesetzten Bestandsgrenzen zu berücksichtigen und geeignete Beprobungsmaßnahmen für jeden Bestand festzulegen.				Häufigkeit der Erhebung biologischer Variablen
Auxis rochei	Unechter Bonito	Westlicher und östlicher Indischer Ozean	mittel	
Auxis thazard	Fregattmakrele	Westlicher und östlicher Indischer Ozean	mittel	
Euthynnus affinis	Euthynnus affinis	Westlicher und östlicher Indischer Ozean	mittel	
Thunnus tonggol	Langschwanz-Thun	Westlicher und östlicher Indischer Ozean	mittel	
Scomberomorus guttatus	Indopazifische Königsmakrele	Westlicher und östlicher Indischer Ozean	mittel	
Scomberomorus commerson	Indische Königsmakrele	Westlicher und östlicher Indischer Ozean	mittel	
Prionace glauca	Blauhai	Westlicher und östlicher Indischer Ozean	hoch	
Alopias superciliosus	Großäugiger Fuchshai	Westlicher und östlicher Indischer Ozean	hoch	
Carcharhinus falciformis	Seidenhai	Westlicher und östlicher Indischer Ozean	hoch	
Carcharhinus longimanus	Weißspitzen-Hochseehai	Westlicher und östlicher Indischer Ozean	hoch	
Alopias pelagicus	Pazifischer Fuchshai	Westlicher und östlicher Indischer Ozean	hoch	
Sphyrna lewini	Bogenstirn-Hammerhai	Westlicher und östlicher Indischer Ozean	hoch	

Andere regionale Fischereiorganisationen (RFO)

ARTEN Bei der Ausarbeitung der Stichprobenpläne für die Erhebung von biologischen Informationen gemäß Kapitel III dieses Anhangs sind die von den zuständigen regionalen Fischereiorganisationen festgesetzten Bestandsgrenzen zu berücksichtigen und geeignete Beprobungsmaßnahmen für jeden Bestand festzulegen.				Häufigkeit der Erhebung biologischer Variablen
Wissenschaftliche Bezeichnung	Gebräuchliche Bezeichnung	Geografisches Gebiet	Priorität	Die Datenerhebung erfolgt jährlich, und die Aktualisierung/Verarbeitung der Daten muss zeitnah erfolgen, um in den Zeitplan für die Bestandsabschätzung zu passen.
Trachurus murphyi	Bastardmakrele	SPRFMO-Übereinkommensbereich	hoch	
Euphausia superba	Krill	CCAMLR-Übereinkommensbereich	hoch	

ARTEN Bei der Ausarbeitung der Stichprobenpläne für die Erhebung von biologischen Informationen gemäß Kapitel III dieses Anhangs sind die von den zuständigen regionalen Fischereiorganisationen festgesetzten Bestandsgrenzen zu berücksichtigen und geeignete Beprobungsmaßnahmen für jeden Bestand festzulegen.				Häufigkeit der Erhebung biologischer Variablen
Dissostichus spp. Dissostichus eleginoides und Dissostichus mawsoni	Zahnfische	CCAMLR-Übereinkommensbereich	hoch	
Champsocephalus gunnari	Bändereisfisch	CCAMLR-Übereinkommensbereich	niedrig	
Bestände an Fisch, Weichtieren, Krebstieren und anderen ortsgebundenen Arten im Zuständigkeitsbereich, mit Ausnahme von i) unter die Fischereigerichtsbarkeit der Küstenstaaten fallenden ortsgebundenen Arten gemäß Artikel 77 Absatz 4 des Seerechtsübereinkommens der Vereinten Nationen von 1982 und ii) weit wandernden Arten gemäß Anhang I des Seerechtsübereinkommens der Vereinten Nationen von 1982.		SIOFA-Übereinkommensbereich		

BIOLOGISCHE DATEN

Tabelle 1D

Im Rahmen von Schutzprogrammen in der Union oder von internationalen Verpflichtungen zu überwachende Arten

Gebräuchliche Bezeichnung	Wissenschaftliche Bezeichnung	Region/RFO	Rechtsrahmen
Knochenfische	Teleostei		
Störe	*Acipenser* spp.	Mittelmeer und Schwarzes Meer; Ostsee; OSPAR II, IV	Anhang II des Übereinkommens von Barcelona ([1]), Anhang IV des Protokolls über die Erhaltung der biologischen Vielfalt und Landschaft des Schwarzen Meeres; OSPAR ([2]); HELCOM ([3])
Glattköpfe	*Alepocephalidae*	Alle Regionen	Für die Tiefseefischerei relevant ([4])
Bairds Glattkopf	*Alepocephalus bairdii*	Alle Regionen	Für die Tiefseefischerei relevant
Rissos Glattkopf	*Alepocephalus rostratus*	Alle Regionen	Für die Tiefseefischerei relevant
Donauhering	*Alosa immaculata*	Schwarzes Meer	Anhang IV des Protokolls über die Erhaltung der biologischen Vielfalt und Landschaft des Schwarzen Meeres
Maifisch	*Alosa alosa*	OSPAR II, III, IV	OSPAR
Ostseeschnäpel	*Coregonus lavaretus*	OSPAR II	OSPAR
Kabeljau	*Gadus morhua*	OSPAR II, III; Ostsee	OSPAR; HELCOM

Gebräuchliche Bezeichnung	Wissenschaftliche Bezeichnung	Region/RFO	Rechtsrahmen
Langschnäuziges Seepferdchen	*Hippocampus guttulatus* (Synonym: *Hippocampus ramulosus*)	OSPAR II, III, IV, V	OSPAR
Kurzschnäuziges Seepferdchen	*Hippocampus hippocampus*	OSPAR II, III, IV, V	OSPAR
Kerchen-Maifisch	*Alosa tanaica*	Schwarzes Meer	Anhang IV des Protokolls über die Erhaltung der biologischen Vielfalt und Landschaft des Schwarzen Meeres
Blauhecht	*Antimora rostrata*	Alle Regionen	Für die Tiefseefischerei relevant
Schwarzer Degenfisch	*Aphanopus carbo*	Alle Regionen	Für die Tiefseefischerei relevant
Degenfisch	*Aphanopus intermedius*	Alle Regionen	Für die Tiefseefischerei relevant
Flusskrebse	*Astacus* spp.	Schwarzes Meer	Anhang IV des Protokolls über die Erhaltung der biologischen Vielfalt und Landschaft des Schwarzen Meeres
Kleiner Ährenfisch	*Atherina Pontica*	Schwarzes Meer	Anhang IV des Protokolls über die Erhaltung der biologischen Vielfalt und Landschaft des Schwarzen Meeres
Hornhecht	*Belone belone euxini Günther*	Schwarzes Meer	Anhang IV des Protokolls über die Erhaltung der biologischen Vielfalt und Landschaft des Schwarzen Meeres
Kaiserbarsch	*Beryx* spp.	Alle Regionen	Für die Tiefseefischerei relevant
Brotula	*Cataetyx laticeps*	Alle Regionen	Für die Tiefseefischerei relevant
Kleine Maräne	*Coregonus albula*	Ostsee	Empfehlung der regionalen Koordinierungssitzung für die Ostsee
Seehase	*Cyclopterus lumpus*	Alle Regionen	Für die Tiefseefischerei relevant
Ringelbrasse	*Diplodus annularis*	Mittelmeer	Verordnung (EG) Nr. 1967/2006 des Rates [5] (Mindestgröße für die Bestandserhaltung)
Spitzbrasse	*Diplodus puntazzo*	Mittelmeer	Verordnung (EG) Nr. 1967/2006 (Mindestgröße für die Bestandserhaltung)
Große Geißbrasse	*Diplodus sargus*	Mittelmeer	Verordnung (EG) Nr. 1967/2006 (Mindestgröße für die Bestandserhaltung)
Zweibindenbrasse	*Diplodus vulgaris*	Mittelmeer	Verordnung (EG) Nr. 1967/2006 (Mindestgröße für die Bestandserhaltung)
Schwarzer Seehecht	*Dissostichus eleginoides*	Alle Regionen	Für die Tiefseefischerei relevant
Antarktischer Seehecht	*Dissostichus mawsoni*	Alle Regionen	Für die Tiefseefischerei relevant

Gebräuchliche Bezeichnung	Wissenschaftliche Bezeichnung	Region/RFO	Rechtsrahmen
Zackenbarsche	*Epinephelus* spp.	Mittelmeer	Verordnung (EG) Nr. 1967/2006 (Mindestgröße für die Bestandserhaltung)
Teleskop-Kardinalfisch	*Epigonus telescopus*	Alle Regionen	Gefährdete Art; für die Tiefseefischerei relevant
Grundeln	*Gobiidae*	Schwarzes Meer	Anhang IV des Protokolls über die Erhaltung der biologischen Vielfalt und Landschaft des Schwarzen Meeres
Blaumaul	*Helicolenus dactylopterus*	Alle Regionen	Für die Tiefseefischerei relevant
Atlantischer Heilbutt	*Hippoglossus hippoglossus*	Alle Regionen	Für die Tiefseefischerei relevant
Granatbarsch	*Hoplostethus atlanticus*	Alle Regionen OSPAR I, V	Gefährdete Art; für die Tiefseefischerei relevant
Mittelmeer-Kaiserbarsch	*Hoplosthetus mediterraneus*	Alle Regionen	Für die Tiefseefischerei relevant
Degenfisch	*Lepidopus caudatus*	Alle Regionen	Für die Tiefseefischerei relevant
Marmorbrassen	*Lithognathus mormyrus*	Mittelmeer	Verordnung (EG) Nr. 1967/2006 (Mindestgröße für die Bestandserhaltung)
Goldmeeräsche	*Liza aurata*	Schwarzes Meer	Anhang IV des Protokolls über die Erhaltung der biologischen Vielfalt und Landschaft des Schwarzen Meeres
Springmeeräsche	*Liza saliens*	Schwarzes Meer	Anhang IV des Protokolls über die Erhaltung der biologischen Vielfalt und Landschaft des Schwarzen Meeres
Wolfsfisch	*Lycodes esmarkii*	Alle Regionen	Für die Tiefseefischerei relevant
Grenadierfische (Rattenschwänze), andere als Rundnasen-Grenadier und Nordatlantik-Grenadier	Macrouridae andere als Coryphaenoides rupestris und Macrourus berglax	Alle Regionen	Für die Tiefseefischerei relevant
Nordatlantik-Grenadier	*Macrourus berglax*	Alle Regionen	Für die Tiefseefischerei relevant
Wittling	*Merlangius merlangus*	Mittelmeer und Schwarzes Meer	Empfehlung der regionalen Koordinierungssitzung für die Ostsee; Anhang IV des Protokolls über die Erhaltung der biologischen Vielfalt und Landschaft des Schwarzen Meeres
Europäischer Aal	*Anguilla anguilla*	OSPAR I, II, III, IV, Ostsee	OSPAR; HELCOM
Atlantischer Lachs	*Salmo salar	OSPAR I, II, III, IV, Ostsee	OSPAR; HELCOM
Roter Thun	*Thunnus thynnus	OSPAR V	OSPAR; HELCOM

Gebräuchliche Bezeichnung	Wissenschaftliche Bezeichnung	Region/RFO	Rechtsrahmen
Blauleng	*Molva dypterygia*	Alle Regionen	Für die Tiefseefischerei relevant
Tiefseedorsch	*Mora moro*	Alle Regionen	Für die Tiefseefischerei relevant
Meeräsche	*Mugil* spp.	Schwarzes Meer	Anhang IV des Protokolls über die Erhaltung der biologischen Vielfalt und Landschaft des Schwarzen Meeres
Schwarzer Hechtkopf	*Nesiarchus nasutus*	Alle Regionen	Für die Tiefseefischerei relevant
Dornrückenaal	*Notocanthus chemnitzii*	Alle Regionen	Für die Tiefseefischerei relevant
Stint	*Osmerus eperlanus*	Ostsee	Empfehlung der regionalen Koordinierungssitzung für die Ostsee, HELCOM
Spanische Meerbrasse	*Pagellus acarne*	Mittelmeer	Verordnung (EG) Nr. 1967/2006 (Mindestgröße für die Bestandserhaltung)
Rote Fleckbrasse	*Pagellus bogaraveo*	Mittelmeer	Verordnung (EG) Nr. 1967/2006 (Mindestgröße für die Bestandserhaltung)
Gemeine Sackbrasse	*Pagrus pagrus*	Mittelmeer	Verordnung (EG) Nr. 1967/2006 (Mindestgröße für die Bestandserhaltung)
Wrackbarsch	*Polyprion americanus*	Mittelmeer	Verordnung (EG) Nr. 1967/2006 (Mindestgröße für die Bestandserhaltung)
Wrackbarsch	*Polyprion americanus*	Alle Regionen	Für die Tiefseefischerei relevant
Blaufisch	*Pomatomus saltatrix*	Schwarzes Meer	Anhang IV des Protokolls über die Erhaltung der biologischen Vielfalt und Landschaft des Schwarzen Meeres
Kleiner Rotbarsch	*Sebastes viviparus*	Alle Regionen	Für die Tiefseefischerei relevant
Weißwal	*Huso huso*	Schwarzes Meer	Anhang IV des Protokolls über die Erhaltung der biologischen Vielfalt und Landschaft des Schwarzen Meeres
Skorpionfisch (Tiefsee)	*Trachyscorpia cristulata*	Alle Regionen	Für die Tiefseefischerei relevant
Brachsenmakrele	*Brama* spp.	GSA 1.1, 1.2, 1.3 und Schwarzes Meer GSA 29	Anhang VIII der Verordnung (EG) Nr. 894/97 des Rates [6]
Spanische Makrele	*Scomber colias Gmelin*	Schwarzes Meer	Anhang IV des Protokolls über die Erhaltung der biologischen Vielfalt und Landschaft des Schwarzen Meeres
Glasgrundel	*Crystallogobius linearis*	Schwarzes Meer	Nationale Bewirtschaftungspläne
Seeratte	*Chimaera monstrosa*	Ostsee	HELCOM

Gebräuchliche Bezeichnung	Wissenschaftliche Bezeichnung	Region/RFO	Rechtsrahmen
Maifisch	*Alosa alosa*	Ostsee	HELCOM
Finte	*Alosa fallax*	Ostsee	HELCOM
Herbstlaichender Hering	Clupea harengus subsp.	Ostsee	HELCOM
Zope	*Abramis ballerus*	Ostsee	HELCOM
Ukelei	*Alburnus alburnus*	Ostsee	HELCOM
Rapfen	*Aspius aspius*	Ostsee	HELCOM
Barbe	*Barbus barbus*	Ostsee	HELCOM
Gründling	*Gobio gobio*	Ostsee	HELCOM
Sichling	*Pelecus cultratus*	Ostsee	HELCOM
Eurasische Elritze	*Phoxinus phoxinus*	Ostsee	HELCOM
Zährte	*Vimba vimba*	Ostsee	HELCOM
Steinbeißer	*Cobitis taenia*	Ostsee	HELCOM
Forelle	*Salmo trutta*	Ostsee	HELCOM
Kleine Maräne	*Coregonus albula*	Ostsee	HELCOM
Ostseeschnäpel	*Coregonus balticus,* Synonym: *Coregonus lavaretus*	Ostsee	HELCOM
Maräne	*Coregonus maraena* 'Synonym: *Coregonus lavaretus*	Ostsee	HELCOM
Coregonus pallasii	*Coregonus pallasii*	Ostsee	HELCOM
Stint	*Osmerus eperlanomarinus*	Ostsee	HELCOM
Budegassa-Anglerfisch	*Lophius budegassa*	Ostsee	HELCOM
Seestichling	*Spinachia spinachia*	Ostsee	HELCOM
Große Schlangennadel	*Entelurus aequoreus*	Ostsee	HELCOM
Kleine Schlangennadel	*Nerophis ophidion*	Ostsee	HELCOM
Nerophis lumbriciformis	*Nerophis lumbriciformis*	Ostsee	HELCOM

Gebräuchliche Bezeichnung	Wissenschaftliche Bezeichnung	Region/RFO	Rechtsrahmen
Große Seenadel	*Syngnathus acus*	Ostsee	HELCOM
Grasnadel	*Syngnathus typhle*	Ostsee	HELCOM
Rundnasen-Grenadier	*Coryphaenoides rupestris*	Ostsee	HELCOM
Schellfisch	*Melanogrammus aeglefinus*	Ostsee	HELCOM
Pollack	*Pollachius pollachius*	Ostsee	HELCOM
Leng	*Molva molva*	Ostsee	HELCOM
Spitzschwanz-Schlangenstachelrücken	*Lampretaeformis lumpenus*	Ostsee	HELCOM
Goldbarsch	*Sebastes marinus*	Ostsee	HELCOM
Norwegischer Rotbarsch	*Sebastes viviparus*	Ostsee	HELCOM
Groppe	*Cottus gobio*	Ostsee	HELCOM
Sibirische Groppe	*Cottus poecilopus*	Ostsee	HELCOM
Seeskorpion	*Myoxocephalus scorpius*	Ostsee	HELCOM
Langstacheliger Seeskorpion	*Taurulus bubalis*	Ostsee	HELCOM
Vierhörniger Seeskorpion	*Triglopsis quadricornis*	Ostsee	HELCOM
Seehase	*Cyclopterus lumpus*	Ostsee	HELCOM
Großer Scheibenbauch	*Liparis Liparis*	Ostsee	HELCOM
Kleiner Scheibenbauch	*Liparis montagui*	Ostsee	HELCOM
Petersfisch	*Zeus faber*	Ostsee	HELCOM
Wolfsbarsch	*Dicentrarchus labrax*	Ostsee	HELCOM
Gefleckter Lippfisch	*Bergylta labrus*	Ostsee	HELCOM
Kuckuckslippfisch	*Labrus mixtus*	Ostsee	HELCOM
Goldmaid	*Symphodus melops*	Ostsee	HELCOM
Gewöhnliches Petermännchen	*Trachinus draco*	Ostsee	HELCOM

Gebräuchliche Bezeichnung	Wissenschaftliche Bezeichnung	Region/RFO	Rechtsrahmen
Gestreifter Seewolf	*Anarhichas lupus*	Ostsee	HELCOM
Kleiner Sandaal	*Ammodytes marinus*	Ostsee	HELCOM
Tobiasfisch	*Ammodytes tobianus*	Ostsee	HELCOM
Bunte Grundel	*Pomatoschistus pictus*	Ostsee	HELCOM
Unechter Bonito	*Auxis rochei*	Ostsee	HELCOM
Thonine	*Euthynnus alleteratus*	Ostsee	HELCOM
Ungestreifte Pelamide	*Orcynopsis unicolor*	Ostsee	HELCOM
Makrele	*Scomber scombrus*	Ostsee	HELCOM
Atlantischer Heilbutt	*Hippoglossus hippoglossus*	Ostsee	HELCOM
Schwertfisch	*Xiphias gladius*	Ostsee	HELCOM
Schwarzfisch	*Centrolophus niger*	Ostsee	HELCOM
Knorpelfische	Chondrichthyes		
Messerzahn-Sägerochen	*Anoxypristis cuspidata*	Alle Ozeane	RFO, hohe Priorität
Schnabeldornhai	*Deania calcea*	Alle Ozeane	RFO, hohe Priorität
Glatter Schwarzer Dornhai	*Etmopterus pusillus*	Alle Ozeane	RFO, hohe Priorität
Zwergsägerochen	*Pristis clavata*	Alle Ozeane	RFO, hohe Priorität
Grüner Sägefisch	*Pristis zijsron*	Alle Ozeane	RFO, hohe Priorität
Schwarzbäuchiger Glattrochen	*Raja (Dipturus) nidarosiensis*	Alle Ozeane	RFO, hohe Priorität
Nagelrochen	*Raja clavata*	Alle Ozeane	RFO, hohe Priorität, OSPAR; HELCOM
Perlrochen	*Raja undulata*	Alle Ozeane	RFO, hohe Priorität
Pelagischer Drescher	*Alopias pelagicus*	Alle Ozeane	RFO, hohe Priorität
Drescher	*Alopias superciliosus*	Alle Ozeane	RFO, hohe Priorität
Gemeiner Drescher	*Alopias vulpinus*	Alle Ozeane	RFO, hohe Priorität; HELCOM
Atlantischer Sternrochen	*Amblyraja radiata*	Alle Ozeane	RFO, hohe Priorität

Gebräuchliche Bezeichnung	Wissenschaftliche Bezeichnung	Region/RFO	Rechtsrahmen
Isländischer Katzenhai	*Apristurus* spp.	Alle Ozeane	RFO, hohe Priorität, gefährdete Art; für die Tiefseefischerei relevant
Seidenhai	*Carcharhinus falciformis*	Alle Ozeane	RFO, hohe Priorität
Galapagoshai	*Carcharhinus galapagensis*	Alle Ozeane	RFO, hohe Priorität
Weißspitzen-Hochseehai	*Carcharhinus longimanus*	Alle Ozeane	RFO, hohe Priorität
Atlantischer Braunhai	*Carcharhinus plumbeus*	Alle Ozeane, Mittelmeer und Schwarzes Meer	RFO, hohe Priorität, Anhang II des Übereinkommens von Barcelona
Sandhai	*Carcharias taurus*	Alle Ozeane, Mittelmeer und Schwarzes Meer	RFO, hohe Priorität, Anhang II des Übereinkommens von Barcelona
Weißer Hai	*Carcharodon carcharias*	Alle Ozeane	RFO, hohe Priorität
Schlinghai	*Centrophorus granulosus*	Alle Ozeane und Meere	RFO, hohe Priorität, Anhang III des Übereinkommens von Barcelona; OSPAR
Schlinghai-Arten	*Centrophorus* spp.	Alle Regionen	Für die Tiefseefischerei relevant
Blattschuppiger Schlingerhai	*Centrophorus squamosus*	Alle Ozeane und Meere	RFO, hohe Priorität; OSPAR
Schwarzer Fabricius-Dornhai	*Centroscyllium fabricii*	Alle Ozeane	RFO, hohe Priorität, für die Tiefseefischerei relevant
Portugiesenhai	*Centroscymnus coelolepis*	Alle Ozeane	RFO, hohe Priorität, für die Tiefseefischerei relevant; OSPAR
Samtiger Langnasen-Dornhai	*Centroscymnus crepidater*	Alle Ozeane	RFO, hohe Priorität, gefährdete Art; für die Tiefseefischerei relevant
Riesenhai	*Cetorhinus maximus*	Alle Ozeane und Meere	RFO, hohe Priorität; OSPAR; HELCOM
Seeratte	*Chimaera monstrosa*	Alle Regionen	Für die Tiefseefischerei relevant
Kragenhai	*Chlamydoselachus anguineus*	Alle Ozeane	RFO, hohe Priorität, gefährdete Art; für die Tiefseefischerei relevant
Schokoladenhai	*Dalatias licha*	Alle Ozeane	RFO, hohe Priorität, gefährdete Art; für die Tiefseefischerei relevant
Stechrochen	*Dasyatis pastinaca*	Schwarzes Meer	Anhang IV des Protokolls über die Erhaltung der biologischen Vielfalt und Landschaft des Schwarzen Meeres; HELCOM

Gebräuchliche Bezeichnung	Wissenschaftliche Bezeichnung	Region/RFO	Rechtsrahmen
Schnabeldornhai	*Deania calcea*	Alle Ozeane	RFO, hohe Priorität, für die Tiefseefischerei relevant
Glattrochen	*Dipturus batis*	Alle Ozeane und Meere	RFO, hohe Priorität, Anhang II des Übereinkommens von Barcelona; OSPAR; HELCOM
Weißer Gabeldorsch	*Rostroraja alba	OSPAR II, III, IV	OSPAR
Großer Schwarzer Dornhai	*Etmopterus princeps*	Alle Ozeane	RFO, hohe Priorität, gefährdete Art; für die Tiefseefischerei relevant
Kleiner Schwarzer Dornhai	*Etmopterus spinax*	Alle Ozeane	RFO, hohe Priorität, für die Tiefseefischerei relevant; HELCOM
Flügelkopf-Hammerhai	*Eusphyra blochii*	Alle Ozeane	RFO, hohe Priorität
Hundshai	*Galeorhinus galeus*	Alle Ozeane, Mittelmeer und Schwarzes Meer	RFO, hohe Priorität, Anhang II des Übereinkommens von Barcelona; HELCOM
Fleckhai	*Galeus melastomus*	Alle Ozeane	RFO, hohe Priorität, für die Tiefseefischerei relevant
Maus-Katzenhai	*Galeus murinus*	Alle Ozeane	RFO, hohe Priorität, für die Tiefseefischerei relevant
Schmetterlingsrochen	*Gymnura altavela*	Alle Ozeane, Mittelmeer und Schwarzes Meer	RFO, hohe Priorität, Anhang II des Übereinkommens von Barcelona
Spitzkopf-Siebenkiemenhai	*Heptranchias perlo*	Alle Ozeane, Mittelmeer und Schwarzes Meer	RFO, hohe Priorität, Anhang III des Übereinkommens von Barcelona
Grauhai	*Hexandus griseus*	Alle Ozeane, Mittelmeer und Schwarzes Meer	RFO, hohe Priorität, Anhang II des Übereinkommens von Barcelona; HELCOM
Kleine Tiefenseeratte	*Hydrolagus mirabilis*	Alle Regionen	Für die Tiefseefischerei relevant
Kurzflossen-Mako	*Isurus oxyrinchus*	Alle Ozeane	RFO, hohe Priorität
Langflossen-Mako	*Isurus paucus*	Alle Ozeane	RFO, hohe Priorität
Heringshai	*Lamna nasus*	Alle Ozeane	RFO, hohe Priorität, OSPAR; HELCOM
Sandrochen	*Leucoraja circularis*	Alle Ozeane, Mittelmeer und Schwarzes Meer	RFO, hohe Priorität, Anhang II des Übereinkommens von Barcelona

Gebräuchliche Bezeichnung	Wissenschaftliche Bezeichnung	Region/RFO	Rechtsrahmen
Malteser Rochen	*Leucoraja melitensis*	Alle Ozeane, Mittelmeer und Schwarzes Meer	RFO, hohe Priorität, Anhang II des Übereinkommens von Barcelona
Riffmantarochen	*Manta alfredi*	Alle Ozeane	RFO, hohe Priorität
Großer Teufelsrochen	*Manta birostris*	Alle Ozeane	RFO, hohe Priorität
Zwerg-Teufelsrochen	*Mobula eregoodootenkee*	Alle Ozeane	RFO, hohe Priorität
Adlerrochen	*Mobula hypostoma*	Alle Ozeane	RFO, hohe Priorität
Japanischer Teufelsrochen	*Mobula japanica*	Alle Ozeane	RFO, hohe Priorität
Kuhls Teufelsrochen	*Mobula kuhlii*	Alle Ozeane	RFO, hohe Priorität
Teufelsfisch	*Mobula mobular*	Alle Ozeane	RFO, hohe Priorität
Munkiana-Teufelsrochen	*Mobula munkiana*	Alle Ozeane	RFO, hohe Priorität
Mobula rochebrunei	*Mobula rochebrunei*	Alle Ozeane	RFO, hohe Priorität
Chilenischer Teufelsrochen	*Mobula tarapacana*	Alle Ozeane	RFO, hohe Priorität
Glatter Teufelsrochen	*Mobula thurstoni*	Alle Ozeane	RFO, hohe Priorität
Nördlicher Glatthai	*Mustelus asterias*	Alle Ozeane, Mittelmeer und Schwarzes Meer	RFO, hohe Priorität, Anhang III des Übereinkommens von Barcelona
Grauer Glatthai	*Mustelus mustelus*	Alle Ozeane, Mittelmeer und Schwarzes Meer	RFO, hohe Priorität, Anhang III des Übereinkommens von Barcelona
Schwarzpunkt-Glatthai	*Mustelus punctulatus*	Alle Ozeane, Mittelmeer und Schwarzes Meer	RFO, hohe Priorität, Anhang III des Übereinkommens von Barcelona
Fleckhai	*Galeus melastomus*	Ostsee	HELCOM
Kleingefleckter Katzenhai	*Scyliorhinus canicula*	Ostsee	HELCOM
Atlantischer Sternrochen	*Amblyraja radiata*	Ostsee	HELCOM
Chagrinrochen	*Leucoraja fullonica*	Ostsee	HELCOM
Marmor-Zitterrochen	*Torpedo marmorata*	Ostsee	HELCOM

Gebräuchliche Bezeichnung	Wissenschaftliche Bezeichnung	Region/RFO	Rechtsrahmen
Segelflossen-Meersau	*Oxynotus paradoxus*	Alle Ozeane	RFO, hohe Priorität, gefährdete Art; für die Tiefseefischerei relevant
Kleinzahniger Sägerochen	*Pristis pectinata*	Alle Ozeane, Mittelmeer und Schwarzes Meer	RFO, hohe Priorität, Anhang II des Übereinkommens von Barcelona
Gewöhnlicher Sägefisch	*Pristis pristis*	Alle Ozeane, Mittelmeer und Schwarzes Meer	RFO, hohe Priorität, Anhang II des Übereinkommens von Barcelona
Krokodilshai	*Pseudocarcharias kamoharai*	Alle Ozeane	RFO, hohe Priorität
Violetter Stechrochen	*Pteroplatytrygon violacea*	Alle Ozeane	RFO, hohe Priorität
Fyllasrochen	*Raja fyllae*	Alle Regionen	Für die Tiefseefischerei relevant
Eisrochen	*Raja hyperborea*	Alle Regionen	Für die Tiefseefischerei relevant
Schwarzbäuchiger Glattrochen	*Raja nidarosiensis*	Alle Regionen	Für die Tiefseefischerei relevant
Fleckrochen	*Raja montagui*	OSPAR I, II, III, IV	OSPAR; HELCOM
Walhai	*Rhincodon typus*	Alle Ozeane	RFO, hohe Priorität
Schwarzkinn-Geigenrochen	*Rhinobatos cemiculus*	Alle Ozeane, Mittelmeer und Schwarzes Meer	RFO, hohe Priorität, Anhang II des Übereinkommens von Barcelona
Gemeiner Geigenrochen	*Rhinobatos rhinobatos*	Alle Ozeane, Mittelmeer und Schwarzes Meer	RFO, hohe Priorität, Anhang II des Übereinkommens von Barcelona
Atlantische Rüsselchimäre	*Rhinochimaera atlantica*	Alle Regionen	Für die Tiefseefischerei relevant
Graurochen	*Rostroraja alba*	Alle Ozeane, Mittelmeer und Schwarzes Meer	RFO, hohe Priorität, Anhang II des Übereinkommens von Barcelona
Messerzahnhai	*Scymnodon ringens*	Alle Ozeane	RFO, hohe Priorität, für die Tiefseefischerei relevant
Sonstige Haie	Selachimorpha (oder Selachii), Batoidea (nach Arten zu definieren, abhängig von den Daten zu Anlandungen, Überwachung und Fängen)	Alle Ozeane	RFO, hohe Priorität; HELCOM
Grönlandhai	*Somniosus microcephalus*	Alle Ozeane	RFO, hohe Priorität, für die Tiefseefischerei relevant; HELCOM

Gebräuchliche Bezeichnung	Wissenschaftliche Bezeichnung	Region/RFO	Rechtsrahmen
Bogenstirn-Hammerhai	*Sphyrna lewini*	Alle Ozeane	RFO, hohe Priorität
Großer Hammerhai	*Sphyrna mokarran*	Alle Ozeane	RFO, hohe Priorität
Glatter Hammerhai	*Sphyrna zygaena*	Alle Ozeane	RFO, hohe Priorität
Dornhai	*Squalus acanthias*	Alle Ozeane, Mittelmeer und Schwarzes Meer	RFO, hohe Priorität, Anhang III des Übereinkommens von Barcelona, OSPAR; HELCOM
Sägerücken-Engelhai	*Squatina aculeata*	Alle Ozeane, Mittelmeer und Schwarzes Meer	RFO, hohe Priorität, Anhang II des Übereinkommens von Barcelona
Weichrücken-Engelhai	*Squatina oculata*	Alle Ozeane, Mittelmeer und Schwarzes Meer	RFO, hohe Priorität, Anhang II des Übereinkommens von Barcelona
Engelhai	*Squatina squatina*	Alle Ozeane, Mittelmeer und Schwarzes Meer	RFO, hohe Priorität, Anhang II des Übereinkommens von Barcelona, OSPAR; HELCOM
Meerneunauge	*Petromyzon marinus*	OSPAR I, II, III, IV	OSPAR; HELCOM
Flussneunauge	*Lampetra fluviatilis*	Ostsee	HELCOM
Säugetiere	Mammalia		
Wale — alle Arten	*Cetacea* — alle Arten	Alle Gebiete	Richtlinie 92/43/EWG des Rates ([7])
Zwergwal	*Balaenoptera acutorostrata*	Mittelmeer	Empfehlung GFCM ([8])/36/2012/2 und Anhang II des Übereinkommens von Barcelona
Grönlandwal	*Balaena mysticetus*	OSPAR I	OSPAR
Blauwal	*Balaenoptera musculus*	Alle OSPAR	OSPAR
Atlantischer Nordkaper	*Eubalaena glacialis*	Alle OSPAR	OSPAR
Seiwal	*Balaenoptera borealis*	Mittelmeer	Empfehlung GFCM/36/2012/2 und Anhang II des Übereinkommens von Barcelona
Finnwal	*Balaenoptera physalus*	Mittelmeer	Empfehlung GFCM/36/2012/2 und Anhang II des Übereinkommens von Barcelona
Kurzschnäuziger Gemeiner Delfin	*Delphinus delphis*	Mittelmeer	Empfehlung GFCM/36/2012/2 und Anhang II des Übereinkommens von Barcelona
Atlantischer Nordkaper	*Eubalaena glacialis*	Mittelmeer	Empfehlung GFCM/36/2012/2 und Anhang II des Übereinkommens von Barcelona

Gebräuchliche Bezeichnung	Wissenschaftliche Bezeichnung	Region/RFO	Rechtsrahmen
Grindwal	*Globicephala melas*	Mittelmeer	Empfehlung GFCM/36/2012/2 und Anhang II des Übereinkommens von Barcelona
Rissos Glattkopf	*Grampus grisus*	Mittelmeer	Empfehlung GFCM/36/2012/2 und Anhang II des Übereinkommens von Barcelona
Kleiner Pottwal	*Kogia simus*	Mittelmeer	Empfehlung GFCM/36/2012/2 und Anhang II des Übereinkommens von Barcelona
Buckelwal	*Megaptera novaeangliae*	Mittelmeer	Empfehlung GFCM/36/2012/2 und Anhang II des Übereinkommens von Barcelona
Blainville-Schnabelwal	*Mesoplodon densirostris*	Mittelmeer	Empfehlung GFCM/36/2012/2 und Anhang II des Übereinkommens von Barcelona
Schwertwal	*Orcinus Orca*	Mittelmeer	Empfehlung GFCM/36/2012/2 und Anhang II des Übereinkommens von Barcelona
Schweinswal	*Phocoena phocoena*	Mittelmeer; OSPAR II, III	Empfehlung GFCM/36/2012/2 und Anhang II des Übereinkommens von Barcelona Richtlinie 92/43/EWG, OSPAR
Pottwal	*Physeter macrocephalus*	Mittelmeer	Empfehlung GFCM/36/2012/2 und Anhang II des Übereinkommens von Barcelona
Kleiner Schwertwal	*Pseudorca crassidens*	Mittelmeer	Empfehlung GFCM/36/2012/2 und Anhang II des Übereinkommens von Barcelona
Streifendelfin	*Stenella coeruleoalba*	Mittelmeer	Empfehlung GFCM/36/2012/2 und Anhang II des Übereinkommens von Barcelona
Rauzahndelfin	*Steno bredanensis*	Mittelmeer	Empfehlung GFCM/36/2012/2 und Anhang II des Übereinkommens von Barcelona
Großer Tümmler	*Tursiops truncatus*	Mittelmeer	Empfehlung GFCM/36/2012/2 und Anhang II des Übereinkommens von Barcelona
Cuvier-Schnabelwal	*Ziphius cavirostris*	Mittelmeer	Empfehlung GFCM/36/2012/2 und Anhang II des Übereinkommens von Barcelona
Mönchsrobbe	*Monachus monachus*	Alle Gebiete	Empfehlung GFCM/35/2011/5 und Anhang II des Übereinkommens von Barcelona Richtlinie 92/43/EWG
Saimaa Ringelrobbe	*Phoca hispida saimensis*	Alle Gebiete	Richtlinie 92/43/EWG
Kegelrobbe	*Halichoerus grypus*	Alle Gebiete	Richtlinie 92/43/EWG
Seehund	*Phoca vitulina*	Alle Gebiete	Richtlinie 92/43/EWG
Ostsee-Ringelrobbe	*Phoca hispida bottnica*	Alle Gebiete	Richtlinie 92/43/EWG

Gebräuchliche Bezeichnung	Wissenschaftliche Bezeichnung	Region/RFO	Rechtsrahmen
Vögel	Aves		
Gelbschnabel-Sturmtaucher	*Calonectris borealis*	Alle Gebiete	Richtlinie 2009/147/EG des Europäischen Parlaments und des Rates [9]
Kormoran	*Phalacrocorax carbo*	Alle Gebiete	Richtlinie 2009/147/EG
Basstölpel	*Morus bassanus*	Alle Gebiete	Richtlinie 2009/147/EG
Papageitaucher	*Fratercula arctica*	Alle Gebiete	Richtlinie 2009/147/EG n
Balearen-Sturmtaucher	*Puffinus mauretanicus*	Alle Gebiete	Richtlinie 2009/147/EG
Lachmöwe	*Larus ridibundus*	Alle Gebiete	Richtlinie 2009/147/EG
Trauerente	*Melanitta nigra*	Alle Gebiete	Richtlinie 2009/147/EG
Krähenscharbe	*Phalacrocorax aristotelis*	Alle Gebiete	Richtlinie 2009/147/EG
Großer Sturmtaucher	*Ardenna gravis*	Alle Gebiete	Richtlinie 2009/147/EG
Schwarzschnabel-Sturmtaucher	*Puffinus puffinus*	Alle Gebiete	Richtlinie 2009/147/EG
Eissturmvogel	*Fulmarus glacialis*	Alle Gebiete	Richtlinie 2009/147/EG
Gelbschnabel-Sturmtaucher	*Calonectris diomedea*	Alle Gebiete	Richtlinie 2009/147/EG
Dunkler Sturmtaucher	*Ardenna grisea*	Alle Gebiete	Richtlinie 2009/147/EG
Mittelmeer-Sturmtaucher	*Puffinus yelkouan*	Alle Gebiete	Richtlinie 2009/147/EG
Korallenmöwe	*Larus audouinii*	Alle Gebiete	Richtlinie 2009/147/EG
Spatente	*Bucephala islandica*	Alle Gebiete	Richtlinie 2009/147/EG
Bulwersturmvogel	*Bulweria bulwerii*	Alle Gebiete	Richtlinie 2009/147/EG
Schellente	*Bucephala clangula*	Alle Gebiete	Richtlinie 2009/147/EG
Silbermöwe	*Larus argentatus*	Alle Gebiete	Richtlinie 2009/147/EG
Eismöwe	*Larus hyperboreus*	Alle Gebiete	Richtlinie 2009/147/EG
Mantelmöwe	*Larus marinus*	Alle Gebiete	Richtlinie 2009/147/EG
Große Raubmöwe	*Catharacta skua*	Alle Gebiete	Richtlinie 2009/147/EG

Gebräuchliche Bezeichnung	Wissenschaftliche Bezeichnung	Region/RFO	Rechtsrahmen
Bergente	*Aythya marila*	Alle Gebiete	Richtlinie 2009/147/EG; Anhang IV des Protokolls über die Erhaltung der biologischen Vielfalt und Landschaft des Schwarzen Meeres
Tafelente	*Aythya ferina*	Schwarzes Meer	Anhang IV des Protokolls über die Erhaltung der biologischen Vielfalt und Landschaft des Schwarzen Meeres
Heringsmöwe	*Larus fuscus*	Alle Gebiete	Richtlinie 2009/147/EG
Krabbentaucher	*Alle alle*	Alle Gebiete	Richtlinie 2009/147/EG
Falkenraubmöwe	*Stercorarius longicaudus*	Alle Gebiete	Richtlinie 2009/147/EG
Tordalk	*Alca torda*	Alle Gebiete	Richtlinie 2009/147/EG
Schmarotzerraubmöve	*Stercorarius parasiticus*	Alle Gebiete	Richtlinie 2009/147/EG
Prqchttaucher	*Gavia arctica*	Alle Gebiete	Richtlinie 2009/147/EG
Audubon-Sturmtaucher	*Puffinus lherminieri*	Alle Gebiete	Richtlinie 2009/147/EG
Grylleiste	*Grylle cepphus*	Alle Gebiete	Richtlinie 2009/147/EG
Amerikanische Meerente	*Melanitta americana*	Alle Gebiete	Richtlinie 2009/147/EG
Schwarzhalstaucher	*Podiceps nigricollis*	Alle Gebiete	Richtlinie 2009/147/EG
Steppenmöwe	*Larus cachinnans*	Alle Gebiete	Richtlinie 2009/147/EG
Eiderente	*Somateria mollissima*	Alle Gebiete	Richtlinie 2009/147/EG
Trottellumme	*Uria aalge*	Alle Gebiete	Richtlinie 2009/147/EG
Eistaucher	*Gavia immer*	Alle Gebiete	Richtlinie 2009/147/EG
Gänsesäger	*Mergus merganser*	Alle Gebiete	Richtlinie 2009/147/EG
Haubentaucher	*Podiceps cristatus*	Alle Gebiete	Richtlinie 2009/147/EG
Kragenente	*Histrionicus histrionicus*	Alle Gebiete	Richtlinie 2009/147/EG
Ohrentaucher	*Podiceps auritus*	Alle Gebiete	Richtlinie 2009/147/EG
Polarmöwe	*Larus glaucoides*	Alle Gebiete	Richtlinie 2009/147/EG
Prachteiderente	*Somateria spectabilis*	Alle Gebiete	Richtlinie 2009/147/EG

Gebräuchliche Bezeichnung	Wissenschaftliche Bezeichnung	Region/RFO	Rechtsrahmen
Eisente	*Clangula hyemalis*	Alle Gebiete	Richtlinie 2009/147/EG
Schwarzkopfmöwe	*Larus melanocephalus*	Alle Gebiete	Richtlinie 2009/147/EG
Sturmmöwe	*Larus canus*	Alle Gebiete	Richtlinie 2009/147/EG
Mittelsäger	*Mergus serrator*	Alle Gebiete	Richtlinie 2009/147/EG
Rothalstaucher	*Podiceps grisegena*	Alle Gebiete	Richtlinie 2009/147/EG
Sterntaucher	*Gavia stellata*	Alle Gebiete	Richtlinie 2009/147/EG
Dünnschnabelmöwe	*Larus genei*	Alle Gebiete	Richtlinie 2009/147/EG
Scheckente	*Polysticta stelleri*	Alle Gebiete	Richtlinie 2009/147/EG
Spatelraubmöve	*Stercorarius pomarinus*	Alle Gebiete	Richtlinie 2009/147/EG
Dickschnabellumme	*Uria lomvia*	Alle Gebiete	Richtlinie 2009/147/EG
Samtente	*Melanitta fusca*	Alle Gebiete	Richtlinie 2009/147/EG
Gelbschnabeleistaucher	*Gavia adamsii*	Alle Gebiete	Richtlinie 2009/147/EG
Mittelmeermöwe	*Larus michahellis*	Alle Gebiete	Richtlinie 2009/147/EG
Madeira-Sturmvogel	*Pterodroma madeira*	Alle Gebiete	Richtlinie 2009/147/EG
Fischmöwe	*Larus ichthyaetus*	Alle Gebiete	Richtlinie 2009/147/EG
Dreizehenmöwe	*Rissa tridactyla*	Alle Gebiete	Richtlinie 2009/147/EG
Rosapelikan	*Pelecanus onocrotalus*	Alle Gebiete	Richtlinie 2009/147/EG
Wellenläufer	*Oceanodroma leucorhoa*	Alle Gebiete	Richtlinie 2009/147/EG
Thorshühnchen	*Phalaropus fulicarius*	Alle Gebiete	Richtlinie 2009/147/EG
Odinshühnchen	*Phalaropus lobatus*	Alle Gebiete	Richtlinie 2009/147/EG
Buntfuß-Sturmschwalbe	*Oceanites oceanicus*	Alle Gebiete	Richtlinie 2009/147/EG
Küstenseeschwalbe	*Sterna paradisaea*	Alle Gebiete	Richtlinie 2009/147/EG
Madeira-Wellenläufer	*Hydrobates castro*	Alle Gebiete	Richtlinie 2009/147/EG
Trauerseeschwalbe	*Chlidonias niger*	Alle Gebiete	Richtlinie 2009/147/EG
Raubseeschwalbe	*Hydroprogne caspia*	Alle Gebiete	Richtlinie 2009/147/EG

Gebräuchliche Bezeichnung	Wissenschaftliche Bezeichnung	Region/RFO	Rechtsrahmen
Lachseeschwalbe	*Gelochelidon nilotica*	Alle Gebiete	Richtlinie 2009/147/EG
Flussseeschwalbe	*Sterna hirundo*	Alle Gebiete	Richtlinie 2009/147/EG
Desertas-Sturmvogel	*Pterodroma Deserta*	Alle Gebiete	Richtlinie 2009/147/EG
Elfenbeinmöwe	*Pagophila eburnea*	Alle Gebiete	Richtlinie 2009/147/EG
Rüppellseeschwalbe	*Thalasseus bengalensis*	Alle Gebiete	Richtlinie 2009/147/EG
Zwergmöwe	*Hydrocoloeus minutus*	Alle Gebiete	Richtlinie 2009/147/EG
Zwergseeschwalbe	*Sternula albifrons*	Alle Gebiete	Richtlinie 2009/147/EG
Monteiro-Sturmvogel	*Hydrobates monteiroi*	Alle Gebiete	Richtlinie 2009/147/EG
Rosenseeschwalbe	*Sterna dougallii*	Alle Gebiete	Richtlinie 2009/147/EG
Rosenmöve	*Rhodostethia rosea*	Alle Gebiete	Richtlinie 2009/147/EG
Schwalbenmöwe	*Xema sabini*	Alle Gebiete	Richtlinie 2009/147/EG
Brandseeschwalbe	*Thalasseus sandvicensis*	Alle Gebiete	Richtlinie 2009/147/EG
Thayermöve	*Larus thayeri*	Alle Gebiete	Richtlinie 2009/147/EG
Fregattensturmschwalbe	*Pelagodroma marina*	Alle Gebiete	Richtlinie 2009/147/EG
Sturmschwalbe	*Hydrobates pelagicus*	Alle Gebiete	Richtlinie 2009/147/EG
Heringsmöwe	*Larus fuscus fuscus*	OSPAR I	OSPAR-Liste der bedrohten und rückläufigen Arten
Elfenbeinmöwe	*Pagophila eburnea*	OSPAR I	OSPAR-Liste der bedrohten und rückläufigen Arten
Scheckente	*Polysticta stelleri*	OSPAR I	OSPAR-Liste der bedrohten und rückläufigen Arten
Kleiner Sturmtaucher	Puffinus assimilis baroli (auct.incert.)	OSPAR V	OSPAR-Liste der bedrohten und rückläufigen Arten
Balearen-Sturmtaucher	*Puffinus mauretanicus*	OSPAR II, III, IV, V	OSPAR-Liste der bedrohten und rückläufigen Arten
Dreizehenmöwe	*Rissa tridactyla*	OSPAR I, II	OSPAR-Liste der bedrohten und rückläufigen Arten
Rosenseeschwalbe	*Sterna dougallii*	OSPAR II, III, IV, V	OSPAR-Liste der bedrohten und rückläufigen Arten

Gebräuchliche Bezeichnung	Wissenschaftliche Bezeichnung	Region/RFO	Rechtsrahmen
Iberische Trottellumme	*Uria aalge* — Iberische Art (Synonyme: *Uria aalge albionis Uria aalge ibericus*)	OSPAR IV	OSPAR-Liste der bedrohten und rückläufigen Arten
Dickschnabellumme	*Uria lomvia*	OSPAR I	OSPAR-Liste der bedrohten und rückläufigen Arten
Reptilien	Reptilia		
Atlantik-Bastardschilldkröte	*Lepidochelys kempii*	Alle Gebiete	Richtlinie 92/43/EWG; Empfehlung GFCM/35/2011/4 und Anhang II des Übereinkommens von Barcelona
Unechte Karettschildkröte	*Caretta caretta*	Alle Gebiete	Richtlinie 92/43/EWG; Empfehlung GFCM/35/2011/4 und Anhang II des Übereinkommens von Barcelona OSPAR
Lederschildkröte	*Dermochelys coriacea*	Alle Gebiete	Richtlinie 92/43/EWG; Empfehlung GFCM/35/2011/4 und Anhang II des Übereinkommens von Barcelona OSPAR
Echte Karettschildkröte	*Eretmochelys imbricata*	Alle Gebiete	Richtlinie 92/43/EWG; Empfehlung GFCM/35/2011/4 und Anhang II des Übereinkommens von Barcelona
Suppenschildkröte	*Chelonia mydas*	Alle Gebiete	Richtlinie 92/43/EWG; Empfehlung GFCM/35/2011/4 und Anhang II des Übereinkommens von Barcelona
Afrikanische Weichschildkröte	*Trionyx triunguis*	Mittelmeer	Empfehlung GFCM/35/2011/4 und Anhang II des Übereinkommens von Barcelona
Weichtiere	Mollusca		
Gestreifte Venusmuschel	*Chamelea gallina*	Schwarzes Meer	Anhang IV des Protokolls über die Erhaltung der biologischen Vielfalt und Landschaft des Schwarzen Meeres
Sägezähnchen	*Donacilla cornea*	Schwarzes Meer	Anhang IV des Protokolls über die Erhaltung der biologischen Vielfalt und Landschaft des Schwarzen Meeres
Eledone	*Eledone* spp.	Alle Gebiete	Nationale Bewirtschaftungspläne
Mittelmeer-Miesmuschel	*Mytilus galloprovincialis*	Alle Gebiete des Mittelmeers	Nationale Bewirtschaftungspläne
Mittelmeer-Miesmuschel	*Mytilus galloprovincialis*	Schwarzes Meer	Anhang IV des Protokolls über die Erhaltung der biologischen Vielfalt und Landschaft des Schwarzen Meeres
Napfschnecke	*Patella* spp.	Mittelmeer	Anhang II des Übereinkommens von Barcelona
Rapana venosa	*Rapana venosa*	Schwarzes Meer	Anhang IV des Protokolls über die Erhaltung der biologischen Vielfalt und Landschaft des Schwarzen Meeres
Warzige Herzmuschel	*Acanthocardia tuberculata*	Alle Gebiete	Nationale Bewirtschaftungspläne
Brandhorn	*Brandaris bolinus*	Alle Gebiete	Nationale Bewirtschaftungspläne

Gebräuchliche Bezeichnung	Wissenschaftliche Bezeichnung	Region/RFO	Rechtsrahmen
Nördliche Venusmuschel	*Callista chione*	Alle Gebiete	Nationale Bewirtschaftungspläne
Gebänderte Dreieckmuschel	*Donax trunculus*	Alle Gebiete	Nationale Bewirtschaftungspläne
Islandmuschel	*Arctica islandica*	OSPAR II	OSPAR
Azoren Entenmuschel	*Azoricus megabalanus*	Alle Gebiete von OSPAR V, soweit Vorkommen	OSPAR
Nordische Purpurschnecke	*Nucella lapillus*	OSPAR II, III, IV	OSPAR
Flachauster	*Ostrea edulis*	OSPAR II	OSPAR
Patella ulyssiponensis aspera	*Patella ulyssiponensis aspera*	Alle Gebiete von OSPAR, soweit Vorkommen	OSPAR
Krebstiere	Crustacea		
Hummer	*Homarus gammarus*	Mittelmeer	Verordnung (EG) Nr. 1967/2006 (Mindestgröße für die Bestandserhaltung)
Rote Tiefseekrabbe	*Chaceon (Geryon) affinis*	Alle Regionen	Für die Tiefseefischerei relevant
Nordseegarnele	*Crangon crangon*	Schwarzes Meer	Anhang IV des Protokolls über die Erhaltung der biologischen Vielfalt und Landschaft des Schwarzen Meeres
Ostseegarnele	*Palaemon adspersus*	Schwarzes Meer	Anhang IV des Protokolls über die Erhaltung der biologischen Vielfalt und Landschaft des Schwarzen Meeres
Kleine Felsengarnele	*Palaemon elegans*	Schwarzes Meer	Anhang IV des Protokolls über die Erhaltung der biologischen Vielfalt und Landschaft des Schwarzen Meeres
Languste	*Palinuridae*	Mittelmeer	Verordnung (EG) Nr. 1967/2006 (Mindestgröße für die Bestandserhaltung)
Cnidaria	Cnidaria		
Rote Koralle	*Corallium rubrum*	Mittelmeer	Empfehlung GFCM/36/2012/1 und Empfehlung GFCM/35/2011/2

(1) Übereinkommen von Barcelona zum Schutz der Meeresumwelt und der Küstenregion des Mittelmeers.
(2) OSPAR Übereinkommen zum Schutz der Meeresumwelt des Nordostatlantiks.
(3) HELCOM Übereinkommen zum Schutz der Meeresumwelt im Ostseegebiet.
(4) Verordnung (EG) Nr. 2347/2002 des Rates vom 16. Dezember 2002 mit spezifischen Zugangsbedingungen und einschlägigen Bestimmungen für die Fischerei auf Tiefseebestände (ABl. L 351 vom 28.12.2002, S. 6).
(5) Verordnung (EG) Nr. 1967/2006 des Rates vom 21. Dezember 2006 betreffend die Maßnahmen für die nachhaltige Bewirtschaftung der Fischereiressourcen im Mittelmeer und zur Änderung der Verordnung (EWG) Nr. 2847/93 sowie zur Aufhebung der Verordnung (EG) Nr. 1626/94 (ABl. L 409 vom 30.12.2006, S. 11).
(6) Verordnung (EG) Nr. 894/97 des Rates vom 29. April 1997 über technische Maßnahmen zur Erhaltung der Fischbestände (ABl. L 132 vom 23.5.1997, S. 1).
(7) Richtlinie 92/43/EWG des Rates vom 21. Mai 1992 zur Erhaltung der natürlichen Lebensräume sowie der wildlebenden Tiere und Pflanzen (ABl. L 206 vom 22.7.1992, S. 7).
(8) Allgemeine Kommission für die Fischerei im Mittelmeer.
(9) Richtlinie 2009/147/EG des Europäischen Parlaments und des Rates vom 30. November 2009 über die Erhaltung der wildlebenden Vpogelarten (ABl. L 20 vom 26.1.2010, S. 7)

Für verbotene Arten: Nur tot gefangene Tiere dürfen verwendet werden. Nach den Messungen sind sie zu entsorgen. Die Datenerhebung erfolgt jährlich und die Aktualisierung/Verarbeitung der Daten muss zeitnah erfolgen, um in den Zeitplan für die Bestandsabschätzung zu passen.

BIOLOGISCHE DATEN

Tabelle 1E

Anadrome und katadrome Süßwasserarten

Art (gebräuchliche Bezeichnung)	Art (wissenschaftliche Bezeichnung)	Nicht-Meeresgebiete, in denen sich der Bestand befindet/Bestandscode
Aal	*Anguilla anguilla*	Aal-Bewirtschaftungseinheiten gemäß der Verordnung (EG) Nr. 1100/2007 des Rates [1]
Lachs	*Salmo salar*	In allen Gebieten der natürlichen Verbreitung
Meerforelle	*Salmo trutta*	Alle Binnengewässer, die in die Ostsee münden

[1] Verordnung (EG) Nr. 1100/2007 des Rates vom 18. September 2007 mit Maßnahmen zur Wiederauffüllung des Bestands des Europäischen Aals (ABl. L 248 vom 22.9.2007, S. 17).

Tabelle 2

Fangtätigkeit (Metier) je Region

Ebene 1	Ebene 2	Ebene 3	Ebene 4	Ebene 5	Ebene 6	Längenklassen (in Metern) (d)					
Tätigkeit	Fanggerätekklassen	Fanggerätegruppen	Art des Fanggeräts	Zielartengruppe (a)	Maschenöffnung und sonstige Selektiervorrichtungen	< 10	10- < 12	12- < 18	18- < 24	24- < 40	40 &+
Fangtätigkeit	Dredgen	Dredgen	Bootdredgen [DRB]	Anadrome Arten (ANA) Katadrome Arten (CAT) Kopffüßer (CEP) Krebstiere (CRU) Grundarten (DEF) Tiefseearten (DWS) Flossenfische (FIF) Süßwasserarten (kein Code) Verschiedenes (MIS) Mischung aus Kopffüßern und Grundarten (MCF) Mischung aus Krebstieren und Grundarten (MCD) Mischung aus Tiefseearten und Grundarten (MDD) Mischung aus pelagischen Arten und Grundarten (MPD) Weichtiere (MOL) Große pelagische Fische (LPF) Kleine pelagische Fische (SPF) Große pelagische Fische (LPF) und kleine pelagische Fische (SPF)	(b)						
			Mechanisierte Dredge [HMD]		(b)						
	Schleppnetze	Grundschleppnetze	Grundschleppnetz [OTB]		(b)						
			Mehrfachgrundschleppnetz [OTT]		(b)						
			Zweischiffgrundschleppnetz [PTB]		(b)						
			Baumkurre [TBB]		(b)						
		Pelagische Schleppnetze	Schwimmschleppnetz [OTM]		(b)						
			Zweischiffschwimmschleppnetz [PTM]		(b)						

Ebene 1	Ebene 2	Ebene 3	Ebene 4	Ebene 5	Ebene 6	Längenklassen (in Metern) (d)					
Tätigkeit	Fanggeräteklassen	Fanggerätegruppen	Art des Fanggeräts	Zielartengruppe (a)	Maschenöffnung und sonstige Selektiervorrichtungen	< 10	10- < 12	12- < 18	18- < 24	24- < 40	40 &+
	Haken und Leinen	Angeln und Leinen	Handleinen [LHP] und mechanisierte Angelleinen [LHM]		(b)						
			Schleppangeln [LTL]		(b)						
		Langleinen	Treiblangleinen [LLD]		(b)						
			Grundlangleinen [LLS]		(b)						
	Fischfallen	Fischfallen	Reusen und Fallen [FPO]		(b)						
			Garnreusen [FYK]		(b)						
			Nicht bedeckte stationäre Reusen [FPN]		(b)						
			Ortsfeste Anlagen für Zäune und Wehre (Code erforderlich)		(b)						
	Netze	Netze	Trammelnetz [GTR]		(b)						
			Stellnetz (verankert) [GNS]		(b)						
			Treibnetz [GND]		(b)						
	Waden	Umschließungsnetze	Ringwade [PS]		(b)						
			Lamparanetze [LA]		(b)						
		Waden (c)	Schottische Wade (Snurrewade ohne Anker) [SSC]		(b)						
			Snurrewade mit Anker [SDN]		(b)						

Ebene 1	Ebene 2	Ebene 3	Ebene 4	Ebene 5	Ebene 6	Längenklassen (in Metern) (d)					
Tätigkeit	Fanggeräteklassen	Fanggerätegruppen	Art des Fanggeräts	Zielartengruppe (a)	Maschenöffnung und sonstige Selektiervorrichtungen	< 10	10- < 12	12- < 18	18- < 24	24- < 40	40 &+
			Zweischiffwade [SPR]		(b)						
			Boots- [SB] und Schiffwade [SV]		(b)						
	Sonstiges Fanggerät	Sonstiges Fanggerät	Glasaalfang (kein Code)	Glasaal	(b)						
	Verschiedene (anführen)	Verschiedene (anführen)			(b)						
Fangfremde Tätigkeit				Fangfremde Tätigkeit							
Inaktiv				Inaktiv							

Fußnoten:
(a) Gemäß den in den einschlägigen Verordnungen bestehenden Codes.
(b) Gemäß den in den einschlägigen Verordnungen bestehenden Codes.
(c) Mit Fischsammelgeräten (fish aggregating devices — FAD)/in freien Schulen.
(d) Im Mittelmeer < 6 m und 6-12 m.

Tabelle 3

Zu erfassende Arten in der Freizeitfischerei

	Gebiet	Arten
1	Ostsee (ICES-Unterdivisionen 22-32)	Lachs, Aal und Meerforelle (einschließlich in Süßwasser) und Dorsch
2	Nordsee (ICES-Gebiete IIIa, IV und VIId)	Lachs und Aal (einschließlich in Süßwasser). Seebarsch, Kabeljau, Pollack und Knorpelfische
3	Östliche Arktis (ICES-Gebiete I und II)	Lachs und Aal (einschließlich in Süßwasser). Kabeljau, Pollack und Knorpelfische
4	Nordatlantik (ICES-Gebiete V-XIV und NAFO-Gebiete)	Lachs und Aal (einschließlich in Süßwasser). Seebarsch, Kabeljau, Pollack, Knorpelfische und weit wandernde ICCAT-Arten
5	Mittelmeer	Aal (einschließlich in Süßwasser), Knorpelfische und weit wandernde ICCAT-Arten
6	Schwarzes Meer	Aal (einschließlich in Süßwasser), Knorpelfische und weit wandernde ICCAT-Arten

Tabelle 4

Fangtätigkeit

	Variablen [1]	Einheit
	Kapazität	
	Zahl der Fischereifahrzeuge	Zahl
	BRZ, kW, Alter des Fischereifahrzeugs	Zahl
	Aufwand	
	Tage auf See	Tage
	Fangstunden (fakultativ)	Stunden
	Fangtage	Tage
	kW * Fangtage	Zahl
	BRZ * Fangtage	Zahl
	Anzahl Fangreisen	Anzahl
	Anzahl der Fangeinsätze	Anzahl
	Anzahl der Netze/Länge (*)	Anzahl/Meter
	Anzahl der Haken, Anzahl der Leinen (*)	Anzahl
	Anzahl der Reusen und Fallen (*)	Anzahl
	Anlandungen	
	Wert der Anlandungen insgesamt und nach marktgängigen Arten	EUR
	Lebendgewicht der Anlandungen insgesamt und nach Arten	Tonnen
	Preise nach marktgängigen Arten	EUR/kg

[1] Alle Variablen sind auf der Aggregationsebene (Metiers und Flottensegment) gemäß Tabelle 3 und Tabelle 5B und je Unterregion/Fanggrund gemäß Tabelle 5C anzugeben.

(*) Die Sammlung dieser Variablen für Schiffe mit einer Länge von weniger als 10 m wird auf Ebene der Meeresregion festgelegt.

WIRTSCHAFTSDATEN DER FLOTTE

Tabelle 5A

Wirtschaftliche Variablen für die Flotte

Variablengruppe	Variable	Einheit
Einnahmen	Bruttowert der Anlandungen	EUR
	Einkommen aus der Verpachtung von Quoten oder anderen Fangrechten	EUR
	Sonstige Erträge	EUR
Arbeitskosten	Personalkosten	EUR
	Wert unbezahlter Arbeit	EUR
Energiekosten	Energiekosten	EUR
Reparatur- und Wartungskosten	Reparatur- und Wartungskosten	EUR
Sonstige Betriebskosten	Variable Kosten	EUR
	Nicht variable Kosten	EUR
	Pacht-/Mietzahlungen für Quoten oder andere Fangrechte	EUR
Zuschüsse	Betriebskostenzuschüsse	EUR
	Zuschüsse für Investitionen	EUR
Kapitalkosten	Abschreibungen	EUR
Kapitalwert	Wert des physischen Kapitals	EUR
	Wert von Quoten und anderen Fangrechten	EUR
Investitionen	Investitionen in materielle Vermögenswerte, netto	EUR
Finanzlage	Lang- und kurzfristige Schulden	EUR
	Aktiva insgesamt	EUR
Beschäftigung	Beschäftigte Mannschaft	Anzahl
	Nicht entlohnte Arbeitskräfte	Anzahl
	Gesamtzahl der geleisteten Arbeitsstunden pro Jahr	Anzahl

Variablengruppe	Variable	Einheit
Flotte	Zahl der Schiffe	Anzahl
	Mittlere Länge über alles der Schiffe	Meter
	Gesamttonnage	BRZ
	Gesamtleistung	kW
	Mittleres Alter der Schiffe	Jahre
Aufwand	Tage auf See	Tage
	Energieverbrauch	Liter
Anzahl der Fischereiunternehmen/Einheiten	Anzahl der Fischereiunternehmen/Einheiten	Anzahl
Produktionswert pro Art	Wert der Anlandungen nach Art	EUR
	Durchschnittspreis nach Art	EUR/kg

WIRTSCHAFTSDATEN DER FLOTTE

Tabelle 5B

Flottensegmentierung

		Längenklassen (Länge über alles) [1]					
Aktive Fischereifahrzeuge		0-< 10 m 0-< 6 m	10-< 12 m 6-< 12 m	12-< 18 m	18-< 24 m	24-< 40 m	40 m oder länger
Einsatz „beweglicher“ Fanggeräte	Baumkurrenfänger						
	Grundschleppnetzfischer und/oder Grund-Wadenfischer						
	Pelagische Schleppnetzfänger						
	Ringwadenfänger						
	Dredgenfischer						
	Fischereifahrzeuge mit anderem beweglichem Fanggerät						
	Fischereifahrzeuge, die ausschließlich unterschiedliche bewegliche Fanggeräte einsetzen						

		Längenklassen (Länge über alles) (1)					
Aktive Fischereifahrzeuge		0-< 10 m 0-< 6 m	10-< 12 m 6-< 12 m	12-< 18 m	18-< 24 m	24-< 40 m	40 m oder länger
Einsatz „stationärer" Fanggeräte	Fischereifahrzeuge, die Haken einsetzen	(2)	(2)				
	Treibnetz- oder Stellnetzfischer						
	Fischereifahrzeuge, die Reusen und/oder Fallen einsetzen						
	Fischereifahrzeuge mit anderem stationärem Fanggerät						
	Fischereifahrzeuge, die ausschließlich unterschiedliche stationäre Fanggeräte einsetzen						
Einsatz unterschiedlicher Fanggeräte	Fischereifahrzeuge, die bewegliches und stationäres Fanggerät einsetzen						
Inaktive Fischereifahrzeuge							

(1) Für Fischereifahrzeuge im Mittelmeer und im Schwarzen Meer mit einer Länge von weniger als 12 Metern lauten die Längenklassen 0-< 6 und 6-< 12 Meter. Für alle anderen Regionen gelten die Längenklassen 0-< 10 und 10-< 12 Meter.

(2) Schiffe mit einer Länge von weniger als 12 m mit passiven Fanggeräten im Mittelmeer und im Schwarzen Meer können nach Art der Fanggeräte aufgeschlüsselt werden. Die Definition des Flottensegments umfasst auch eine Angabe zur Supraregion und, sofern verfügbar, einen geografischen Indikator, um Schiffe zu ermitteln, die in Gebieten in äußerster Randlage und ausschließlich außerhalb der EU-Gewässer fischen.

WIRTSCHAFTSDATEN DER FLOTTE

Tabelle 5C

Gebietsunterteilung nach Regionen

Unterregion/Fanggrund	Region(en)	Supraregion
I	II	III
Gruppierung räumlicher Einheiten der Ebene 3 gemäß Tabelle 3 (NAFO-Division)	NAFO (FAO-Gebiet 21)	Ostsee; Nordsee; Östliche Arktis; NAFO; Erweiterte nordwestliche Gewässer (ICES-Gebiete V, VI und VII) und südwestliche Gewässer
Gruppierung räumlicher Einheiten der Ebene 4 gemäß Tabelle 3 (ICES-Unterdivision)	Ostsee (ICES-Gebiete III b-d)	
Gruppierung räumlicher Einheiten der Ebene 3 gemäß Tabelle 3 (ICES-Division)	Nordsee (ICES-Gebiete IIIa und IV) Östliche Arktis (ICES-Gebiete I und II)	
	Nordwestliche Gewässer (ICES-Gebiete Vb (Unionsgewässer), VI und VII)	
	Nordwestliche Gewässer (ICES-Gebiete Va und Vb) (nur Nicht-Unionsgewässer)	

Unterregion/Fanggrund	Region(en)	Supraregion
I	II	III
Gruppierung räumlicher Einheiten der Ebene 3 gemäß Tabelle 3 (ICES/CECAF-Division)	Südwestliche Gewässer (ICES-Gebiete VIII, IX und X (Gewässer um die Azoren), CECAF-Gebiete 34.1.1, 34.1.2 und 34.2.0 (Gewässer um Madeira und die Kanarischen Inseln)	
Gruppierung räumlicher Einheiten der Ebene 4 gemäß Tabelle 3 (GSA)	Mittelmeer (Meeresgewässer des Mittelmeers östlich der Linie 5°36′ West); Schwarzes Meer (das in der Entschließung GFCM/33/2009/2 definierte geografische GFCM-Untergebiet)	Mittelmeer und Schwarzes Meer
Beprobungsuntergebiete der RFO (ohne GFCM)	Sonstige Regionen, in denen Fischereifahrzeuge der Union fischen und die von einer RFO verwaltet werden, deren Vertragspartei die Europäische Union ist oder bei der sie Beobachterstatus hat (z. B. ICCAT, IOTC, CECAF usw.)	Sonstige Regionen

Tabelle 6

Soziale Variablen für den Fischerei- und Aquakultursektor

Variable	Einheit
Beschäftigung nach Geschlecht	Anzahl
VZÄ nach Geschlecht	Anzahl
Nicht entlohnte Arbeitskräfte nach Geschlecht	Anzahl
Beschäftigung nach Alter	Anzahl
Beschäftigung nach Bildungsstand	Anzahl je Bildungsstand
Beschäftigung nach Staatsangehörigkeit	Anzahl aus EU, EWR und Nicht-EU/EWR
Beschäftigung nach Beschäftigungsstatus	Anzahl
VZÄ national	Anzahl

Tabelle 7

Wirtschaftliche Variablen für den Aquakultursektor

Variablengruppe	Variable	Einheit
Einkommen (*)	Bruttoverkäufe insgesamt je Art	EUR
	Sonstige Erträge	EUR

Variablengruppe	Variable	Einheit
Personalkosten	Personalkosten	EUR
	Wert unbezahlter Arbeit	EUR
Energiekosten	Energiekosten	EUR
Rohstoffkosten	Kosten für den Tierbestand	EUR
	Futterkosten	EUR
Reparatur und Wartung	Reparatur und Wartung	EUR
Sonstige Betriebskosten	Sonstige Betriebskosten	EUR
Zuschüsse	Betriebskostenzuschüsse	EUR
	Zuschüsse für Investitionen	EUR
Kapitalkosten	Abschreibungen	EUR
Kapitalwert	Gesamtwert der Vermögenswerte	EUR
Finanzergebnisse	Finanzerträge	EUR
	Ausgaben	EUR
Investitionen	Netto-Investitionen	EUR
Schulden	Schulden	EUR
Rohstoffgewicht	Verwendete Tiere	kg
	Fischfutter	kg
Gewicht der Verkäufe	Gewicht der Verkäufe je Art	kg
Beschäftigung	Beschäftigte	Anzahl/Vollzeitäquivalent
	Nicht entlohnte Arbeitskräfte	Anzahl/Vollzeitäquivalent
	Zahl der von Lohn- und Gehaltsempfängern und nicht entlohnten Arbeitskräften geleisteten Arbeitsstunden	Stunden
Zahl der Unternehmen	Zahl der Unternehmen (nach Kategorien gemäß der Zahl der Beschäftigten)	Anzahl

(*) Umfasst Direktzahlungen, z. B. Ausgleichszahlungen für die Einstellung der Fangtätigkeit, Erstattungen für Treibstoffabgaben oder ähnliche Pauschalausgleichszahlungen. Umfasst nicht Sozialabgaben und indirekte Subventionen wie z. B. verringerte Abgaben auf Betriebsmittel wie Treibstoff oder Investitionsbeihilfen.

Tabelle 8

Umweltbezogene Variablen für den Aquakultursektor

Variable	Spezifikation	Einheit
Arzneimittel oder Behandlungen (1)	Nach Art	Gramm
Mortalität (2)		Prozent

(1) Hochrechnung ausgehend von Daten gemäß Anhang I Nummer 8 Buchstabe b der Verordnung (EG) Nr. 852/2004 des Europäischen Parlaments und des Rates (ABl. L 139 vom 30.4.2004, S. 1).
(2) Hochgerechnet auf einen Prozentsatz der nationalen Erzeugung ausgehend von Daten gemäß Artikel 8 Absatz 1 Buchstabe b der Richtlinie 2006/88/EG des Rates (ABl. L 328 vom 24.11.2006, S. 14).

Tabelle 9

Segmentierung für die Erhebung von Daten zur Aquakultur (1)

	Fischzuchttechniken (2)						Polykultur	Brutanlagen und Aufzuchtanlagen (3)	Techniken für die Zucht von Schalentieren			
	Teiche	Becken und Fließkanäle	Einfriedungen und Gehege (6)	Kreislaufanlagen (5)	Andere Verfahren	Käfige (7)	Alle Verfahren		Off-bottom		On-bottom (4)	Sonstige
									Flöße	Hängeleinen		
Lachs												
Forelle												
Wolfsbarsch und Brassen												
Karpfen												
Thunfisch												
Aal												
Stör (Eier für den menschlichen Verbrauch)												
Sonstige Süßwasserfische												
Sonstige Meeresfische												
Miesmuscheln												

	Fischzuchttechniken ([2])						Polykultur	Brutanlagen und Aufzuchtanlagen ([3])	Techniken für die Zucht von Schalentieren			
	Teiche	Becken und Fließkanäle	Einfriedungen und Gehege ([6])	Kreislaufanlagen ([5])	Andere Verfahren	Käfige ([7])	Alle Verfahren		Off-bottom		On-bottom ([4])	Sonstige
									Flöße	Hängeleinen		
Austern												
Venusmuscheln												
Krebstiere												
Andere Weichtiere												
Multiple Arten												
Algen												
Sonstige aquatische Organismen												

([1]) Definitionen der Aufzuchttechniken gemäß der Verordnung (EG) Nr. 762/2008.
([2]) Unternehmen sollten anhand ihrer wichtigsten Zuchttechnik einem Segment zugeordnet werden.
([3]) Brutanlagen und Aufzuchtanlagen sind Anlagen für die künstliche Vermehrung, das Schlüpfen und die Aufzucht während der ersten Lebensstadien von Wassertieren. Für statistische Zwecke beschränken sich Brutanlagen auf die Erzeugung von befruchteten Eiern. Die weiteren Entwicklungsstadien von Wassertieren werden in Aufzuchtanlagen durchlaufen. Wenn Brutanlagen und Aufzuchtanlagen eng miteinander verbunden sind, beziehen sich die Statistiken nur auf das letzte Jungtierstadium (KOM(2006) 864 vom 19. Juli 2007).
([4]) „On-bottom"-Techniken betreffen den Anbau von Schalentieren in Gezeitenbereichen (unmittelbar auf dem Meeresboden oder ohne Bodenberührung).
([5]) Kreislaufanlagen sind Anlagen, in denen das Wasser nach der Aufbereitung (z. B. Filtern) in das Haltungsbecken zurückgeführt wird.
([6]) Einfriedungen und Gehege sind Gebiete im Wasser, die durch Netze, Maschengewebe oder andere Barrieren, die einen unkontrollierten Wasseraustausch erlauben, umschlossen werden, und unterscheiden sich dadurch, dass Einfriedungen die komplette Wassersäule vom Meeresboden bis zur Oberfläche umfassen; beide Strukturen umschließen im Allgemeinen verhältnismäßig große Wassermengen (KOM(2006) 864 vom 19. Juli 2007).
([7]) Käfige sind offene oder bedeckte umbaute Strukturen aus Netzen, Maschengewebe oder ähnlichen durchlässigen Materialien, die einen natürlichen Wasseraustausch erlauben. Diese Strukturen können an der Oberfläche schwimmen, aufgehängt oder am Meeresboden verankert sein, sie lassen aber in allen Fällen einen Wasseraustausch von unten zu (KOM(2006) 864 vom 19. Juli 2007).

Tabelle 10

Forschungsreisen auf See

Bezeichnung der Forschungsreise	Abkürzung	Gebiet	Zeitraum	Hauptzielarten
Ostsee				
Internationaler Schleppnetz-Survey Ostsee	BITS Q1 BITS Q4	IIIaS, IIIb-d	1. und 4. Quartal	Dorsch und andere Grundfischarten
Internationaler Hydroakustik-Survey Ostsee (Herbst)	BIAS	IIIa, IIIb-d	Sept./Okt.	Hering und Sprotte
Hydroakustik-Survey Hering im Golf von Riga	GRAHS	IIId	3. Quartal	Hering

Bezeichnung der Forschungsreise	Abkürzung	Gebiet	Zeitraum	Hauptzielarten
Hydroakustik-Survey Sprotte	SPRAS	IIId	Mai	Sprotte und Hering
Heringslarven-Survey Rügen	RHLS	IIId	März-Juni	Hering
Nordsee und Östliche Arktis (ICES-Gebiete I und II)				
Internationaler Grundschleppnetz-Survey	IBTS Q1 IBTS Q3	IIIa, IV	1. und 3. Quartal	Schellfisch, Kabeljau, Seelachs, Hering, Sprotte, Wittling, Makrele, Stintdorsch
Baumkurren-Survey Nordsee	BTS	IVb,IVc,VIId	3. Quartal	Scholle, Seezunge
Grundfischnachwuchs-Survey	DYFS	Nordseeküsten	3. und 4. Quartal	Scholle, Seezunge, Sandgarnele
Plattfisch-Survey Netzvergleich	SNS	IVb, IVc	3. Quartal	Seezunge, Scholle
Sandaal-Survey Nordsee	NSSS	IVa, IVb	4. Quartal	Sandaale
Internationaler Ökosystem-Survey in den nördlichen Meeresgebieten	ASH	IIa	Mai	Hering, Blauer Wittling
Rotbarsch-Survey in der Norwegischen See und in den angrenzenden Gewässern	REDNOR	II	August-September	Rotbarsch
Makreleneier-Survey (alle drei Jahre)	NSMEGS	IV	Mai-Juli	Produktion von Makreleneiern
Heringslarven-Survey	IHLS	IV,VIId	1. und 3. Quartal	Larven von Hering und Sprotte
Hydroakustik-Survey Hering Nordsee	NHAS	IIIa, IV,VIa	Juni, Juli	Hering, Sprotte
Kaisergranat-Videosurvey (FU 3&4)	NTV3&4	IIIA	2. oder 3. Quartal	Kaisergranat
Kaisergranat-Videosurvey (FU 6)	NTV6	IVb	September	Kaisergranat
Kaisergranat-Videosurvey (FU 7)	NTV7	IVa	2. oder 3. Quartal	Kaisergranat
Kaisergranat-Videosurvey (FU 8)	NTV8	IVb	2. oder 3. Quartal	Kaisergranat
Kaisergranat-Videosurvey (FU 9)	NTV9	IVa	2. oder 3. Quartal	Kaisergranat

Bezeichnung der Forschungsreise	Abkürzung	Gebiet	Zeitraum	Hauptzielarten
Nordatlantik (ICES-Gebiete V-XIV und NAFO-Gebiete)				
Internationaler Schleppnetz- und Hydroakustik-Survey auf Rotbarsch (alle zwei Jahre)	REDTAS	Va, XII, XIV; NAFO SA 1-3	Juni/Juli	Rotbarsch
Grundfisch-Survey Flämische Kappe	FCGS	3M	Juli	Grundfischarten
Grundfisch-Survey Grönland	GGS	XIV, NAFO SA1	Oktober/November	Kabeljau, Rotbarsch und andere Grundfischarten
3LNO Grundfisch-Survey	PLATUXA	NAFO 3LNO	2. und 3. Quartal	Grundfischarten
Östliche IBTS 4. Quartal (einschl. Porcupine-Survey)	IBTS Q4	VIa, VII, VIII, IXa	4. Quartal	Grundfischarten
Schottisch Western IBTS	IBTS Q1	VIa,VIIa	März	Gadidae, Hering, Makrele
ISBCBTS September	ISBCBTS	VIIa f g	September	Seezunge, Scholle
WCBTS	VIIe BTS	VIIe	Oktober	Seezunge, Scholle, Seeteufel, Limande
Blauer-Wittling-Survey		VI, VII	1. und 2. Quartal	Blauer Wittling
Internationaler Makrelen- und Stöckereier-Survey (alle drei Jahre)	MEGS	VIa, VII,VIII, IXa	Januar-Juli	Eierproduktion Makrele, Stöcker
Hydroakustik-Survey Sardine, Sardelle, Stöcker, Makrele		VIII, IX	März, April, Mai	Abundanzindizes für Sardine, Sardelle, Makrele, Stöcker
Sardine DEPM (alle drei Jahre)		VIIIc, IXa	2. und 4. Quartal	Sardine SSB und Verwendung von CUFES
Hydroakustik-Survey Hering/Eberfisch vor und während des Laichens		VIa, VIIa-g	Juli, September, November, März, Januar	Hering, Sprotte
Sardellen-Biomasse	BIOMAN	VIII	Mai	Sardelle SSB (DEP)
Kaisergranat-UW-Videosurvey (offshore)	UWTV (FU 11-13)	VIa	2. oder 3. Quartal	Kaisergranat

Bezeichnung der Forschungsreise	Abkürzung	Gebiet	Zeitraum	Hauptzielarten
Kaisergranat-UW-Videosurvey Irische See	UWTV (FU 15)	VIIa	August	Kaisergranat
Kaisergranat-UW-Videosurvey Aran Grounds	UWTV (FU 17)	VIIb	Juni	Kaisergranat
Kaisergranat-UW-Videosurvey Keltische See	UWTV (FU 20-22)	VIIg,h,j	Juli	Kaisergranat
Kaisergranat-Survey Portugal NepS (offshore)	UWTV (FU 28-29)	IXa	Juni	Kaisergranat
Mittelmeer und Schwarzes Meer				
Hydroakustik-Survey Mittelmeer ()	MEDIAS	GSA 1, 6, 7, 9, 10, 15, 16, 17, 18, 20, 22	Frühjahr-Sommer (2.-3. Quartal)	Kleine pelagische Arten
Grundschleppnetz-Survey im Schwarzen Meer	BTSBS	GSA 29	Frühjahr-Herbst (2.,3., 4. Quartal)	Steinbutt
Pelagischer Schleppnetz-Survey im Schwarzen Meer	PTSBS	GSA 29	Frühjahr-Herbst (2.,3., 4. Quartal)	Sprotte und Wittling
Internationaler Survey zur Grundschleppnetzfischerei im Mittelmeer ()	MEDITS	GSA 1, 2, 3, 5, 6, 7, 8, 9, 10, 11, 15, 16, 17, 18, 19, 20, 22, 23, 25	Frühjahr-Sommer (2.-3. Quartal)	Grundfischarten

Tabelle 11

Wirtschaftliche und soziale Variablen für den Verarbeitungssektor, die auf freiwilliger Basis erhoben werden können

Variablengruppe	Variable	Einheit
WIRTSCHAFTLICHE VARIABLEN		
Einnahmen	Umsatz	EUR
	Sonstige Erträge	EUR
Personalkosten	Personalkosten	EUR
	Wert unbezahlter Arbeit	EUR
	Zahlungen für externe Leiharbeitskräfte (fakultativ)	EUR
Energiekosten	Energiekosten	EUR
Rohstoffkosten	Kauf von Fischen und anderen Rohstoffen für die Produktion	EUR

Variablengruppe	Variable	Einheit
Sonstige Betriebskosten	Sonstige Betriebskosten	EUR
Zuschüsse	Betriebskostenzuschüsse	EUR
	Zuschüsse für Investitionen	EUR
Kapitalkosten	Abschreibungen	EUR
Kapitalwert	Gesamtwert der Vermögenswerte	EUR
Finanzergebnisse	Finanzerträge	EUR
	Ausgaben	EUR
Investitionen	Netto-Investitionen	EUR
Schulden	Schulden	EUR
Beschäftigung	Zahl der Beschäftigten	Anzahl
	VZÄ national	Anzahl
	Nicht entlohnte Arbeitskräfte	Anzahl
	Zahl der von Lohn- und Gehaltsempfängern und nicht entlohnten Arbeitskräften geleisteten Arbeitsstunden	Anzahl
Zahl der Unternehmen	Zahl der Unternehmen (1)	Anzahl
Gewicht des Ausgangserzeugnisses (FAKULTATIV)	Gewicht des Ausgangserzeugnisses, aufgeschlüsselt nach Art und Ursprung (FAKULTATIV)	Kg

SOZIALE VARIABLEN

Beschäftigung nach Geschlecht	Anzahl
Beschäftigung nach Alter	Anzahl
Beschäftigung nach Bildungsstand	Anzahl je Bildungsstand
Beschäftigung nach Staatsangehörigkeit	Anzahl pro Land in der Welt
VZÄ national	Anzahl

ISSN 1977-0642 (elektronische Ausgabe)
ISSN 1725-2539 (Papierausgabe)

Amt für Veröffentlichungen der Europäischen Union
2985 Luxemburg
LUXEMBURG

DE