DURCHFÜHRUNGSBESCHLUSS (EU) 2023/1795 DER KOMMISSION

vom 10.7.2023

gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates über die Angemessenheit des Schutzniveaus für personenbezogene Daten nach dem Datenschutzrahmen EU-USA

(Bekannt gegeben unter Aktenzeichen C(2023) 4745)

(Text von Bedeutung für den EWR)

DIE EUROPÄISCHE KOMMISSION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union,

gestützt auf die 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) ([1]), insbesondere auf Artikel 45 Absatz 3,

In Erwägung nachstehender Gründe:

1. EINLEITUNG

(1) Die Verordnung (EU) 2016/679 ([2]) enthält die Vorschriften für die Übermittlung personenbezogener Daten durch Verantwortliche oder Auftragsverarbeiter in der Union an Drittländer und internationale Organisationen, soweit die betreffenden Übermittlungen in ihren Anwendungsbereich fallen. Die Vorschriften über internationale Datenübermittlung sind in Kapitel V der Verordnung festgelegt. Der Fluss personenbezogener Daten in Drittländer und aus Drittländern ist zwar für die Ausweitung des grenzüberschreitenden Handels und der internationalen Zusammenarbeit wesentlich, dennoch darf das unionsweit gewährleistete Schutzniveau für personenbezogene Daten bei Übermittlungen in Drittländer oder an internationale Organisationen nicht untergraben werden. ([3])

(2) Nach Artikel 45 Absatz 3 der Verordnung (EU) 2016/679 kann die Kommission im Wege eines Durchführungsrechtsaktes beschließen, dass ein Drittland, ein Gebiet oder ein oder mehrere spezifische Sektoren in einem Drittland ein angemessenes Schutzniveau bieten. Unter dieser Voraussetzung können personenbezogene Daten nach Artikel 45 Absatz 1 und Erwägungsgrund 103 der Verordnung (EU) 2016/679 ohne weitere Genehmigung an ein Drittland übermittelt werden.

(3) Wie in Artikel 45 Absatz 2 der Verordnung (EU) 2016/679 festgelegt, muss die Annahme eines Angemessenheitsbeschlusses auf einer umfassenden Analyse der Rechtsordnung des Drittlands beruhen, und zwar sowohl in Bezug auf die für die Datenimporteure geltenden Vorschriften als auch auf die Einschränkungen und Garantien für den Zugang der Behörden zu personenbezogenen Daten. Im Rahmen ihrer Prüfung muss die Kommission feststellen, ob das betreffende Drittland ein Schutzniveau garantiert, das dem innerhalb der Union gewährleisteten Schutzniveau „der Sache nach gleichwertig" ist (Erwägungsgrund 104 der Verordnung (EU) 2016/679). Dies ist anhand des EU-Rechts, insbesondere der Verordnung (EU) 2016/679, sowie der Rechtsprechung des Gerichtshofs der Europäischen Union (im Folgenden „Gerichtshof") zu prüfen. ([4])

([1]) ABl. L 119 vom 4.5.2016, S. 1.
([2]) Zur besseren Übersicht enthält Anhang VIII eine Liste der in diesem Beschluss verwendeten Abkürzungen.
([3]) Siehe Erwägungsgrund 101 der Verordnung (EU) 2016/679.
([4]) Siehe zuletzt Rechtssache C-311/18, Facebook Ireland und Schrems (im Folgenden „*Schrems II*"), ECLI:EU:C:2020:559.

(4) Wie der Gerichtshof in seinem Urteil vom 6. Oktober 2015 in der Rechtssache C-362/14, Maximilian Schrems gegen Data Protection Commissioner ([5]) (Schrems), klargestellt hat, erfordert dies nicht die Feststellung eines identischen Schutzniveaus. Insbesondere können sich die Mittel, auf die das betreffende Drittland für den Schutz personenbezogener Daten zurückgreift, von denen unterscheiden, die in der Union herangezogen werden, sofern sie sich in der Praxis als wirksam erweisen, um ein angemessenes Schutzniveau zu gewährleisten. ([6]) Daher erfordert die Angemessenheitsfeststellung keine Eins-zu-eins-Übereinstimmung mit den Vorschriften der Union. Die Frage ist vielmehr, ob das ausländische System insgesamt aufgrund des Wesensgehalts der Rechte auf Privatsphäre sowie ihrer wirksamen Anwendung, Überwachung und Durchsetzung das erforderliche Maß an Schutz bietet. ([7]) Darüber hinaus sollte die Kommission nach diesem Urteil bei der Anwendung dieses Kriteriums insbesondere prüfen, ob im Rechtsrahmen des betreffenden Drittlands Regeln vorgesehen sind, die dazu dienen, 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 übermittelt werden, zu begrenzen, und ob ein wirksamer gerichtlicher Rechtsschutz gegen solche Eingriffe besteht. ([8]) Eine weitere Orientierungshilfe bietet die „Referenzgrundlage für Angemessenheit" des Europäischen Datenschutzausschusses, mit der dieser Standard weiter präzisiert werden soll. ([9])

(5) Der für solche Eingriffe in die Grundrechte auf Achtung des Privatlebens und auf Datenschutz geltende Standard wurde vom Gerichtshof in seinem Urteil vom 16. Juli 2020 in der Rechtssache C-311/18, Data Protection Commissioner/Facebook Ireland Limited und Maximilian Schrems (Schrems II), mit dem der Durchführungsbeschluss (EU) 2016/1250 der Kommission ([10]) über einen vorangegangen transatlantischen Rahmen für den Datenverkehr, den EU-US-Datenschutzschild (im Folgenden „Datenschutzschild"), für nichtig erklärt wurde, weiter präzisiert. Der Gerichtshof stellte fest, dass die Einschränkungen des Schutzes personenbezogener Daten, die sich daraus ergeben, dass die amerikanischen Behörden nach dem Recht der Vereinigten Staaten auf solche Daten, die aus der Union in die Vereinigten Staaten übermittelt werden, zugreifen und sie verwenden dürfen, nicht dergestalt geregelt sind, dass damit Anforderungen an die Erforderlichkeit und Verhältnismäßigkeit solcher Eingriffe in das Datenschutzrecht erfüllt würden, die den im Unionsrecht bestehenden Anforderungen der Sache nach gleichwertig wären. ([11]) Der Gerichtshof vertrat ferner die Auffassung, dass kein Rechtsweg zu einem Organ besteht, das den Personen, deren Daten in die Vereinigten Staaten übermittelt werden, Garantien böte, die den nach Artikel 47 der Charta über einen wirksamen Rechtsbehelf erforderlichen Garantien der Sache nach gleichwertig wären. ([12])

(6) Nach dem Urteil in der Rechtssache Schrems II nahm die Kommission Gespräche mit der US-Regierung über einen möglichen neuen Angemessenheitsbeschluss auf, der den Anforderungen des Artikels 45 Absatz 2 der Verordnung (EU) 2016/679 in der Auslegung des Gerichtshofs entsprechen würde. Als Ergebnis dieser Diskussionen erließen die Vereinigten Staaten am 7. Oktober 2022 die Executive Order 14086 „Enhancing Safeguards for US Signals Intelligence Activities" (Durchführungsverordnung 14086 „Verbesserung der Garantien für signalerfassende Aufklärung durch die USA") (im Folgenden „EO 14086"), ergänzt durch einen vom U.S. Attorney General herausgegebenen Regulation on the Data Protection Review Court (Erlass über das Datenschutzüberprüfungsgericht) (im Folgenden „Erlass des US-Justizministers"). ([13]) Darüber hinaus wurde der Rahmen, der für gewerbliche Unternehmen gilt, die im Rahmen dieses Beschlusses aus der Union übermittelte Daten verarbeiten – der „Datenschutzrahmen EU-USA" – aktualisiert.

(7) Die Kommission hat die Rechtslage und die gängige Praxis in den USA, einschließlich der EO 14086 und des Erlasses des US-Justizministers, sorgfältig analysiert. Aufgrund der in den Erwägungsgründen 9 bis 200 dargelegten Erkenntnisse gelangt die Kommission zu dem Schluss, dass die Vereinigten Staaten ein angemessenes Schutzniveau für personenbezogene Daten gewährleisten, die im Rahmen des Datenschutzrahmens EU-USA von einem Verantwortlichen oder Auftragsverarbeiter in der Europäischen Union ([14]) an zertifizierte Organisationen in den Vereinigten Staaten übermittelt werden.

([5]) Rechtssache C-362/14, Maximilian Schrems/Data Protection Commissioner (im Folgenden „Schrems"), ECLI:EU:C:2015:650, Rn. 73.

([6]) Schrems, Rn. 74.

([7]) Siehe Mitteilung der Kommission an das Europäische Parlament und den Rat „Austausch und Schutz personenbezogener Daten in einer globalisierten Welt" (COM(2017) 7 vom 10.1.2017, Abschnitt 3.1, S. 6).

([8]) Schrems, Rn. 88–89.

([9]) Europäischer Datenschutzausschuss, Referenzgrundlage für Angemessenheit, WP 254/rev.01, abrufbar unter folgendem Link: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108.

([10]) 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 (ABl. L 207 vom 1.8.2016, S. 1).

([11]) Schrems II, Rn. 185.

([12]) Schrems II, Rn. 197.

([13]) 28 CFR Teil 302.

([14]) Dieser Beschluss ist von Bedeutung für den EWR. Das Abkommen über den Europäischen Wirtschaftsraum (EWR-Abkommen) regelt die Einbeziehung der drei EWR-Staaten Island, Liechtenstein und Norwegen in den Binnenmarkt der Europäischen Union. Der Beschluss des Gemeinsamen Ausschusses zur Aufnahme der Verordnung (EU) 2016/679 in Anhang XI des EWR-Abkommens wurde am 6. Juli 2018 vom Gemeinsamen EWR-Ausschuss angenommen und ist am 20. Juli 2018 in Kraft getreten. Die Verordnung fällt somit unter das genannte Abkommen. Für die Zwecke des Beschlusses sollten daher Verweise auf die EU und die EU-Mitgliedstaaten so verstanden werden, dass sie auch die EWR-Staaten umfassen.

(8) Der Beschluss hat zur Folge, dass die Übermittlung personenbezogener Daten von Verantwortlichen und Auftragsverarbeitern in der Union ([15]) an zertifizierte Organisationen in den Vereinigten Staaten ohne weitere Genehmigung vorgenommen werden kann. Er wirkt sich nicht auf die unmittelbare Anwendung der Verordnung (EU) 2016/679 auf derartige Organisationen aus, wenn die in Artikel 3 der Verordnung festgelegten Bedingungen für den räumlichen Anwendungsbereich der Verordnung erfüllt sind.

2. DER DATENSCHUTZRAHMEN EU-USA

2.1 Persönlicher und sachlicher Anwendungsbereich

2.1.1 *Zertifizierte Organisationen*

(9) Der Datenschutzrahmen EU-USA basiert auf einem Zertifizierungssystem, mit dem sich US-Organisationen zu einer Reihe von Datenschutzgrundsätzen verpflichten – die „Grundsätze des Datenschutzrahmens EU-USA", einschließlich der Zusatzgrundsätze (im Folgenden zusammen „Grundsätze") – herausgegeben vom U.S. Department of Commerce (Handelsministerium) und in Anhang I dieses Beschlusses enthalten. ([16]) Um für eine Zertifizierung im Rahmen des Datenschutzrahmens EU-USA infrage zu kommen, muss eine Organisation den Untersuchungs- und Durchsetzungsbefugnissen der Federal Trade Commission (FTC) oder des U.S. Department of Transportation (Verkehrsministerium) ([17]) unterliegen. Die Grundsätze gelten unmittelbar vom Zeitpunkt der Zertifizierung an. Wie in den Erwägungsgründen 48 bis 52 näher erläutert wird, sind die Organisationen des Datenschutzrahmens EU-USA verpflichtet, ihre Einhaltung der Grundsätze jährlich neu zertifizieren. ([18])

2.1.2 *Bestimmung der Begriffe „personenbezogene Daten" sowie „Verantwortlicher" und „Beauftragter"*

(10) Der durch den Datenschutzrahmen EU-USA gewährte Schutz gilt für alle personenbezogenen Daten, die aus der Union an Organisationen in den Vereinigten Staaten übermittelt werden, die sich gegenüber dem Handelsministerium zur Einhaltung der Grundsätze verpflichtet haben, mit Ausnahme von Daten, die zum Zwecke der Veröffentlichung, Verbreitung über Rundfunk und Fernsehen oder für andere Formen öffentlicher Kommunikation von journalistischem Material und von Informationen in bereits veröffentlichtem Material aus Medienarchiven erhoben werden. ([19]) Solche Informationen können daher nicht auf der Grundlage des Datenschutzrahmens EU-USA übermittelt werden.

(11) Die Grundsätze definieren personenbezogene Daten/personenbezogene Informationen in derselben Weise wie die Verordnung (EU) 2016/679, d. h. als „in beliebiger Form aufgezeichnete Daten über eine identifizierte oder identifizierbare Person, die unter die DGSVO fallen und aus der Europäischen Union an eine Organisation in den Vereinigten Staaten übermittelt werden". ([20]) Folglich umfassen sie auch pseudonymisierte (oder „verschlüsselte") Forschungsdaten (selbst wenn der Schlüssel nicht mit der empfangenden US-Organisation geteilt wird). ([21]) Ebenso bezeichnet der Begriff „Verarbeitung" „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". ([22])

(12) Der Datenschutzrahmen EU-USA gilt für Organisationen in den USA, die als Verantwortliche (d. h. die Person oder Organisation, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet) ([23]) oder als Auftragsverarbeiter (d. h. Beauftragte, die im Auftrag des Verantwortlichen handeln) ([24]) gelten. Auftragsverarbeiter in den USA müssen sich vertraglich verpflichten, nur auf

([15]) Dieser Beschluss berührt nicht die Anforderungen der Verordnung (EU) 2016/679, die für die Daten übermittelnden Rechtsträger (Verantwortliche und Auftragsverarbeiter) in der Union gelten, z. B. in Bezug auf Zweckbindung, Datenminimierung, Transparenz und Datensicherheit (siehe auch Artikel 44 der Verordnung (EU) 2016/679).

([16]) Siehe hierzu die Rechtssache Schrems Rn. 81, in der der Gerichtshof bestätigt, dass ein System der Selbstzertifizierung ein angemessenes Schutzniveau gewährleisten kann.

([17]) Anhang I Abschnitt I.2. Die FTC verfügt über eine weitreichende Zuständigkeit im wirtschaftlichen Bereich, abgesehen von einigen Einschränkungen ihrer Kompetenzen, die z. B. den Bankensektor, den Luftverkehr, das Versicherungsgewerbe und die Betreiber öffentlicher Telekommunikationsnetze betreffen (obwohl in der Entscheidung des U.S. Court of Appeals for the Ninth Circuit (Berufungsgericht) vom 26. Februar 2018 in der Rechtssache FTC v. AT&T bestätigt wurde, dass die FTC für die nicht-öffentlichen Telekommunikationsnetze solcher Betreiber zuständig ist). Siehe auch Anhang IV Fußnote 2. Das Verkehrsministerium ist für die Durchsetzung der Einhaltung durch Fluggesellschaften und Verkaufsstellen (für Flugtickets) zuständig, siehe Anhang V Abschnitt A.

([18]) Anhang I Abschnitt III.6.

([19]) Anhang I Abschnitt III.2.

([20]) Anhang I Abschnitt I.8.a.

([21]) Anhang I Abschnitt III.14.g.

([22]) Anhang I Abschnitt I.8.b.

([23]) Anhang I Abschnitt I.8.c.

([24]) Siehe z. B. Anhang I Abschnitt II.2.b und Abschnitt II.3.b und 7.d, in denen klargestellt wird, dass Beauftragte im Auftrag des Verantwortlichen handeln sowie dessen Weisungen und besonderen vertraglichen Verpflichtungen unterliegen.

Weisung des Verantwortlichen in der EU zu handeln und Letzteren dabei zu unterstützen, Privatpersonen die Wahrnehmung ihrer Rechte im Rahmen der Grundsätze zu erleichtern. ([25]) Darüber hinaus muss ein Auftragsverarbeiter im Falle der Unterauftragsverarbeitung einen Vertrag mit dem Unterauftragsverarbeiter abschließen, der das gleiche Schutzniveau sicherstellt, wie es die Grundsätze bieten, und für dessen ordnungsgemäße Umsetzung sorgen. ([26])

2.2 **Grundsätze des Datenschutzrahmens EU-USA**

2.2.1 ***Zweckbindung und Auswahl***

(13) Die Verarbeitung personenbezogener Daten sollte rechtmäßig und nach Treu und Glauben erfolgen. Personenbezogene Daten sollten für einen bestimmten Zweck erhoben und anschließend nur verwendet werden, soweit dies mit dem Zweck der Verarbeitung nicht unvereinbar ist.

(14) Im Rahmen des Datenschutzrahmens EU-USA wird dies durch verschiedene Grundsätze sichergestellt. Erstens darf eine Organisation nach dem Grundsatz der *Datenintegrität und Zweckbindung*, ähnlich wie nach Artikel 5 Absatz 1 Buchstabe b der Verordnung (EU) 2016/679, personenbezogene Daten nicht in einer Weise verarbeiten, die mit dem ursprünglichen Erhebungszweck oder mit dem Zweck unvereinbar ist, dem der Betroffene nachträglich zugestimmt hat. ([27])

(15) Zweitens muss die Organisation vor der Verwendung personenbezogener Daten für einen neuen (geänderten) Zweck, der sich deutlich von dem ursprünglichen Zweck unterscheidet, aber mit diesem dennoch vereinbar ist, oder vor der Offenlegung der Daten gegenüber einem Dritten, den betroffenen Personen die Möglichkeit geben, nach dem *Grundsatz der Wahlmöglichkeit* ([28]) durch ein leicht erkennbares, verständliches und leicht zugängliches Verfahren Widerspruch einzulegen (Opt-out). Wichtig ist, dass dieser Grundsatz das ausdrückliche Verbot einer unzulässigen Verarbeitung nicht aufhebt. ([29])

([25]) Anhang I Abschnitt III.10.a. Siehe auch die vom Handelsministerium in Abstimmung mit dem Europäischen Datenschutzausschuss hinsichtlich des Datenschutzschilds ausgearbeiteten Leitlinien, in denen die Pflichten von US-Auftragsverarbeitern präzisiert werden, die im Rahmen des Datenschutzschilds personenbezogene Daten aus der Union erhalten. Da sich diese Vorschriften nicht geändert haben, bleiben diese Leitlinien/FAQ im Rahmen des Datenschutzrahmens EU-USA relevant (https://www.privacyshield.gov/article?id=Processing-FAQs).

([26]) Anhang I Abschnitt II.3.b.

([27]) Anhang I Abschnitt II.5.a. Zu den kompatiblen Zwecken können Wirtschaftsprüfung, Betrugsprävention oder andere Zwecke gehören, die nach vernünftigem Ermessen den Erwartungen im Zusammenhang mit der Erhebung entsprechen (siehe Anhang I, Fußnote 6).

([28]) Anhang I Abschnitt II.2.a. Dies gilt nicht, wenn eine Organisation personenbezogene Daten an einen Auftragsverarbeiter weitergibt, der im Auftrag und nach Weisung der Organisation handelt (Anhang I Abschnitt II.2.b). In diesem Fall muss die Organisation jedoch einen Vertrag abschließen und die Einhaltung des Grundsatzes der *Verantwortlichkeit für die Weitergabe* sicherstellen, wie in Erwägungsgrund 43 näher beschrieben. Darüber hinaus kann der Grundsatz der *Wahlmöglichkeit* (ebenso wie der Grundsatz der *Informationspflicht*) eingeschränkt werden, wenn personenbezogene Daten im Rahmen von Due-Diligence-Prüfungen (im Zusammenhang mit einer potenziellen Fusion oder Übernahme) oder Wirtschaftsprüfungen verarbeitet werden, und zwar soweit und solange das aufgrund gesetzlicher oder im öffentlichen Interesse liegender Erfordernisse notwendig ist, oder soweit und solange die Anwendung dieser Grundsätze den legitimen Interessen der Organisation im spezifischen Kontext der Due-Diligence-Prüfungen oder Wirtschaftsprüfungen zuwiderlaufen würde (Anhang I Abschnitt III.4). Im Zusatzgrundsatz 15 (Anhang I, Abschnitt III.15.a und Abschnitt III.15.b) ist auch eine Ausnahme vom Grundsatz der *Wahlmöglichkeit* (sowie von den Grundsätzen der *Informationspflicht* und der *Verantwortlichkeit für die Weitergabe*) für personenbezogene Daten aus öffentlich zugänglichen Quellen vorgesehen (es sei denn, der EU-Datenexporteur weist darauf hin, dass die Daten Einschränkungen unterliegen, die die Anwendung dieser Grundsätze erforderlich machen) oder für personenbezogene Daten, die aus öffentlich zugänglichen Datenbeständen erhoben wurden (sofern sie nicht mit nichtöffentlichen Datenbeständen kombiniert werden und alle Bedingungen für ihre Abfrage erfüllt sind). In ähnlicher Weise enthält der Zusatzgrundsatz 14 (Anhang I Abschnitt III.14.f) eine Ausnahme vom *Grundsatz der Wahlmöglichkeit* (sowie von den Grundsätzen der *Informationspflicht* und der *Verantwortlichkeit für die Weitergabe*) für die Verarbeitung personenbezogener Daten durch die Hersteller von Arzneimitteln oder Medizinprodukten zum Zwecke der Überwachung der Sicherheit und Wirksamkeit von Produkten, soweit die Einhaltung der Grundsätze mit gesetzlichen Pflichten kollidieren würde.

([29]) Dies betrifft alle Datenübermittlungen im Rahmen des Datenschutzrahmens EU-USA, auch wenn es um Daten geht, die im Rahmen des Beschäftigungsverhältnisses erhoben wurden. Zwar kann eine zertifizierte 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. In Ausnahmefällen darf eine Organisation personenbezogene Daten für einen zusätzlichen, kompatiblen Zweck verwenden, ohne die Grundsätze der *Informationspflicht* und *Wahlmöglichkeit* einzuhalten, jedoch nur in dem Umfang und für den Zeitraum, der erforderlich ist, dass die Fähigkeit der Organisation, Beförderungen, Ernennungen oder ähnliche Beschäftigungsentscheidungen vorzunehmen, nicht beeinträchtigt wird (siehe Anhang I Abschnitt III.9.b.(iv)). 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. Siehe Anhang I Abschnitt III.9.b.(i).

2.2.2 ***Verarbeitung besonderer Kategorien von personenbezogenen Daten***

(16) Betrifft die Verarbeitung besondere Kategorien personenbezogener Daten, sollten besondere Garantien bestehen.

(17) Im Einklang mit dem *Grundsatz der Wahlmöglichkeit* gelten besondere Garantien für die Verarbeitung „sensibler Informationen", 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 der betroffenen Person oder sonstige von Dritten übermittelte Informationen, die der Übermittler als sensibel einstuft und behandelt. ([30]) Dies bedeutet, dass alle Daten, die nach dem Datenschutzrecht der Union als sensibel gelten (einschließlich Daten über die sexuelle Orientierung, genetische Daten und biometrische Daten), nach dem Datenschutzrahmen EU-USA von zertifizierten Organisationen als sensibel behandelt werden.

(18) In der Regel müssen Organisationen die ausdrückliche Zustimmung (d. h. Opt-in) von Privatpersonen einholen, um sensible Daten für einen anderen als den ursprünglichen Erhebungszweck oder für den Zweck zu verwenden, dem die betroffene Person nachträglich (durch Opt-in) zugestimmt hat oder um die Daten an Dritte weiterzugeben. ([31])

(19) Eine solche Zustimmung muss nicht eingeholt werden, wenn bestimmte Umstände vorliegen, die vergleichbaren Ausnahmen im Datenschutzrecht der Union entsprechen, z. B. wenn die Verarbeitung sensibler Daten im lebenswichtigen Interesse einer Person liegt, zur Geltendmachung von Rechtsansprüchen oder für die medizinische Versorgung oder Diagnose erforderlich ist. ([32])

2.2.3 ***Richtigkeit der Daten, Datenminimierung und Datensicherheit***

(20) Daten müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein. Ferner müssen sie dem Zweck angemessen und dafür erheblich sein und dürfen das für die Zwecke der Verarbeitung notwendige Maß nicht überschreiten und sollten grundsätzlich nicht länger gespeichert werden, als dies für den Zweck, zu dem sie verarbeitet werden, erforderlich ist.

(21) Nach dem *Grundsatz der Datenintegrität und Zweckbindung* ([33]) müssen personenbezogene Daten darauf beschränkt werden, was für den Zweck der Verarbeitung erheblich ist. Darüber hinaus müssen die Organisationen, in dem für die Zwecke der Verarbeitung erforderlichen Ausmaß, vernünftige Maßnahmen treffen, um sicherzustellen, dass personenbezogene Daten für den vorgesehenen Zweck hinreichend zuverlässig, genau, vollständig und aktuell sind.

(22) Darüber hinaus dürfen personenbezogene Daten nur so lange in einer Form gespeichert werden, durch die eine Person identifiziert wird oder identifizierbar wird (d. h. als personenbezogene Daten) ([34]), wie dies dem Zweck bzw. den Zwecken dient, für den bzw. die sie ursprünglich erhoben wurden oder zu dem bzw. denen die Person nach dem *Grundsatz der Wahlmöglichkeit* nachträglich zugestimmt hat. Diese Verpflichtung hindert die Organisationen nicht daran, personenbezogene Daten über längere Zeiträume weiter zu verarbeiten, jedoch nur solange und soweit die Verarbeitung nach vernünftigem Ermessen einem der folgenden spezifischen Zwecke dient, die vergleichbaren Ausnahmen nach dem Datenschutzrecht der Union entsprechen: Archivierung im öffentlichen Interesse, Journalismus, Literatur und Kunst, wissenschaftliche und historische Forschung und statistische Analyse. ([35]) Werden personenbezogene Daten für einen dieser Zwecke gespeichert, so unterliegt ihre Verarbeitung den in den Grundsätzen enthaltenen Garantien. ([36])

(23) Personenbezogene Daten müssen zudem in einer Weise verarbeitet werden, die ihre Sicherheit gewährleistet, einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung. Zu diesem Zweck müssen Verantwortliche und Auftragsverarbeiter geeignete technische oder organisatorische Maßnahmen treffen, um personenbezogene Daten vor möglichen Bedrohungen zu schützen. Diese Maßnahmen sollten unter Berücksichtigung des Stands der Technik, der mit ihnen verbundenen Kosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Risiken für die Rechte des Einzelnen bewertet werden.

([30]) Anhang I Abschnitt II.2.c.
([31]) Anhang I Abschnitt II.2.c.
([32]) Anhang I Abschnitt III.1.
([33]) Anhang I Abschnitt II.5.
([34]) Siehe Anhang I Fußnote 7, in der klargestellt wird, dass eine Person als „identifizierbar" gilt, solange eine Organisation oder ein Dritter diese Person 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) nach vernünftigem Ermessen identifizieren kann.
([35]) Anhang I Abschnitt II.5.b.
([36]) *Ebd.*

(24) Im Datenschutzrahmen EU-USA wird dies durch den *Grundsatz der Sicherheit* gewährleistet, wonach, ähnlich wie in Artikel 32 der Verordnung (EU) 2016/679, angemessene und geeignete Sicherheitsvorkehrungen zu treffen sind, mit denen den mit der Verarbeitung verbundenen Risiken und der Art der Daten Rechnung getragen wird. ([37])

2.2.4 ***Transparenz***

(25) Betroffene Personen müssen über die Hauptmerkmale der Verarbeitung ihrer personenbezogenen Daten unterrichtet werden.

(26) Dies wird durch den *Grundsatz der Informationspflicht* ([38]) gewährleistet, der ähnlich den Transparenzanforderungen der Verordnung (EU) 2016/679 von den Organisationen verlangt, die betroffenen Personen unter anderem über Folgendes zu unterrichten: i) die Tatsache, dass die Organisation dem Datenschutzrahmen unterliegt, ii) die Art der erhobenen Daten, iii) den Zweck der Verarbeitung, iv) die Art oder Identität von Dritten, denen personenbezogene Daten offengelegt werden können, und den Zweck der Offenlegung, v) ihre individuellen Rechte, vi) wie die Organisation kontaktiert werden kann und vii) verfügbare Rechtsbehelfe.

(27) Diese Angaben sind den Betroffenen unmissverständlich und deutlich erkennbar zu machen, wenn die betroffenen Personen zum ersten Mal zur Bereitstellung personenbezogener Daten aufgefordert werden oder so bald wie möglich danach, auf jeden Fall aber, bevor die Daten für einen wesentlich anderen (aber kompatiblen) Zweck als den, für den sie erhoben wurden, verwendet oder an Dritte weitergegeben werden. ([39])

(28) Darüber hinaus müssen die Organisationen ihre Datenschutzbestimmungen, in denen die Grundsätze ihren Niederschlag finden, offenlegen (oder im Falle von Personaldaten den betroffenen Personen leicht zugänglich machen) und Links zur Website des Handelsministeriums (wo weitere Angaben zur Zertifizierung, zu den Rechten der betroffenen Personen und zu verfügbaren Rechtsbehelfen zu finden sind), zu der Liste der am Datenschutzrahmen teilnehmenden Organisationen (im Folgenden „Datenschutzrahmen-Liste“) und zur Website eines geeigneten Anbieters alternativer Streitbeilegungsverfahren bereitstellen. ([40])

2.2.5 ***Rechte des Einzelnen***

(29) Betroffene Personen sollten bestimmte Rechte besitzen, die gegenüber dem Verantwortlichen oder dem Auftragsverarbeiter durchgesetzt werden können, insbesondere ein Auskunftsrecht, das Recht, der Verarbeitung zu widersprechen, und das Recht auf Berichtigung und Löschung von Daten.

(30) Das *Auskunftsrecht* ([41]) des Datenschutzrahmens EU-USA räumt dem Einzelnen diese Rechte ein. Insbesondere haben betroffene Personen das Recht, ohne Angabe von Gründen von einer Organisation die Auskunft einzuholen, ob die Organisation sie betreffende personenbezogene Daten verarbeitet, sich die Daten binnen einer angemessenen Frist übermitteln zu lassen und Auskunft über den Zweck der Verarbeitung, die Kategorien personenbezogener Daten, die verarbeitet werden, und die (Kategorien von) Empfängern, denen die Daten offengelegt werden, zu erhalten. ([42]) Die Organisationen sind verpflichtet, Auskunftsersuchen innerhalb einer angemessenen Frist zu beantworten. ([43]) Eine

([37]) Anhang I Abschnitt II.4.a. Darüber hinaus müssen Arbeitgeber in Bezug auf Personaldaten nach dem Datenschutzrahmen EU-USA 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 (Anhang I Abschnitt III.9.b.(iii)).

([38]) Anhang I Abschnitt II.1.

([39]) Anhang I Abschnitt II.1.b. Der Zusatzgrundsatz 14 (Anhang I Abschnitt III.14.b und Abschnitt III.14.c) enthält besondere Bestimmungen für die Verarbeitung personenbezogener Daten im Rahmen von Gesundheitsforschung und klinischen Versuchen. Insbesondere erlaubt dieser Grundsatz Organisationen, Daten aus klinischen Versuchen auch dann noch zu verarbeiten, wenn sich eine Person aus dem Versuch zurückzieht, wenn sie darauf hingewiesen wurde, als sie ihre Bereitschaft zur Teilnahme erklärte. Ebenso darf eine Organisation, die dem Datenschutzrahmen EU-USA angehört und personenbezogene Daten für Zwecke der Gesundheitsforschung erhält, diese Daten nur für neue Forschungszwecke in Übereinstimmung mit den Grundsätzen der *Informationspflicht* und der *Wahlmöglichkeit* verwenden. In diesem Fall sollte die Benachrichtigung der betroffenen Person grundsätzlich Informationen über die künftige spezifische Verwendung der Daten (z. B. für Studien) enthalten. Wenn es nicht möglich ist, von vornherein alle künftigen Verwendungszwecke der Daten einzubeziehen (weil sich aus neuen Erkenntnissen oder Entwicklungen in der Medizin/Forschung ein neuer Verwendungszweck ergeben könnte), muss darauf hingewiesen werden, dass die Daten in künftigen, nicht vorhersehbaren medizinischen und pharmazeutischen Forschungsarbeiten verwendet werden können. Entspricht die neue Verwendung nicht dem allgemeinen Forschungszweck, für den die personenbezogenen Daten ursprünglich erhoben wurden (d. h., wenn die neuen Zwecke sich wesentlich unterscheiden, aber dennoch mit dem ursprünglichen Zweck vereinbar sind, siehe die Erwägungsgründe 14 und 15), muss erneut eine Zustimmung (z. B. Opt-in) eingeholt werden. Siehe auch die spezifischen Einschränkungen/Ausnahmen vom Grundsatz der *Informationspflicht* in Fußnote 28.

([40]) Anhang I Abschnitt III.6.d.

([41]) Siehe auch Zusatzgrundsatz „Auskunftsrecht“ (Anhang II Abschnitt III.8).

([42]) Anhang I Abschnitt III.8.a.(i)-(ii).

([43]) Anhang I Abschnitt III.8.i.

Organisation kann die Anzahl der Auskunftsersuchen einer bestimmten Person innerhalb eines bestimmten Zeitraums angemessen begrenzen und eine Gebühr erheben, die nicht überhöht sein darf, z. B. wenn die Auskunftsersuchen offensichtlich überzogen sind, insbesondere bei ständiger Wiederholung. ([44])

(31) Das Auskunftsrecht darf nur unter außergewöhnlichen Umständen eingeschränkt werden, die den im Datenschutzrecht der Union vorgesehenen Umständen ähnlich sind, insbesondere wenn die legitimen Rechte anderer Personen verletzt würden, wenn die Belastung oder die Kosten für die Gewährung des Zugangs zu den Daten in einem Missverhältnis zu den Risiken für die Privatsphäre der betroffenen Person stehen (obwohl Kosten und Aufwand bei der Beurteilung der Angemessenheit der Gewährung des Zugangs nicht ausschlaggebend sind), insoweit, als ihre Bekanntgabe wesentliche öffentliche Belange gefährden würde wie die nationale Sicherheit, die Verteidigung oder die öffentliche Sicherheit, die Daten vertrauliche Geschäftsinformationen enthalten oder die Daten ausschließlich zu Forschungs- oder statistischen Zwecken verarbeitet werden. ([45]) Jede Verweigerung oder Einschränkung des Auskunftsrechts muss notwendig und hinreichend gerechtfertigt sein, wobei die Organisation die Beweislast dafür trägt, dass die Voraussetzungen erfüllt sind. ([46]) Bei dieser Beurteilung hat die Organisation insbesondere die Interessen des Einzelnen zu berücksichtigen. ([47]) Wenn sich bestimmte Daten von anderen Daten, für die eine Einschränkung gilt, trennen lassen, muss die Organisation die geschützten Daten unkenntlich machen und die übrigen Daten offenlegen. ([48])

(32) Darüber hinaus haben die betroffenen Personen das Recht, die Berichtigung oder Änderung unrichtiger Daten sowie die Löschung von unter Verstoß gegen die Grundsätze verarbeiteter Daten zu verlangen. ([49]) Wie in Erwägungsgrund 15 erläutert, haben natürliche Personen auch das Recht, der Verarbeitung ihrer Daten für Zwecke, die sich wesentlich von den Zwecken, für die die Daten erhoben wurden, unterscheiden (aber damit vereinbar sind), und der Weitergabe ihrer Daten an Dritte zu widersprechen. Werden personenbezogene Daten zu Zwecken der Direktwerbung verwendet, hat der Einzelne das allgemeine Recht, der Verarbeitung jederzeit zu widersprechen. ([50])

(33) Die Grundsätze befassen sich nicht speziell mit der Problematik von Entscheidungen, die sich auf die betroffene Person auswirken und ausschließlich auf der automatisierten Verarbeitung personenbezogener Daten beruhen. Bei personenbezogenen Daten, die in der Union erhoben wurden, wird jedoch jede Entscheidung, die auf einer automatisierten Verarbeitung beruht, typischerweise vom Verantwortlichen in der Union getroffen (der eine direkte Beziehung zu der betroffenen Person unterhält) und unterliegt somit unmittelbar der Verordnung (EU) 2016/679. ([51]) Dazu gehören auch Übermittlungsszenarien, bei denen die Verarbeitung von einem ausländischen (z. B. US-amerikanischen) Unternehmer vorgenommen wird, der als Beauftragter (Auftragsverarbeiter) im Namen des Verantwortlichen in der EU (oder als Unterauftragsverarbeiter im Namen des Auftragsverarbeiters in der EU, der die Daten von einem Verantwortlichen in der EU erhalten hat, der sie erhoben hat) handelt, der dann auf dieser Grundlage die Entscheidung trifft.

(34) Dies wurde durch eine von der Kommission 2018 im Rahmen der zweiten jährlichen Überprüfung der Funktionsweise des Datenschutzschilds ([52]) in Auftrag gegebene Studie bestätigt, in der festgestellt wurde, dass es zum damaligen Zeitpunkt keine Belege dafür gab, dass die unter dem Datenschutzschild tätigen Organisationen in der Regel automatisierte Entscheidungen auf der Grundlage der im Rahmen des Datenschutzschilds übermittelten personenbezogenen Daten treffen.

([44]) Anhang I Abschnitt III.8.f.(i)-(ii) und Abschnitt III.8.g.

([45]) Anhang I Abschnitt III.4; Abschnitt III.8.b, c, e; Abschnitt III.14.e, f und Abschnitt III.15.d.

([46]) Anhang I Abschnitt III.8.e.(ii). Die Organisation muss die betroffene Person über die Gründe für die Verweigerung/Einschränkung informieren und eine Kontaktstelle für Rückfragen angeben (Abschnitt III.8.a.(iii)).

([47]) Anhang I Abschnitt III.8.a.(ii)-(iii).

([48]) Anhang I Abschnitt III.8.a.(i).

([49]) Anhang I Abschnitt II.6 und Abschnitt III.8.a.(i).

([50]) Anhang I Abschnitt III.8.12.

([51]) Hingegen wird dies in dem Ausnahmefall, dass die US-Organisation eine direkte Beziehung zu der betroffenen Person in der Union unterhält, typischerweise darauf zurückzuführen sein, dass sie die Person in der Union gezielt angesprochen hat, indem sie ihr Waren oder Dienstleistungen angeboten oder ihr Verhalten beobachtet hat. In diesem Szenario gilt für die US-Organisation selbst die Verordnung (EU) 2016/679 (Artikel 3 Absatz 2), sodass sie das EU-Datenschutzrecht unmittelbar einhalten muss.

([52]) SWD(2018) 497 final, Abschnitt 4.1.5. Der Schwerpunkt der Studie lag auf i) dem Ausmaß, in dem Organisationen in den USA, die im Rahmen des Datenschutzschilds tätig sind, personenbezogene Entscheidungen auf der Grundlage der automatisierten Verarbeitung personenbezogener Daten treffen, die von Unternehmen in der EU im Rahmen des Datenschutzschilds übermittelt wurden, und ii) den Schutzvorkehrungen für Privatpersonen, die das US-Bundesrecht für diese Art von Situationen vorsieht, und den Bedingungen für die Anwendung dieser Schutzvorkehrungen.

(35) In jedem Fall bietet das US-Recht 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, Wohnungswesen und Versicherungen), spezifische Schutzvorkehrungen bei ablehnenden Entscheidungen. ([53]) 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. Im Bereich des Verbraucherkredits enthalten der Fair Credit Reporting Act (Gesetz zur Regelung des Datenschutzes bei Konsumentenkrediten, im Folgenden „FCRA") und der Equal Credit Opportunity Act (Gesetz über die Chancengleichheit bei der Kreditvergabe, im Folgenden „ECOA") Schutzbestimmungen, die dem Verbraucher eine Art Erklärungs- und Widerspruchsrecht einräumen. Diese Gesetze sind für eine Vielzahl von Bereichen von Bedeutung, darunter Kredite, Stellenbesetzung, Wohnungswesen und Versicherungen. Darüber hinaus bieten bestimmte Antidiskriminierungsgesetze, wie Titel VII des Civil Rights Act (Gesetz zum Schutz der Bürgerrechte) und der Fair Housing Act (Gesetz über fairen Wohnraum), Privatpersonen Schutz vor Modellen, die bei der automatisierten Entscheidungsfindung verwendet werden und zu Diskriminierung aufgrund bestimmter Merkmale führen können, und geben Privatpersonen das Recht, solche Entscheidungen, einschließlich automatisierter Entscheidungen, anzufechten. In Bezug auf Gesundheitsinformationen gewährt der Health Insurance Portability and Accountability Act (Gesetz über die Übertragbarkeit und Rechenschaftspflicht von Krankenversicherungen, im Folgenden „HIPAA") bestimmte Rechte, die denen in Verordnung (EU) 2016/679 in Bezug auf den Zugang zu persönlichen Gesundheitsinformationen ähnlich sind. Darüber hinaus verlangen die US-Behörden in ihren Leitlinien, dass medizinische Dienstleister Informationen erhalten, die sie in die Lage versetzen, Privatpersonen über Systeme zur automatisierten Entscheidungsfindung zu informieren, die im medizinischen Bereich eingesetzt werden. ([54])

(36) In dem unwahrscheinlichen Fall, dass die dem Datenschutzrahmen EU-USA angehörende Organisation selbst automatisierte Entscheidungen trifft, bieten diese Bestimmungen daher einen ähnlichen Schutz wie das EU-Datenschutzrecht.

2.2.6 ***Einschränkungen für Weitergaben***

(37) Das Schutzniveau für personenbezogene Daten, die aus der Union an Organisationen in den Vereinigten Staaten übermittelt werden, darf nicht durch die Weitergabe dieser Daten an Empfänger in den USA oder einem anderen Drittland beeinträchtigt werden.

(38) Nach dem *Grundsatz der Verantwortlichkeit für die Weitergabe* ([55]) gelten besondere Regeln für die sogenannte „Weitergabe", d. h. die Übermittlung personenbezogener Daten von einer dem Datenschutzrahmen EU-USA angehörenden Organisation an einen als Verantwortlicher oder Auftragsverarbeiter fungierenden Dritten, unabhängig davon, ob Letzterer sich in den USA oder einem Drittstaat außerhalb der USA (und der Union) befindet. Eine Weitergabe darf nur erfolgen i) für begrenzte und genau festgelegte Zwecke, ii) auf der Grundlage eines Vertrags zwischen der Organisation, die dem Datenschutzrahmen EU-USA angehört, und dem Dritten ([56]) (oder einer vergleichbaren Vereinbarung innerhalb einer Unternehmensgruppe ([57])) und iii) nur, wenn dieser Vertrag den Dritten verpflichtet, das gleiche Schutzniveau zu gewährleisten, das durch die Grundsätze garantiert wird.

(39) Diese Verpflichtung, das gleiche Schutzniveau wie die Grundsätze zu gewährleisten, bedeutet in Verbindung mit dem *Grundsatz der Datenintegrität und der Zweckbindung* insbesondere, dass der Dritte die ihm übermittelten personenbezogenen Daten nur für Zwecke verarbeiten darf, die nicht mit den Zwecken unvereinbar sind, für die sie erhoben wurden oder nachträglich vom Betroffenen autorisiert wurden (nach dem *Grundsatz der Wahlmöglichkeit*).

([53]) Siehe z. B. Equal Credit Opportunity Act (15 U.S.C. 1691 ff.), Fair Credit Reporting Act (15 USC § 1681 ff.) oder Fair Housing Act (42 U.S.C. 3601 ff.). Darüber hinaus haben sich die USA den KI-Prinzipien der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung angeschlossen, die u. a. Grundsätze zu Transparenz, Erklärbarkeit, Sicherheit und Rechenschaftspflicht enthalten.

([54]) Siehe z. B. die Leitlinien unter 2042-What personal health information do individuals have a right under HIPAA to access from their health care providers and health plans? | HHS.gov.

([55]) Siehe Anhang I Abschnitt II.3 und Zusatzgrundsatz „Obligatorische Verträge bei Weitergabe" (Anhang II Abschnitt III.10).

([56]) Als Ausnahme von diesem allgemeinen Grundsatz kann eine Organisation personenbezogene Daten an eine kleine Anzahl von Mitarbeitern weitergeben, ohne einen Vertrag mit dem Empfänger zu schließen, wenn es sich um gelegentliche betriebliche Erfordernisse im Zusammenhang mit der Beschäftigung handelt, wie z. B. die Buchung eines Fluges, eines Hotelzimmers oder den Abschluss von Versicherungen. Aber auch in diesem Fall muss die Organisation die Grundsätze der *Informationspflicht* und der *Wahlmöglichkeit* einhalten (siehe Anhang I Abschnitt III.9.e).

([57]) Siehe Zusatzgrundsatz „Obligatorische Verträge bei Weitergabe" (Anhang I 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 zertifizierten 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.

(40) Der *Grundsatz der Verantwortlichkeit für die Weitergabe* ist auch in Verbindung mit dem *Grundsatz der Informationspflicht* und bei der Weitergabe an einen als Verantwortlichen fungierenden Dritten ([58]), dem *Grundsatz der Wahlmöglichkeit* zu sehen, wonach betroffene Personen (unter anderem) über die Art/Identität des Drittempfängers, den Zweck der Weitergabe und 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).

(41) 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 den 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.

(42) In allen Fällen muss der Vertrag mit dem Drittempfänger die Bestimmung enthalten, dass Letzterer die dem Datenschutzrahmen EU-USA angehörende Organisation benachrichtigt, wenn er zu dem Schluss kommt, dass er diese Verpflichtung nicht länger einhalten kann. Wenn diese Situation eintritt, muss die Verarbeitung durch den Dritten eingestellt oder es müssen andere sinnvolle und geeignete Schritte unternommen werden, um Abhilfe zu schaffen. ([59])

(43) Zusätzliche Schutzmaßnahmen sind für den Fall der Weitergabe an einen im Auftrag handelnden Dritten vorgesehen (d. h. einen Auftragsverarbeiter). In solch einem Fall muss die US-Organisation sicherstellen, dass der Beauftragte nur auf ihre Weisung hin handelt und angemessene und geeignete Maßnahmen treffen, 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. ([60]) Die Organisation kann vom Handelsministerium aufgefordert werden, eine Zusammenfassung oder eine repräsentative Kopie der Datenschutzbestimmungen des Vertrags vorzulegen. ([61]) Falls in der (Weiter-)Verarbeitungskette Compliance-Probleme auftreten, so haftet grundsätzlich die Organisation, die als Verantwortliche für die personenbezogenen Daten auftritt, nach dem *Grundsatz des Rechtsschutzes, der Durchsetzung und Haftung*, es sei denn, sie weist nach, dass sie für das Ereignis, das den Schaden bewirkt hat, nicht verantwortlich ist. ([62])

2.2.7 ***Rechenschaftspflicht***

(44) Nach dem Grundsatz der Rechenschaftspflicht müssen Daten verarbeitende Unternehmen geeignete technische und organisatorische Maßnahmen treffen, um ihren Datenschutzverpflichtungen wirksam nachzukommen und dies, insbesondere gegenüber der zuständigen Aufsichtsbehörde, nachweisen zu können.

(45) Sobald sich eine Organisation freiwillig für eine Zertifizierung ([63]) im Rahmen des Datenschutzrahmens EU-USA entschieden hat, ist die wirksame Einhaltung der Grundsätze verbindlich und durchsetzbar. Nach dem *Grundsatz des Rechtsschutzes, der Durchsetzung und der Haftung* ([64]) müssen die dem Datenschutzrahmen EU-USA angehörenden Organisationen wirksame Mechanismen schaffen, um die Einhaltung der anderen Grundsätze sicherzustellen. Überdies müssen die Organisationen Maßnahmen treffen, um sich zu vergewissern ([65]), dass die 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 Wirtschaftsprüfungen und Stichprobenkontrollen sowie der Einsatz von technischen Hilfsmitteln gehören können.

([58]) 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.

([59]) Je nachdem, ob der Dritte als 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 Datenschutzrahmen EU-USA angehörenden Organisation als Verantwortliche, deren Weisungen der Beauftragte unterliegt, diese Maßnahmen zu treffen. Siehe Anhang I Abschnitt II.3.

([60]) Anhang I Abschnitt II.3.b.

([61]) *Ebd.*

([62]) Anhang I Abschnitt II.7.d.

([63]) Siehe auch Zusatzgrundsatz „Selbstzertifizierung" (Anhang I Abschnitt III.6).

([64]) Siehe auch Zusatzgrundsatz „Beschwerdeverfahren und Durchsetzung" (Anhang I Abschnitt III.11).

([65]) Siehe auch Zusatzgrundsatz „Anlassunabhängige Kontrolle" (Anhang I Abschnitt III.7).

(46) Darüber hinaus müssen Organisationen ihre Unterlagen zur Umsetzung ihrer nach den Grundsätzen des Datenschutzrahmens EU-USA konzipierten Datenschutzbestimmungen dokumentieren und im Fall einer Untersuchung oder einer Beschwerde wegen Verletzung der Datenschutzvorschriften ihre Unterlagen einer unabhängigen Beschwerdestelle oder einer zuständigen Durchsetzungsbehörde übergeben. ([66])

2.3 **Verwaltung, Aufsicht und Durchsetzung**

(47) Der Datenschutzrahmen EU-USA wird vom Handelsministerium verwaltet und überwacht. Der Rahmen sieht Überwachungs- und Durchsetzungsmechanismen vor, um zu überprüfen und sicherzustellen, dass die Organisationen, die dem Datenschutzrahmen EU-USA angehören, die Grundsätzen einhalten und dass bei Verstößen gegen diese Grundsätze vorgegangen wird. Diese Mechanismen werden in den Grundsätzen (Anhang I), in den Zusagen des Handelsministeriums (Anhang III), der FTC (Anhang IV) und des Verkehrsministeriums (Anhang V) beschrieben.

2.3.1 ***(Erneute) Zertifizierung***

(48) Um sich im Rahmen des Datenschutzrahmens EU-USA zu zertifizieren (bzw. jährlich neu zu zertifizieren), müssen Organisationen öffentlich erklären, dass sie sich zur Einhaltung der Grundsätze verpflichten, ihre Datenschutzbestimmungen zur Verfügung stellen und diese vollständig umsetzen. ([67]) Im Rahmen ihres Antrags auf (erneute) Zertifizierung müssen die Organisationen dem Handelsministerium unter anderem Informationen über den Namen der betreffenden Organisation, eine Beschreibung der Zwecke, für die die Organisation personenbezogene Daten verarbeiten wird, die personenbezogenen Daten, auf die sich die Zertifizierung erstrecken soll, die gewählte Überprüfungsmethode, die entsprechende unabhängige Beschwerdestelle und die für die Durchsetzung der Einhaltung der Grundsätze zuständige Behörde vorlegen. ([68])

(49) Organisationen können ab dem Datum, an dem sie vom Handelsministerium in die Datenschutzrahmen-Liste aufgenommen werden, personenbezogene Daten auf der Grundlage des Datenschutzrahmens EU-USA erhalten. Um Rechtssicherheit zu gewährleisten und „falsche Behauptungen" zu vermeiden, dürfen Organisationen, die sich zum ersten Mal zertifizieren lassen, erst dann öffentlich auf ihre Einhaltung der Grundsätze hinweisen, wenn das Handelsministerium festgestellt hat, dass der Zertifizierungsantrag der Organisation vollständig ist, und die Organisation in die Datenschutzrahmen-Liste aufgenommen hat. ([69]) Damit sich diese Organisationen weiterhin auf den Datenschutzrahmen EU-USA stützen können, um personenbezogene Daten aus der Union zu erhalten, müssen sie ihre Beteiligung daran jährlich neu zertifizieren. Wenn eine Organisation aus irgendeinem Grund aus dem Datenschutzrahmen EU-USA austritt, muss sie alle Erklärungen entfernen, die darauf hindeuten, dass die Organisation weiterhin an dem Rahmenwerk beteiligt ist. ([70])

(50) Wie in den Verpflichtungen in Anhang III dargelegt, wird das Handelsministerium überprüfen, ob die Organisationen alle Zertifizierungsanforderungen erfüllen und eine (öffentliche) Datenschutzerklärung erstellt haben, die die nach dem *Grundsatz der Informationspflicht* erforderlichen Informationen enthält. ([71]) Aufbauend auf den Erfahrungen mit dem (erneuten) Zertifizierungsverfahren im Rahmen des Datenschutzschilds wird das Handelsministerium eine Reihe von Überprüfungen durchführen, u. a. um festzustellen, ob die Datenschutzbestimmungen der Organisationen einen Hyperlink zum richtigen Beschwerdeformular auf der Website der entsprechenden Beschwerdestelle enthalten und, wenn mehrere Einrichtungen und Tochterunternehmen einer Organisation in einem Antrag auf Zertifizierung enthalten sind, ob die Datenschutzbestimmungen jeder dieser Einrichtungen die Zertifizierungsanforderungen erfüllen und für die betroffenen Personen leicht zugänglich sind. ([72]) Darüber hinaus wird das Handelsministerium bei Bedarf Gegenkontrollen mit der FTC und dem Verkehrsministerium durchführen, um zu überprüfen, ob die Organisationen der in ihrem Antrag auf (erneute) Zertifizierung angegebenen Aufsichtsstelle unterliegen, und mit alternativen Streitbeilegungsstellen zusammenarbeiten, um zu überprüfen, ob die Organisationen bei der in ihrem Antrag auf (erneute) Zertifizierung angegebenen unabhängigen Beschwerdestelle registriert sind. ([73])

([66]) Anhang I Abschnitt III.7.
([67]) Anhang I Abschnitt I. 2.
([68]) Anhang I Abschnitt III.6.b und Anhang III, siehe Abschnitt „Prüfung der Selbstzertifizierungs-Anforderungen".
([69]) Anhang I Fußnote 12.
([70]) Anhang I Abschnitt III.6.h.
([71]) Anhang I Abschnitt III.6.a und Fußnote 12 sowie Anhang III, siehe Abschnitt „Prüfung der Selbstzertifizierungs-Anforderungen".
([72]) Anhang III Abschnitt „Prüfung der Selbstzertifizierungs-Anforderungen".
([73]) In ähnlicher Weise wird die Datenschutzbehörde mit dem Dritten zusammenarbeiten, der als Verwahrer der Mittel fungiert, die durch eine Gebühr für das Gremium der Datenschutzbehörden eingenommen werden (siehe Erwägungsgrund 73), um zu überprüfen, ob die Organisationen, die die Datenschutzbehörden als ihre unabhängige Beschwerdestelle gewählt haben, die Gebühr für das betreffende Jahr entrichtet haben. Siehe Anhang III Abschnitt „Prüfung der Selbstzertifizierungs-Anforderungen".

(51) Das Handelsministerium wird die Organisationen darüber informieren, dass sie alle während der Überprüfung festgestellten Probleme lösen müssen, um die (erneute) Zertifizierung abschließen zu können. Reagiert eine Organisation nicht innerhalb der vom Handelsministerium gesetzten Frist (z. B. wird bei der erneuten Zertifizierung erwartet, dass das Verfahren innerhalb von 45 Tagen abgeschlossen ist) ([74]) oder schließt sie ihre Zertifizierung nicht anderweitig ab, wird der Antrag als aufgegeben betrachtet. In diesem Fall können falsche Angaben zur Beteiligung an dem Datenschutzrahmen EU-USA oder zu seiner Einhaltung Gegenstand von Durchsetzungsmaßnahmen der FTC oder des Verkehrsministeriums sein. ([75])

(52) Um die ordnungsgemäße Anwendung des Datenschutzrahmens EU-USA zu gewährleisten, müssen interessierte Parteien wie betroffene Personen, Datenexporteure und die nationalen Datenschutzbehörden in der Lage sein, die Organisationen zu erkennen, die sich an die Grundsätze halten. Um diese Transparenz an der „Zugangsstelle" zu gewährleisten, hat sich das Handelsministerium verpflichtet, eine Liste der Organisationen zu führen und öffentlich zugänglich zu machen, die ihre Einhaltung der Grundsätze bescheinigt haben und in den Zuständigkeitsbereich mindestens einer der in den Anhängen IV und V dieses Beschlusses aufgeführten Durchsetzungsbehörden fallen. ([76]) Das Handelsministerium aktualisiert die Liste auf der Grundlage der jährlichen Anträge auf erneute Zertifizierung und streicht die Organisationen, die ausscheiden oder nicht mehr dem Datenschutzrahmen EU-USA angehören. Um Transparenz auch an der „Ausgangsstelle" zu gewährleisten, wird das Handelsministerium ein Verzeichnis der Organisationen, die von der Liste gestrichen wurden, führen und öffentlich zugänglich machen, wobei in jedem Fall der Grund für die Streichung angegeben wird. ([77]) Schließlich wird es einen Link zur Website der FTC zum EU-US Datenschutzrahmen geben, auf der die Durchsetzungsmaßnahmen der FTC auf der Grundlage des Rechtsrahmens aufgeführt sind. ([78])

2.3.2 *Überwachung der Einhaltung von Grundsätzen*

(53) Das Handelsministerium wird die tatsächliche Einhaltung der Grundsätze durch die dem Datenschutzrahmen EU-USA angehörenden Organisationen mithilfe verschiedener Mechanismen fortlaufend überwachen. ([79]) Insbesondere wird sie „Stichproben" bei nach dem Zufallsprinzip ausgewählten Organisationen sowie Ad-hoc-Stichproben bei bestimmten Organisationen durchführen, wenn potenzielle Probleme bei der Einhaltung der Grundsätze festgestellt werden (z. B. wenn Dritte der Kommission Bericht erstatten), um zu überprüfen, ob i) Kontaktstellen für die Bearbeitung von Beschwerden und Anfragen betroffener Personen vorhanden sind und auf diese reagiert wird, ii) die Datenschutzpolitik der Organisation sowohl auf ihrer Website als auch über einen Hyperlink auf der Website des Handelsministeriums leicht zugänglich ist, iii) die Datenschutzbestimmungen der Organisation weiterhin den Zertifizierungsanforderungen entsprechen und iv) die von der Organisation gewählte unabhängige Beschwerdestelle für die Bearbeitung von Beschwerden zur Verfügung steht. ([80])

(54) Wenn es stichhaltige Beweise dafür gibt, dass eine Organisation ihren Verpflichtungen im Rahmen der Datenschutzrahmens EU-USA nicht nachkommt (auch wenn das Handelsministerium Beschwerden erhält oder die Organisation nicht zufriedenstellend auf Anfragen des Handelsministeriums antwortet), wird das Handelsministerium die Organisation auffordern, einen detaillierten Fragebogen auszufüllen und einzureichen. ([81]) Eine Organisation, die den Fragebogen nicht zufriedenstellend und fristgerecht beantwortet, wird an die zuständige Behörde (die FTC oder das Verkehrsministerium) verwiesen, damit diese gegebenenfalls Durchsetzungsmaßnahmen trifft. ([82]) Im Rahmen der Überwachung der Einhaltung des Datenschutzschilds führte das Handelsministerium

([74]) Anhang III Fußnote 2.
([75]) Siehe Anhang III, Abschnitt „Prüfung der Selbstzertifizierungs-Anforderungen".
([76]) Informationen über die Verwaltung der Datenschutzrahmen-Liste sind in Anhang III (siehe Einleitung unter „Verwaltung und Überwachung des Datenschutzrahmenprogramms durch das Handelsministerium") und in Anhang I (Abschnitt I.3, Abschnitt I.4, Abschnitt III.6.d und Abschnitt III.11.g) enthalten.
([77]) Anhang III, siehe die Einleitung unter „Verwaltung und Überwachung des Datenschutzrahmenprogramms durch das Handelsministerium".
([78]) Siehe Anhang III Abschnitt „Anpassung der Website des Datenschutzrahmens an die Zielgruppen".
([79]) Siehe Anhang III Abschnitt „Regelmäßige Durchführung der von Amts wegen vorgenommenen Kontrollen der Einhaltung und Bewertungen des Datenschutzrahmens".
([80]) Im Rahmen seiner Überwachungsmaßnahmen kann das Handelsministerium verschiedene Instrumente einsetzen, z. B. um nach defekten Links zu Datenschutzbestimmungen zu suchen oder um aktiv Nachrichten nach Berichten zu durchsuchen, die stichhaltige Beweise für eine Nichteinhaltung erhalten.
([81]) Siehe Anhang III Abschnitt „Regelmäßige Durchführung der von Amts wegen vorgenommenen Kontrollen der Einhaltung und Bewertungen des Datenschutzrahmens".
([82]) Siehe Anhang III Abschnitt „Regelmäßige Durchführung der von Amts wegen vorgenommenen Kontrollen der Einhaltung und Bewertungen des Datenschutzrahmens".

regelmäßig die in Erwägungsgrund 53 erwähnten Stichproben durch und verfolgte kontinuierlich die öffentliche Berichterstattung, um Probleme bei der Einhaltung der Grundsätze zu ermitteln, anzugehen und zu beheben. ([83]) Organisationen, die fortwährend gegen die Grundsätze verstoßen, werden von der Datenschutzrahmen-Liste gestrichen und müssen die im Rahmen des Datenschutzrahmens empfangenen Daten zurückgeben oder löschen. ([84])

(55) In anderen Fällen der Streichung, etwa beim freiwilligen Ausscheiden oder beim Unterbleiben der erneuten Zertifizierung, muss die Organisation die Daten entweder löschen oder zurückgeben, oder sie kann sie 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). ([85]) In diesem Falle muss die Organisation auch eine Kontaktstelle benennen, die innerhalb der Organisation für alle mit dem Datenschutzrahmen EU-USA zusammenhängenden Fragen zuständig ist.

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

(56) Das Handelsministerium wird sowohl von Amts wegen als auch auf der Grundlage von Beschwerden (z. B. von Datenschutzbehörden) alle falschen Behauptungen über die Beteiligung am Datenschutzrahmen EU-USA oder die missbräuchliche Verwendung des Zertifizierungszeichens für den Datenschutzrahmen EU-USA überwachen. ([86]) Insbesondere wird das Handelsministerium fortlaufend überprüfen, ob Organisationen, die i) aus dem Datenschutzrahmen EU-USA ausscheiden, ii) die jährliche erneute Zertifizierung nicht abschließen (d. h. entweder begonnen haben, aber das jährliche Verfahren der erneuten Zertifizierung nicht rechtzeitig abgeschlossen haben, oder das jährliche Verfahren der erneuten Zertifizierung gar nicht erst begonnen haben), iii) insbesondere aufgrund „fortgesetzter Missachtung der Grundsätze“ von der Beteiligung am Datenschutzrahmen ausgeschlossen werden oder iv) eine erste Zertifizierung nicht abschließen (d. h. begonnen haben, aber das erste Zertifizierungsverfahren nicht rechtzeitig abgeschlossen haben), aus allen relevanten veröffentlichten Datenschutzbestimmungen Verweise auf den Datenschutzrahmen EU-USA entfernen, die auf eine aktive Beteiligung der Organisation an dem Datenschutzrahmen hindeuten. ([87]) Das Handelsministerium wird auch Internet-Recherchen durchführen, um Verweise auf den Datenschutzrahmen EU-USA in den Datenschutzbestimmungen von Organisationen zu finden, einschließlich falscher Behauptungen von Organisationen, die sich nie am Datenschutzrahmen EU-USA beteiligt haben. ([88])

(57) Stellt das Handelsministerium fest, dass Verweise auf den Datenschutzrahmen EU-USA nicht entfernt wurden oder missbräuchlich verwendet werden, wird es die Organisation über eine mögliche Verweisung an die FTC/das Verkehrsministerium informieren. ([89]) Wenn eine Organisation nicht zufriedenstellend antwortet, wird das Handelsministerium die Angelegenheit an die zuständige Behörde weiterleiten, damit diese gegebenenfalls Maßnahmen trifft. ([90]) 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 Durchsetzungsbehörden der USA tätig. Falsche Angaben gegenüber dem Handelsministerium unterliegen dem False Statements Act (18 U.S.C. § 1001).

([83]) Bei der zweiten jährlichen Überprüfung des Datenschutzschilds teilte das Handelsministerium mit, dass es Stichproben bei 100 Organisationen durchgeführt und in 21 Fällen Fragebögen zur Einhaltung der Grundsätze versandt hatte (woraufhin die festgestellten Probleme behoben wurden), siehe SWD (2018) 497 final der Kommission, S. 9. In ähnlicher Weise berichtete das Handelsministerium anlässlich der dritten jährlichen Überprüfung des Datenschutzschilds, dass es durch die Überwachung der öffentlichen Berichterstattung drei Vorfälle aufgedeckt habe und damit begonnen habe, jeden Monat Stichproben bei 30 Unternehmen durchzuführen, was in 28 % der Fälle zu Folgemaßnahmen mit Fragebögen zur Einhaltung der Grundsätze geführt habe (woraufhin die aufgedeckten Probleme sofort oder in drei Fällen nach einem Warnschreiben behoben wurden), siehe SWD (2019) 495 final der Kommission, S. 8.

([84]) Anhang I Abschnitt III.11.g. Eine fortgesetzte Missachtung liegt insbesondere dann vor, wenn sich eine Organisation weigert, einer endgültigen Entscheidung einer Einrichtung der freiwilligen Selbstkontrolle, einer unabhängigen Beschwerdestelle oder einer Datenschutzbehörde nachzukommen.

([85]) Anhang I Abschnitt III.6.f.

([86]) Anhang III Abschnitt „Aufdeckung und Handhabung von Fällen, in denen zu Unrecht eine Beteiligung an der Regelung geltend gemacht wird“.

([87]) *Ebd.*

([88]) *Ebd.*

([89]) *Ebd.*

([90]) Im Rahmen des Datenschutzschilds berichtete das Handelsministerium anlässlich der dritten jährlichen Überprüfung des Schilds, dass es 669 Fälle von falschen Angaben zur Beteiligung festgestellt habe (zwischen Oktober 2018 und Oktober 2019), von denen die meisten nach einem Warnschreiben des Handelsministeriums gelöst wurden, wobei 143 Fälle an die FTC verwiesen wurden (siehe Erwägungsgrund 62). Siehe SWD(2019) 495 final der Kommission, S. 10.

2.3.4 ***Durchsetzung***

(58) Um sicherzustellen, dass in der Praxis ein angemessenes Datenschutzniveau gewährleistet ist, sollte eine unabhängige Aufsichtsbehörde mit der Befugnis zur Überwachung und Durchsetzung der Einhaltung der Datenschutzvorschriften eingerichtet werden.

(59) Organisationen, die dem Datenschutzrahmen EU-USA angehören, müssen der Gerichtsbarkeit der zuständigen US-Behörden – der FTC und des Verkehrsministeriums – unterstehen, die über die notwendigen Ermittlungs- und Durchsetzungsbefugnisse verfügen, um die Einhaltung der Grundsätze wirksam zu gewährleisten. ([91])

(60) Die FTC ist eine unabhängige Behörde, die sich aus fünf Kommissaren zusammensetzt, die vom Präsidenten mit dem Rat und der Zustimmung des Senats ernannt werden. ([92]) Die Kommissare werden für eine Amtszeit von sieben Jahren ernannt und können nur vom Präsidenten wegen Unfähigkeit, Pflichtversäumnis oder Amtsmissbrauch entlassen werden. Nicht mehr als drei Kommissare dürfen derselben politischen Partei angehören und die Kommissare dürfen während ihrer Amtszeit keine anderen Geschäfte betreiben und Berufstätigkeiten ausüben sowie keine anderen Beschäftigungsverhältnisse eingehen.

(61) Die FTC kann sowohl die Einhaltung der Grundsätze als auch falsche Behauptungen über die Einhaltung der Grundsätze oder die Beteiligung am Datenschutzrahmen EU-USA durch Organisationen untersuchen, die entweder nicht mehr auf der Datenschutzrahmen-Liste stehen oder nie zertifiziert wurden. ([93]) Die FTC kann die Einhaltung der Vorschriften durchsetzen, indem sie behördliche oder bundesgerichtliche Anordnungen (einschließlich im Wege durch Vergleiche erzielten „Consent orders") ([94]) für vorläufige oder dauerhafte Unterlassungsverfügungen oder andere Abhilfemaßnahmen erwirkt, und sie wird die Einhaltung solcher Anordnungen systematisch überwachen ([95]). Bei Nichtbefolgung solcher Anordnungen kann die FTC zivilrechtliche Sanktionen und sonstige Abhilfemaßnahmen einfordern, was auch etwaigen Schadensersatz für die Folgen des rechtswidrigen Verhaltens einschließt. Jeder an eine dem Datenschutzrahmen EU-USA angehörende Organisation ergangene Consent order enthält Bestimmungen zur Selbstberichterstattung ([96]), und die Organisationen sind verpflichtet, alle relevanten Abschnitte eines der FTC vorgelegten Einhaltungs- oder Bewertungsberichts, die sich auf den Datenschutzrahmen EU-USA beziehen, zu veröffentlichen. Darüber hinaus führt die FTC eine Online-Liste der Organisationen, die Anordnungen der FTC oder eines Gerichts im Zusammenhang mit dem Datenschutzrahmen EU-USA unterliegen. ([97])

(62) Im Zusammenhang mit dem Datenschutzschild hat die FTC in etwa 22 Fällen Durchsetzungsmaßnahmen getroffen, und zwar sowohl bei Verstößen gegen die spezifischen Anforderungen des Rahmenwerks (z. B. Versäumnis, dem Handelsministerium zu bestätigen, dass die Organisation auch nach dem Ausscheiden aus dem Rahmenwerk weiterhin den Schutz des Datenschutzschilds anwendet, Versäumnis, durch Selbstkontrolle oder durch die Kontrolle einer externen Stelle zu überprüfen, ob die Organisation die Grundsätze einhält) ([98]), als auch bei falschen Behauptungen über die Beteiligung am Rahmenwerk (z. B. durch Organisationen, die es versäumt haben, die erforderlichen Schritte zu unternehmen, um die Zertifizierung zu erhalten, oder die ihre Zertifizierung auslaufen ließen, aber ihre weitere Beteiligung falsch darstellten) ([99]). Diese Durchsetzungsmaßnahme resultierte unter anderem aus dem proaktiven Einsatz von behördlichen Anordnungen zur Einholung von Informationen von bestimmten Teilnehmern des Datenschutzschilds, um zu prüfen, ob materielle Verstöße gegen die Verpflichtungen des Datenschutzschilds vorliegen. ([100])

([91]) Eine Organisation, die dem Datenschutzrahmen EU-USA angehört, muss 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 nach Abschnitt 5 des FTC Act zur Verhinderung unlauterer und irreführender Praktiken, die im Handel erfolgen oder den Handel beeinträchtigen (15 U.S.C. §45) und 49 U.S.C. §41712 zur Verhinderung unlauterer oder irreführender Praktiken im Luftverkehr oder beim Verkauf von Luftverkehrsdienstleistungen durch Luftfahrtunternehmen oder Vermittler, verfolgbar.

([92]) 15 U.S.C. § 41.

([93]) Anhang IV.

([94]) 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.

([95]) Siehe Anhang IV Abschnitt „Beantragung und Überwachung von Anordnungen".

([96]) 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.

([97]) Anhang IV Abschnitt „Beantragung und Überwachung von Anordnungen".

([98]) SWD(2019) 495 final der Kommission, S. 11.

([99]) Siehe die auf der Website der FTC aufgeführten Fälle, abrufbar unter https://www.ftc.gov/business-guidance/privacy-security/privacy-shield. Siehe auch SWD(2017) 344 final der Kommission, S. 17; SWD (2018) 497 final der Kommission, S. 12 und SWD (2019) 495 final der Kommission, S. 11.

([100]) Siehe beispielsweise Prepared Remarks of Chairman Joseph Simons at the Second Privacy Shield Annual Review (ftc.gov).

(63) Generell hat die FTC in den vergangenen Jahren Durchsetzungsmaßnahmen in einer Reihe von Fällen getroffen, in denen es um die Einhaltung spezifischer Datenschutzanforderungen ging, die auch im Rahmen des Datenschutzrahmens EU-USA vorgesehen sind, z. B. in Bezug auf die Grundsätze der Zweckbindung und der Vorratsdatenspeicherung ([101]), der Datenminimierung ([102]), der Datensicherheit ([103]) und der Datenrichtigkeit ([104]).

(64) Das Verkehrsministerium verfügt 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. Die Mitarbeiter des Verkehrsministeriums bemühen sich zunächst um eine Vereinbarung und können, wenn dies nicht möglich ist, ein Durchsetzungsverfahren mit einer Beweisverhandlung vor einem Verwaltungsrichter des Verkehrsministeriums einleiten, der befugt ist, Unterlassungsanordnungen und zivilrechtliche Sanktionen festzulegen. ([105]) Verwaltungsrichter genießen nach dem Administrative Procedure Act (APA) (Verwaltungsverfahrensgesetz) eine Reihe von Schutzmaßnahmen, die ihre Unabhängigkeit und Unparteilichkeit gewährleisten. Sie können z. B. nur aus wichtigem Grund entlassen werden, werden nach dem Rotationsprinzip mit Rechtssachen betraut, dürfen keine Aufgaben wahrnehmen, die mit ihren Pflichten und Verantwortlichkeiten als Verwaltungsrichter unvereinbar sind, unterliegen nicht der Aufsicht der Ermittlungsgruppe der Behörde, bei der sie angestellt sind (in diesem Fall das Verkehrsministerium) und müssen ihr Amt als Richter/Vollzugsrichter unparteiisch ausüben. ([106]) Das Verkehrsministerium hat sich verpflichtet, die Durchsetzungsmaßnahmen zu überwachen und sicherzustellen, dass Anordnungen, die sich aus Fällen im Zusammenhang mit dem Datenschutzrahmen EU-USA ergeben, auf seiner Website verfügbar sind. ([107])

2.4 **Rechtsbehelfe**

(65) Um einen angemessenen Schutz und insbesondere die Durchsetzung der Rechte des Einzelnen zu gewährleisten, sollten der betroffenen Person wirksame behördliche und gerichtliche Rechtsbehelfe zur Verfügung stehen.

(66) Im Rahmen des *Grundsatzes des Rechtsschutzes, der Durchsetzung und der Haftung* verpflichtet der Datenschutzrahmen EU-USA die Organisationen, Personen, die von der Nichteinhaltung der Vorschriften betroffen sind, Rechtsbehelfe zur Verfügung zu stellen und somit den betroffenen Personen in der Union die Möglichkeit einzuräumen, Beschwerden wegen der Nichteinhaltung der Grundsätze durch die Organisationen, die dem Datenschutzrahmen EU-USA angehören, einzulegen und eine Klärung herbeizuführen, erforderlichenfalls durch eine Entscheidung, die wirksam Abhilfe schafft. ([108]) Im Rahmen ihrer Zertifizierung müssen die Organisationen den Anforderungen dieses Grundsatzes 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. ([109])

([101]) Siehe z. B. die Anordnung der FTC in Drizzly, LLC, in der das Unternehmen unter anderem verpflichtet wird, 1) alle von ihm erhobenen personenbezogenen Daten zu vernichten, die für die Bereitstellung von Produkten oder Dienstleistungen für Verbraucher nicht erforderlich sind, 2) keine personenbezogenen Daten zu erheben oder zu speichern, es sei denn, dies ist für bestimmte Zwecke erforderlich, die in einem Aufbewahrungszeitplan dargelegt sind.

([102]) Siehe z. B. die Anordnung der FTC in CafePress (24. März 2022), in der unter anderem gefordert wird, die Menge der erhobenen Daten zu minimieren.

([103]) Siehe z. B. die Durchsetzungsmaßnahmen der FTC in Drizzly, LLC und CafePress, in denen die betreffenden Unternehmen aufgefordert wurden, ein spezielles Sicherheitsprogramm oder spezifische Sicherheitsmaßnahmen einzuführen. In Bezug auf Datenschutzverletzungen siehe auch die Anordnung der FTC vom 27. Januar 2023 in Chegg, die mit Equifax im Jahr 2019 erzielte Einigung (https://www.ftc.gov/news-events/news/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related-2017-data-breach).

([104]) Siehe z. B. die Rechtssache RealPage, Inc (16. Oktober 2018), in dem die FTC nach dem FCRA Durchsetzungsmaßnahmen gegen ein Unternehmen zur Überprüfung von Mietern getroffen hat, das Immobilieneigentümern und Immobilienverwaltungsgesellschaften Hintergrundberichte über Personen zur Verfügung stellte, die auf Informationen aus Miethistorien, Daten aus öffentlichen Registern (einschließlich über Straftaten und Räumungen) und Kreditinformationen basierten und als Faktoren für die Feststellung des Anspruchs auf Wohnraum herangezogen wurden. Die FTC stellte fest, dass das Unternehmen keine angemessenen Maßnahmen getroffen habe, die Richtigkeit der auf der Grundlage seines autonomen Entscheidungsinstruments zur Verfügung gestellten Informationen sicherzustellen.

([105]) Siehe Anhang V Abschnitt „Durchsetzungsmaßnahmen".

([106]) Siehe 5 U.S.C. §§ 3105, 7521(a), 554(d) und 556(b)(3).

([107]) Anhang V, siehe Abschnitt „Überwachung von Durchsetzungsmaßnahmen bei Verstößen gegen den Datenschutzrahmen EU-USA und Unterrichtung der Öffentlichkeit darüber".

([108]) Anhang I Abschnitt II.7.

([109]) Anhang I Abschnitt III.11.

(67) Die Organisationen können sich für unabhängige Beschwerdestellen in der Europäischen Union oder in den Vereinigten Staaten entscheiden. Wie in Erwägungsgrund 73 näher erläutert, schließt dies die Möglichkeit ein, sich freiwillig zur Zusammenarbeit mit den Datenschutzbehörden der EU zu verpflichten. Wenn Organisationen Personaldaten verarbeiten, ist eine solche Verpflichtung zur Zusammenarbeit mit den Datenschutzbehörden in der EU obligatorisch. 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.

(68) Folglich bietet der Datenschutzrahmen EU-USA betroffenen Personen eine Reihe von Möglichkeiten, ihr Recht durchzusetzen, Beschwerden über Verstöße von dem Datenschutzrahmen EU-USA angehörenden Organisationen einzulegen 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 Beschwerdestelle, nationale Datenschutzbehörden, das Handelsministerium oder die FTC richten. In Fällen, in denen die Beschwerden durch keines dieser Rechtsschutz- oder Durchsetzungsinstrumente geklärt werden konnten, haben Privatpersonen auch das Recht, ein verbindliches Schiedsverfahren zu beantragen (Anhang 1 zu Anhang I des vorliegenden Beschlusses). Mit Ausnahme des Schiedspanels, dessen Anrufung die Ausschöpfung bestimmter Rechtsbehelfe voraussetzt, können sich Privatpersonen frei für ein oder alle Rechtsinstrument(e) ihrer Wahl entscheiden und sind nicht verpflichtet, ein bestimmtes Instrument zu bevorzugen oder eine bestimmte Reihenfolge einzuhalten.

(69) Erstens können betroffene Personen in der Union durch direkte Kontakte zu den dem Datenschutzrahmen EU-USA angehörenden Organisationen ihre Rechte geltend machen und Verstößen gegen die Datenschutzgrundsätze nachgehen. ([110]) 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 der benannten unabhängigen Beschwerdestelle (siehe Erwägungsgrund 70). 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 Union darauf antworten. ([111]) Des Weiteren sind die Organisationen verpflichtet, unverzüglich auf Anfragen und andere Auskunftsbegehren des Handelsministeriums oder einer Datenschutzbehörde ([112]) (sofern sich die Organisation zur Zusammenarbeit mit den Datenschutzbehörden verpflichtet hat) zu reagieren, die sich auf die Einhaltung der Datenschutzgrundsätze beziehen.

(70) 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. ([113]) 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 infrage stehenden personenbezogenen Daten nicht weiter bearbeitet und/oder gelöscht werden sowie die festgestellten Verstöße öffentlich bekannt gemacht werden. ([114]) Die von einer Organisation benannten unabhängigen Beschwerdestellen sind verpflichtet, auf ihren öffentlichen Websites einschlägige Informationen zum Datenschutzrahmen EU-USA und zu den in diesem Rahmen erbrachten Dienstleistungen zu veröffentlichen. ([115]) Alljährlich müssen sie einen Bericht vorlegen, der zusammengefasste statistische Angaben zu diesen Dienstleistungen enthält. ([116])

([110]) Anhang I Abschnitt III.11.d.(i).
([111]) Anhang I Abschnitt III.11.d.(i).
([112]) Die vom Gremium der Datenschutzbehörden benannte zuständige Behörde, wie im Zusatzgrundsatz „Die Rolle der Datenschutzbehörden" vorgesehen (Anhang II Abschnitt III.5).
([113]) Anhang I Abschnitt III.11.d.
([114]) Anhang I Abschnitt II.7 und Abschnitt III.11.e.
([115]) Anhang I Abschnitt III.11.d.(ii).
([116]) Der Jahresbericht muss Folgendes umfassen: 1) die Gesamtzahl der Beschwerden im Zusammenhang mit dem EU-USA-Datenschutzrahmen, die während des Berichtsjahres eingegangen sind, 2) die Art der eingegangenen Beschwerden, 3) die Qualität der Streitbeilegung, z. B. die Dauer der Bearbeitung von Beschwerden, und 4) die Ergebnisse der eingegangenen Beschwerden, insbesondere die Anzahl und Art der auferlegten Abhilfemaßnahmen oder Sanktionen.

(71) Das Handelsministerium kann sich im Rahmen seiner Überprüfungsverfahren vergewissern, dass die Organisationen, die dem Datenschutzrahmen EU-USA angehören, tatsächlich bei den unabhängigen Beschwerdestellen registriert sind, die sie angegeben haben. ([117]) Sowohl die Organisationen als auch die zuständigen unabhängigen Beschwerdestellen sind gehalten, rasch auf Anfragen und Auskunftsbegehren des Handelsministeriums in Bezug auf den Datenschutzrahmens EU-USA zu reagieren. Das Handelsministerium wird mit unabhängigen Beschwerdestellen zusammenarbeiten, um zu überprüfen, ob diese auf ihren Websites Informationen über die Grundsätze und Dienstleistungen bereitstellen, die sie im Rahmen des Datenschutzrahmens EU-USA erbringen, und ob sie Jahresberichte veröffentlichen. ([118])

(72) 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 von Verstößen der Organisation zuständige US-Behörde) bzw. ein zuständiges Gericht davon in Kenntnis setzen. ([119]) 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, kann dies als fortgesetzte Missachtung der Grundsätze gewertet werden 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 Datenschutzrahmen-Liste streicht. ([120]) Sollte sich diese nach Streichung von der Liste weiterhin auf die Zertifizierung beim Datenschutzrahmen EU-USA berufen, verweist das Ministerium den Fall an die FTC oder eine andere Durchsetzungsinstanz. ([121])

(73) Drittens können Privatpersonen ihre Beschwerden auch bei einer nationalen Datenschutzbehörde in der Union einreichen, die von ihren Untersuchungs- und Abhilfebefugnissen nach der Verordnung (EU) 2016/679 Gebrauch machen kann. 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. ([122]) 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 getroffen wurden. ([123]) Im Falle der Nichtbefolgung der Empfehlungen der Datenschutzbehörde leitet diese solche Fälle an das Handelsministerium (das Organisationen von der Liste des Datenschutzrahmens EU-USA streichen kann) oder, für mögliche Durchsetzungsmaßnahmen, an die FTC oder das Verkehrsministerium weiter (die Nichtzusammenarbeit mit den Datenschutzbehörden oder die Nichteinhaltung der Grundsätze sind nach US-Recht strafbar). ([124])

(74) Um die Zusammenarbeit im Hinblick auf eine effiziente Bearbeitung von Beschwerden zu erleichtern, haben sowohl das Handelsministerium als auch die FTC eine spezielle Kontaktstelle eingerichtet, die für den direkten Kontakt mit den Datenschutzbehörden zuständig ist. ([125]) Diese Kontaktstellen helfen bei der Beantwortung von Anfragen der Datenschutzbehörde in Bezug auf die Einhaltung der Grundsätze durch eine Organisation.

(75) Die Datenschutzbehörde ([126]) gibt erst dann eine Empfehlung ab, wenn beide Parteien hinreichend Gelegenheit zur Stellungnahme oder zum Vorlegen von Beweisen hatten. Das Gremium kann die Empfehlungen so rasch zur Verfügung stellen, wie ein ordnungsgemäßes Vorgehen dies erlaubt, in der Regel binnen 60 Tagen nach Eingang einer Beschwerde. ([127]) Kommt die Organisation den Empfehlungen des Gremiums nicht binnen 25 Tagen nach und hat sie keine befriedigende Erklärung für die Verzögerung gegeben, so kann das Gremium seine Absicht mitteilen, die Angelegenheit an die FTC (oder eine andere zuständige amerikanische Durchsetzungsinstanz) zu verweisen oder

([117]) Anhang I Abschnitt „Prüfung der Selbstzertifizierungs-Anforderungen".
([118]) Siehe Anhang III Abschnitt „Erleichterung der Zusammenarbeit mit alternativen Streitbeilegungsstellen, die grundsatzbezogene Dienstleistungen erbringen". Siehe auch Anhang I Abschnitt III.11.d.(ii)-(iii).
([119]) Siehe Anhang I Abschnitt III.11.e.
([120]) Siehe Anhang I, Abschnitt III.11.g, insbesondere Ziffern ii und iii.
([121]) Siehe Anhang III Abschnitt „Aufdeckung und Handhabung von Fällen, in denen zu Unrecht eine Beteiligung an der Regelung geltend gemacht wird".
([122]) Anhang I Abschnitt II.7.b.
([123]) Anhang I Abschnitt III.5.
([124]) Anhang I Abschnitt III.5.c.(ii).
([125]) Anhang III (siehe Abschnitt „Erleichterung der Zusammenarbeit mit den Datenschutzbehörden") und Anhang IV (siehe Abschnitte „Vorrangige Behandlung von überwiesenen Fällen und Ermittlungen" und „Zusammenarbeit mit den EU-Datenschutzbehörden bei der Durchsetzung").
([126]) Die Geschäftsordnung des informellen Gremiums der Datenschutzbehörden sollte von diesen auf der Grundlage ihrer Kompetenz für die Arbeitsorganisation und die gegenseitige Zusammenarbeit erarbeitet werden.
([127]) Anhang I Abschnitt III.5.c.(i).

gelangt zu dem Schluss, dass eine gravierende Verletzung der Verpflichtungen zur Kooperation vorliegt. Im erstgenannten Fall kann dies zu Durchsetzungsmaßnahmen auf der Grundlage von Abschnitt 5 des FTC Act (oder eines vergleichbaren Gesetzes) führen. ([128]) 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 Datenschutzrahmen-Liste nach sich zieht.

(76) 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 EU-Mitgliedstaats anzufechten.

(77) Privatpersonen können auch dann Beschwerden bei Datenschutzbehörden einreichen, wenn das Gremium der Datenschutzbehörden 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 dem Datenschutzrahmen EU-USA angehörenden Organisationen 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. ([129]) Die FTC hat ihrerseits zugesagt, eine spezielle Kontaktstelle einzurichten. ([130])

(78) Viertens hat das Handelsministerium zugesagt, Beschwerden über Verstöße einer Organisation gegen die Grundsätze entgegenzunehmen, zu überprüfen und nach Möglichkeit zu klären. ([131]) Zu diesem Zweck sieht das Handelsministerium spezielle Verfahren vor, wonach Datenschutzbehörden Beschwerden einer dafür eingerichteten Kontaktstelle vorlegen und dann bei den Organisationen weiterverfolgen, um eine Klärung zu erleichtern. ([132]) 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. ([133]) Dies ermöglicht es betroffenen Personen, Beschwerden über Verstöße der Mitgliedsorganisationen des Datenschutzrahmens EU-USA direkt bei den nationalen Datenschutzbehörden einzureichen, die sie dann an das Handelsministerium als der für die Verwaltung des Datenschutzrahmens EU-USA zuständigen Behörde weiterleiten.

(79) 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 Grundsätze verstoßen hat, kann es diese Organisation von der Datenschutzrahmen-Liste streichen. ([134]) 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. ([135])

(80) Fünftens müssen sich die Organisationen, die dem Datenschutzrahmen EU-USA angehören, der Gerichtsbarkeit der zuständigen US-Behörden, insbesondere der FTC ([136]) unterwerfen, die über die notwendigen Ermittlungs- und Durchsetzungsbefugnisse verfügen, um die Einhaltung der Grundsätze wirksam zu gewährleisten. Die FTC behandelt vorrangig Fälle der Missachtung der Grundsätze, 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 Abschnitt 5 des FTC Act verstoßen wurde. ([137]) Die FTC hat zugesagt, ein standardisiertes Befassungsverfahren einzurichten, eine Kontaktstelle für von den Datenschutzbehörden überwiesene Fälle zu benennen und Informationen darüber auszutauschen. Überdies kann sie Beschwerden direkt von Privatpersonen entgegennehmen und von sich aus Ermittlungen einleiten, die den Datenschutzrahmen EU-USA betreffen, insbesondere im Rahmen breiter angelegter Untersuchungen zu Fragen des Datenschutzes.

([128]) Anhang I Abschnitt III.5.c.(ii).
([129]) Siehe Anhang III Abschnitt „Erleichterung der Zusammenarbeit mit den Datenschutzbehörden".
([130]) Siehe Anhang IV Abschnitte „Vorrangige Behandlung von überwiesenen Fällen und Ermittlungen" und „Zusammenarbeit mit den EU-Datenschutzbehörden bei der Durchsetzung".
([131]) Anhang III, siehe z. B. Abschnitt „Erleichterung der Zusammenarbeit mit den Datenschutzbehörden".
([132]) Anhang I Abschnitt II.7.e und Anhang III Abschnitt „Erleichterung der Zusammenarbeit mit den Datenschutzbehörden".
([133]) *Ebd.*
([134]) Anhang I Abschnitt III.11.g.
([135]) Anhang I Abschnitt III.11.g.
([136]) Eine Organisation, die dem Datenschutzrahmen EU-USA angehört, muss 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 nach Abschnitt 5 des FTC Act zur Verhinderung unlauterer und irreführender Praktiken, die im Handel erfolgen oder den Handel beeinträchtigen, verfolgbar.
([137]) Siehe auch ähnliche Verpflichtungen des Verkehrsministeriums, die in Anhang V aufgeführt sind.

(81) Sechstens kann eine betroffene Person in der Union, sofern es nicht gelingt, einen Streit mithilfe einer dieser Möglichkeiten beizulegen, als letztes Mittel das Panel des Datenschutzrahmens EU-USA (im Folgenden „Datenschutzrahmen-Panel“), ein verbindliches Schiedsforum, in Anspruch nehmen. ([138]) Die Organisationen müssen Privatpersonen darüber informieren, dass sie sich 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. ([139])

(82) Das Datenschutzrahmen-Panel besteht aus einem Pool von mindestens zehn 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 ([140]) Schiedsrichtern bestehendes Panel aus.

(83) Das International Centre for Dispute Resolution (ICDR), die internationale Abteilung der American Arbitration Association (AAA), wurde vom Handelsministerium mit der Durchführung von Schiedsverfahren beauftragt. Für die Verfahren vor dem Datenschutzrahmen-Panel gelten vereinbarte Schiedsregeln und ein Verhaltenskodex für die ernannten Schiedsrichter. Die Website des ICDR-AAA enthält klare und präzise Informationen über das Schiedsverfahren und das Verfahren zur Beantragung eines Schiedsverfahrens.

(84) Die zwischen dem Handelsministerium und der Kommission vereinbarten Schiedsregeln ergänzen den Datenschutzrahmen EU-USA, der mehrere Merkmale enthält, welche die Zugänglichkeit dieses Instruments für die betroffenen Personen in der Union verbessern: i) Bei der Vorbereitung einer Beschwerde vor dem Panel kann die betroffene Person von ihrer nationalen Datenschutzbehörde unterstützt werden. ii) Das Schiedsverfahren findet zwar in den Vereinigten Staaten statt, die betroffenen Personen in der Union können sich jedoch per Video- oder Telefonkonferenz beteiligen, was für sie kostenlos ist. iii) Während die im Schiedsverfahren verwendete Sprache in der Regel Englisch ist, werden Dolmetschdienste für die mündliche Verhandlung und Übersetzungen grundsätzlich auf begründeten Antrag und ohne zusätzliche Kosten für die betroffenen Personen zur Verfügung gestellt. iv) Schließlich wird das Handelsministerium einen Fonds unterhalten, der durch jährliche Beiträge der Organisationen, die dem Datenschutzrahmen EU-USA angehören, gespeist wird, um die Kosten des Schiedsverfahrens bis zu einem von den US-Behörden in Absprache mit der Kommission festzulegenden Höchstbetrag zu decken, während jede Partei ihre eigenen Anwaltskosten trägt, wenn sie sich vor dem Panel durch einen Anwalt vertreten lässt. ([141])

(85) Das Datenschutzrahmen-Panel ist befugt, einzelfallbezogene, nichtmonetäre billigkeitsrechtliche Ansprüche ([142]) anzuerkennen, um Verstöße gegen die Grundsätze abzustellen. Zwar berücksichtigt das Panel dabei die bereits von anderen Instrumenten des Datenschutzrahmens EU-USA 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 Union in allen Fällen auf das Schiedsverfahren zurückgreifen, in denen die Vorgehensweise oder Untätigkeit der dem Datenschutzrahmen EU-USA angehörenden Organisationen, unabhängigen Beschwerdestellen oder zuständigen US-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 einer dem Datenschutzrahmen EU-USA angehörenden Organisation die infrage 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. Privatpersonen können den Schiedsspruch auf der Grundlage des Federal Arbitration Act vor amerikanischen Gerichten durchsetzen, sodass ihnen ein Rechtsbehelf zur Verfügung steht, falls sich eine Organisation nicht daran hält.

([138]) Siehe Anhang I Anhang I „Schiedsmodell“.
([139]) Siehe Anhang I Abschnitt II.1.a.(xi) und Abschnitt II.7.c.
([140]) Die Anzahl der Schiedsrichter ist zwischen den Parteien zu vereinbaren.
([141]) Anhang I von Anhang I Abschnitt G.6.
([142]) Privatpersonen können im Schiedsverfahren keinen Schadensersatz geltend machen, doch schließt die Inanspruchnahme des Schiedsverfahrens nicht die Möglichkeit aus, vor ordentlichen Gerichten der USA auf Schadensersatz zu klagen.

(86) Siebtens: Wenn sich eine Organisation nicht an ihre Zusage hält, die Grundsätze und die veröffentlichten Datenschutzbestimmungen einzuhalten, stehen nach US-Recht zusätzliche Rechtsbehelfe zur Verfügung, darunter auch die Möglichkeit, Schadensersatz zu erhalten. So kann der Einzelne unter bestimmten Voraussetzungen nach den Verbraucherschutzgesetzen der einzelnen Staaten in Fällen von arglistiger Täuschung, unlauterer oder irreführender Handlungen oder Praktiken ([143]) sowie im Rahmen des Deliktsrechts (insbesondere bei Verletzung der Privatsphäre ([144]), widerrechtlicher Aneignung von Namen oder Bildnissen ([145]) und öffentlicher Bekanntgabe privater Tatsachen ([146])) Rechtsbehelfe (einschließlich Schadensersatz) in Anspruch nehmen.

(87) Zusammen stellen die verschiedenen oben beschriebenen Rechtsbehelfe sicher, dass jede Beschwerde über einen Verstoß gegen den Datenschutzrahmen EU-USA durch zertifizierte Organisationen wirksam entschieden wird und Abhilfe geschaffen wird.

3. ZUGANG ZU UND VERWENDUNG VON AUS DER EUROPÄISCHEN UNION ÜBERMITTELTEN PERSONENBEZOGENEN DATEN DURCH BEHÖRDEN IN DEN VEREINIGTEN STAATEN

(88) Die Kommission hat auch die Einschränkungen und Garantien geprüft, einschließlich der Kontrollmechanismen und der Rechtsbehelfe für den Einzelnen, die nach dem US-Recht in Bezug auf die Erhebung und nachfolgende Verwendung personenbezogener Daten durch US-Behörden, die im öffentlichen Interesse an Datenverantwortliche und Auftragsverarbeiter in den USA übermittelt wurden, insbesondere zur Strafverfolgung und zur nationalen Sicherheit (im Folgenden „staatlicher Zugriff"), verfügbar sind. ([147]) Bei der Beurteilung der Frage, ob die Bedingungen für den staatlichen Zugriff auf Daten, die nach diesem Beschluss an die Vereinigten Staaten übermittelt werden, das Kriterium der „wesentlichen Gleichwertigkeit" nach Artikel 45 Absatz 1 der Verordnung (EU) 2016/679 in der Auslegung des Gerichtshofs im Lichte der Charta der Grundrechte erfüllen, hat die Kommission mehrere Kriterien berücksichtigt.

(89) Insbesondere muss jede Einschränkung des Rechts auf den Schutz personenbezogener Daten gesetzlich vorgesehen sein, und die gesetzliche Grundlage für den Eingriff in dieses Recht muss selbst den Umfang der Einschränkung der Ausübung des betreffenden Rechts festlegen. ([148]) Darüber hinaus muss die Rechtsgrundlage, um dem Erfordernis der Verhältnismäßigkeit zu genügen, wonach Ausnahmen und Einschränkungen in Bezug auf den Schutz personenbezogener Daten nur insoweit gelten dürfen, als dies in einer demokratischen Gesellschaft zur Verwirklichung spezifischer Ziele von allgemeinem Interesse, die den von der Union anerkannten Zielen gleichwertig sind, unbedingt erforderlich ist, klare und präzise Regeln für die Tragweite und die Anwendung der betreffenden Maßnahme vorsehen und Mindesterfordernisse aufstellen, sodass die Personen, deren Daten übermittelt wurden, über ausreichende Garantien verfügen, die einen wirksamen Schutz ihrer personenbezogenen Daten vor Missbrauchsrisiken ermöglichen. ([149]) Außerdem müssen diese Regeln und Schutzmaßnahmen rechtsver-

([143]) Siehe z. B. die bundesstaatlichen Verbraucherschutzgesetze in Kalifornien (Cal. Civ. Code §§ 1750–1785 (West) Consumers Legal Remedies Act); District of Columbia (D.C. Code §§ 28-3901); Florida (Fla. Stat. §§ 501.201–501.213, Deceptive and Unfair Trade Practices Act); Illinois (815 Ill. Comp. Stat. 505/1–505/12, Consumer Fraud and Deceptive Business Practices Act); Pennsylvania (73 Pa. Stat. Ann. §§ 201-1–201-9.3 (West) Unfair Trade Practices and Consumer Protection Law).

([144]) D. h. bei vorsätzlicher Einmischung in die Privatangelegenheiten einer anderen Person in einer Weise, die für eine vernünftige Person äußerst beleidigend wäre (Restatement (2nd) of Torts, §652(b)).

([145]) Diese unerlaubte Handlung ist in der Regel auf die Aneignung und Verwendung des Namens oder des Bildnisses einer Person zum Zwecke der Werbung für ein Unternehmen oder ein Produkt oder für ähnliche kommerzielle Zwecke anwendbar (siehe Restatement (2nd) of Torts, §652C).

([146]) D. h., wenn Informationen über das Privatleben einer Person veröffentlicht werden, die für eine vernünftige Person in hohem Maße beleidigend wären und an denen kein legitimes öffentliches Interesse besteht (Restatement (2nd) of Torts, §652D).

([147]) Dies ist auch im Hinblick auf Anhang I Abschnitt I.5 von Bedeutung. Nach diesem Abschnitt und ähnlich der DSGVO kann die Einhaltung der Datenschutzanforderungen und -rechte, die Teil der Datenschutzgrundsätze sind, Einschränkungen unterworfen werden. Solche Einschränkungen sind jedoch nicht absolut, sondern können nur unter verschiedenen Bedingungen geltend gemacht werden, z. B. insoweit, als dies erforderlich ist, um einer richterlichen Anordnung nachzukommen oder Erfordernissen des öffentlichen Interesses, der Strafverfolgung oder der nationalen Sicherheit gerecht zu werden. In diesem Zusammenhang und im Interesse der Klarheit wird in diesem Abschnitt auch auf die in der EO 14086 festgelegten Bedingungen verwiesen, die unter anderem in den Erwägungsgründen 127 bis 141 bewertet werden.

([148]) Siehe Schrems II, Rn. 174–175, und die darin aufgeführte Rechtsprechung. Zum Zugriff durch Behörden der Mitgliedstaaten siehe auch Rechtssache C-623/17, Privacy International, ECLI:EU:C:2020:790, Rn. 65 sowie die verbundenen Rechtssachen C-511/18, C-512/18 und C-520/18, La Quadrature du Net u. a., EU:C:2020:791, Rn. 175.

([149]) Siehe Schrems II, Rn. 176 und 181, und die darin aufgeführte Rechtsprechung. Zum Zugriff durch Behörden der Mitgliedstaaten siehe auch die Rechtssachen Privacy International, Rn. 68 und La Quadrature du Net u. a., Rn. 132.

bindlich sein und von Privatpersonen durchgesetzt werden können. ([150]) Insbesondere müssen betroffene Personen die Möglichkeit haben, Rechtsbehelfe vor einem unabhängigen und unparteiischen Gericht einzulegen, um Zugang zu den sie betreffenden personenbezogenen Daten zu erlangen oder die Berichtigung oder Löschung solcher Daten zu erwirken. ([151])

3.1 **Zugriff und Verwendung durch US-Behörden für Strafverfolgungszwecke**

(90) Im Hinblick auf Eingriffe in personenbezogene Daten, die gemäß dem Datenschutzrahmen EU-USA aus Gründen der Strafverfolgung übermittelt werden, so sind in den Rechtsvorschriften der Vereinigten Staaten neben einer Reihe von Einschränkungen für den Zugang zu und die Verwendung von personenbezogenen Daten auch Aufsichtsmechanismen und Rechtsbehelfe vorgesehen, die den in Erwägungsgrund 89 dieses Beschlusses genannten Anforderungen entsprechen. Die folgenden Abschnitte enthalten eine detaillierte Bewertung der Bedingungen, unter denen ein solcher Zugriff erfolgen kann, sowie der Garantien, die für die Nutzung dieser Befugnisse gelten. In diesem Zusammenhang hat die Regierung der USA (über das Justizministerium) Zusicherungen zu den dafür geltenden Einschränkungen und Garantien gemacht (Anhang VI zu diesem Beschluss).

3.1.1 ***Rechtsgrundlagen, Einschränkungen und Garantien***

3.1.1.1 *Einschränkungen und Garantien in Bezug auf die Erhebung personenbezogener Daten zu Strafverfolgungszwecken*

(91) Personenbezogene Daten, die von zertifizierten US-Organisationen verarbeitet und auf der Grundlage des Datenschutzrahmens EU-USA aus der Union übermittelt werden, können von US-Bundesstaatsanwälten und Ermittlern des Bundes zu Strafverfolgungszwecken nach verschiedenen Verfahren eingesehen werden (vgl. die Erwägungsgründe 92 bis 99). Diese Verfahren gelten in gleicher Weise, wenn Informationen bei einer US-Organisation beschafft werden, unabhängig von der Staatsangehörigkeit oder dem Wohnort der betroffenen Personen. ([152])

(92) Erstens kann ein Richter auf Antrag eines Strafverfolgungsbeamten oder eines Staatsanwalts eine Durchsuchung oder Beschlagnahme (auch von elektronisch gespeicherten Daten) anordnen. ([153]) Ein solcher Beschluss kann nur erlassen werden, wenn ein „hinreichender Verdacht" ([154]) besteht, dass „beschlagnahmefähige Gegenstände" (Beweismittel für eine Straftat, rechtswidrig im Besitz befindliche oder zur Begehung einer Straftat bestimmte oder verwendete Gegenstände) an dem im Beschluss bezeichneten Ort aufgefunden werden können. Im Beschluss sind die zu beschlagnahmenden Gegenstände zu bezeichnen und der Richter anzugeben, an den der Beschluss zurückzusenden ist. Eine Person, die einer Durchsuchung unterzogen wird oder deren Eigentum durchsucht wird, kann die

([150]) Siehe Schrems II, Rn. 181–182.

([151]) Siehe Schrems I, Rn. 95, und Schrems II, Rn. 194. In diesem Zusammenhang hat der Gerichtshof insbesondere betont, dass die Einhaltung von Artikel 47 der Charta der Grundrechte, der das Recht auf einen wirksamen Rechtsbehelf vor einem unabhängigen und unparteiischen Gericht garantiert, „für das in der Union erforderliche Schutzniveau maßgebend ist und [von der] Kommission [festgestellt werden] muss, bevor sie einen Angemessenheitsbeschluss im Sinne von Art. 45 Abs. 1 der [Verordnung (EU) 2016/679] erlässt" (Schrems II, Rn. 186).

([152]) Siehe Anhang VI. Siehe z. B. in Bezug auf den Wiretap Act, den Stored Communications Act und den Pen Register Act (ausführlicher in den Erwägungsgründen 95 bis 98) Suzlon Energy Ltd. v. Microsoft Corp., 671 F.3d 726, 729 (9th Cir. 2011).

([153]) Federal Rules of Criminal Procedure, 41. In einem Urteil aus dem Jahr 2018 bestätigte der Oberste Gerichtshof der Vereinigten Staaten, dass ein Durchsuchungsbefehl oder eine Ausnahme von dem Durchsuchungsbefehl erforderlich ist, damit Strafverfolgungsbehörden auf historische Aufzeichnungen von Mobilfunkstandorten zugreifen können, die einen umfassenden Überblick über die Bewegungen eines Nutzers geben, und dass der Nutzer ein berechtigtes Vertrauen in den Schutz seiner Privatsphäre in Bezug auf diese Informationen haben kann (Timothy Ivory Carpenter v. United States of America, Nr. 16-402, 585 U.S. (2018)). Folglich können solche Daten von einem Mobilfunkunternehmen in der Regel nicht auf der Grundlage einer richterlichen Anordnung erlangt werden, wenn hinreichende Gründe für die Annahme bestehen, dass die Informationen für eine laufende strafrechtliche Ermittlung relevant und wesentlich sind, sondern es muss ein hinreichender Verdacht nachgewiesen werden, wenn eine richterliche Anordnung verwendet wird.

([154]) Dem Obersten Gerichtshof zufolge ist der „hinreichende Verdacht" ein „praktischer, nicht technischer" Standard, der auf „faktischen und praktischen Erwägungen des täglichen Lebens beruht, nach denen vernünftige und umsichtige Personen … handeln" (Illinois v. Gates, 462 U.S.). 213, 232 (1983)). Bei Durchsuchungsbefehlen liegt ein hinreichender Verdacht vor, wenn die Durchsuchung mit an Sicherheit grenzender Wahrscheinlichkeit zum Auffinden von Beweismitteln für eine Straftat führt (ebd).

Beseitigung von Beweismitteln verlangen, die bei einer rechtswidrigen Durchsuchung erlangt wurden, wenn diese Beweismittel in einem Strafverfahren gegen diese Person verwendet werden. ([155]) Wird ein Dateninhaber (z. B. ein Unternehmen) kraft einer Anordnung zur Offenlegung von Daten verpflichtet, kann er insbesondere die Verpflichtung zur Offenlegung als unverhältnismäßige Belastung anfechten. ([156])

(93) Zweitens kann eine Grand Jury (eine Anklagekammer, deren Mitglieder von einem Richter oder Magistrate ausgewählt werden) im Rahmen von Ermittlungen wegen bestimmter schwerer Straftaten ([157]), in der Regel auf Antrag eines Bundesstaatsanwalts, eine Anordnung erlassen, um jemanden zur Vorlage oder Zurverfügungstellung von Geschäftsunterlagen, elektronisch gespeicherten Informationen oder sonstigen materiellen Beweismitteln zu verpflichten. Darüber hinaus ist es nach verschiedenen Gesetzen 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 relevant sind, vorzulegen bzw. zur Verfügung zu stellen. ([158]) In beiden Fällen müssen die Informationen für die Ermittlungen relevant sein, und die Anordnung zur Herausgabe darf nicht unverhältnismäßig, d. h. überzogen, repressiv oder belastend sein (der Empfänger der Anordnung kann die Anordnung aus diesen Gründen anfechten). ([159])

(94) Sehr ähnliche Voraussetzungen gelten für behördliche Anordnungen, die erlassen werden, um für zivil- oder aufsichtsrechliche („öffentliches Interesse“) Zwecke Zugang zu Daten zu erhalten, die sich im Besitz von Unternehmen in den USA befinden. Die Befugnis der mit zivilrechtlichen und regulatorischen Zuständigkeiten ausgestatteten Behörden, solche behördlichen Anordnungen zu erlassen, muss gesetzlich festgelegt sein. Die Anwendung einer behördlichen Anordnung unterliegt einer „Angemessenheitsprüfung“, die voraussetzt, dass die Untersuchung einem legitimen Zweck dient, die im Rahmen der Anordnung angeforderten Informationen für diesen Zweck relevant sind, die Behörde nicht bereits über die Informationen verfügt, die sie mit der Anordnung anfordert, und die erforderlichen administrativen Schritte zur Ausstellung der Anordnung unternommen wurden. ([160]) In der Rechtsprechung des Obersten Gerichtshofs wurde auch klargestellt, dass die Bedeutung des öffentlichen Interesses an den angeforderten Informationen gegen die Bedeutung persönlicher und organisatorischer Datenschutzinteressen abgewogen werden muss. ([161]) Die Anwendung einer behördlichen Anordnung bedarf zwar keiner vorherigen gerichtlichen Genehmigung, unterliegt jedoch einer gerichtlichen Überprüfung, wenn der Empfänger aus den oben genannten Gründen Widerspruch einlegt oder wenn die ausstellende Behörde versucht, die Anordnung vor Gericht durchzusetzen. ([162]) Zusätzlich zu diesen allgemeinen umfassenden Einschränkungen können sich aus einzelnen Gesetzen spezifische (strengere) Anforderungen ergeben. ([163])

([155]) Mapp v. Ohio, 367 U.S. 643 (1961).

([156]) Siehe die Rechtssache In re Application of United States, 610 F.2d 1148, 1157 (3d Cir. 1979) (in der festgestellt wird, dass „ein ordnungsgemäßes Verfahren eine Anhörung zur Frage der Aufwendigkeit erfordert, bevor eine Telefongesellschaft zur Unterstützung eines Durchsuchungsbefehls verpflichtet werden kann“) und die Rechtssache In re Application of United States, 616 F.2d 1122 (9th Cir.). 1980).

([157]) Nach dem fünften Zusatzartikel der US-Verfassung ist eine Anklage vor einer Grand Jury für jedes „Kapital- oder andere schwerwiegende Verbrechen“ erforderlich. Die Grand Jury besteht aus 16 bis 23 Mitgliedern und entscheidet, ob ein hinreichender Verdacht auf ein Verbrechen besteht. Um zu dieser Schlussfolgerung zu gelangen, sind die Grand Jurys mit Ermittlungsbefugnissen ausgestattet, die es ihnen ermöglichen, Anordnungen zu erlassen.

([158]) Siehe Anhang VI.

([159]) Federal Rules of Criminal Procedure, 17.

([160]) United States v. Powell, 379 U.S. 48 (1964).

([161]) Oklahoma Press Publishing Co. v. Walling, 327 U.S. 186 (1946).

([162]) Der Oberste Gerichtshof hat klargestellt, dass ein Gericht im Fall der Anfechtung einer behördlichen Anordnung prüfen muss, ob 1) die Untersuchung einem rechtmäßig genehmigten Zweck dient, 2) die betreffende Anordnungsbehörde in die Zuständigkeit des Kongresses fällt und 3) die „angeforderten Dokumente für die Untersuchung relevant sind“. Der Gerichtshof stellte ferner fest, dass ein Antrag auf behördliche Anordnung „angemessen“ sein muss, d. h., dass die „Spezifizierung der vorzulegenden Dokumente für die Zwecke der betreffenden Untersuchung angemessen sein muss, aber nicht überzogen sein darf“ und „die zu durchsuchende Örtlichkeit und die in Gewahrsam zu nehmenden Personen oder Gegenstände genau zu bezeichnen sind“.

([163]) Beispielsweise sieht der Right to Financial Privacy Act für eine Regierungsbehörde nur dann die Befugnis vor, mithilfe einer behördlichen Anordnung Finanzunterlagen eines Finanzinstituts zu erhalten, wenn 1) Grund zu der Annahme besteht, dass die angeforderten Unterlagen für eine rechtmäßige Strafverfolgungsuntersuchung relevant sind und 2) dem Kunden eine Kopie der Anordnung oder Vorladung zusammen mit einer Mitteilung übermittelt wurde, in der die Art der Untersuchung hinreichend genau angegeben wird (12 U.S.C. §3405). Ein weiteres Beispiel ist der Fair Credit Reporting Act, der es Verbraucherauskunfteien untersagt, aufgrund einer behördlichen Anordnung Berichte über Verbraucher offenzulegen (und es ihnen nur gestattet, auf behördliche Anordnungen der Grand Jury oder auf Gerichtsbeschlüsse zu reagieren, 15 U.S.C.§1681 ff.). In Bezug auf den Zugriff auf Kommunikationsdaten gelten die besonderen Anforderungen des Stored Communications Act, auch in Bezug auf die Möglichkeit der Anwendung behördlicher Anordnungen (für einen detaillierten Überblick siehe die Erwägungsgründe 96 und 97).

(95) Drittens gibt es mehrere Rechtsgrundlagen, die es Strafverfolgungsbehörden ermöglichen, auf Kommunikationsdaten zuzugreifen. Ein Gericht kann eine Anordnung erlassen, mit der die Erhebung von in Echtzeit nichtinhaltlichen Wähl-, Routing-, Anschluss- und Signalinformationen zu einer Telefonnummer oder E-Mail-Adresse (unter Einsatz von Geräten zur Rufnummernerfassung von ausgehenden und eingehenden Anrufen) genehmigt wird, wenn es feststellt, dass die Behörde bescheinigt hat, dass die Informationen, die wahrscheinlich erlangt werden, für ein laufendes strafrechtliches Ermittlungsverfahren relevant sind. ([164]) Die Anordnung muss unter anderem die Identität des Verdächtigen, soweit bekannt, die Merkmale der Kommunikation, die Gegenstand der Anordnung ist, und die Straftat, auf die sich die zu erlangenden Informationen beziehen, enthalten. Der Einsatz von Geräten zur Rufnummernerfassung kann für einen Zeitraum von höchstens 60 Tagen genehmigt werden, der nur durch eine neue richterliche Anordnung verlängert werden kann.

(96) Darüber hinaus kann der Zugriff auf Teilnehmerdaten, Verkehrsdaten und gespeicherte Kommunikationsinhalte bei Internetdienstanbietern, Telefongesellschaften und anderen dritten Dienstanbietern zu Strafverfolgungszwecken auf der Grundlage des Stored Communications Act gewährt werden. ([165]) Um an die gespeicherten Inhalte elektronischer Kommunikation zu gelangen, benötigen die Strafverfolgungsbehörden in der Regel eine entsprechende richterliche Anordnung, die auf dem hinreichenden Verdacht basiert, dass das betreffende Konto Nachweise für eine Straftat enthält. ([166]) Um Informationen über die registrierten Abonnenten, IP-Adressen und dazugehörigen Zeitstempel und Rechnungsinformationen einholen zu können, können die Strafverfolgungsbehörden eine entsprechende Anordnung verwenden. Für die meisten anderen gespeicherten, nichtinhaltlichen Informationen wie E-Mail-Header ohne Betreffzeile, müssen die Strafverfolgungsbehörden eine richterliche Anordnung einholen, die erteilt wird, wenn der Richter überzeugt ist, dass es hinreichende Gründe für die Annahme gibt, dass die beantragten Informationen für laufende strafrechtliche Ermittlungen relevant sind.

(97) Anbieter, die Anfragen nach dem Stored Communications Act erhalten, können den Kunden oder Teilnehmer, dessen Informationen angefordert wurden, freiwillig benachrichtigen, es sei denn, die zuständige Strafverfolgungsbehörde erwirkt eine Schutzanordnung, die eine solche Benachrichtigung untersagt. ([167]) Eine solche Schutzanordnung ist eine richterliche Anordnung, die einen Anbieter von elektronischen Kommunikationsdiensten oder von ausgelagerten Rechendiensten, an den ein Befehl, eine Anordnung zur Herausgabe von Daten oder eine richterliche Anordnung gerichtet ist, verpflichtet, keine andere Person von dem Befehl, der Anordnung oder der richterlichen Anordnung in Kenntnis zu setzen, solange das Gericht es nicht für angemessen hält. Schutzanordnungen werden erlassen, wenn ein Gericht feststellt, dass Grund zu der Annahme besteht, dass eine Offenlegung die Ermittlungen ernsthaft gefährden oder das Verfahren unangemessen verzögern würde, z. B. weil dadurch Leib oder Leben einer Person gefährdet, die Flucht vor der Strafverfolgung ermöglicht oder potenzielle Zeugen eingeschüchtert würden. In einer Absichtserklärung des stellvertretenden Justizministers (die für alle Rechtsanwälte und Mitarbeiter des Justizministeriums verbindlich ist) werden die Staatsanwälte aufgefordert, die Notwendigkeit einer Schutzanordnung eingehend zu prüfen und dem Gericht gegenüber zu begründen, inwieweit die gesetzlichen Kriterien für den Erlass einer Schutzanordnung im konkreten Fall erfüllt sind. ([168]) In der Absichtserklärung wird auch gefordert, dass Anträge auf Schutzanordnungen in der Regel nicht darauf abzielen sollten, die Benachrichtigung um mehr als ein Jahr zu verzögern. In Ausnahmefällen, in denen Anordnungen von längerer Dauer erforderlich sein können, dürfen solche Anordnungen nur mit schriftlicher Zustimmung eines vom US-Justizminister oder dem zuständigen stellvertretenden Justizminister benannten Aufsichtsbeamten beantragt werden. Darüber hinaus muss die Staatsanwaltschaft nach Abschluss der Ermittlungen unverzüglich prüfen, ob es eine Grundlage für die Aufrechterhaltung noch bestehender Schutzanordnungen gibt, und, wenn dies nicht der Fall ist, die Schutzanordnung aufheben und sicherstellen, dass der Diensteanbieter davon in Kenntnis gesetzt wird. ([169])

([164]) 18 U.S.C. §3123.

([165]) 18 U.S.C. §§ 2701-2713.

([166]) 18 U.S.C. §§ 2701(a)-(b)(1)(A). Wenn der betroffene Teilnehmer oder Kunde benachrichtigt wird (entweder im Voraus oder unter bestimmten Umständen durch eine verzögerte Benachrichtigung), können inhaltliche Informationen, die länger als 180 Tage gespeichert werden, auch aufgrund einer behördlichen Anordnung oder einer Anordnung der Grand Jury (18 U.S.C. §§ 2701(b)(1)(B)) oder aufgrund einer richterlichen Anordnung erlangt werden (wenn berechtigte Gründe für die Annahme bestehen, dass die Informationen für eine laufende strafrechtliche Ermittlung relevant und wesentlich sind) (18 U.S.C. §§ 2701(d)). Nach einem Urteil des Bundesberufungsgerichts erhalten Ermittlungsbeamte der Regierung jedoch in der Regel eine richterliche Anordnung, um den Inhalt privater Kommunikation oder gespeicherte Daten von einem kommerziellen Kommunikationsdienstleister zu erhalten. United States v. Warshak, 631 F.3d 266 (6th Cir. 2010).

([167]) 18 U.S.C. § 2705(b).

([168]) Siehe die Absichtserklärung des stellvertretenden Justizminister Rod Rosenstein vom 19. Oktober 2017 über eine restriktivere Politik bei Anträgen auf Schutzanordnungen (oder Geheimhaltungsanordnungen), abrufbar unter https://www.justice.gov/criminal-ccips/page/file/1005791/download.

([169]) Absichtserklärung der stellvertretenden Justizministerin Lisa Moncao vom 27. Mai 2022 über eine ergänzende Richtlinie zu Anträgen auf Schutzanordnungen nach 18 U.S.C. §2705(b).

(98) Strafverfolgungsbehörden können auch leitungsgebundene, mündliche oder elektronische Kommunikation in Echtzeit auf der Grundlage einer richterlichen Anordnung abhören, in der ein Richter unter anderem feststellt, 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. ([170])

(99) Weitere Schutzmaßnahmen sind in verschiedenen Strategien und Richtlinien des Justizministeriums enthalten, darunter die Attorney General Guidelines for Domestic FBI Operations (Leitlinien des Justizministers für Inlandseinsätze des FBI) (im Folgenden „AGG-DOM"), die das Federal Bureau of Investigation (FBI) unter anderem verpflichten, die mit den geringsten Eingriffen verbundenen Ermittlungsmethoden anzuwenden und die Auswirkungen auf die Privatsphäre und die Bürgerrechte zu berücksichtigen. ([171])

(100) Den Erklärungen der US-Regierung zufolge gilt bei strafrechtlichen Ermittlungen auf einzelstaatlicher Ebene (wenn diese auf Rechtsvorschriften der Bundesstaaten basieren) das gleiche oder ein noch höheres Schutzniveau, wie das vorstehend Beschriebene. ([172]) Insbesondere in den Verfassungsbestimmungen sowie in den Gesetzen und der Rechtsprechung auf Ebene der einzelnen Bundesstaaten wird der oben genannte Schutz vor unangemessenen Durchsuchungen und Beschlagnahmen bekräftigt, indem die Ausstellung eines Durchsuchungsbefehls vorgeschrieben wird. ([173]) Ähnlich wie bei dem auf Bundesebene gewährten Schutz dürfen Durchsuchungsbefehle nur nach Nachweis eines hinreichenden Verdachts ausgestellt werden und müssen die zu durchsuchende Örtlichkeit und die in Gewahrsam zu nehmenden Personen oder Gegenstände genau bezeichnen. ([174])

([170]) 18 U.S.C. §§ 2510-2522.

([171]) Attorney General's Guidelines for Domestic Federal Bureau of Investigation (FBI) Operations (September 2008), abrufbar unter http://www.justice.gov/archive/opa/docs/guidelines.pdf. Weitere Vorschriften und Strategien, die die Ermittlungsaktivitäten von Bundesanwälten einschränken, sind im United States Attorneys' Manual (Anwaltshandbuch der Vereinigten Staaten) niedergelegt, das unter http://www.justice.gov/usam/united-states-attorneys-manual abgerufen werden kann. Abweichungen von diesen Leitlinien bedürfen der vorherigen Genehmigung durch den Direktor, den stellvertretenden Direktor oder den vom Direktor benannten stellvertretenden Exekutivdirektor des FBI, es sei denn, eine solche Genehmigung kann wegen der Unmittelbarkeit oder Schwere der Bedrohung für die Sicherheit von Personen oder Eigentum oder für die nationale Sicherheit nicht eingeholt werden (in diesem Fall ist der Direktor oder eine andere befugte Person so bald wie möglich zu benachrichtigen). Werden die Leitlinien nicht eingehalten, muss das FBI das Justizministerium benachrichtigen, das seinerseits den Justizminister und den stellvertretenden Justizminister benachrichtigt.

([172]) Anhang VI Fußnote 2. Siehe auch z. B. Arnold v. City of Cleveland, 67 Ohio St.3d 35, 616 N. E.2d 163, 169 (1993) („In den Bereichen der Rechte des Einzelnen und der Bürgerrechte sieht die Verfassung der Vereinigten Staaten, soweit für die Bundesstaaten anwendbar, eine Untergrenze vor, die bei Entscheidungen staatlicher Gerichte einzuhalten ist"); Cooper v. California, 386 U.S. 58, 62, 87 S.Ct. 788, 17 L.Ed.2d 730 (1967) („Unsere Entscheidung berührt natürlich nicht die Befugnis des Staates, in Bezug auf Durchsuchungen und Beschlagnahmen höhere Standards vorzuschreiben, als in der Bundesverfassung vorgesehenen sind, wenn dieser sich dafür entscheidet."); Petersen v. City of Mesa, 63 P.3d 309, 312 (Ariz. Ct. App. 2003) („Obwohl die Verfassung von Arizona strengere Standards für Durchsuchungen und Beschlagnahmen vorschreiben kann, als dies die Bundesverfassung tut, dürfen die Gerichte von Arizona nicht einen geringeren Schutz gewähren als der Vierte Zusatzartikel").

([173]) Die meisten Bundesstaaten haben den Schutz des Vierten Zusatzartikels in ihre Verfassungen übernommen. Siehe Alabama Const. art. I, § 5); Alaska Const. art. I, § 14; 1; Arkansas Const. art. II,§ 15; California Const. art. I, § 13; Colorado Const. art. II, § 7; Connecticut Const. art. I, § 7; Delaware Const. art. I, § 6; Florida. Const. art. I, § 12; Georgia Const. art. I, § I, para. XIII; Hawaii Const. art. I, § 7; Idaho Const. art. I, § 17; Illinois Const. art. I, § 6; Indiana Const. art. I, § 11; Iowa Const. art. I, § 8; Kansas Const. Bill of Rights, § 15; Kentucky Const. § 10; Louisiana Const. art. I, § 5; Maine Const. art. I, § 5; Massachusetts Const. Decl. of Rights art. 14; Michigan Const. art. I, § 11; Minnesota Const. art. I, § 10; Mississippi Const. art. III, § 23; Missouri Const. art. I, § 15; Montana Const. art. II, § 11; Nebraska Const. art. I, § 7; Nevada Const. art. I, § 18; New Hampshire Const. pt. 1, art. 19; N.J. Const. art. II, § 7; New Mexico Const. art. II, § 10; New York Const. art. I, § 12; North Dakota Const. art. I, § 8; Ohio Const. art. I, § 14; Oklahoma Const. art. II, § 30; Oregon Const. art. I, § 9; Pennsylvania Const. art. I, § 8; Rhode Island Const. art. I, § 6; South Carolina Const. art. I, § 10; South Dakota Const. art. VI, § 11; Tennessee Const. art. I, § 7; Texas Const. art. I, § 9; Utah Const. art. I, § 14; Vermont Const. ch. I, art. 11; West Virginia Const. art. III, § 6; Wisconsin Const. art. I, § 11; Wyoming Const. art. I, § 4. Andere (z. B. Maryland, North Carolina und Virginia) haben in ihren Verfassungen spezifische Formulierungen in Bezug auf gerichtliche Anordnungen verankert, die von den Gerichten so ausgelegt wurden, dass sie einen dem Schutz des Vierten Zusatzartikels ähnlichen oder höheren Schutz bieten (siehe Maryland. Decl. of Rts. art. 26; North Carolina Const. art. I, § 20; Virginia Const. art. I, § 10, und einschlägige Rechtsprechung, z. B. Hamel v. State, 943 A.2d 686, 701 (Md. Ct. Spec. App. 2008; State v. Johnson, 861 S.E.2d 474, 483 (N.C. 2021) und Lowe v. Commonwealth, 337 S.E.2d 273, 274 (Va. 1985)). Schließlich haben Arizona und Washington verfassungsrechtliche Bestimmungen, die die Privatsphäre allgemeiner schützen (Arizona Const. Art. 2 § 8; Washington Const. art. I, § 7), die von den Gerichten so ausgelegt wurden, dass sie mehr Schutz als der Vierte Zusatzartikel bieten (siehe z. B. State v. Bolt, 689 P.2d 519, 523 (Ariz. 1984), State v. Ault, 759 P.2d 1320, 1324 (Ariz. 1988), State v. Myrick, 102 Wn.2d 506, 511, 688 P.2d 151, 155 (1984), State v. Young, 123 Wn.2d 173, 178, 867 P.2d 593, 598 (1994)).

([174]) Siehe z. B. California Penal Code § 1524.3(b); Rule 3.6-3.13 Alabama Rules of Criminal Procedure; Section 10.79.035; Revised Code of Washington; Section 19.2-59 of Chapter 5, Title 19.2 Criminal Procedure, Code of Virginia.

3.1.1.2 *Weiterverwendung der erhobenen Daten*

(101) Für die Weiterverwendung von Daten, die von den Strafverfolgungsbehörden des Bundes erhoben wurden, sind in verschiedenen Gesetzen, Leitlinien und Normen spezifische Schutzmaßnahmen vorgesehen. Mit Ausnahme der spezifischen Instrumente, die für die Tätigkeiten des FBI gelten (AGG-DOM und FBI Domestic Investigations and Operations Guide), gelten die in diesem Abschnitt beschriebenen Anforderungen im Allgemeinen für die Weiterverwendung von Daten durch eine Bundesbehörde, einschließlich Daten, auf die zu zivilen oder regulatorischen Zwecken zugegriffen wird. Dazu gehören die Anforderungen, die sich aus den Mitteilungen/Verordnungen des Office of Management and Budget, des Federal Information Security Management Modernization Act, des E-Government Act und des Federal Records Act ergeben.

(102) Das Office of Management and Budget (OMB) hat aufgrund seiner Befugnisse nach dem Clinger-Cohen Act (P.L. 104-106, Division E) und dem Computer Security Act of 1987 (P.L.100-235) das Circular No. A-130 (Rundschreiben Nr. A-130) erlassen, um allgemeine verbindliche Leitlinien für alle Bundesbehörden (einschließlich Strafverfolgungsbehörden) bei der Verarbeitung personenbezogener Daten festzulegen. ([175]) Insbesondere verpflichtet das Rundschreiben alle Bundesbehörden, „die Erstellung, Erhebung, Nutzung, Verarbeitung, Speicherung, Verwaltung, Verbreitung und Weitergabe personenbezogener Daten auf das zu beschränken, was rechtlich zulässig, sachdienlich und nach vernünftigem Ermessen zur ordnungsgemäßen Erfüllung der der Behörde übertragenen Aufgaben erforderlich ist". ([176]) Darüber hinaus müssen die Bundesbehörden weitestgehend sicherstellen, dass personenbezogene Daten richtig, sachdienlich, aktuell und vollständig sind und auf das für die ordnungsgemäße Erfüllung der Aufgaben der Behörde erforderliche Mindestmaß beschränkt werden. Im Allgemeinen müssen Bundesbehörden ein umfassendes Datenschutzprogramm einrichten, um die Einhaltung der geltenden Datenschutzanforderungen zu gewährleisten, Datenschutzmaßnahmen zu entwickeln und zu evaluieren und Datenschutzrisiken zu verwalten, Verfahren zur Erkennung, Dokumentation und Meldung von Vorfällen im Zusammenhang mit der Einhaltung der Datenschutzbestimmungen unterhalten, Programme zur Sensibilisierung für den Datenschutz und zur Schulung von Mitarbeitern und Auftragnehmern entwickeln, Strategien und Verfahren einführen, um sicherzustellen, dass das Personal die Verantwortung für die Einhaltung der Datenschutzanforderungen und -maßnahmen übernimmt. ([177])

(103) Darüber hinaus verpflichtet der E-Government Act ([178]) alle Bundesbehörden (einschließlich der Strafverfolgungsbehörden), Schutzmaßnahmen für die Informationssicherheit zu treffen, die dem Risiko und dem Ausmaß des Schadens angemessen sind, der durch unbefugten Zugang, unbefugte Nutzung, Offenlegung, Störung, Veränderung oder Vernichtung entstehen könnte, einen Chief Information Officer (IT-Beauftragter) zu ernennen, der die Einhaltung der Informationssicherheitsanforderungen sicherstellt, und eine jährliche unabhängige Evaluierung (z. B. durch einen Generalinspekteur, siehe Erwägungsgrund 109) ihrer Informationssicherheitsprogramme und -praktiken durchzuführen. ([179]) In ähnlicher Weise müssen Informationen, die sich im Besitz von Bundesbehörden befinden, nach dem Federal Records Act (FRA) ([180]) und den ergänzenden Vorschriften ([181]) Schutzmaßnahmen unterliegen, die die physische Integrität der Informationen gewährleisten und sie vor unbefugtem Zugriff schützen.

(104) Auf der Grundlage von Bundesgesetzen, einschließlich des Federal Information Security Modernisation Act von 2014, haben das OMB und das National Institute of Standards and Technology (NIST) Standards entwickelt, die für Bundesbehörden (einschließlich Strafverfolgungsbehörden) verbindlich sind und in denen die Mindestanforderungen an die Informationssicherheit, die eingeführt werden müssen, weiter spezifiziert werden. Hierzu gehören Zugangskontrollen, Sensibilisierung und Schulung, Notfallplanung, Reaktion auf Vorfälle, Prüfungs- und Rechenschaftsinstrumente, Gewährleistung der System- und Informationsintegrität, Durchführung von Bewertungen des Datenschutzes und der Sicherheitsrisiken usw. ([182]) Darüber hinaus müssen alle Bundesbehörden

([175]) D. h. „Informationen, die dazu benutzt werden können, die Identität einer Person zu bestimmen oder zurückzuverfolgen, entweder allein oder in Verbindung mit anderen Informationen, die mit einer bestimmten Person in Verbindung gebracht werden oder werden können", siehe OMB Circular No. A-130, S. 33 (Definition von „personenbezogenen Daten").

([176]) OMB Circular No. A-130, Managing Information as a Strategic Resource, Anlage II, Responsibilities for Managing Personally Identifiable Information, 81 Fed. Reg. 49,689 (28. Juli 2016), S. 17.

([177]) Anlage II §5(a)-(h).

([178]) 44 U.S.C. Kapitel 36.

([179]) 44 U.S.C. §§ 3544-3545.

([180]) FAC, 44 U.S.C. § 3105.

([181]) 36 C.F.R. §§ 1228.150 ff., 1228.228 und Anlage A.

([182]) Siehe z. B. OMB Circular No. A-130; NIST SP 800-53, Rev. 5, Security and Privacy Controls for Information Systems and Organizations (10. Dezember 2020) und die NIST Federal Information Processing Standards 200: Minimum Security Requirements for Federal Information and Information Systems.

(einschließlich der Strafverfolgungsbehörden) einen Plan für den Umgang mit Datenschutzverletzungen, einschließlich der Reaktion auf solche Datenschutzverletzungen und der Bewertung des Schadensrisikos, nach den Leitlinien des OMB unterhalten und umsetzen. ([183])

(105) In Bezug auf die Aufbewahrung von Daten verpflichtet der FRA ([184]) die US-Bundesbehörden (einschließlich der Strafverfolgungsbehörden), für ihre Akten Aufbewahrungsfristen festzulegen (nach deren Ablauf die Akten vernichtet werden müssen), die von der National Archives and Record Administration ([185]) zu genehmigen sind. Die Dauer dieser Aufbewahrungsfristen wird unter Berücksichtigung verschiedener Faktoren festgelegt, z. B. der Art der Ermittlung, der Frage, ob das Beweismaterial für die Ermittlung noch relevant ist, usw. Im Fall des FBI müssen die Behörden nach den AGG-DOM über einen solchen Aufbewahrungsplan verfügen und ein System unterhalten, das es ihnen ermöglicht, den Stand und die Grundlage der Ermittlungen sofort abzurufen.

(106) Schließlich enthält auch das OMB Circular No. A-130 bestimmte Anforderungen an die Weitergabe personenbezogener Daten. Die Verbreitung und Offenlegung personenbezogener Daten ist grundsätzlich auf das zu beschränken, was rechtlich zulässig, sachdienlich und nach vernünftigem Ermessen zur ordnungsgemäßen Erfüllung der der Behörde übertragenen Aufgaben erforderlich ist. ([186]) Wenn sie personenbezogene Daten an andere Regierungsstellen weitergeben, müssen US-Bundesbehörden gegebenenfalls Bedingungen (einschließlich der Durchführung spezifischer Sicherheits- und Datenschutzkontrollen) festlegen, die die Verarbeitung der Daten durch schriftliche Vereinbarungen (einschließlich Verträgen, Vereinbarungen zur Datennutzung, Vereinbarungen zum Informationsaustausch und Absichtserklärungen) regeln. ([187]) Im Hinblick auf die Gründe, aus denen Informationen verbreitet werden dürfen, bestimmen die AGG-DOM und der FBI Domestic Investigations and Operations Guide ([188]) beispielsweise, dass das FBI gesetzlich dazu verpflichtet sein kann (z. B. im Rahmen eines internationalen Abkommens) oder es ihm unter bestimmen Umständen gestattet ist, Informationen zu verbreiten, z. B. an andere US-Behörden, wenn die Offenlegung mit dem Zweck, für den die Informationen erhoben wurden, vereinbar ist und diese in deren Zuständigkeitsbereich fallen, an Kongressausschüsse, an ausländische Behörden, wenn die Informationen in deren Zuständigkeitsbereich fallen und die Verbreitung mit den Interessen der Vereinigten Staaten vereinbar ist, insbesondere zum Schutz der Sicherheit von Personen oder Eigentum oder zum Schutz vor oder zur Verhinderung von Straftaten oder Bedrohungen der nationalen Sicherheit erforderlich ist und die Offenlegung mit dem Zweck vereinbar ist, für den die Informationen erhoben wurden. ([189])

3.1.2 *Aufsicht*

(107) Die Tätigkeit der Strafverfolgungsbehörden des Bundes unterliegt der Aufsicht durch verschiedene Stellen. ([190]) Wie in den Erwägungsgründen 92 bis 99 erläutert, umfasst dies in den meisten Fällen die vorherige Aufsicht durch die Justiz, die individuelle Erhebungsmaßnahmen genehmigen muss, bevor diese eingesetzt werden können. Darüber hinaus überwachen andere Stellen verschiedene Phasen der Tätigkeit der Strafverfolgungsbehörden, einschließlich der Erhebung und Verarbeitung personenbezogener Daten. Zusammen stellen diese gerichtlichen und außergerichtlichen Stellen sicher, dass die Strafverfolgungsbehörden einer unabhängigen Aufsicht unterliegen.

([183]) Absichtserklärung 17–12, „Preparing for and Responding to a Breach of Personally Identifiable Information" abrufbar unter https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12_0.pdf und OMB Circular No. A-130. Zum Beispiel die Verfahren zur Reaktion auf Datenschutzverletzungen des Justizministeriums, siehe https://www.justice.gov/file/4336/download.

([184]) FRA, 44 U.S.C. §§ 3101 ff.

([185]) Die National Archives and Records Administration ist befugt, die Aktenführung der Behörden zu bewerten und zu entscheiden, ob die weitere Aufbewahrung bestimmter Akten gerechtfertigt ist (44 U.S.C. §§ 2904(c), 2906).

([186]) OMB Circular No. A-130, Abschnitt 5.f.1.(d).

([187]) OMB Circular No. A-130, Anlage I §3(d).

([188]) Siehe auch FBI Domestic Investigations and Operations Guide (DIOG), Abschnitt 14.

([189]) AGG-DOM, Abschnitt VI, B und C; FBI Domestic Investigations and Operations Guide (DIOG), Abschnitt 14.

([190]) Die in diesem Abschnitt genannten Instrumente gelten auch für die Erhebung und Nutzung von Daten für zivile und regulatorische Zwecke durch Bundesbehörden. Die Zivil- und Regulierungsbehörden des Bundes unterliegen der Kontrolle durch ihre jeweiligen Generalinspektoren und der Aufsicht durch den Kongress, einschließlich des Government Accountability Office, der Rechnungsprüfungs- und Untersuchungsbehörde des Kongresses. Sofern die Behörde nicht über einen Datenschutz- und Bürgerrechtsbeauftragten (Privacy and Civil Liberties Officer) verfügt – eine Stelle, die typischerweise in Behörden wie dem Justizministerium und dem Ministerium für Innere Sicherheit (Department of Homeland Security) aufgrund deren Zuständigkeiten im Bereich der Strafverfolgung und der nationalen Sicherheit angesiedelt ist – fallen diese Aufgaben in den Zuständigkeitsbereich des Senior Agency Official for Privacy. Alle Bundesbehörden sind rechtlich verpflichtet, einen Senior Agency Official for Privacy zu benennen, der dafür verantwortlich ist, die Einhaltung der Datenschutzgesetze durch die Behörde sicherzustellen und damit zusammenhängende Angelegenheiten zu überwachen. Siehe z. B. OMB M-16-24, Role and Designation of Senior Agency Officials for Privacy (2016).

(108) Zunächst gibt es in verschiedenen Abteilungen, die für die Strafverfolgung zuständig sind, Datenschutz- und Bürgerrechtsbeauftragte. ([191]) 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 Privatpersonen nachzugehen, die der Meinung sind, dass ihre Privatsphäre oder ihre Bürgerrechte verletzt wurden. Die Leiter der einzelnen Abteilungen oder Nachrichtendienste müssen sicherstellen, dass die Datenschutz- und Bürgerrechtsbeauftragten über die für die Erfüllung ihrer Aufgaben erforderlichen Materialien und Ressourcen verfügen, dass sie Zugang zu den für die Erfüllung ihrer Aufgaben erforderlichen Materialien und zum Personal haben und dass sie über vorgeschlagene politische Änderungen informiert und dazu konsultiert werden. ([192]) Datenschutz- und Bürgerrechtsbeauftragte übermitteln dem Kongress regelmäßig einen Bericht mit Angaben zur Anzahl und Art der bei der Abteilung/beim Nachrichtendienst eingegangenen Beschwerden sowie einen Überblick über die Bearbeitung der Beschwerden, die durchgeführten Überprüfungen und Recherchen und die Auswirkungen der von den Beauftragten geleisteten Arbeit. ([193])

(109) Zweitens beaufsichtigt ein unabhängiger Generalinspekteur die Aktivitäten des Justizministeriums, einschließlich des FBI. ([194]) Die Generalinspekteure sind rechtlich unabhängig ([195]) und haben die Aufgabe, unabhängige Untersuchungen, Prüfungen und Inspektionen der Programme und Operationen des Ministeriums durchzuführen. Sie haben Zugriff auf alle Unterlagen, Berichte, Audits, Überprüfungen, Dokumente, Schriftstücke, Empfehlungen oder sonstiges einschlägiges Material, dessen Herausgabe sie notfalls unter Strafandrohung anordnen können, und sind zur Beweisaufnahme berechtigt. ([196]) Zwar geben Generalinspekteure Empfehlungen für Korrekturmaßnahmen ab, die nicht bindend sind, doch werden ihre Berichte, auch über die getroffenen (oder unterlassenen) ([197]) Folgemaßnahmen, in der Regel öffentlich gemacht und dem Kongress übermittelt, der auf dieser Grundlage seine Kontrollfunktion wahrnehmen kann (siehe Erwägungsgrund 111) ([198]).

([191]) Siehe 42 U.S.C. § 2000ee-1. Dazu gehören beispielsweise das Justizministerium, das Ministerium für Innere Sicherheit und das FBI. Im Ministerium für Innere Sicherheit ist zusätzlich ein Datenschutzbeauftragter (Chief Privacy Officer) für die Wahrung und Verbesserung des Datenschutzes und die Förderung der Transparenz innerhalb des Ministeriums zuständig (6 U.S.C. 142, Abschnitt 222). Alle Systeme, Technologien, Formulare und Programme des Ministeriums für Innere Sicherheit, die personenbezogene Daten erfassen oder Auswirkungen auf den Datenschutz haben, unterliegen der Aufsicht des Datenschutzbeauftragten, der Zugang zu allen Unterlagen, Berichten, Prüfungen, Dokumenten, Schriftstücken, Empfehlungen und anderen Materialien hat, die dem Ministerium vorliegen, und dessen Herausgabe sie notfalls anordnen können. Der Datenschutzbeauftragte hat dem Kongress jährlich über die datenschutzrelevanten Aktivitäten des Ministeriums, einschließlich der Beschwerden über Datenschutzverletzungen, zu berichten.

([192]) 42 U.S.C. § 2000ee-1(d).

([193]) Siehe 42 U.S.C. §§ 2000ee-1 (f)(1)-(2). So geht aus dem Bericht des leitenden Datenschutz- und Bürgerrechtsbeauftragten des Justizministeriums und des Büros für Datenschutz und Bürgerrechte (Office of Data Protection and Civil Rights) für den Zeitraum von Oktober 2020 bis März 2021 hervor, dass 389 Datenschutzprüfungen durchgeführt wurden, einschließlich von Informationssystemen und anderen Programmen. (https://www.justice.gov/d9/pages/attachments/2021/05/10/2021-4-21opclsection803reportfy20sa1_final.pdf).

([194]) In ähnlicher Weise wurde mit dem Homeland Security Act von 2002 ein Büro des Generalinspekteurs (Office of Inspector General) im Ministerium für Innere Sicherheit eingerichtet.

([195]) Generalinspekteure genießen Kündigungsschutz und können nur vom Präsidenten abberufen werden, der dem Kongress schriftlich die Gründe für die Abberufung darlegen muss.

([196]) Siehe Inspector General Act of 1978,§ 6.

([197]) Vgl. in diesem Zusammenhang z. B. die Übersicht des Büros des Generalinspekteurs des Justizministeriums über die von ihm abgegebenen Empfehlungen und deren Umsetzung durch Folgemaßnahmen der Regierungsstellen, https://oig.justice.gov/sites/default/files/reports/22-043.pdf.

([198]) Siehe Inspector General Act of 1978, §§ 4(5), 5. So hat beispielsweise das Büro des Generalinspekteurs des Justizministeriums kürzlich seinen Halbjahresbericht an den Kongress (1. Oktober 2021–31. März 2022, https://oig.justice.gov/node/23596) veröffentlicht, der einen Überblick über seine Prüfungen, Bewertungen, Inspektionen, Sonderprüfungen und Untersuchungen von Programmen und Operationen des Justizministeriums gibt. Zu diesen Maßnahmen gehörte eine Untersuchung gegen einen ehemaligen Auftragnehmer wegen der unrechtmäßigen Weitergabe von elektronischen Überwachungsdaten (Abhören einer Person) im Rahmen einer laufenden Ermittlung, die zu einer Verurteilung des Auftragnehmers führte. Das Büro des Generalinspekteurs führte auch eine Untersuchung der Informationssicherheitsprogramme und -praktiken der Behörden des Justizministeriums durch, bei der die Wirksamkeit der Informationssicherheitsstrategien, -verfahren und -praktiken einer repräsentativen Untergruppe von Behördensystemen geprüft wurde.

(110) Drittens unterliegen Abteilungen mit Zuständigkeiten im Bereich der Strafverfolgung, soweit sie Maßnahmen zur Terrorismusbekämpfung durchführen, der Aufsicht durch die Stelle zur Überwachung des Schutzes der Privatsphäre und der bürgerlichen Freiheiten (Privacy and Civil Liberties Oversight Board) (PCLOB), einer unabhängigen Stelle innerhalb der Exekutive, die sich aus einem aus fünf Mitgliedern bestehenden überparteilichen Gremium zusammensetzt, das vom Präsidenten mit Zustimmung des Senats für eine festgelegte Amtszeit von sechs Jahren ernannt wird. ([199]) Nach seinem Gründungsstatut ist das PCLOB mit Aufgaben im Bereich der Terrorismusbekämpfung und deren Umsetzung betraut, wobei der Schutz der Privatsphäre und der bürgerlichen Freiheiten im Vordergrund steht. Bei der Überprüfung hat es 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. ([200]) Es erhält Berichte von Bürgerrechts- und Datenschutzbeauftragten verschiedener Regierungsstellen ([201]), kann gegenüber den Regierungs- und Strafverfolgungsbehörden Empfehlungen abgeben und erstattet regelmäßig den Ausschüssen des Kongresses und dem Präsidenten Bericht. ([202]) Die Berichte des PCLOB, einschließlich der Berichte an den Kongress, müssen so weit wie möglich veröffentlicht werden. ([203])

(111) Schließlich unterliegen die Strafverfolgungsmaßnahmen der Aufsicht durch spezielle Ausschüsse des US-Kongresses (die Justizausschüsse des Repräsentantenhauses und des Senats). Die Justizausschüsse üben ihre regelmäßige Aufsicht auf verschiedene Weise aus, insbesondere durch Anhörungen, Untersuchungen, Überprüfungen und Berichte. ([204])

3.1.3 ***Rechtsbehelfe***

(112) Wie bereits erwähnt, benötigen die Strafverfolgungsbehörden in den meisten Fällen eine vorherige richterliche Genehmigung für die Erhebung personenbezogener Daten. Dies gilt zwar nicht für behördliche Anordnungen zur Herausgabe von Daten, doch sind diese auf bestimmte Situationen beschränkt und unterliegen zumindest dann einer unabhängigen gerichtlichen Überprüfung, wenn die Regierung sie vor Gericht durchsetzen will. Insbesondere 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. ([205])

(113) Privatpersonen können in Bezug auf die Verarbeitung ihrer personenbezogenen Daten zunächst Ersuchen oder Beschwerden bei den Strafverfolgungsbehörden einreichen. Dies schließt die Möglichkeit ein, den Zugang zu personenbezogenen Daten und deren Berichtigung zu beantragen. ([206]) In Bezug auf Maßnahmen im Zusammenhang mit der Terrorismusbekämpfung können Privatpersonen auch eine Beschwerde bei Datenschutz- und Bürgerrechtsbeauftragen (oder anderen Datenschutzbeauftragten) bei Strafverfolgungsbehörden einreichen. ([207])

(114) Darüber hinaus gewährt das amerikanische Recht Privatpersonen eine Reihe gerichtlicher Rechtsbehelfe gegen staatliche Behörden oder einzelne Mitarbeiter, sofern diese Behörden personenbezogene Daten verarbeiten. ([208]) Diese Rechtsschutzmöglichkeiten, die insbesondere der APA, der Freedom of Information Act (FOIA) und der Electronic Communications Privacy Act (ECPA) einräumen, stehen allen Personen unabhängig von ihrer Nationalität offen, sofern die erforderlichen Voraussetzungen gegeben sind.

([199]) Die Mitglieder der Stelle werden ausschließlich aufgrund ihrer beruflichen Qualifikation, ihrer Verdienste, ihres Ansehens in der Öffentlichkeit, ihres Sachverstands auf dem Gebiet der bürgerlichen Freiheiten und des Schutzes der Privatsphäre sowie ihrer einschlägigen Erfahrung und unabhängig von ihrer Parteizugehörigkeit ausgewählt. In keinem Fall dürfen mehr als drei Mitglieder der Stelle derselben politischen Partei angehören. Eine Person, die in die Stelle berufen wird, darf während ihrer Amtszeit im PCLOB kein Mandatsträger, Beamter oder Angestellter der Bundesregierung sein, außer in ihrer Eigenschaft als Mitglied des PCLOB. Siehe 42 U.S.C. § 2000ee (h).

([200]) 42 U.S.C. § 2000ee (g).

([201]) Siehe 42 U.S.C. § 2000ee-1 (f)(1)(A)(iii). Dazu zählen zumindest das Justizministerium, das Verteidigungsministerium, das Ministerium für Innere Sicherheit sowie andere Regierungsstellen oder Einrichtungen der Exekutive, deren Einbeziehung das PCLOB für sinnvoll erachtet.

([202]) 42 U.S.C. § 2000ee, (e).

([203]) 42 U.S.C. § 2000ee (f).

([204]) So veranstalten die Ausschüsse thematische Anhörungen (vgl. z. B. die jüngste Anhörung des Justizausschusses des Repräsentantenhauses zum Thema „Digitale Rasterfahndung“, https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4983) sowie regelmäßige Aufsichtsanhörungen, z. B. durch das FBI und das Justizministerium, vgl. https://www.judiciary.senate.gov/meetings/08/04/2022/oversight-of-the-federal-bureau-of-investigation; https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4966 und https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4899.

([205]) Siehe Anhang VI.

([206]) OMB Circular No. A-130, Anlage II, Abschnitt 3(a) and (f), wonach Bundesbehörden auf Antrag von Privatpersonen einen angemessenen Zugang und eine Berichtigung gewährleisten und Verfahren für die Entgegennahme und Bearbeitung von Beschwerden und Anträgen im Zusammenhang mit der Privatsphäre festlegen müssen.

([207]) Siehe 42 U.S.C. § 2000ee-1 in Bezug auf das Justizministerium und das Ministerium für Innere Sicherheit. Siehe auch das OMB Memorandum M-16-24, Role and Designation of Senior Agency Officials for Privacy.

([208]) Die in diesem Abschnitt genannten Rechtsmittel gelten auch für die Erhebung und Nutzung von Daten durch Bundesbehörden für zivile und regulatorische Zwecke.

(115) Nach den Bestimmungen des APA über die gerichtliche Überprüfung ([209]) kann „eine Person, die durch Handlungen einer Behörde einen Schaden oder Nachteil erleidet“, eine gerichtliche Nachprüfung beantragen. ([210]) 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“. ([211])

(116) Konkreter ist in diesem Zusammenhang Titel II des ECPA ([212]), 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. ([213]) 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.

(117) Darüber hinaus gewähren verschiedene weitere Gesetze Privatpersonen das Recht, wegen der Verarbeitung ihrer personenbezogenen Daten staatliche Behörden der USA oder Beamte zu verklagen, so etwa der Wiretap Act ([214]), der Computer Fraud and Abuse Act ([215]), der Federal Torts Claim Act ([216]), der Right to Financial Privacy Act ([217]) und der Fair Credit Reporting Act ([218]).

([209]) 5 U.S.C. § 702.

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

([211]) 5 U.S.C. § 706(2)(A).

([212]) 18 U.S.C. §§ 2701-2712.

([213]) 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) von ausgelagerten Rechendiensten zur Fernspeicherung oder -verarbeitung.

([214]) 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 wegen Verstoßes gegen den Wiretap Act einreichen, unter bestimmten Umständen auch gegen einen einzelnen Regierungsbeamten oder gegen die Vereinigten Staaten. Zur Erhebung von 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).

([215]) 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.

([216]) 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.

([217]) 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 staatliche Zugriff 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.

([218]) 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.

(118) Dem FOIA ([219]), 5 U.S.C. § 552, zufolge hat jede Person das Recht, Zugang zu Unterlagen der Bundesbehörden zu erhalten, auch wenn diese die personenbezogenen Daten der betreffenden Person enthalten. Nach Ausschöpfung aller behördlichen Rechtsbehelfe kann eine Privatperson dieses Recht auf Zugriff vor Gericht geltend machen, sofern die Unterlagen nicht durch eine Ausnahmeregelung oder Strafverfolgungsklausel vor der Offenlegung geschützt sind. ([220]) In diesem Fall prüft das Gericht, ob eine Ausnahmeregelung gilt oder von der zuständigen Behörde rechtmäßig geltend gemacht wurde.

3.2 **Sammlung und Nutzung durch staatliche Stellen der USA aus Gründen der nationalen Sicherheit**

(119) Das Recht der Vereinigten Staaten umfasst verschiedene Einschränkungen und Garantien in Bezug auf den Zugriff auf und die Verwendung von personenbezogenen Daten für die Zwecke der nationalen Sicherheit; ferner sieht es Aufsichtsmechanismen und Rechtsbehelfe vor, die den in Erwägungsgrund 89 dieses Beschlusses genannten Anforderungen entsprechen. Die folgenden Abschnitte enthalten eine detaillierte Bewertung der Bedingungen, unter denen ein solcher Zugriff erfolgen kann, sowie der Garantien, die für die Nutzung dieser Befugnisse gelten.

3.2.1 ***Rechtsgrundlagen, Einschränkungen und Garantien***

3.2.1.1 *Anwendbarer Rechtsrahmen*

(120) Personenbezogene Daten, die von der Union an Organisationen, die dem Datenschutzrahmen EU-USA angehören, übermittelt werden, können von US-Behörden für Zwecke der nationalen Sicherheit auf der Grundlage verschiedener Rechtsinstrumente und vorbehaltlich besonderer Bedingungen und Garantien erhoben werden.

(121) Sobald personenbezogene Daten bei Organisationen mit Sitz in den Vereinigten Staaten eingegangen sind, können US-Nachrichtendienste nur dann Zugang zu diesen Daten für Zwecke der nationalen Sicherheit beantragen, wenn sie dazu gesetzlich ermächtigt sind, insbesondere nach dem Foreign Intelligence Surveillance Act (FISA) oder nach Rechtsvorschriften, die den Zugang durch National Security Letters (NSL) erlauben. ([221]) Der FISA enthält verschiedene Rechtsgrundlagen, die herangezogen werden können, um die im Rahmen des Datenschutzrahmens EU-USA von betroffenen Personen in der EU übermittelten personenbezogenen Daten zu erheben (und anschließend zu verarbeiten) (Abschnitt 105 FISA ([222]), Abschnitt 302 FISA ([223]), Abschnitt 402 FISA ([224]), Abschnitt 501 FISA ([225]) und Abschnitt 702 FISA ([226])), wie in den Erwägungsgründen 142 bis 152 ausführlicher beschrieben.

([219]) 5 U.S.C. § 552.

([220]) Diese Ausnahmen sind jedoch klar umrissen. So 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 zu einer Beeinträchtigung von Strafverfolgungsverfahren führen würde, 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)).

([221]) 12 U.S.C. § 3414, 15 U.S.C. §§ 1681u-1681v und 18 U.S.C. § 2709. Siehe Erwägungsgrund 153.

([222]) 50 U.S.C. § 1804 über die herkömmliche individuelle elektronische Überwachung.

([223]) 50 U.S.C. § 1822 über Durchsuchungen für die Zwecke der Auslandsaufklärung.

([224]) 50 U.S.C. § 1842 in Verbindung mit § 1841(2) und Abschnitt 3127 des Titels 18 über den Einsatz von Geräten zur Rufnummernerfassung von ausgehenden und eingehenden Anrufen.

([225]) 50 U.S.C. § 1861, wonach das FBI „einen Antrag auf Erlass einer Anordnung stellen kann, die es einem Beförderungsunternehmen, einer öffentlichen Einrichtung, einem Lagerhaus oder einer Mietwagenfirma gestattet, Unterlagen, die sich in ihrem Besitz befinden, für eine Untersuchung zur Sammlung von Informationen im Bereich der Auslandsaufklärung oder für eine Untersuchung über den internationalen Terrorismus herauszugeben“.

([226]) 50 U.S. Code § 1881a, der es den US-Nachrichtendiensten erlaubt, Zugang zu Informationen, einschließlich des Inhalts von Internet-Kommunikationen, von US-Unternehmen zu erhalten, wobei bestimmte Nicht-US-Bürger außerhalb der Vereinigten Staaten mit der gesetzlich vorgeschriebenen Unterstützung von Anbietern elektronischer Kommunikation ins Visier genommen werden.

(122) Die Nachrichtendienste der Vereinigten Staaten haben auch die Möglichkeit, personenbezogene Daten außerhalb der Vereinigten Staaten zu erheben, einschließlich personenbezogener Daten bei der Übermittlung zwischen der Union und den Vereinigten Staaten. Die Erhebung außerhalb der Vereinigten Staaten stützt sich auf die Executive Order 12333 ([227])des Präsidenten der Vereinigten Staaten (im Folgenden „EO 12333"). ([228])

(123) Die Erhebung von Informationen im Bereich der signalerfassenden Auslandsaufklärung ist die für die vorliegende Angemessenheitsfeststellung relevanteste Form der nachrichtendienstlichen Erhebung, da sie die Erhebung elektronischer Kommunikation und von Daten aus Informationssystemen betrifft. Eine solche Erhebung kann von den US-Nachrichtendiensten sowohl innerhalb der Vereinigten Staaten (auf der Grundlage des FISA) als auch bei der Übermittlung von Daten in die Vereinigten Staaten (auf der Grundlage der EO 12333) durchgeführt werden.

(124) Am 7. Oktober 2022 erließ der Präsident der Vereinigten Staaten die EO 14086 zur Verbesserung der Garantien für die Nachrichtendienste der Vereinigten Staaten, die Einschränkungen und Garantien für alle Signalaufklärungsaktivitäten der Vereinigten Staaten festlegt. Diese EO ersetzt weitgehend die Presidential Policy Directive (PPD-28) ([229]), und verschärft die Bedingungen, Einschränkungen und Garantien, die für alle Signalaufklärungsaktivitäten gelten (d. h. auf der Grundlage des FISA und der EO 12333), unabhängig davon, wo sie stattfinden, ([230]) und führt einen neuen Rechtsbehelf ein, mit dem diese Garantien von Privatpersonen geltend gemacht und durchgesetzt werden können ([231]) (siehe im Einzelnen die Erwägungsgründe 176 bis 194). Damit werden die Ergebnisse der Gespräche zwischen der EU und den USA, die nach der Nichtigerklärung des Angemessenheitsbeschlusses der Kommission zum Datenschutzschild durch den Gerichtshof (siehe Erwägungsgrund 6) geführt wurden, in US-Recht umgesetzt. Sie ist daher ein besonders wichtiger Bestandteil des in diesem Beschluss bewerteten Rechtsrahmens.

(125) Die mit der EO 14086 eingeführten Einschränkungen und Garantien ergänzen die in Abschnitt 702 FISA und in der EO 12333 vorgesehenen Einschränkungen und Garantien. Die nachstehend beschriebenen Anforderungen (Abschnitte 3.2.1.2 und 3.2.1.3) sind von Nachrichtendiensten bei der Ausübung von Signalaufklärungstätigkeiten nach Abschnitt 702 FISA und der EO 12333 anzuwenden, z. B. bei der Auswahl/Ermittlung von Kategorien von ausländischen Aufklärungsdaten, die nach Abschnitt 702 FISA zu beschaffen sind, bei der Erhebung von Daten zur Auslandsaufklärung oder Spionageabwehr nach der EO 12333 sowie individuelle Entscheidungen hinsichtlich der zielgenauen Datenerhebung nach Abschnitt 702 FISA und der EO 12333.

(126) Die in dieser Executive Order des Präsidenten festgelegten Anforderungen sind für alle Nachrichtendienste verbindlich. Sie müssen von den Diensten durch Strategien und Verfahren umgesetzt werden, die sie in konkrete Anweisungen für den täglichen Betrieb umwandeln. Dabei räumt die EO 14086 den US-Nachrichtendiensten eine Frist von maximal einem Jahr ein, um ihre bestehenden Strategien und Verfahren zu aktualisieren (d. h. bis zum 7. Oktober 2023) und mit den Anforderungen der EO in Einklang zu bringen. Diese aktualisierten Strategien und Verfahren müssen in Absprache mit dem Justizminister, dem Civil Liberties Protection Officer (Bürgerrechtsbeauftragter) des Director of National Intelligence (Direktor des Nationalen Nachrichtendienstes) (ODNI CLPO) und dem PCLOB – einem unabhängigen Aufsichtsgremium, das befugt ist, die Strategien der Exekutive und deren Umsetzung im Hinblick auf den Schutz der Privatsphäre und der bürgerlichen Freiheiten zu überprüfen (siehe Erwägungsgrund 110 zur Rolle und zum Status des PCLOB) – entwickelt und veröffentlicht werden. ([232]) Sobald die

([227]) EO 12333: United States Intelligence Activities, Federal Register Vol. 40, No. 235 (8. Dezember 1981, geändert am 30. Juli 2008). Die EO 12333 regelt 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.

([228]) Nach Artikel II der US-Verfassung fällt die Gewährleistung der nationalen Sicherheit, einschließlich der Gewinnung von Auslandsnachrichten, in die Zuständigkeit des Präsidenten als Oberbefehlshaber der Streitkräfte.

([229]) Die EO 14086 ersetzt eine frühere Presidential Directive, die PPD 28, mit Ausnahme von Abschnitt 3 und einem ergänzenden Anhang (der von den Nachrichtendiensten eine jährliche Überprüfung ihrer Prioritäten und Anforderungen im Bereich der Signalaufklärung unter Berücksichtigung des Nutzens von Signalaufklärungsaktivitäten für die nationalen Interessen der Vereinigten Staaten und des mit diesen Aktivitäten verbundenen Risikos verlangt) sowie Abschnitt 6 (der allgemeine Bestimmungen enthält), siehe National Security Memorandum on Partial Revocation of Presidential Policy Directive 28, abrufbar unter https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/national-security-memorandum-on-partial-revocation-of-presidential-policy-directive-28/.

([230]) Siehe Abschnitt 5(f) EO 14086, in dem erklärt wird, dass die EO den gleichen Anwendungsbereich hat wie die PPD-28, die nach Fußnote 3 für Signalaufklärungsaktivitäten zur Sammlung von Nachrichten oder Informationen über Kommunikationen galt, mit Ausnahme von Signalaufklärungsaktivitäten zur Erprobung oder Entwicklung nachrichtendienstlicher Fähigkeiten.

([231]) Vgl. in diesem Zusammenhang z. B. Abschnitt 5(h) EO 14086, wonach die durch die EO vorgesehenen Garantien einen Rechtsanspruch begründen und von Privatpersonen über den Rechtsbehelfsmechanismus durchgesetzt werden können.

([232]) Siehe Abschnitt 2(c)(iv)(C) EO 14086.

aktualisierten Strategien und Verfahren in Kraft getreten sind, wird das PCLOB eine Überprüfung durchführen, um sicherzustellen, dass sie mit der EO übereinstimmen. Innerhalb von 180 Tagen nach Abschluss einer solchen Überprüfung durch das PCLOB muss jeder Nachrichtendienst alle Empfehlungen des PCLOB sorgfältig prüfen und umsetzen oder anderweitig berücksichtigen. Am 3. Juli 2023 veröffentlichte die US-Regierung diese aktualisierten Strategien und Verfahren ([233]).

3.2.1.2 *Einschränkungen und Garantien in Bezug auf die Erhebung personenbezogener Daten für Zwecke der nationalen Sicherheit*

(127) Die EO 14086 stellt eine Reihe von weitreichenden Anforderungen auf, die für alle Tätigkeiten im Bereich der Signalaufklärung (Erhebung, Verwendung, Verbreitung usw. von personenbezogenen Daten) gelten.

(128) Erstens müssen diese Tätigkeiten auf einem Gesetz oder einer Ermächtigung des Präsidenten beruhen und im Einklang mit den Rechtsvorschriften der Vereinigten Staaten, einschließlich der Verfassung, durchgeführt werden. ([234])

(129) Zweitens müssen geeignete Garantien getroffen werden, um sicherzustellen, dass der Schutz der Privatsphäre und der bürgerlichen Freiheiten bei der Planung solcher Tätigkeiten in vollem Umfang berücksichtigt wird. ([235])

(130) Insbesondere darf die signalerfassende Aufklärung nur durchgeführt werden, „nachdem auf der Grundlage einer angemessenen Bewertung aller relevanten Faktoren festgestellt wurde, dass die Maßnahme zur Förderung einer validierten Aufklärungspriorität erforderlich ist“ (zum Begriff der „validierten Aufklärungspriorität“ siehe Erwägungsgrund 135). ([236])

(131) Darüber hinaus dürfen solche Maßnahmen nur „in einem Umfang und in einer Art und Weise durchgeführt werden, die in einem angemessenen Verhältnis zu der validierten Aufklärungspriorität stehen, für die sie genehmigt wurden“. ([237]) Mit anderen Worten: Es muss ein angemessenes Gleichgewicht hergestellt werden „zwischen der Bedeutung der angestrebten Aufklärungspriorität und den Auswirkungen auf die Privatsphäre und die bürgerlichen Freiheiten der betroffenen Personen, unabhängig von ihrer Staatsangehörigkeit oder ihrem Wohnort“. ([238])

(132) Um die Einhaltung dieser allgemeinen Anforderungen – die die Grundsätze der Rechtmäßigkeit, Notwendigkeit und Verhältnismäßigkeit widerspiegeln – zu gewährleisten, unterliegt die signalerfassende Aufklärung der Aufsicht (siehe im Einzelnen Abschnitt 3.2.2). ([239])

(133) Diese allgemeinen Anforderungen werden in Bezug auf die Erhebung von Signalaufklärungsdaten durch eine Reihe von Bedingungen und Einschränkungen untermauert, die sicherstellen, dass der Eingriff in die Rechte natürlicher Personen auf das zur Erreichung eines rechtmäßigen Zwecks notwendige und verhältnismäßige Maß beschränkt bleibt.

(134) Erstens schränkt die EO die Gründe für die Erhebung von Signalaufklärungsdaten in zweierlei Hinsicht ein. Einerseits definiert die EO die legitimen Ziele, die mit der Erhebung von Signalaufklärungsdaten verfolgt werden können, z. B. das Verständnis oder die Bewertung der Fähigkeiten, Absichten oder Aktivitäten ausländischer Organisationen, einschließlich internationaler terroristischer Organisationen, die eine tatsächliche oder potenzielle Bedrohung für die nationale Sicherheit der Vereinigten Staaten darstellen, der Schutz vor ausländischen militärischen Kapazitäten und Aktivitäten, das Verständnis oder die Bewertung transnationaler Bedrohungen, die sich auf die globale Sicherheit auswirken, wie Klima- und andere Umweltveränderungen, Risiken für die öffentliche Gesundheit und humanitäre Bedrohungen. ([240]) Auf der anderen Seite listet die EO eine Reihe von Zielen auf, die niemals mittels

([233]) https://www.intel.gov/ic-on-the-record-database/results/oversight/1278-odni-releases-ic-procedures-implementing-new-safeguards-in-executive-order-14086.

([234]) Abschnitt 2(a)(i) EO 14086.

([235]) Abschnitt 2(a)(ii) EO 14086.

([236]) Abschnitt 2(a)(ii)(A) EO 14086. Es ist nicht immer erforderlich, dass die Signalaufklärung das einzige Mittel ist, um eine validierte Aufklärungspriorität zu fördern. Beispielsweise kann die Erhebung von Signalaufklärungsdaten dazu dienen, alternative Mittel zur Validierung (z. B. zur Bestätigung von Informationen aus anderen nachrichtendienstlichen Quellen) oder zur Aufrechterhaltung eines zuverlässigen Zugangs zu denselben Informationen bereitzustellen (Abschnitt 2(c)(i)(A) EO 14086).

([237]) Abschnitt 2(a)(ii)(B) EO 14086.

([238]) Abschnitt 2(a)(ii)(B) EO 14086.

([239]) Abschnitt 2(a)(iii) in Verbindung mit Abschnitt 2(d) EO 14086.

([240]) Abschnitt 2(b)(i) EO 14086. Aufgrund der begrenzten Liste legitimer Ziele in der EO, die mögliche zukünftige Bedrohungen nicht umfasst, wird in der EO die Möglichkeit vorgesehen, dass der Präsident diese Liste aktualisiert, wenn sich neue nationale Sicherheitsbedürfnisse ergeben, z. B. neue Bedrohungen der nationalen Sicherheit. Solche Aktualisierungen sind grundsätzlich zu veröffentlichen, es sei denn, der Präsident stellt fest, dass dies selbst eine Bedrohung für die nationale Sicherheit der Vereinigten Staaten darstellen würde (Abschnitt 2(b)(i)(B) EO 14086).

signalerfassender Aufklärung verfolgt werden dürfen, z. B. die Beeinträchtigung von Kritik, Dissens oder der freien Äußerung von Ideen oder politischen Meinungen durch Privatpersonen oder die Presse, die Diskriminierung von Personen aufgrund ihrer ethnischen Zugehörigkeit, Rasse, Geschlecht, Geschlechtsidentität, sexuellen Orientierung oder Religion oder die Verschaffung eines Wettbewerbsvorteils für US-Unternehmen. ([241])

(135) Darüber hinaus können sich die Nachrichtendienste nicht allein auf die in der EO 14086 festgelegten legitimen Ziele berufen, um die Erhebung von Signalaufklärungsdaten zu rechtfertigen, sondern müssen für operative Zwecke konkretere Prioritäten festlegen, für die Signalaufklärungsdaten erhoben werden können. Mit anderen Worten, die tatsächliche Erhebung kann nur zur Unterstützung einer spezifischeren Priorität erfolgen. Diese Prioritäten werden im Rahmen eines besonderen Verfahrens festgelegt, das die Einhaltung der geltenden Rechtsvorschriften, einschließlich der Bestimmungen zum Schutz der Privatsphäre und der bürgerlichen Freiheiten, gewährleisten soll. Konkret werden die Aufklärungsprioritäten zunächst vom Direktor des Nationalen Nachrichtendienstes (im Rahmen des sogenannten National Intelligence Priorities Framework) entwickelt und dem Präsidenten zur Genehmigung vorgelegt. ([242]) Bevor der Direktor des Nationalen Nachrichtendienstes dem Präsidenten Aufklärungsprioritäten vorschlägt, muss er nach der EO 14086 für jede Priorität eine Bewertung des ODNI CLPO einholen, um festzustellen, ob sie 1) einem oder mehreren der in der EO aufgeführten legitimen Ziele dient, 2) nicht dazu bestimmt ist und voraussichtlich nicht dazu führen wird, Signalaufklärungsdaten für ein in der EO aufgeführtes verbotenes Ziel zu erheben und 3) unter gebührender Berücksichtigung der Privatsphäre und der bürgerlichen Freiheiten aller Personen, ungeachtet ihrer Nationalität oder ihres Wohnorts, festgelegt wurde. ([243]) Stimmt der Direktor der Bewertung des Beauftragten nicht zu, sind beide Stellungnahmen dem Präsidenten vorzulegen. ([244])

(136) Dieses Verfahren stellt daher insbesondere sicher, dass Datenschutzbelange bereits in der Anfangsphase der Entwicklung von Aufklärungsprioritäten berücksichtigt werden.

(137) Zweitens wird, sobald eine Aufklärungspriorität festgelegt ist, anhand einer Reihe von Anforderungen entschieden, ob und in welchem Umfang Signalaufklärungsdaten erhoben werden dürfen, um diese Priorität zu fördern. Mit diesen Anforderungen werden die allgemeinen Standards der Notwendigkeit und Verhältnismäßigkeit nach Abschnitt 2(a) EO umgesetzt.

(138) Insbesondere dürfen Signalaufklärungsdaten nur erhoben werden, „wenn auf der Grundlage einer angemessenen Bewertung aller relevanten Faktoren festgestellt wurde, dass die Erhebung erforderlich ist, um eine bestimmte Aufklärungspriorität zu fördern". ([245]) Bei der Entscheidung, ob eine bestimmte Signalaufklärungstätigkeit erforderlich ist, um eine bestätigte Aufklärungspriorität zu fördern, müssen die US-Nachrichtendienste die Verfügbarkeit, Durchführbarkeit und Angemessenheit anderer, weniger eingreifender Quellen und Methoden, einschließlich diplomatischer und öffentlicher Quellen, berücksichtigen. ([246]) Stehen solche alternativen, weniger eingreifenden Quellen und Methoden zur Verfügung, sind sie vorrangig zu nutzen. ([247])

(139) Wenn in Anwendung dieser Kriterien die Erhebung von Signalaufklärungsdaten als notwendig erachtet wird, muss sie so „maßgeschneidert wie möglich" sein und darf „die Privatsphäre und die bürgerlichen Freiheiten nicht unverhältnismäßig beeinträchtigen". ([248]) Um sicherzustellen, dass die Privatsphäre und die bürgerlichen Freiheiten nicht unverhältnismäßig beeinträchtigt werden, d. h. um ein angemessenes Gleichgewicht zwischen den Erfordernissen der nationalen Sicherheit und dem Schutz der Privatsphäre und der bürgerlichen Freiheiten herzustellen, müssen alle relevanten Faktoren berücksichtigt werden, wie etwa die Art des verfolgten Ziels, die Eingriffsintensität der Erhebung, einschließlich ihrer Dauer, der voraussichtliche Beitrag der Erhebung zur Erreichung des verfolgten Ziels, die nach vernünftigem Ermessen vorhersehbaren Folgen für Privatpersonen und Art und Sensibilität der zu erhebenden Daten. ([249])

([241]) Abschnitt 2(b)(ii) EO 14086.
([242]) Abschnitt 102A des National Security Act und Abschnitt 2(b)(iii) EO 14086.
([243]) In Ausnahmefällen (insbesondere, wenn ein solches Verfahren nicht durchgeführt werden kann, weil ein neuer oder sich entwickelnder nachrichtendienstlicher Bedarf gedeckt werden muss) können solche Prioritäten direkt vom Präsidenten oder vom Leiter eines Nachrichtendienstes festgelegt werden, wobei grundsätzlich die gleichen Kriterien wie in Abschnitt 2(b)(iii)(A)(1)-(3) anzuwenden sind, siehe Abschnitt 4(n) EO 14086.
([244]) Abschnitt 2(b)(iii)(C) EO 14086.
([245]) Abschnitt 2(b) und (c)(i)(A) EO 14086.
([246]) Abschnitt 2(c)(i)(A) EO 14086.
([247]) Abschnitt 2(c)(i)(A) EO 14086.
([248]) Abschnitt 2(c)(i)(B) EO 14086.
([249]) Abschnitt 2(c)(i)(B) EO 14086.

(140) Was die Art der Erhebung der Signalaufklärungsdaten anbelangt, so muss die Datenerhebung in den Vereinigten Staaten, die für die vorliegende Angemessenheitsfeststellung am relevantesten ist, da sie Daten betrifft, die an Organisationen in den Vereinigten Staaten übermittelt werden, stets gezielt erfolgen, wie in den Erwägungsgründen 142 bis 153 näher erläutert wird.

(141) Die „Sammelerhebung" ([250]) darf nur außerhalb der USA auf der Grundlage der EO 12333 durchgeführt werden. Auch in diesem Fall ist nach der EO 14086 der gezielten Erhebung der Vorzug zu geben. ([251]) Umgekehrt ist eine Sammelerhebung nur dann zulässig, wenn die für die Förderung einer validierten Aufklärungspriorität erforderlichen Informationen nicht in angemessener Weise durch eine gezielte Erhebung gewonnen werden können. ([252]) Wenn eine Sammelerhebung außerhalb der Vereinigten Staaten erforderlich ist, gelten besondere Garantien nach der EO 14086. ([253]) Erstens müssen Methoden und technische Maßnahmen angewandt werden, um die gesammelten Daten auf das zu beschränken, was für die Förderung einer validierten Aufklärungspriorität erforderlich ist, und um die Erhebung irrelevanter Informationen so gering wie möglich zu halten. ([254]) Zweitens beschränkt die EO die Verwendung von Informationen, die durch die Sammelerhebung (einschließlich Abfragen) gewonnen wurden, auf sechs spezifische Zwecke, darunter Schutz vor Terrorismus, Geiselnahme und Gefangennahme von Personen durch oder im Namen einer ausländischen Regierung, Organisation oder Person sowie Schutz vor ausländischer Spionage, Sabotage oder Ermordung, Schutz vor Bedrohungen, die sich aus der Entwicklung, dem Besitz oder der Verbreitung von Massenvernichtungswaffen oder damit zusammenhängender Technologien und Bedrohungen ergeben, usw. ([255]) Schließlich darf die Abfrage von Daten, die durch eine Sammelerhebung gewonnen wurden, nur dann erfolgen, wenn dies zur Förderung einer validierten Aufklärungspriorität erforderlich ist, und zwar in Verfolgung dieser sechs Ziele und in Übereinstimmung mit Strategien und Verfahren, die den Auswirkungen der Abfragen auf die Privatsphäre und die bürgerlichen Freiheiten aller Personen, unabhängig von ihrer Staatsangehörigkeit oder ihrem Wohnort, gebührend Rechnung tragen. ([256])

(142) Zusätzlich zu den Anforderungen der EO 14086 unterliegt die Erhebung von Signalaufklärungsdaten, die an eine Organisation in den USA übermittelt werden, besonderen Einschränkungen und Garantien, die in Abschnitt 702 FISA geregelt sind. ([257]) Nach Abschnitt 702 FISA ist es möglich, Auslandsaufklärungsdaten durch die gezielte Überwachung von Nicht-US-Bürgern zu sammeln, von denen vermutet wird, dass sie sich außerhalb der Vereinigten Staaten aufhalten, wobei amerikanische Anbieter elektronischer Kommunikationsdienste zur Unterstützung verpflichtet sind. ([258]) Um nach Abschnitt 702 FISA Auslandsaufklärungsdaten sammeln zu können, legen der

([250]) D. h. die Sammlung großer Mengen von Signalaufklärungsdaten aus technischen oder operativen Gründen ohne Verwendung von Unterscheidungsmerkmalen (z. B. ohne Verwendung spezifischer Identifikatoren oder Auswahlbegriffe), siehe Abschnitt 4(b) EO 14086. Nach der EO 14086 und wie in Erwägungsgrund 141 näher erläutert, findet eine Sammelerhebung nach der EO 12333 nur statt, wenn dies zur Förderung bestimmter validierter Aufklärungsprioritäten erforderlich ist, und unterliegt einer Reihe von Einschränkungen und Garantien, die sicherstellen sollen, dass nicht auf wahllose Weise auf Daten zugegriffen wird. Sammelerhebungen sind daher von einer allgemeinen und wahllosen Erfassung („Massenüberwachung") ohne Einschränkungen und Garantien zu unterscheiden.

([251]) Abschnitt 2(c)(ii)(A) EO 14086.

([252]) Abschnitt 2(c)(ii)(A) EO 14086.

([253]) Die besonderen Vorschriften der EO 14086 für die Sammelerhebung gelten auch für eine gezielte Signalaufklärungstätigkeit, bei der vorübergehend Daten verwendet werden, die ohne Unterscheidungsmerkmale (z. B. spezifische Auswahlbegriffe oder Identifikatoren) beschafft wurden, d. h. in großen Mengen (was nur außerhalb des Hoheitsgebiets der Vereinigten Staaten möglich ist). Dies ist nicht der Fall, wenn solche Daten nur zur Unterstützung der anfänglichen technischen Phase der gezielten Signalaufklärungstätigkeit verwendet werden, nur für einen kurzen Zeitraum gespeichert werden, der für den Abschluss dieser Phase erforderlich ist, und unmittelbar danach gelöscht werden (Abschnitt 2(c)(ii)(D) EO 14086). In diesem Fall besteht der einzige Zweck der ursprünglichen Erhebung ohne Unterscheidungsmerkmale darin, eine gezielte Datenerhebung unter Verwendung eines spezifischen Identifikators oder Auswahlbegriffs zu ermöglichen. In einem solchen Szenario werden nur die Daten, die auf die Anwendung eines bestimmten Unterscheidungsmerkmals reagieren, in staatliche Datenbanken eingegeben, während die übrigen Daten vernichtet werden. Eine solche gezielte Erhebung unterliegt daher weiterhin den allgemeinen Regeln für die Erhebung von Signalaufklärungsdaten, einschließlich Abschnitt 2(a)-(b) und § 2(c)(i) EO 14086.

([254]) Abschnitt 2(c)(ii)(A) EO 14086.

([255]) Abschnitt 2(c)(ii)(B) EO 14086. Sollten sich neue nationale Sicherheitsbedürfnisse ergeben, z. B. neue Bedrohungen der nationalen Sicherheit, kann der Präsident diese Liste aktualisieren. Solche Aktualisierungen sind grundsätzlich zu veröffentlichen, es sei denn, der Präsident stellt fest, dass dies selbst eine Bedrohung für die nationale Sicherheit der Vereinigten Staaten darstellen würde (Abschnitt 2(c)(ii)(C) EO 14086). Hinsichtlich der Abfrage von Daten, die durch Sammelerhebung gewonnen wurden, siehe Abschnitt 2(c)(iii)(D) EO 14086.

([256]) Abschnitt 2(a)(ii)(A) in Verbindung mit Abschnitt 2(c)(iii)(D) EO 14086. Siehe auch Anhang VII.

([257]) 50 U.S.C. § 1881.

([258]) 50 U.S.C. § 1881a (a). Wie das PCLOB feststellte, besteht die Aufsicht nach Abschnitt 702 „ausschließlich in der Überwachung, konkreter Zielpersonen [die nicht Bürger der USA sind], deren Auswahl eine Einzelfallprüfung voraussetzt" (Privacy and Civil Liberties Oversight Board, Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, 2. Juli 2014, Section 702 Report, S. 111). Siehe auch NSA CLPO, NSA's Implementation of Foreign Intelligence Act Section 702, 16. April 2014. Der Begriff „Anbieter elektronischer Kommunikationsdienste" ist in 50 U.S.C. § 1881(a)(4) definiert.

Justizminister und der Direktor des Nationalen Nachrichtendienstes dem Foreign Intelligence Surveillance Court (FISC) (Gericht zur Überwachung der Auslandsgeheimdienste) jährliche Zertifizierungen vor, in denen die Kategorien der zu erhebenden Auslandsaufklärungsdaten aufgeführt sind. ([259]) Die Zertifizierungen müssen mit Verfahren zur zielgenauen Erfassung, Minimierung und Abfrage einhergehen, die ebenfalls vom Gericht gebilligt werden und für die amerikanischen Nachrichtendienste rechtsverbindlich sind.

(143) Das FISC ist ein durch Bundesgesetz geschaffenes unabhängiges Gericht ([260]), dessen Entscheidungen vor dem Foreign Intelligence Surveillance Court of Review (FISCR) ([261]) (Rechtsmittelgericht für Entscheidungen im Bereich der Überwachung der Auslandsgeheimdienste) und schließlich vor dem Obersten Gerichtshof der Vereinigten Staaten angefochten werden können. ([262]) Das FISC (und das FISCR) werden von einer ständigen Expertengruppe unterstützt, die aus fünf Rechtsanwälten und fünf Sachverständigen für nationale Sicherheit und Bürgerrechte besteht. ([263]) 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. ([264]) Auf diese Weise wird vor allem sichergestellt, dass Datenschutzbelange bei der gerichtlichen Prüfung hinreichend Berücksichtigung finden. Das Gericht kann auch eine Privatperson oder Organisation als Amicus curiae benennen, um bestimmte rechtliche Aspekte zu beleuchten, sofern ihm dies geboten erscheint, oder auf Antrag einer Privatperson oder einer Organisation gestatten, einen Amicus-Curiae-Schriftsatz („brief“) einzureichen. ([265])

(144) Das FISC prüft die Zertifizierungen und die damit verbundenen Verfahren (insbesondere die Verfahren zur zielgenauen Erfassung und zur Minimierung der Datenmenge) auf ihre Übereinstimmung mit den Anforderungen des FISA. Ist es der Auffassung, dass die Anforderungen nicht erfüllt sind, kann es die Zertifizierung ganz oder teilweise verweigern und eine Änderung der Verfahren verlangen. ([266]) In diesem Zusammenhang hat das FISC wiederholt bestätigt, dass seine Überprüfung der Verfahren zur zielgenauen Erfassung und Datenminimierung nach Abschnitt 702 nicht auf die schriftlichen Verfahren beschränkt ist, sondern auch die Art und Weise umfasst, wie die Verfahren von der Regierung umgesetzt werden. ([267])

(145) Die National Security Agency (NSA, der Nachrichtendienst, der nach Abschnitt 702 FISA für die zielgenaue Datenerhebung zuständig ist) trifft die Auswahl der einzelnen Zielpersonen nach den vom FISC genehmigten Verfahren für die zielgenaue Erfassung, wonach die NSA auf der Grundlage der Gesamtumstände beurteilen muss, dass die zielgenaue Datenerfassung gegen eine bestimmte Person wahrscheinlich zur Erlangung einer in einer Zertifizierung genannten Kategorie von Informationen der Auslandsaufklärung führen wird. ([268]) Diese Bewertung

([259]) 50 U.S.C. § 1881a (g).

([260]) Das FISC besteht aus 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 50 U.S.C. § 1803 (a). Den Richtern stehen erfahrene Rechtsassistenten zur Seite, die das juristische Personal darstellen und Rechtsgutachten zu Auskunftsersuchen erstellen. Siehe 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 (29. Juli 2013) (Walton Letter), S. 2, abrufbar unter https://fas.org/irp/news/2013/07/fisc-leahy.pdf.

([261]) Das FISCR besteht aus Richtern, die vom Obersten Richter der Vereinigten Staaten ernannt und aus Richtern an US-Bezirksgerichten oder Berufungsgerichten ausgewählt werden und dem FISCR jeweils sieben Jahre lang angehören. Siehe 50 U.S.C. § 1803 (b).

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

([263]) 50 U.S.C. § 1803 (i)(1),(3)(A).

([264]) 50 U.S.C. § 1803 (i)(2)(A).

([265]) 50 U.S.C. § 1803 (i)(2)(B).

([266]) Siehe z. B. das Gutachten des FISC vom 18. Oktober 2018, abrufbar unter athttps://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opin_18Oct18.pdf, bestätigt durch das Gutachten des Foreign Intelligence Court of Review vom 12. Juli 2019, abrufbar unter athttps://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISCR_Opinion_12Jul19.pdf.

([267]) Siehe z. B. FISC, Memorandum Opinion and Order, S. 35 (18. November 2020) (zur Veröffentlichung freigegeben am 26. April 2021), (Anhang D).

([268]) 50 U.S.C. § 1881a(a), Procedures used by the National Security Agency for Targeting Non-United States Persons Reasonably Believed to be Located outside the United States to Acquire Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, in der geltenden Fassung, vom März 2018 (NSA-Verfahren für eine zielgenaue Erfassung), abrufbar unter https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_NSA_Targeting_27Mar18.pdf, S. 1-4, näher erläutert im PCLOB-Bericht, S. 41–42.

muss spezifisch und faktengestützt sein und sich auf das analytische Urteilsvermögen, die spezifische Ausbildung und Erfahrung des Analysten sowie auf die Art der zu beschaffenden Auslandsaufklärungsdaten stützen. ([269]) Die zielgenaue Ausrichtung der Erhebung erfolgt über sogenannte Selektoren, die bestimmte Kommunikationseinrichtungen wie die E-Mail-Adresse oder die Telefonnummer der Zielperson identifizieren, jedoch niemals Schlüsselwörter oder Namen von Personen. ([270])

(146) NSA-Analysten werden zunächst Nicht-US-Bürger ermitteln, die sich im Ausland befinden und deren Überwachung nach Einschätzung der Analysten zu den in der Zertifizierung angegebenen Auslandsaufklärungsdaten führt. ([271]) Wie in den NSA-Verfahren zur zielgenauen Datenerhebung dargelegt, kann die NSA eine Überwachung nur dann auf eine Zielperson ausrichten, wenn sie bereits Informationen über diese Zielperson hat. ([272]) Diese Informationen können aus verschiedenen Quellen stammen, z. B. aus der Aufklärung mit menschlichen Quellen. Über diese anderen Quellen muss der Analyst auch etwas über einen bestimmten Selektor (d. h. ein Kommunikationskonto) erfahren, der von der potenziellen Zielperson verwendet wird. Sobald diese Personen identifiziert sind und ihre gezielte Überwachung nach einem gründlichen Kontrollverfahren innerhalb der NSA ([273]) genehmigt wurde, werden Selektoren, die Kommunikationseinrichtungen (wie E-Mail-Adressen) identifizieren, „aktiviert“ (d. h. erstellt und angewandt). ([274])

(147) Die NSA muss die sachliche Grundlage für die Auswahl des Ziels ([275]) dokumentieren und nach der erstmaligen Erfassung in regelmäßigen Abständen bestätigen, dass die Norm für die gezielte Erfassung weiterhin erfüllt ist. ([276]) Sobald die Norm für die gezielte Erfassung nicht mehr erfüllt ist, ist die Erhebung einzustellen. ([277]) Die Auswahl der einzelnen Zielpersonen durch die NSA und die Dokumentation jeder aufgezeichneten Bewertung und Begründung der Erfassung werden alle zwei Monate von Beamten der für die Überwachung der Nachrichtendienste zuständigen Abteilungen des Justizministeriums auf die Einhaltung der Verfahren für eine zielgenaue Erfassung überprüft, die verpflichtet sind, dem FISC und dem Kongress jeden Verstoß zu melden. ([278]) Die schriftliche Dokumentation der NSA erleichtert dem FISC die Überwachung der ordnungsgemäßen Auswahl bestimmter Zielpersonen nach Abschnitt 702 FISA im Einklang mit seinen in den Erwägungsgründen 173 und 174 beschriebenen Aufsichtsbefugnissen. ([279]) Schließlich ist der Direktor des nationalen Nachrichtendienstes verpflichtet, jedes Jahr die Gesamtzahl der Personen, die nach Abschnitt 702 FISA als Zielpersonen ausgewählt wurden, in öffentlichen jährlichen statistischen Transparenzberichten bekannt zu geben. Unternehmen, die Anweisungen nach Abschnitt 702 FISA erhalten, können aggregierte Daten (über Transparenzberichte) über die bei ihnen eingegangenen Anfragen veröffentlichen. ([280])

([269]) NSA-Verfahren für eine zielgenaue Erfassung, S. 4.

([270]) Siehe PCLOB, Section 702 Report, S. 32–33 und 45 mit weiterführenden Informationen. Siehe auch Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, vorgelegt vom Justizminister und dem Direktor des Nationalen Nachrichtendienstes, Berichtszeitraum: 1. Dezember 2016–31. Mai 2017, S. 41 (Oktober 2018), abrufbar unter https://www.dni.gov/files/icotr/18th_Joint_Assessment.pdf.

([271]) PCLOB, Section 702 Report, S. 42–43.

([272]) NSA-Verfahren für eine zielgenaue Erfassung, S. 2.

([273]) PCLOB, Section 702 Report, S. 46. Beispielsweise 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, Abschnitt 702, 16. April 2014.

([274]) 50 U.S.C. § 1881a (h).

([275]) NSA-Verfahren für eine zielgenaue Erfassung, S. 8. Siehe auch PCLOB, Section 702 Report, S. 46. Das Fehlen einer schriftlichen Begründung stellt einen Verstoß gegen die Dokumentationspflicht dar, der dem FISC und dem Kongress zu melden ist. Siehe Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, vorgelegt vom Justizminister und dem Direktor des nationalen Nachrichtendienstes, Berichtszeitraum: 1. Dezember 2016–31. Mai 2017, S. 41 (Oktober 2018), DOJ/ODNI Compliance Report to FISC for Dec. 2016–May 2017 auf S. A-6, abrufbar unter https://www.dni.gov/files/icotr/18th_Joint_Assessment.pdf.

([276]) Siehe U.S. Government Submission to Foreign Intelligence Surveillance Court, 2015 Summary of Notable Section 702 Requirements, S. 2-3 (15. Juli 2015) und die in Anhang VII enthaltenen Informationen.

([277]) Siehe U.S. Government Submission to Foreign Intelligence Surveillance Court, 2015 Summary of Notable Section 702 Requirements, S. 2-3 (15. Juli 2015), in der es heißt: „[W]enn die Regierung zu einem späteren Zeitpunkt feststellt, dass die weitere Verwendung des Selektors für eine Zielperson wahrscheinlich nicht zur Erlangung von Auslandsaufklärungsdaten führen wird, muss die Abfrage unverzüglich eingestellt werden, und jede Verzögerung kann zu einem meldepflichtigen Compliance-Verstoß führen“. Siehe auch die in Anhang VII enthaltenen Informationen. Siehe auch die in Anhang VII enthaltenen Informationen.

([278]) PCLOB, Section 702 Report, S. 70–72; Rule 13(b) der Rules of Procedures des United States Intelligence Surveillance Court, abrufbar unter https://www.fisc.uscourts.gov/sites/default/files/FISC%20Rules%20of%20Procedure.pdf.

([279]) Siehe auch DOJ/ODNI Compliance Report to FISC for Dec. 2016–May 2017, S. A-6.

([280]) 50 U.S.C. § 1874.

(148) Für die anderen Rechtsgrundlagen zur Erhebung personenbezogener Daten, die an Organisationen in den USA übermittelt werden, gelten andere Einschränkungen und Garantien. Im Allgemeinen ist die Sammelerhebung von Daten auf der Grundlage von Abschnitt 402 FISA (Befugnis zum Einsatz von Geräten zur Rufnummernerfassung) und durch die Verwendung von NSL ausdrücklich verboten und erfordert stattdessen die Verwendung spezifischer „Suchbegriffe". ([281])

(149) Um eine herkömmliche individualisierte elektronische Überwachung (nach Abschnitt 105 FISA) durchführen zu können, müssen die Nachrichtendienste einen Antrag beim FISC stellen, in dem sie die Tatsachen und Umstände darlegen, die die Annahme rechtfertigen, dass ein hinreichender Verdacht besteht, dass die Einrichtung von einer ausländischen Macht oder einem Vertreter einer ausländischen Macht genutzt wird oder dies beabsichtigt ist. ([282]) Das FISC beurteilt unter anderem, ob diese Annahme auf der Grundlage der vorgelegten Tatsachen vermutlich zutrifft. ([283])

(150) Für die Durchführung einer Hausdurchsuchung oder Durchsuchung des Eigentums zur Überprüfung, Beschlagnahme usw. von Informationen, Unterlagen oder Vermögensgegenständen (z. B. eines Computergeräts) auf der Grundlage von Abschnitt 301 FISA ist ein Antrag auf Erlass einer Anordnung beim FISC erforderlich. ([284]) Ein solcher Antrag muss unter anderem darlegen, dass ein hinreichender Verdacht besteht, dass das Ziel der Durchsuchung eine ausländische Macht oder ein Vertreter einer ausländischen Macht ist, dass die zu durchsuchenden Räumlichkeiten oder Gegenstände Auslandsaufklärungsdaten enthalten und dass die zu durchsuchenden Räumlichkeiten einer ausländischen Macht gehören, von einer ausländischen Macht benutzt werden, in ihrem Besitz sind oder sich auf dem Weg zu oder von einer ausländischen Macht (bzw. einem Vertreter der ausländischen Macht) befinden. ([285])

(151) In ähnlicher Weise erfordert der Einsatz von Geräten zur Rufnummernerfassung von ausgehenden und eingehenden Anrufen (nach Abschnitt 402 FISA) die Beantragung einer Anordnung des FISC (oder eines U.S. Magistrate Judge) und die Verwendung eines konkreten Suchbegriffs, d. h. eines Begriffs, der eine Person, ein Konto usw. präzise bezeichnet und den Suchbereich möglichst stark eingrenzen soll. ([286]) 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).

(152) Abschnitt 501 FISA ([287]), der die Erhebung von Geschäftsunterlagen eines gewöhnlichen Beförderungsunternehmens (d. h. einer Person oder Einrichtung, die gegen Entgelt Personen oder Güter auf dem Land-, Schienen-, Wasser- oder Luftweg befördert), einer öffentlichen Beherbergungseinrichtung (z. B. Hotel, Motel oder Gasthof), einer Mietwagenfirma oder einer physischen Lagereinrichtung (d. h. einer Einrichtung, die Raum für die Lagerung von Waren und Materialien bereitstellt oder Dienstleistungen im Zusammenhang mit der Lagerung von Waren erbringt) ([288]) erlaubt, erfordert ebenfalls einen Antrag beim FISC oder einem Magistrate Judge. In diesem Antrag sind die angeforderten Unterlagen sowie die konkreten und nachvollziehbaren Tatsachen anzugeben, die die Annahme rechtfertigen, dass es sich bei der Person, auf die sich die Unterlagen beziehen, um eine ausländische Macht oder einen Vertreter einer ausländischen Macht handelt. ([289])

(153) Schließlich sind NSL nach verschiedenen Gesetzen zulässig und erlauben es den Ermittlungsbehörden, von bestimmten Stellen (z. B. Finanzinstituten, Kreditauskunfteien, Anbietern elektronischer Kommunikation) bestimmte Informationen aus Kreditauskünften, Finanzunterlagen und elektronischen Teilnehmer- und Transaktionsdatensätzen (mit Ausnahme des Inhalts der Kommunikation) zu erhalten. ([290]) Nach dem NSL-Statut, das den Zugriff auf elektronische Kommunikation gestattet, ist nur das FBI befugt, von diesem Recht Gebrauch zu machen, und die Anträge müssen sich auf eine Person, eine Stelle, eine Telefonnummer oder ein Konto beziehen und bestätigen, dass die Informationen für eine autorisierte Ermittlung zu Fragen der nationalen Sicherheit erforderlich sind, die dem Schutz vor internationalem Terrorismus und verdeckten nachrichtendienstlichen Tätigkeiten dient. ([291]) Empfänger eines NSL haben das Recht, diesen vor Gericht anzufechten. ([292])

([281]) 50 U.S.C. § 1842(c)(3) und für die NSL 12 U.S.C. § 3414(a)(2), 15 U.S.C. § 1681u, 15 U.S.C. § 1681v(a) und 18 U.S.C. § 2709(a).

([282]) Als „Vertreter einer ausländischen Macht" können auch Nicht-US-Bürger gelten, die am internationalen Terrorismus oder an der internationalen Verbreitung von Massenvernichtungswaffen (einschließlich Vorbereitungshandlungen) beteiligt sind (50 U.S. C. § 1801 (b)(1)).

([283]) 50 U.S.C. § 1804. Siehe auch § 1841(4) in Bezug auf die Auswahl der Suchbegriffe.

([284]) 50 U.S.C. § 1821(5).

([285]) 50 U.S.C. § 1823(a).

([286]) 50 U.S.C. § 1842 mit § 1841(2) und Abschnitt 3127 des Titels 18.

([287]) 50 U.S.C. § 1862.

([288]) 50 U.S.C. §§ 1861–1862.

([289]) 50 U.S.C. § 1862(b).

([290]) 12 U.S.C. § 3414, 15 U.S.C. §§ 1681u-1681v und 18 U.S.C. § 2709.

([291]) 18 U.S.C. § 2709(b).

([292]) Z. B. 18 U.S.C. § 2709(d).

3.2.1.3 *Weiterverwendung der erhobenen Daten*

(154) Für die Verarbeitung personenbezogener Daten, die von den US-Nachrichtendiensten im Rahmen der Signalaufklärung erhoben wurden, gelten mehrere Garantien.

(155) Erstens muss jeder Nachrichtendienst eine angemessene Datensicherheit gewährleisten und den Zugriff Unbefugter auf die im Rahmen der Signalaufklärung erhobenen personenbezogenen Daten verhindern. In diesem Zusammenhang werden die Mindestanforderungen an die Informationssicherheit (z. B. mehrstufige Authentifizierung, Verschlüsselung usw.) in verschiedenen Instrumenten wie Gesetzen, Leitlinien und Normen weiter spezifiziert. ([293]) Der Zugang zu erhobenen Daten ist auf befugte und geschulte Mitarbeiter zu beschränken, die diese Informationen zur Erfüllung ihres Auftrags benötigen. ([294]) Generell müssen die Nachrichtendienste ihre Mitarbeiter angemessen schulen, einschließlich der Verfahren zur Meldung und Behandlung von Rechtsverstößen (einschließlich Verstößen gegen die EO 14086). ([295])

(156) Zweitens müssen Nachrichtendienste die Standards der Genauigkeit und Objektivität der Intelligence Community einhalten, insbesondere im Hinblick auf die Gewährleistung der Datenqualität und -zuverlässigkeit, die Berücksichtigung alternativer Informationsquellen und die Objektivität bei der Durchführung von Analysen. ([296])

(157) Drittens wird in der EO 14086 im Hinblick auf die Vorratsdatenspeicherung klargestellt, dass für personenbezogene Daten von Nicht-US-Bürgern die gleichen Speicherfristen gelten wie für Daten von US-Bürgern. ([297]) Die Nachrichtendienste sind verpflichtet, spezifische Speicherfristen und/oder die Faktoren festzulegen, die bei der Bestimmung der Dauer der anwendbaren Speicherfristen zu berücksichtigen sind (z. B. ob es sich bei den Informationen um Beweise für eine Straftat handelt, ob es sich bei den Informationen um ausländische Aufklärungsdaten handelt, ob die Informationen zum Schutz der Sicherheit von Personen oder Organisationen, einschließlich Opfern oder Zielpersonen des internationalen Terrorismus, erforderlich sind). Diese sind in unterschiedlichen Rechtsinstrumenten festgelegt. ([298])

(158) Viertens gelten besondere Regeln für die Verbreitung personenbezogener Daten, die im Rahmen der Signalaufklärung erhoben wurden. Im Allgemeinen dürfen personenbezogene Daten von Nicht-US-Bürgern nur dann verbreitet werden, wenn es sich um die gleiche Art von Daten handelt, die auch von US-Bürgern verbreitet werden dürfen, z. B. Daten, die erforderlich sind, um die Sicherheit einer Person oder Organisation zu schützen (z. B. Zielpersonen, Opfer oder Geiseln internationaler terroristischer Organisationen). ([299]) Darüber hinaus dürfen personenbezogene Daten nicht allein aufgrund der Staatsangehörigkeit oder des Wohnsitzlandes einer Person oder zum Zwecke der Umgehung der Anforderungen der EO 14086 verbreitet werden. ([300]) Eine Verbreitung innerhalb

([293]) Abschnitt 2(c)(iii)(B)(1) EO 14086. Siehe auch Titel VIII des National Security Act (mit Einzelheiten zu den Voraussetzungen für den Zugriff auf Informationen, die der Geheimhaltung unterliegen), E.O. 12333 Abschnitt 1.5 (wonach die Leiter der Nachrichtendienste verpflichtet sind, die Leitlinien für den Informationsaustausch und die Sicherheit, den Datenschutz und andere rechtliche Anforderungen zu befolgen), National Security Directive 42, „National Policy for the Security of National Security Telecommunications and Information Systems" (wonach der Committee on National Security Systems (Ausschuss für nationale Sicherheitssysteme) angewiesen wird, den Exekutivabteilungen und -behörden Leitlinien für die Systemsicherheit der nationalen Sicherheitssysteme zur Verfügung zu stellen), und National Security Memorandum 8, „Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems" (Festlegung von Zeitplänen und Leitlinien für die Umsetzung von Cybersicherheitsanforderungen für nationale Sicherheitssysteme, einschließlich Multifaktor-Authentifizierung, Verschlüsselung, Cloud-Technologien und Endpunkterkennungsdienste).

([294]) Abschnitt 2(c)(iii)(B)(2) EO 14086. Darüber hinaus darf auf personenbezogene Daten, für die noch keine endgültige Entscheidung über die Speicherung getroffen wurde, nur zugegriffen werden, um eine solche Entscheidung zu treffen oder zu unterstützen oder um genehmigte Verwaltungs-, Test-, Entwicklungs-, Sicherheits- oder Aufsichtsfunktionen durchzuführen (Abschnitt 2(c)(iii)(B)(3) EO 14086.

([295]) Abschnitt 2(d)(ii) EO 14086.

([296]) Abschnitt 2(c)(iii)(C) EO 14086.

([297]) Abschnitt 2(c)(iii)(A)(2)(a)-(c) EO 14086. Generell muss jede Behörde Strategien und Verfahren einführen, um die Verbreitung und Speicherung personenbezogener Daten, die im Rahmen der Signalaufklärung erhoben wurden, auf ein Mindestmaß zu beschränken (Abschnitt 2(c)(iii)(A) EO 14086).

([298]) Siehe z. B. Abschnitt 309 of the Intelligence Authorization Act for Fiscal Year 2015; Verfahren zur Minimierung der Datenmenge, die von einzelnen Nachrichtendiensten nach Abschnitt 702 FISA angenommen und vom FISC genehmigt wurden, vom Justizminister und nach dem FRA genehmigte Verfahren (nach denen die US-Bundesbehörden, einschließlich der nationalen Sicherheitsbehörden, Speicherfristen für ihre Unterlagen festlegen müssen, die von der National Archives and Record Administration genehmigt werden müssen).

([299]) Abschnitt 2(c)(iii)(A)(1)(a) und Abschnitt 5(d) EO 14086 in Verbindung mit Abschnitt 2.3 EO 12333.

([300]) Abschnitt 2(c)(iii)(A)(1)(b) und (e) EO 14086.

der US-Regierung darf nur erfolgen, wenn eine befugte und geschulte Person Grund zu der Annahme hat, dass der Empfänger die Informationen kennen muss ([301]) und sie angemessen schützen wird. ([302]) Bei der Entscheidung, ob personenbezogene Daten an Empfänger außerhalb der US-Regierung (einschließlich ausländischer Regierungen oder internationaler Organisationen) weitergegeben werden dürfen, müssen der Zweck der Verbreitung, die Art und der Umfang der verbreiteten Daten sowie mögliche nachteilige Auswirkungen auf die betroffene(n) Person(en) berücksichtigt werden. ([303])

(159) Schließlich ist nach der EO 14086 jeder Nachrichtendienst verpflichtet, eine angemessene Dokumentation über die Erhebung von Signalaufklärungsdaten zu führen, auch um die Überwachung der Einhaltung der geltenden rechtlichen Anforderungen und wirksame Rechtsbehelfe zu erleichtern. Die Dokumentationspflicht umfasst Elemente wie die faktische Grundlage für die Einschätzung, dass eine bestimmte Datenerhebung notwendig ist, um eine validierte Aufklärungspriorität zu fördern. ([304])

(160) Zusätzlich zu den oben genannten Garantien der EO 14086 für die Verwendung von Informationen, die im Rahmen der Signalaufklärung erhoben wurden, unterliegen alle US-Nachrichtendienste allgemeineren Anforderungen in Bezug auf die Zweckbindung, Datenminimierung, Richtigkeit, Sicherheit, Speicherung und Verbreitung, wie insbesondere aus dem OMB Circular No. A-130, dem E-Government Act, dem Federal Records Act (siehe die Erwägungsgründe 101 bis 106) und den Leitlinien des Committee on National Security Systems (CNSS) hervorgeht. ([305])

3.2.2 *Aufsicht*

(161) Die Tätigkeit der US-Nachrichtendienste unterliegt der Aufsicht verschiedener Stellen.

(162) Erstens verlangt die EO 14086, dass jeder Nachrichtendienst über hochrangige Beamte für Recht, Aufsicht und Compliance verfügt, um die Einhaltung der geltenden US-Rechtsvorschriften zu gewährleisten. ([306]) Insbesondere müssen sie die Tätigkeiten im Rahmen der Signalaufklärung regelmäßig überwachen und dafür sorgen, dass Verstöße abgestellt werden. Die Nachrichtendienste müssen diesen Beamten Zugang zu allen einschlägigen Daten gewähren, damit sie ihre Aufsichtsaufgaben wahrnehmen können, und dürfen keine Maßnahmen treffen, die ihre Aufsichtstätigkeit behindern oder unangemessen beeinflussen. ([307]) Darüber hinaus muss jeder schwerwiegende Verstoß ([308]), der von einer Aufsichtsbehörde oder einem anderen Mitarbeiter festgestellt wird, unverzüglich dem Leiter des Nachrichtendienstes und dem Direktor des nationalen Nachrichtendienstes gemeldet werden, die dafür sorgen müssen, dass alle erforderlichen Maßnahmen getroffen werden, um Abhilfe zu schaffen und eine Wiederholung des schwerwiegenden Verstoßes zu verhindern. ([309])

(163) Diese Aufsichtsfunktion wird von Beauftragten, die für die Einhaltung der Vorschriften zuständig sind, sowie von den Datenschutz- und Bürgerrechtsbeauftragen und den Generalinspekteuren wahrgenommen. ([310])

([301]) Siehe z. B. die AGG-DOM, denen zufolge das FBI Informationen nur dann weitergeben darf, wenn der Empfänger diese benötigt, um seinen Auftrag zu erfüllen oder die Öffentlichkeit zu schützen.

([302]) Abschnitt 2(c)(iii)(A)(1)(c) EO 14086. Nachrichtendienste können beispielsweise unter Umständen, die für strafrechtliche Ermittlungen oder im Zusammenhang mit einer Straftat maßgeblich sind, Informationen verbreiten, z. B. durch die Verbreitung von Warnungen vor der Bedrohung durch Mord, schwere Körperverletzung oder Entführung, Verbreitung von Informationen über Cyberbedrohungen und -vorfälle oder Intrusion Response, Benachrichtigung der Opfer oder Warnung potenzieller Opfer von Straftaten.

([303]) Abschnitt 2(c)(iii)(A)(1)(d) EO 14086.

([304]) Abschnitt 2(c)(iii)(E) EO 14086.

([305]) Siehe CNSS Policy No. 22, Cybersecurity Risk Management Policy and CNSS Instruction 1253, die detaillierte Leitlinien zu Sicherheitsmaßnahmen enthält, die für nationale Sicherheitssysteme zu treffen sind.

([306]) Abschnitt 2(d)(i)(A)-(B) EO 14086.

([307]) Abschnitt 2(d)(i)(B)-(C) EO 14086.

([308]) D. h. ein systematischer oder vorsätzlicher Verstoß gegen geltendes US-Recht, der geeignet ist, den Ruf oder die Integrität eines Nachrichtendienstes zu schädigen oder anderweitig die Angemessenheit signalerfassender Aufklärung infrage zu stellen, auch im Hinblick auf erhebliche Auswirkungen auf die Privatsphäre und die bürgerlichen Freiheiten der betroffenen Person(en), vgl. Abschnitt 5(l) EO 14086.

([309]) Abschnitt 2(d)(iii) EO 14086.

([310]) Abschnitt 2(d)(i)(B) EO 14086.

(164) Wie bei den Strafverfolgungsbehörden gibt es auch bei allen Nachrichtendiensten Datenschutz- und Bürgerrechtsbeauftrage. ([311]) Die Befugnisse dieser Beauftragten umfassen 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 Privatpersonen nachzugehen, die der Meinung sind, dass ihre Privatsphäre oder ihre Bürgerrechte verletzt wurden (in manchen Fällen, so im Büro des Direktors des Nationalen Nachrichtendienstes (Office of the Director of National Intelligence, ODNI), sind die Beauftragten selbst zur Untersuchung von Beschwerden befugt). ([312]) Die Leiter der Nachrichtendienste müssen sicherstellen, dass die Datenschutz- und Bürgerrechtsbeauftragten über die für die Erfüllung ihrer Aufgaben erforderlichen Ressourcen verfügen, dass sie Zugang zu den für die Erfüllung ihrer Aufgaben erforderlichen Materialien und zum Personal haben und dass sie über vorgeschlagene politische Änderungen informiert und dazu konsultiert werden. ([313]) Datenschutz- und Bürgerrechtsbeauftragte übermitteln dem Kongress und dem PCLOB regelmäßig einen Bericht mit Angaben zur Anzahl und Art der bei der Abteilung/beim Nachrichtendienst eingegangenen Beschwerden mit einer Zusammenfassung der Bearbeitung der Beschwerden, der durchgeführten Überprüfungen und Recherchen und der Auswirkungen der von den Beauftragten geleisteten Arbeit. ([314])

(165) Zweitens hat jeder Nachrichtendienst einen unabhängigen Generalinspekteur, der unter anderem für die Kontrolle der Auslandsaufklärung zuständig ist. Im ODNI besteht ein Büro des Generalinspekteurs der Intelligence Community 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. ([315]) Ähnlich wie die Strafverfolgungsbehörden (siehe Erwägungsgrund 109) sind die Generalinspekteure rechtlich unabhängig ([316]) und für die Durchführung von Prüfungen und Untersuchungen im Zusammenhang mit den Programmen und Aktivitäten des jeweiligen Nachrichtendienstes zuständig, darunter auch für Missbrauchsfälle oder Rechtsverstöße. ([317]) Sie haben Zugriff auf alle Unterlagen, Berichte, Audits, Überprüfungen, Dokumente,

([311]) Siehe 42 U.S.C. § 2000ee-1. Dazu zählen beispielsweise das Außenministerium, das Justizministerium. das Ministerium für Innere Sicherheit, das Verteidigungsministerium, die NSA, die Central Intelligence Agency (Zentraler Nachrichtendienst der Vereinigten Staaten, CIA), das FBI und das ODNI.

([312]) Siehe Abschnitt 3(c) EO 14086.

([313]) 42 U.S.C. § 2000ee-1(d).

([314]) Siehe 42 U.S.C. § 2000ee-1 (f)(1),(2). Aus dem Bericht des NSA Civil Liberties, Privacy and Transparency Office (NSA-Büro für Bürgerrechte, Datenschutz und Transparenz) für den Zeitraum Januar 2021 bis Juni 2021 geht beispielsweise hervor, dass 591 Überprüfungen der Auswirkungen auf die Bürgerrechte und die Privatsphäre in verschiedenen Zusammenhängen durchgeführt wurden, z. B. in Bezug auf Erhebungstätigkeiten, Vereinbarungen und Entscheidungen über den Informationsaustausch, Entscheidungen über die Vorratsspeicherung von Daten usw., wobei verschiedene Faktoren berücksichtigt wurden, z. B. die Menge und Art der mit der Tätigkeit verbundenen Informationen, die beteiligten Personen, der Zweck und die voraussichtliche Verwendung der Daten, die bestehenden Schutzmaßnahmen zur Minderung potenzieller Risiken für die Privatsphäre, usw. (https://media.defense.gov/2022/Apr/11/2002974486/-1/-1/1/REPORT%207_CLPT%20JANUARY%20-%20JUNE%202021%20_FINAL.PDF). Die Berichte des CIA Office of Privacy and Civil Liberties (CIA-Büro für Datenschutz und bürgerliche Freiheiten) für den Zeitraum Januar bis Juni 2019 enthalten auch Informationen über die Aufsichtstätigkeiten des Büros, z. B. eine Überprüfung der Einhaltung der Leitlinien des Justizministers nach der EO 12333 in Bezug auf die Speicherung und die Verbreitung von Informationen, Leitlinien für die Umsetzung der PPD 28 und der Anforderungen für die Ermittlung und Behebung von Verstößen gegen den Schutz personenbezogener Daten sowie Überprüfungen der Nutzung und Verarbeitung personenbezogener Daten. (https://www.cia.gov/static/9d762fbef6669c7e6d7f17e227fad82c/2019-Q1-Q2-CIA-OPCL-Semi-Annual-Report.pdf).

([315]) Dieser Generalinspekteur wird mit Zustimmung des Senats vom Präsidenten ernannt und kann nur vom Präsidenten abberufen werden.

([316]) 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 z. B. Inspector General Act of 1978, § 8 (für das Verteidigungsministerium); § 8E (für das Justizministerium), § 8G (d)(2)(A),(B) (für die NSA); 50 U.S.C. § 403q (b) (für die CIA); Intelligence Authorization Act For Fiscal Year 2010, Abschnitt 405(f) (für die Intelligence Community).

([317]) Inspector General Act of 1978, in der geltenden Fassung, Pub. L. 117-108 vom 8. April 2022. Wie in seinen halbjährlichen Berichten an den Kongress für den Zeitraum vom 1. April 2021 bis zum 31. März 2022 dargelegt, hat der Generalinspekteur der NSA beispielsweise den Umgang mit Informationen über US-Bürger, die im Rahmen der EO 12333 gesammelt wurden, das Verfahren zur Bereinigung von Signalaufklärungsdaten, ein von der NSA verwendetes automatisches Targeting-Tool und die Einhaltung der Dokumentations- und Abfrageanforderungen in Bezug auf die Erhebung nach Abschnitt 702 FISA bewertet und in diesem Zusammenhang mehrere Empfehlungen ausgesprochen (siehe https://oig.nsa.gov/Portals/71/Reports/SAR/NSA%20OIG%20SAR%20-%20APR%202021%20-%20SEP%202021%20-%20Unclassified.pdf?ver=IwtrthntGdfEb-EKTOm3gg%3d%3d, S. 5-8 und https://oig.nsa.gov/Portals/71/Images/NSAOIGMAR2022.pdf?ver=jbq2rCrJ00HJ9qDXGHqHLw%3d%3d&timestamp=1657810395907, S. 10-13). Siehe auch die jüngsten Audits und Untersuchungen des Generalinspekteurs der Intelligence Community zur Informationssicherheit und zur unbefugten Weitergabe von Informationen, die aus Gründen der nationalen Sicherheit der Geheimhaltung unterliegen (https://www.dni.gov/files/ICIG/Documents/Publications/Semiannual%20Report/2021/ICIG_Semiannual_Report_April_2021_to_September_2021.pdf, S. 8, 11 und https://www.dni.gov/files/ICIG/Documents/News/ICIGNews/2022/Oct21_SAR/Oct%202021-Mar%202022%20ICIG%20SAR_Unclass_FINAL.pdf, S. 19-20).

Schriftstücke, Empfehlungen oder sonstiges einschlägiges Material, dessen Herausgabe sie notfalls unter Strafandrohung anordnen können, und sind zur Beweisaufnahme berechtigt. ([318]) Die Generalinspekteure leiten Fälle mutmaßlicher strafrechtlicher Verstöße an die Strafverfolgungsbehörden weiter und geben den Leitern der Nachrichtendiensten Empfehlungen für Abhilfemaßnahmen. ([319]) Zwar sind ihre Empfehlungen nicht bindend, doch werden ihre Berichte, auch über die getroffenen (oder unterlassenen) Folgemaßnahmen ([320]), in der Regel öffentlich gemacht und dem Kongress übermittelt, der auf dieser Grundlage seine eigene Aufsichtsfunktion wahrnehmen kann (siehe die Erwägungsgründe 168 und 169). ([321])

(166) Drittens überwacht das Intelligence Oversight Board (IOB) (Nachrichtendienstaufsichtsgremium), das im Rahmen des President's Intelligence Advisory Board (PIAB) (Beratungsgremium des Präsidenten für Nachrichtendienste) eingerichtet wurde, die Einhaltung der Verfassung und aller einschlägigen Vorschriften durch die US-Nachrichtendienste. ([322]) Das PIAB ist ein beratendes Gremium innerhalb des Executive Office of the President (Exekutivbüro des Präsidenten der Vereinigten Staaten), das sich aus 16 Mitgliedern zusammensetzt, die vom Präsidenten von außerhalb der US-Regierung ernannt werden. Das IOB besteht aus maximal fünf Mitgliedern, die vom Präsidenten aus den Reihen der PIAB-Mitglieder ernannt werden. Nach der EO 12333 ([323]) sind die Leiter aller Nachrichtendienste verpflichtet, dem IOB jede nachrichtendienstliche Tätigkeit zu melden, bei der Grund zu der Annahme besteht, dass sie möglicherweise rechtswidrig ist oder gegen eine Executive Order oder eine Presidential Directive verstößt. Um sicherzustellen, dass das IOB Zugang zu den Informationen hat, die es zur Erfüllung seiner Aufgaben benötigt, weist die Executive Order 13462 den Direktor des Nationalen Nachrichtendienstes und die Leiter der Nachrichtendienste an, dem IOB alle Informationen und Unterstützung zur Verfügung zu stellen, die es zur Erfüllung seiner Aufgaben benötigt, soweit dies gesetzlich zulässig ist. ([324]) Das IOB ist seinerseits verpflichtet, den Präsidenten über nachrichtendienstliche Tätigkeiten zu informieren, die seiner Ansicht nach gegen US-Recht (einschließlich Executive Orders) verstoßen und die vom Justizminister, dem Direktor des Nationalen Nachrichtendienstes oder dem Leiter eines Nachrichtendienstes nicht angemessen behandelt werden. ([325]) Darüber hinaus ist das IOB verpflichtet, den Justizminister über mögliche Verstöße gegen das Strafrecht zu informieren.

(167) Viertens unterliegen die Nachrichtendienste der Aufsicht des PCLOB. Nach seinem Gründungsstatut ist das PCLOB mit Aufgaben im Bereich der Terrorismusbekämpfung und deren Umsetzung betraut, wobei der Schutz der Privatsphäre und der bürgerlichen Freiheiten im Vordergrund steht. Bei der Überprüfung der Tätigkeit der Nachrichtendienste hat es 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. ([326]) Es erhält Berichte von Bürgerrechts- und Datenschutzbeauftragten verschiedener Regierungsstellen ([327]), kann gegenüber der Regierung und den Nachrichtendiensten Empfehlungen abgeben und erstattet regelmäßig den Ausschüssen des Kongresses und dem Präsidenten Bericht. ([328]) Die Berichte des PCLOB, einschließlich der Berichte an den Kongress, müssen so weit wie möglich veröffentlicht werden. ([329]) Das PCLOB hat mehrere Aufsichts- und Folgeberichte veröffentlicht, darunter eine Analyse der auf der Grundlage von Abschnitt 702 FISA durchgeführten Programme und des Schutzes der Privatsphäre in diesem Zusammenhang, die Umsetzung der PPD 28 und der EO 12333. ([330]) Das PCLOB hat auch

([318]) Siehe Inspector General Act of 1978, § 6.

([319]) Siehe ebenda §§ 4, 6-5.

([320]) Was die Folgemaßnahmen zu den Berichten und Empfehlungen der Generalinspekteure betrifft, siehe beispielsweise die Reaktion auf den Bericht des Generalinspekteurs des Justizministeriums, in dem festgestellt wurde, dass das FBI in den Jahren 2014 bis 2019 gegenüber dem FISC nicht ausreichend transparent war, was zu Reformen führte, um die Einhaltung der Vorschriften, die Aufsicht und die Rechenschaftspflicht beim FBI zu verbessern (z. B. der FBI-Direktor ordnete mehr als 40 Abhilfemaßnahmen an, von denen 12 speziell das FISA-Verfahren in Bezug auf Dokumentation, Aufsicht, Aktenführung, Schulung und Audits betrafen) (siehe https://www.justice.gov/opa/pr/department-justice-and-federal-bureau-investigation-announce-critical-reforms-enhance und https://oig.justice.gov/reports/2019/o20012.pdf). Siehe z. B. auch den Audit des Generalinspekteurs des Justizministeriums über die Aufgaben und Verantwortlichkeiten des Office of the General Counsel des FBI bei der Überwachung der Einhaltung der geltenden Gesetze, Strategien und Verfahren in Bezug auf die Aktivitäten des FBI im Bereich der nationalen Sicherheit sowie Anlage 2, die ein Schreiben des FBI enthält, in dem alle Empfehlungen angenommen werden. Anlage 3 gibt einen Überblick über die Folgemaßnahmen und Informationen, die der Generalinspekteur vom FBI angefordert hat, um seine Empfehlungen abschließen zu können (https://oig.justice.gov/sites/default/files/reports/22-116.pdf).

([321]) Siehe Inspector General Act of 1978, §§ 4(5), 5.

([322]) Siehe die EO 13462.

([323]) Abschnitt 1.6(c) EO 12333.

([324]) Abschnitt 8(a) EO 13462.

([325]) Abschnitt 6(b) EO 13462.

([326]) 42 U.S.C. § 2000ee (g).

([327]) Siehe 42 U.S.C. § 2000ee-1 (f)(1)(A)(iii). Dazu zählen zumindest das Justizministerium, das Verteidigungsministerium, das Ministerium für Innere Sicherheit, der Direktor des Nationalen Nachrichtendienstes und die Central Intelligence Agency (Zentraler Nachrichtendienst der Vereinigten Staaten) sowie andere Regierungsstellen oder Einrichtungen der Exekutive, deren Einbeziehung das PCLOB für sinnvoll erachtet.

([328]) 42 U.S.C. § 2000ee (e).

([329]) 42 U.S.C. § 2000ee (f).

([330]) Abrufbar unter https://www.pclob.gov/Oversight.

die Aufgabe, die Umsetzung der EO 14086 zu überwachen, indem es insbesondere prüft, ob die Verfahren der Nachrichtendienste mit der EO vereinbar sind (siehe Erwägungsgrund 126), und indem es das Funktionieren des Rechtsbehelfsverfahrens bewertet (siehe Erwägungsgrund 194).

(168) Fünftens nehmen zusätzlich zu den Kontrollmechanismen innerhalb der Exekutive spezielle Ausschüsse des US-Kongresses (House and Senate Intelligence and Judiciary Committees (Ausschüsse des Repräsentantenhauses und des Senats für Nachrichtendienste und Justiz)) Kontrollaufgaben wahr, die alle Formen der Auslandsaufklärung betreffen. Die Mitglieder dieser Ausschüsse haben Zugriff auf Informationen, die der Geheimhaltung unterliegen, sowie auf nachrichtendienstliche Methoden und Programme. ([331]) Die Justizausschüsse üben ihre Aufsicht auf verschiedene Weise aus, insbesondere durch Anhörungen, Untersuchungen, Überprüfungen und Berichte. ([332])

(169) Die Kongressausschüsse erhalten regelmäßig Berichte über nachrichtendienstliche Tätigkeiten, u. a. vom Justizminister, dem Direktor des Nationalen Nachrichtendienstes, den Nachrichtendiensten und anderen Aufsichtsgremien (z. B. den Generalinspekteuren), siehe die Erwägungsgründe 164 und 165. Der National Security Act besagt insbesondere: „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". ([333]) 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 getroffen wurden bzw. geplant sind". ([334])

(170) Darüber hinaus ergeben sich aus bestimmten Gesetzen zusätzliche Berichtspflichten. So 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. ([335]) Das Gesetz verpflichtet die Regierung auch dazu, den Kongressausschüssen Kopien sämtlicher Entscheidungen, Anordnungen oder Stellungnahmen des FISC oder des FISCR zukommen zu lassen, die eine „wichtige Auslegung oder Interpretation" der FISA-Bestimmungen beinhalten. Bei der Überwachung nach Abschnitt 702 FISA erfolgt die parlamentarische 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 Abschnitt 702 FISA, mit Belegen, einschließlich der Compliance-Berichte des Justizministeriums und des ODNI und einer Beschreibung von Verstößen ([336]), und eine gesonderte halbjährliche Einschätzung des Justizministers und des DNI, in der die Einhaltung der Verfahren zur zielgenauen Datenerhebung und zur Datenminimierung dokumentiert wird ([337]).

([331]) 50 U.S.C. § 3091.

([332]) So veranstalten die Ausschüsse thematische Anhörungen (vgl. z. B. die jüngste Anhörung des Justizausschusses des Repräsentantenhauses zum Thema „Digitale Rasterfahndung", https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4983 und eine Anhörung des House Intelligence Committee zum Einsatz von KI durch die Intelligence Community, (https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=114263) sowie regelmäßige Anhörungen zur Aufsicht, z. B. über die für nationale Sicherheit zuständige Abteilung des FBI und des Justizministeriums, vgl. https://www.judiciary.senate.gov/meetings/08/04/2022/oversight-of-the-federal-bureau-of-investigation; https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4966 und https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4899. Ein Beispiel ist die Ermittlung des Senate Intelligence Committee zur russischen Einmischung in die US-Wahlen 2016, siehe https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-russian-active-measures. Zur Berichterstattung vgl. etwa die Übersicht über die (Aufsichts-) Tätigkeiten des Ausschusses im Bericht des Senate Intelligence Committee an den Senat für den Zeitraum 4. Januar 2019–3. Januar 2021, https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-covering-period-january-4.

([333]) Siehe 50 U.S.C. § 3091(a)(1). Diese Bestimmungen regeln die allgemeinen Anforderungen an die Kontrolltätigkeit des Kongresses im Bereich der nationalen Sicherheit.

([334]) Siehe 50 U.S.C. §3091(b).

([335]) Siehe 50 U.S.C. §§ 1808, 1846, 1862, 1871, 1881f.

([336]) Siehe 50 U.S.C. § 1881f.

([337]) Siehe 50 U.S.C. § 1881a(l)(1).

(171) Nach dem FISA muss die US-Regierung ferner alljährlich gegenüber dem Kongress (und der Öffentlichkeit) unter anderem die Anzahl der beantragten und genehmigten FISA-Anordnungen sowie die geschätzte Anzahl der von Überwachungsmaßnahmen betroffenen US-Bürger und Nicht-US-Bürger offenlegen. ([338]) Das Gesetz verlangt zudem, die Öffentlichkeit zusätzlich über die Anzahl der erteilten NSL zu unterrichten, wiederum aufgeschlüsselt nach US-Bürgern und Nicht-US-Bürgern (wobei gleichzeitig aber den Empfängern von FISA-Anordnungen und -Zertifizierungen sowie NSL-Auskunftsersuchen gestattet wird, unter bestimmten Voraussetzungen Transparenzberichte vorzulegen). ([339])

(172) Generell unternimmt die US-Intelligence Community verschiedene Anstrengungen, um Transparenz in Bezug auf ihre (Auslands-)Aufklärungsaktivitäten zu gewährleisten. So hat das ODNI im Jahr 2015 Grundsätze für die Transparenz der Nachrichtendienste und einen Umsetzungsplan für die Transparenz verabschiedet und jeden Nachrichtendienst angewiesen, einen Beauftragten für die Transparenz der Nachrichtendienste zu ernennen, der die Transparenz fördern und Transparenzinitiativen leiten soll. ([340]) Im Rahmen dieser Bemühungen hat die Intelligence Community freigegebene Teile von Strategien, Verfahren, Aufsichtsberichten, Berichten über Tätigkeiten nach Abschnitt 702 FISA und der EO 12333, FISC-Entscheidungen und andere Materialien veröffentlicht und wird dies auch weiterhin tun, unter anderem auf einer speziellen, vom ODNI betriebenen Website „IC on the Record". ([341])

(173) Schließlich unterliegt die Erhebung personenbezogener Daten nach Abschnitt 702 FISA zusätzlich zu der in den Erwägungsgründen 162 bis 168 genannten Aufsicht durch die Aufsichtsbehörden auch der Aufsicht durch das FISC. ([342]) Nach Rule 13 der FISC Rules of Procedure sind die Compliance-Beauftragten der US-Nachrichtendienste verpflichtet, alle Verstöße gegen die Verfahren nach Abschnitt 702 FISA zur zielgenauen Datenerhebung, -minimierung und -abfrage dem Justizministerium und dem ODNI zu melden, die ihrerseits das FISC unterrichten. Darüber hinaus legen das Justizministerium und das ODNI dem FISC halbjährlich gemeinsame Berichte zur Bewertung der Aufsicht vor, in denen Trends bei der Einhaltung der Vorschriften aufgezeigt, statistische Daten bereitgestellt, Kategorien von Vorfällen im Zusammenhang mit der Einhaltung der Vorschriften beschrieben, die Gründe für das Auftreten bestimmter Vorfälle bei der Einhaltung der Zielvorgaben detailliert erläutert und die Maßnahmen dargelegt werden, die die Nachrichtendienste getroffen haben, um eine Wiederholung zu vermeiden. ([343])

(174) Erforderlichenfalls (z. B. wenn Verstöße gegen die zielgenaue Erfassung festgestellt werden) kann das Gericht den betreffenden Nachrichtendienst anweisen, Abhilfemaßnahmen zu treffen. ([344]) Die möglichen Abhilfemaßnahmen können von individuellen bis zu strukturellen Maßnahmen reichen, z. B. von der Einstellung der Datenerhebung und der Löschung unrechtmäßig erlangter Daten bis hin zur Änderung der Erhebungspraxis, die sich auch auf Leitlinien und Mitarbeiterschulungen erstrecken kann. ([345]) Darüber hinaus prüft das FISC im Rahmen seiner jährlichen Überprüfung der Zertifizierungen nach Abschnitt 702, ob die vorgelegten Zertifizierungen den

([338]) 50 U.S.C. § 1873(b). Des Weiteren besagt Abschnitt 402: „Der Direktor des Nationalen Nachrichtendienstes 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 Abschnitt 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."

([339]) 50 U.S.C. §§ 1873(b)(7) und 1874.

([340]) https://www.dni.gov/index.php/ic-legal-reference-book/the-principles-of-intelligence-transparency-for-the-ic.

([341]) Siehe „IC on the Record", abrufbar unter https://icontherecord.tumblr.com/.

([342]) In der Vergangenheit kam das FISC zu dem Schluss, dass „es für das Gericht offensichtlich ist, dass die Vollzugsbehörden sowie [das ODNI] und [die Abteilung für nationale Sicherheit des Justizministeriums] beträchtliche Ressourcen für die Einhaltung und Aufsicht über die Einhaltung der Grundsätze nach Abschnitt 702 aufwenden. In der Regel werden Verstöße unverzüglich festgestellt und geeignete Abhilfemaßnahmen getroffen, einschließlich der Löschung von Informationen, die unrechtmäßig erlangt wurden oder nach den geltenden Verfahren anderweitig zerstört werden müssen." FISA Court, Memorandum Opinion and Order [Überschrift unkenntlich gemacht] (2014), abrufbar unter https://www.dni.gov/files/documents/0928/FISC%20Memorandum%20Opinion%20and%20Order%2026%20August%202014.pdf.

([343]) Siehe z. B. DOJ/ODNI FISA 702 Compliance Report to FISC for June 2018–Nov. 2018, S. 21–65.

([344]) 50 U.S.C. § 1803(h). Siehe auch PCLOB, Section 702 Report, S. 76. Siehe auch FISC Memorandum Opinion and Order vom 3. Oktober 2011 als Beispiel für eine Mängelverfügung, in der die Regierung angewiesen wurde, die festgestellten Mängel innerhalb von 30 Tagen zu beheben. Abrufbar unter https://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf. Siehe Walton Letter, Abschnitt 4, S. 10–11. Siehe auch die Stellungnahme des FISC vom 18. Oktober 2018, abrufbar unter https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opin_18Oct18.pdf, die vom Foreign Intelligence Court of Review in seiner Stellungnahme vom 12. Juli 2019, abrufbar unter https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISCR_Opinion_12Jul19.pdf, bestätigt wurde, in der das FISC die Regierung unter anderem anordnete, bestimmte Melde-, Dokumentations- und Berichtspflichten gegenüber dem FISC zu erfüllen.

([345]) Siehe z. B. FISC, Memorandum Opinion and Order, S. 76 (6. Dezember 2019) (zur Veröffentlichung freigegeben am 4. September 2020), in dem das FISC der Regierung anordnet, bis zum 28. Februar 2020 einen schriftlichen Bericht über die Maßnahmen vorzulegen, die die Regierung trifft, um die Verfahren zur Identifizierung und Löschung von Berichten zu verbessern, die auf Informationen nach Abschnitt 702 FISA beruhen und aus Compliance-Gründen zurückgezogen wurden, sowie über andere Fragen. Siehe auch Anhang VII.

Anforderungen des FISA entsprechen. Stellt das FISC fest, dass die Zertifizierungen der Regierung unzureichend sind, insbesondere aufgrund bestimmter Compliance-Verstöße, kann es eine sogenannte „deficiency order" (Mängelverfügung) erlassen, mit der die Regierung aufgefordert wird, den Mangel innerhalb von 30 Tagen zu beheben, oder die Durchführung der Zertifizierung nach Abschnitt 702 auszusetzen oder nicht zu beginnen. Schließlich bewertet das FISC die von ihm beobachteten Compliance-Trends und kann Verfahrensänderungen oder zusätzliche Überwachung und Berichterstattung verlangen, um Compliance-Trends anzugehen. ([346])

3.2.3 *Rechtsbehelfe*

(175) Wie in diesem Abschnitt näher erläutert wird, gibt es in den Vereinigten Staaten eine Reihe von Möglichkeiten für betroffene Personen in der Union, vor einem unabhängigen und unparteiischen Gericht mit der Befugnis zu verbindlichen Entscheidungen Klage zu erheben. Zusammen ermöglichen sie es Privatpersonen, Zugang zu ihren personenbezogenen Daten zu erhalten, die Rechtmäßigkeit des staatlichen Zugriffs auf ihre Daten überprüfen zu lassen und im Falle eines Verstoßes Abhilfe zu erwirken, einschließlich der Berichtigung oder Löschung ihrer personenbezogenen Daten.

(176) Erstens wird im Rahmen der EO 14086 eine spezielle Beschwerdestelle eingerichtet, ergänzt durch den Erlass des US-Justizministers zur Einrichtung eines Datenschutzüberprüfungsgerichts, das Beschwerden von Privatpersonen im Zusammenhang mit der signalerfassenden Aufklärung der USA bearbeiten und lösen soll. Jede Person in der EU hat das Recht, bei der Beschwerdestelle eine Beschwerde wegen einer mutmaßlichen Verletzung des US-Rechts im Bereich der signalerfassenden Aufklärung (z. B. EO 14086 Abschnitt 702 FISA, EO 12333) einzureichen, die ihre Interessen in Bezug auf Privatsphäre und bürgerliche Freiheiten beeinträchtigt. ([347]) Diese Beschwerdestelle steht Personen aus Ländern oder Organisationen der regionalen Wirtschaftsintegration offen, die vom US-Justizminister als „zugelassene Staaten" benannt wurden. ([348]) Am 30. Juni 2023 wurden die Europäische Union und die drei Länder der Europäischen Freihandelsassoziation, die zusammen den Europäischen Wirtschaftsraum bilden, vom Justizminister nach Abschnitt 3(f) EO 14086 als „zugelassene Staaten" benannt. ([349]) Diese Benennung lässt Artikel 4 Absatz 2 des Vertrags über die Europäische Union unberührt.

(177) Eine Beschwerde ist von einer betroffenen Person in der Union bei einer für die Überwachung der Verarbeitung von personenbezogenen Daten durch Behörden zuständigen Aufsichtsstelle eines EU-Mitgliedstaats (Datenschutzbehörde) einzureichen. ([350]) Dies erleichtert den Zugang zum Rechtsbehelfsverfahren, da sich der Einzelne an eine Behörde in seiner Nähe wenden kann, mit der er in seiner eigenen Sprache kommunizieren kann. Nachdem geprüft wurde, ob die in Erwägungsgrund 178 genannten Voraussetzungen für die Einreichung einer Beschwerde erfüllt sind, leitet die zuständige Datenschutzbehörde die Beschwerde über das Sekretariat des Europäischen Datenschutzausschusses an die Beschwerdestelle weiter.

(178) Die Zulässigkeitsvoraussetzungen für eine Beschwerde bei der Beschwerdestelle sind niedrig, da die betroffenen Personen nicht nachweisen müssen, dass ihre Daten tatsächlich Gegenstand der Signalaufklärung durch die USA waren. ([351]) Als Ausgangspunkt für die Überprüfung durch die Beschwerdestelle müssen einige grundlegende Informationen zur Verfügung gestellt werden, z. B. die personenbezogenen Daten, die mutmaßlich in die USA übermittelt wurden, und die Mittel, mit denen sie übermittelt wurden, die Identität der US-Regierungsstellen, denen eine Beteiligung an dem mutmaßlichen Verstoß vorgeworfen wird (sofern bekannt), die Grundlage für die Behauptung, dass ein Verstoß gegen US-Recht vorliegt (obwohl auch hier nicht nachgewiesen werden muss, dass die personenbezogenen Daten tatsächlich von US-Nachrichtendiensten erhoben wurden) und die Art der beantragten Maßnahme.

([346]) Siehe Anhang VII.

([347]) Siehe Abschnitt 4(k)(iv) EO 14086, wonach ein Beschwerdeführer in eigenem Namen (d. h. nicht als Vertreter einer Regierung, einer Nichtregierungsorganisation oder einer zwischenstaatlichen Organisation) eine Beschwerde bei der Beschwerdestelle einreichen muss. Der Begriff „beeinträchtigt" verlangt nicht, dass der Beschwerdeführer einen bestimmten Grenzwert erfüllen muss, um Zugang zum Rechtsbehelfsverfahren zu erhalten (siehe hierzu Erwägungsgrund 178). Vielmehr wird klargestellt, dass der ODNI CLPO und das Datenschutzüberprüfungsgericht befugt sind, Verletzungen des US-Rechts im Bereich der signalerfassenden Aufklärung zu beheben, die die individuellen Interessen des Beschwerdeführers in Bezug auf die Privatsphäre und die bürgerlichen Freiheiten beeinträchtigen. Umgekehrt fallen Verstöße gegen Anforderungen nach geltendem US-Recht, die nicht dem Schutz von Einzelpersonen dienen (z. B. Haushaltsanforderungen), nicht in die Zuständigkeit des ODNI CLPO und des Datenschutzüberprüfungsgerichts.

([348]) Abschnitt 3(f) EO 14086.

([349]) https://www.justice.gov/opcl/executive-order-14086.

([350]) Abschnitt 4(d)(v) EO 14086.

([351]) Siehe Abschnitt 4(k)(i)-(iv) EO 14086.

(179) Die erste Untersuchung von Beschwerden durch die Beschwerdestelle wird vom ODNI CLPO durchgeführt, dessen bestehende gesetzliche Rolle und Befugnisse für die spezifischen Maßnahmen nach der EO 14086 erweitert wurden. ([352]) Innerhalb der Intelligence Community ist das CLPO unter anderem zuständig für die Sicherstellung, dass der Schutz der bürgerlichen Freiheiten und der Privatsphäre angemessen in die Strategien und Verfahren des ODNI und der Nachrichtendienste integriert wird, die Überwachung der Einhaltung der geltenden Anforderungen an den Schutz der bürgerlichen Freiheiten und der Privatsphäre durch das ODNI und die Durchführung von Datenschutz-Folgeabschätzungen. ([353]) Der ODNI CLPO kann nur aus wichtigem Grund vom Direktor des Nationalen Sicherheitsdienstes aufgelöst werden, d. h. wegen Fehlverhaltens, Amtsmissbrauchs, Verstoßes gegen Sicherheitsvorschriften, Pflichtversäumnis oder Unfähigkeit. ([354])

(180) Bei der Durchführung seiner Überprüfungen hat der ODNI CLPO Zugang zu den für seine Bewertung erforderlichen Informationen und kann sich auf die obligatorische Unterstützung der Datenschutz- und Bürgerrechtsbeauftragten der einzelnen Nachrichtendienste stützen. ([355]) Den Nachrichtendiensten ist es untersagt, die Überprüfungen des ODNI CLPO zu behindern oder in unzulässiger Weise zu beeinflussen. Dies gilt auch für den Direktor des Nationalen Nachrichtendienstes, der nicht in die Überprüfung eingreifen darf. ([356]) Bei der Prüfung einer Beschwerde muss der ODNI CLPO die Rechtsvorschriften „unparteiisch" anwenden und dabei sowohl die nationalen Sicherheitsinteressen in Bezug auf signalerfassende Aufklärung als auch den Schutz der Privatsphäre berücksichtigen. ([357])

(181) Im Rahmen seiner Überprüfung stellt der ODNI CLPO fest, ob ein Verstoß gegen geltendes US-Recht vorliegt und entscheidet gegebenenfalls über geeignete Abhilfemaßnahmen. ([358]) Letzteres bezieht sich auf Maßnahmen, mit denen ein festgestellter Verstoß vollständig behoben wird, z. B. die Einstellung der unrechtmäßigen Datenerhebung, die Löschung unrechtmäßig erhobener Daten, die Löschung der Ergebnisse unrechtmäßig durchgeführter Abfragen von ansonsten rechtmäßig erhobenen Daten, die Einschränkung des Zugriffs auf rechtmäßig erhobene Daten auf entsprechend geschulte Mitarbeiter oder die Rücknahme von Aufklärungsberichten, die unrechtmäßig erhobene oder unrechtmäßig verbreitete Daten enthalten. ([359]) Die Entscheidungen des ODNI CLPO über einzelne Beschwerden (einschließlich der Abhilfemaßnahmen) sind für die betroffenen Nachrichtendienste bindend. ([360])

(182) Der ODNI CLPO muss seine Überprüfung dokumentieren und eine vertrauliche Entscheidung vorlegen, in der er die Grundlage für seine Tatsachenfeststellungen erläutert, feststellt, ob ein betroffener Verstoß vorliegt, und geeignete Abhilfemaßnahmen festlegt. ([361]) Wird bei der Überprüfung durch den ODNI CLPO ein Verstoß gegen eine Behörde festgestellt, die der Aufsicht des FISC unterliegt, muss der CLPO auch einen der Geheimhaltung unterliegenden Bericht an den stellvertretenden Justizminister für nationale Sicherheit übermitteln, der seinerseits verpflichtet ist, den Verstoß an das FISC zu melden, das weitere Durchsetzungsmaßnahmen ergreifen kann (nach dem in den Erwägungsgründen 173 und 174 beschriebenen Verfahren). ([362])

(183) Nach Abschluss der Überprüfung teilt der ODNI CLPO dem Beschwerdeführer über die nationale Behörde mit, dass „bei der Überprüfung entweder keine einschlägigen Verstöße festgestellt wurden oder der ODNI CLPO eine Feststellung getroffen hat, die angemessene Abhilfemaßnahmen erfordert". ([363]) Dadurch kann die Vertraulichkeit von Tätigkeiten zum Schutz der nationalen Sicherheit gewahrt werden, während die betroffenen Personen eine Entscheidung erhalten, die bestätigt, dass ihre Beschwerde ordnungsgemäß geprüft und entschieden wurde. Diese Entscheidung kann zudem von der Privatperson angefochten werden. Zu diesem Zweck wird sie über die Möglichkeit informiert, bei dem Datenschutzprüfungsgericht (Data Protection Review Court, im Folgenden „DPRC") eine Überprüfung der Entscheidungen des CLPO zu beantragen (siehe die Erwägungsgründe 184 ff.), und darüber, dass im Falle der Anrufung des Gerichts ein spezieller Anwalt bestellt wird, der die Interessen des Antragstellers vertritt. ([364])

([352]) Abschnitt 3(c)(iv) EO 14086. Siehe auch National Security Act 1947, 50 U.S.C. §403-3d, Abschnitt 103D betreffend die Rolle des CLPO innerhalb des ODNI.
([353]) 50 U.S.C. § 3029 (b).
([354]) Abschnitt 3(c)(iv) EO 14086.
([355]) Abschnitt 3(c)(iii) EO 14086.
([356]) Abschnitt 3(c)(iv) EO 14086.
([357]) Abschnitt 3(c)(i)(B)(i) und (iii) EO 14086.
([358]) Abschnitt 3(c)(i) EO 14086.
([359]) Abschnitt 4(a) EO 14086.
([360]) Abschnitt 3(c)(d) EO 14086.
([361]) Abschnitt 3(c)(i)(F)-(G) EO 14086.
([362]) Siehe auch Abschnitt 3(c)(i)(D) EO 14086.
([363]) Abschnitt 3(c)(i)(E)(1) EO 14086.
([364]) Abschnitte 3(c)(i)(E)(2)-(3) EO 14086.

(184) Jeder Beschwerdeführer und jeder Teil der Intelligence Community kann bei dem DPRC eine Überprüfung der Entscheidung des ODNI CLPO beantragen. Solche Anträge müssen innerhalb von 60 Tagen nach Erhalt der Benachrichtigung durch den ODNI CLPO, dass die Überprüfung abgeschlossen ist, eingereicht werden und alle Informationen enthalten, die die betroffene Person dem DPRC zur Verfügung stellen möchte (z. B. Argumente zu Rechtsfragen oder zur Anwendung des Rechts auf den Sachverhalt). ([365]) Die betroffenen Personen in der Union können ihren Antrag erneut bei der zuständigen Datenschutzbehörde einreichen (siehe Erwägungsgrund 177).

(185) Das DPRC ist ein unabhängiges Rechtsorgan, das vom Justizminister auf der Grundlage der EO 14086 eingerichtet wurde. ([366]) Es besteht aus mindestens sechs Richtern, die vom Justizminister in Absprache mit dem PCLOB, dem Handelsminister und dem Direktor des Nationalen Nachrichtendienstes für eine verlängerbare Amtszeit von vier Jahren ernannt werden. ([367]) Die Ernennung von Richtern durch den Justizminister erfolgt nach den Kriterien, die die Exekutive bei der Beurteilung von Bewerbern für das Amt eines Bundesrichters anwendet, wobei etwaige richterliche Vorerfahrungen berücksichtigt werden. ([368]) Darüber hinaus müssen die Richter Rechtspraktiker sein (d. h. aktive Mitglieder der Anwaltskammer und ordnungsgemäß zur Ausübung des Rechtsberufs zugelassen sein) und über angemessene Erfahrung im Bereich des Datenschutzes und der nationalen Sicherheit verfügen. Der Justizminister muss sicherstellen, dass mindestens die Hälfte der Richter über richterliche Erfahrung verfügt, und alle Richter müssen über eine Zugangsberechtigung zu vertraulichen Informationen über die nationale Sicherheit verfügen. ([369])

(186) Zum Mitglied des DPRC können nur Personen ernannt werden, die die in Erwägungsgrund 185 genannten Voraussetzungen erfüllen und weder zum Zeitpunkt ihrer Ernennung noch in den zwei Jahren davor in der Exekutive beschäftigt waren. Ebenso dürfen die Richter während ihrer Amtszeit bei dem DPRC kein offizielles Amt oder Anstellung bei der US-Regierung haben (außer als Richter des DPRC). ([370])

(187) Die Unabhängigkeit der Urteilsfindung wird durch eine Reihe von Garantien gewährleistet. Insbesondere ist es der Exekutive (dem Justizminister und den Nachrichtendiensten) untersagt, in die Überprüfung durch das DPRC einzugreifen oder diese unangemessen zu beeinflussen. ([371]) Das DPRC selbst ist zu einer unparteiischen Rechtsprechung verpflichtet ([372]) und arbeitet nach einer eigenen Geschäftsordnung (die durch Mehrheitsbeschluss angenommen wird). Darüber hinaus können die Richter des DPRC nur vom Justizminister und nur aus wichtigem Grund entlassen werden (d. h. wegen Fehlverhaltens, Amtsmissbrauchs, Verstoßes gegen Sicherheitsvorschriften, Pflichtversäumnis oder Unfähigkeit), jedoch nach gebührender Berücksichtigung der für Bundesrichter geltenden Standards, die in den Rules for Judicial-Conduct and Judicial-Disability Proceedings (Regeln für Verfahren im Zusammenhang mit richterlichem Verhalten und der Unfähigkeit von Richtern) festgelegt sind. ([373])

([365]) Abschnitte 201.6(a)-(b) des Erlasses des US-Justizministers.

([366]) Abschnitt 3(d)(i)) und der Erlass des US-Justizministers. Der Oberste Gerichtshof der Vereinigten Staaten hat dem Justizminister die Möglichkeit eingeräumt, unabhängige Gremien mit Entscheidungsbefugnis einzurichten, die auch in Einzelfällen entscheiden können, siehe insbesondere United States ex rel. Accardi v. Shaughnessy, 347 U.S. 260 (1954) und United States v. Nixon, 418 U.S. 683, 695 (1974). Die Einhaltung der unterschiedlichen Anforderungen der EO 14086, z. B. der Kriterien und Verfahren für die Ernennung und Entlassung von Richtern des DPRC, unterliegt insbesondere der Aufsicht des Generalinspektors des Justizministeriums (siehe auch Erwägungsgrund 109 über die gesetzlichen Befugnisse der Generalinspektoren).

([367]) Abschnitt 3(d)(i)(A) EO 14086 und Abschnitt 201.3(a) des Erlasses des US-Justizministers.

([368]) Abschnitt 201.3(b) des Erlasses des US-Justizministers.

([369]) Abschnitt 3(d)(i)(B) EO 14086.

([370]) Abschnitt 3(d)(i)(A) EO 14086 und Abschnitt 201.3(a) und (c) des Erlasses des US-Justizministers. Die Mitglieder des DPRC dürfen außergerichtliche Tätigkeiten einschließlich Handels- und Finanztätigkeiten, gemeinnützige und treuhänderische Tätigkeiten sowie die anwaltliche Tätigkeit ausüben, solange diese Tätigkeiten nicht die unparteiische Ausübung ihrer Pflichten oder die Wirksamkeit oder Unabhängigkeit des DPRC beeinträchtigen (Abschnitt 201.7(c) des Erlasses des US-Justizministers).

([371]) Abschnitte 3(d)(iii)-(iv) EO 14086 und Abschnitt 201.7(d) des Erlasses des US-Justizministers.

([372]) Abschnitt 3(d)(i)(D) EO 14086 und Abschnitt 201.9 des Erlasses des US-Justizministers.

([373]) Abschnitt 3(d)(iv) EO 14086 und Abschnitt 201.7(d) des Erlasses des US-Justizministers. Siehe auch Bumap v. United States, 252 U. S. 512, 515 (1920), wo der seit Langem bestehende Grundsatz des US-Rechts bestätigt wurde, dass die Befugnis zur Entlassung mit der Befugnis zur Ernennung verbunden ist (worauf auch vom Office of Legal Counsel of the DoJ in The Constitutional Separation of Powers between the President and Congress, 20 Op. O.L.C. 124, 166 (1996) hingewiesen wurde).

(188) Die Beschwerden an das DPRC werden von einem dreiköpfigen Panel von Richtern, einschließlich eines vorsitzenden Richters, geprüft, die im Einklang mit dem Code of Conduct for U.S. Judges (Verhaltenskodex für US-Richter) handeln müssen. ([374]) Jedes Panel wird von einem Spezialanwalt ([375]) unterstützt, der Zugang zu allen Informationen hat, die den Fall betreffen, einschließlich vertraulicher Informationen. ([376]) Die Rolle des Spezialanwalts besteht darin, sicherzustellen, dass die Interessen des Beschwerdeführers vertreten werden und dass das DPRC-Panel über alle relevanten rechtlichen und sachlichen Fragen gut informiert ist. ([377]) Um seine Position in Bezug auf eine Beschwerde einer Privatperson beim DPRC zu untermauern, kann der Spezialanwalt den Beschwerdeführer schriftlich um Informationen ersuchen. ([378])

(189) Das DPRC prüft die Feststellungen des ODNI CLPO (sowohl hinsichtlich der Frage, ob ein Verstoß gegen geltendes US-Recht vorliegt, als auch hinsichtlich der Frage, welche Abhilfemaßnahmen angemessen sind) und stützt sich dabei zumindest auf die Untersuchungsunterlagen des ODNI CLPO sowie auf alle vom Beschwerdeführer, dem Spezialanwalt oder einem Nachrichtendienst vorgelegten Informationen und Eingaben. ([379]) Ein Panel des DPRC hat Zugang zu allen für die Durchführung einer Überprüfung erforderlichen Informationen, die es über den ODNI CLPO erhalten kann (z. B. kann das Panel den CLPO auffordern, seine Unterlagen durch zusätzliche Informationen oder Tatsachenfeststellungen zu ergänzen, wenn dies für die Durchführung der Überprüfung erforderlich ist). ([380])

(190) Nach Abschluss seiner Überprüfung kann das DPRC 1) entscheiden, dass es keine Beweise dafür gibt, dass in Bezug auf die personenbezogenen Daten des Beschwerdeführers eine signalerfassende Aufklärung stattgefunden hat, 2) entscheiden, dass die Feststellungen des ODNI CLPO rechtlich korrekt und durch stichhaltige Beweise untermauert sind, oder 3) wenn das DPRC mit den Feststellungen des ODNI CLPO nicht einverstanden ist (ob ein Verstoß gegen geltendes US-Recht vorliegt oder welche Abhilfemaßnahmen angemessen sind), seine eigenen Feststellungen treffen. ([381])

([374]) Abschnitt 3(d)(i)(B) EO 14086 und Abschnitt 201.7(a)-(c) des Erlasses des US-Justizministers. Das Büro für Datenschutz und Bürgerrechte (Office of Privacy and Civil Liberties, im Folgenden „OPCL") des Justizministeriums, das für die administrative Unterstützung des DPRC und der Spezialanwälte zuständig ist (siehe Abschnitt 201.5 des Erlasses des US-Justizministers), wählt nach dem Rotationsprinzip ein dreiköpfiges Panel aus, wobei darauf zu achten ist, dass in jedem Panel mindestens ein Richter mit richterlicher Erfahrung vertreten ist (wenn keiner der Richter im Panel über eine solche Erfahrung verfügt, übernimmt der vom OPCL zuerst ausgewählte Richter den Vorsitz).

([375]) Abschnitt 201.4 des Erlasses des US-Justizministers. Mindestens zwei Spezialanwälte werden vom Justizminister in Absprache mit dem Handelsminister, dem Direktor des Nationalen Nachrichtendienstes und dem PCLOB für eine Amtszeit ernannt, die zweimal verlängert werden kann. Die Spezialanwälte müssen über einschlägige Erfahrungen auf dem Gebiet des Datenschutzes und des Rechts der nationalen Sicherheit verfügen, erfahrene Rechtsanwälte, aktive Mitglieder der Anwaltskammer und ordnungsgemäß zur Ausübung des Rechtsanwaltsberufs zugelassen sein. Außerdem dürfen sie zum Zeitpunkt ihrer ersten Ernennung in den vorangegangenen zwei Jahren nicht bei der Exekutive beschäftigt gewesen sein. Für jede Überprüfung eines Antrags wählt der vorsitzende Richter einen Spezialanwalt zur Unterstützung des Panels aus, siehe Abschnitt 201.8(a) des Erlasses des US-Justizministers.

([376]) Abschnitt 201.8(c) und 201.11 des Erlasses des US-Justizministers.

([377]) Abschnitt 3(d)(i)(C) EO 14086 und Abschnitt 201.8(e) des Erlasses des US-Justizministers. Der Spezialanwalt handelt nicht als Vertreter des Beschwerdeführers und steht in keinem Mandatsverhältnis zu ihm.

([378]) Siehe Abschnitt 201.8(d)(e) des Erlasses des US-Justizministers. Solche Fragen werden zunächst vom OPCL in Absprache mit der zuständigen Stelle der Intelligence Community geprüft, um der Geheimhaltung unterliegende, privilegierte oder geschützte Informationen zu identifizieren und auszuschließen, bevor sie an den Beschwerdeführer weitergeleitet werden. Zusätzliche Informationen, die der Spezialanwalt in Beantwortung solcher Anfragen erhält, werden in die Anträge des Spezialanwalts an das DPRC aufgenommen.

([379]) Abschnitt 3(d)(i)(D) EO 14086.

([380]) Abschnitt 3(d)(iii) EO 14086 und Abschnitt 201.9(b) des Erlasses des US-Justizministers.

([381]) Abschnitt 3(d)(i)(E) EO 14086 und Abschnitt 201.9(c)-(e) des Erlasses des US-Justizministers. Nach der Definition des Begriffs „angemessene Abhilfemaßnahmen" in Abschnitt 4(a) EO 14086 muss das Datenschutzüberprüfungsgericht bei der Entscheidung über eine Abhilfemaßnahme zur vollständigen Behebung eines Verstoßes unter anderem berücksichtigen, „auf welche Weise ein Verstoß dieser Art üblicherweise behoben wurde", d. h das Datenschutzüberprüfungsgericht wird unter anderem prüfen, wie ähnliche Compliance-Probleme in der Vergangenheit behoben wurden, um sicherzustellen, dass die Abhilfe wirksam und angemessen ist.

(191) In allen Fällen trifft das DPRC eine schriftliche Entscheidung mit der Mehrheit der Stimmen. Wird bei der Überprüfung ein Verstoß gegen die geltenden Vorschriften festgestellt, werden in der Entscheidung angemessene Abhilfemaßnahmen festgelegt, z. B. die Löschung unrechtmäßig erhobener Daten, die Löschung der Ergebnisse unrechtmäßig durchgeführter Abfragen, die Einschränkung des Zugriffs auf rechtmäßig erhobene Daten auf entsprechend geschulte Mitarbeiter oder die Rücknahme von Aufklärungsberichten, die unrechtmäßig erhobene oder unrechtmäßig verbreitete Daten enthalten. ([382]) Die Entscheidung des DPRC ist in Bezug auf die ihm vorliegende Beschwerde bindend und endgültig. ([383]) Wird bei der Überprüfung ein Verstoß gegen eine Behörde festgestellt, die der Aufsicht des FISC unterliegt, muss das DPRC auch einen der Geheimhaltung unterliegenden Bericht an den stellvertretenden Justizminister für nationale Sicherheit übermitteln, der seinerseits verpflichtet ist, den Verstoß an das FISC zu melden, das weitere Durchsetzungsmaßnahmen ergreifen kann (nach dem in den Erwägungsgründen 173 und 174 beschriebenen Verfahren). ([384])

(192) Jede Entscheidung eines DPRC-Panels wird dem ODNI CLPO übermittelt. ([385]) In Fällen, in denen die Überprüfung durch das DPRC durch einen Antrag des Beschwerdeführers ausgelöst wurde, wird der Beschwerdeführer über die nationale Behörde benachrichtigt, dass das DPRC seine Überprüfung abgeschlossen hat und dass „bei der Überprüfung entweder keine einschlägigen Verstöße festgestellt wurden oder das DPRC eine Feststellung getroffen hat, die angemessene Abhilfemaßnahmen erfordert". ([386]) Das Office of Privacy and Civil Liberties des Justizministeriums führt ein Verzeichnis aller vom DPRC geprüften Informationen und Entscheidungen, das künftigen DPRC-Panels als unverbindlicher Präzedenzfall zur Verfügung gestellt wird. ([387])

(193) Das Justizministerium führt außerdem ein Verzeichnis aller Beschwerdeführer, die eine Beschwerde eingereicht haben. ([388]) Um die Transparenz zu erhöhen, muss das Justizministerium mindestens alle fünf Jahre mit den zuständigen Nachrichtendiensten Kontakt aufnehmen, um sich zu vergewissern, dass die von dem DPRC überprüften Informationen freigegeben wurden. ([389]) Ist dies der Fall, so ist die betroffene Person darauf hinzuweisen, dass diese Informationen nach geltendem Recht zugänglich sein können (d. h. dass sie nach dem Freedom of Information Act Zugang zu diesen Informationen beantragen kann, siehe Erwägungsgrund 199).

(194) Schließlich wird das ordnungsgemäße Funktionieren dieses Rechtsbehelfsmechanismus regelmäßig und unabhängig evaluiert. Insbesondere wird das Funktionieren des Rechtsbehelfsmechanismus nach der EO 14086 jährlich von dem PCLOB, einer unabhängigen Stelle, überprüft (siehe Erwägungsgrund 110). ([390]) Im Rahmen dieser Überprüfung wird das PCLOB unter anderem beurteilen, ob der ODNI CLPO und das DPRC Beschwerden fristgerecht bearbeitet haben, ob sie vollständigen Zugang zu den erforderlichen Informationen hatten, ob die grundlegenden Garantien der EO 14086 im Überprüfungsprozess angemessen berücksichtigt wurden und ob die Intelligence Community den Feststellungen des ODNI CLPO und des DPRC in vollem Umfang nachgekommen ist. Das PCLOB wird dem Präsidenten, dem Justizminister, dem Direktor des Nationalen Nachrichtendienstes, den Leitern der Nachrichtendienste, dem ODNI CLPO und den Nachrichtendienstausschüssen des Kongresses einen Bericht über die Ergebnisse seiner Überprüfung vorlegen, der auch in einer nicht vertraulichen Fassung veröffentlicht wird und der wiederum in die regelmäßige Überprüfung der Funktionsweise dieses Beschlusses durch die Kommission einfließen wird. Der Justizminister, der Direktor des Nationalen Nachrichtendienstes, der ODNI CLPO und die Leiter der Nachrichtendienste sind verpflichtet, alle in diesen Berichten enthaltenen Empfehlungen umzusetzen oder anderweitig zu berücksichtigen. Darüber hinaus wird das PCLOB jährlich öffentlich bescheinigen, dass Beschwerden im Rahmen des Rechtsbehelfsmechanismus nach den Anforderungen der EO 14086 behandelt werden.

([382]) Abschnitt 4(a) EO 14086.

([383]) Abschnitt 3(d)(ii) EO 14086 und Abschnitt 201.9(g) des Erlasses des US-Justizministers. Da die Entscheidung des Datenschutzüberprüfungsgerichts endgültig und bindend ist, kann kein anderes Organ/keine andere Stelle der Exekutive oder Verwaltung (einschließlich des Präsidenten der Vereinigten Staaten) die Entscheidung des Datenschutzüberprüfungsgerichts aufheben. Dies wurde auch in der Rechtsprechung des Obersten Gerichtshofs bestätigt. Dieser stellte klar, dass der Justizminister dadurch, dass er seine in der Exekutive einzigartige Befugnis, bindende Entscheidungen zu erlassen, an eine unabhängige Stelle überträgt, sich selbst die Möglichkeit nimmt, die Entscheidung dieser Stelle in irgendeiner Weise zu bestimmen (siehe United States ex rel. Accardi v. Shaughnessy, 347 U.S. 260 (1954).

([384]) Abschnitt 3(d)(i)(F) EO 14086 und Abschnitt 201.9(i) des Erlasses des US-Justizministers.

([385]) Abschnitt 201.9(h) des Erlasses des US-Justizministers.

([386]) Abschnitt 3(d)(i)(H) EO 14086 und Abschnitt 201.9(h) des Erlasses des US-Justizministers. Zur Art der Benachrichtigung siehe Abschnitt 201.9 (h)(3) des Erlasses des US-Justizministers.

([387]) Abschnitt 201.9(j) des Erlasses des US-Justizministers.

([388]) Abschnitt 3(d)(v)(A) EO 14086.

([389]) Abschnitt 3(d)(v) EO 14086.

([390]) Abschnitt 3(e) EO 14086. Siehe auch https://documents.pclob.gov/prod/Documents/EventsAndPress/4db0a50d-cc62-4197-af2e-2687b14ed9b9/Trans-Atlantic%20Data%20Privacy%20Framework%20EO%20press%20release%20(FINAL).pdf.

(195) Neben dem spezifischen Rechtsbehelfsmechanismus nach der EO 14086 stehen jeder Privatperson (unabhängig von der Nationalität oder dem Wohnort) auch Rechtsbehelfe vor den ordentlichen US-Gerichten zur Verfügung. ([391])

(196) Insbesondere bieten das FISA und ein damit zusammenhängendes Gesetz Privatpersonen die Möglichkeit, eine Zivilklage auf Schadensersatz gegen die Vereinigten Staaten anzustrengen, wenn Informationen, die sie betreffen, gesetzwidrig und vorsätzlich genutzt oder offengelegt wurden, ([392]) US-Regierungsbeamte, die in ihrer Eigenschaft als Privatpersonen handeln, auf Schadensersatz zu verklagen ([393]) 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 ([394]). Beabsichtigt die Regierung, Informationen, die sie durch nachrichtendienstliche Tätigkeit erlangt hat, in einem Strafverfahren gegen einen Verdächtigen zu verwenden, so ist sie aufgrund verfassungsrechtlicher und gesetzlicher Bestimmungen ([395]) verpflichtet, bestimmte Informationen offenzulegen, damit der Angeklagte die Rechtmäßigkeit der Beweiserhebung und -verwendung durch die Regierung anfechten kann.

(197) Darüber hinaus gibt es verschiedene Möglichkeiten, rechtliche Schritte gegen Regierungsbeamte wegen des unrechtmäßigen staatlichen Zugriffs auf personenbezogene Daten oder ihrer unrechtmäßigen Verwendung, auch zu angeblichen Zwecken der nationalen Sicherheit, einzuleiten (d. h. der Computer Fraud and Abuse Act ([396]), Der Electronic Communications Privacy Act ([397]) und der Right to Financial Privacy Act ([398])). All diese Klagen 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).

(198) Eine allgemeinere Möglichkeit des Rechtsschutzes bietet der Administrative Procedure Act ([399]), wonach „eine Person, die durch Handlungen einer Behörde einen Schaden oder Nachteil erleidet", berechtigt ist, eine gerichtliche Nachprüfung zu beantragen. ([400]) 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". ([401]) So entschied beispielsweise ein Bundesberufungsgericht im Jahr 2015 über eine APA-Klage, dass die Sammelerhebung von Telefonie-Metadaten durch die US-Regierung nach Abschnitt 501 FISA nicht zulässig war. ([402])

([391]) Der Zugang zu diesen Instrumenten ist nur möglich, wenn eine Klagebefugnis nachgewiesen wird. Dieses Kriterium, das für jede Person unabhängig von ihrer Staatsangehörigkeit gilt, ergibt sich aus dem Artikel III der US-Verfassung, wonach sich die richterliche Gewalt nur auf reale Fälle und Streitigkeiten erstreckt. Nach Auffassung des Obersten Gerichtshofs der Vereinigten Staaten setzt dies voraus, dass 1) der Einzelne einen „tatsächlichen Schaden" erlitten hat (d. h. eine Beeinträchtigung eines rechtlich geschützten Interesses, die konkret und spezifiziert ist und bereits eingetreten ist oder unmittelbar droht), 2) ein Kausalzusammenhang zwischen dem Schaden und dem vor Gericht angefochtenen Verhalten besteht und 3) es wahrscheinlich und nicht bloß spekulativ ist, dass eine positive Entscheidung des Gerichts den Schaden beseitigen wird (vgl. Lujan v. Defenders of Wildlife, 504 U.S. 555 (1992)).

([392]) 18 U.S.C. § 2712.

([393]) 50 U.S.C. § 1810.

([394]) 50 U.S.C. § 1806.

([395]) Siehe entsprechend Brady v. Maryland, 373 U.S. 83 (1963) und Jencks Act, 18 U.S.C. § 3500.

([396]) 18 U.S.C. § 1030.

([397]) 18 U.S.C. §§ 2701–2712.

([398]) 12 U.S.C. § 3417.

([399]) 5 U.S.C. § 702.

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

([401]) 5 U.S.C. § 706(2)(A).

([402]) *ACLU v. Clapper*, 785 F.3d 787 (2d Cir. 2015). Das in diesen Fällen angefochtene Programm zur Sammelerhebung von Telefonaten wurde 2015 durch den USA FREEDOM Act beendet.

(199) Zusätzlich zu den in den Erwägungsgründen 176 bis 198 genannten Rechtsbehelfen hat jede Person das Recht, im Rahmen des FOIA Einsicht in bestehende Unterlagen von Bundesbehörden zu verlangen, einschließlich solcher Unterlagen, die personenbezogene Daten der betreffenden Person enthalten. ([403]) Die Gewährung dieses Zugangs kann auch die Einleitung von Verfahren vor den ordentlichen Gerichten erleichtern, einschließlich des Nachweises der Klagebefugnis. Die Behörden können Informationen zurückhalten, die unter bestimmte aufgelistete Ausnahmen fallen, einschließlich des Zugriffs auf Informationen, die aus Gründen der nationalen Sicherheit der Geheimhaltung unterliegen, und Informationen über Ermittlungen der Strafverfolgungsbehörden ([404]), aber Beschwerdeführer, die mit der Antwort unzufrieden sind, haben die Möglichkeit, die Antwort anzufechten, indem sie eine administrative Überprüfung und anschließend eine gerichtliche Überprüfung (vor den Bundesgerichten) beantragen. ([405])

(200) Aufgrund der vorstehenden Ausführungen lässt sich Folgendes festhalten: Der Zugriff der US-Strafverfolgungsbehörden und nationaler Sicherheitsbehörden auf personenbezogene Daten, die in den Anwendungsbereich des vorliegenden Beschlusses fallen, wird durch einen Rechtsrahmen geregelt, mit dem die Bedingungen für den Zugriff festgelegt werden und sichergestellt wird, dass der Zugriff und die weitere Verwendung der Daten auf das beschränkt sind, was im Hinblick auf das verfolgte Ziel des öffentlichen Interesses notwendig und angemessen ist. Diese Garantien können von Personen in Anspruch genommen werden, die das Recht auf einen wirksamen Rechtsbehelf haben.

4. **SCHLUSSFOLGERUNG**

(201) Nach Auffassung der Kommission gewährleisten die Vereinigten Staaten – durch die vom US-Handelsministerium aufgestellten Grundsätze – ein Schutzniveau für personenbezogene Daten, die aus der Union an zertifizierte Organisationen in den Vereinigten Staaten im Rahmen des Datenschutzrahmens EU-USA übermittelt werden, das dem durch die Verordnung (EU) 2016/679 garantierten Schutzniveau im Wesentlichen gleichwertig ist.

(202) Darüber hinaus ist die Kommission der Auffassung, dass die wirksame Anwendung der Grundsätze durch die Transparenzverpflichtungen und die Verwaltung des Datenschutzrahmens durch das Handelsministerium gewährleistet ist. Des Weiteren ermöglichen es die Kontrollmechanismen und Rechtsbehelfe des US-Rechts insgesamt, Verstöße gegen die Datenschutzvorschriften in der Praxis festzustellen und zu ahnden, und bieten den betroffenen Personen Rechtsmittel, um Zugang zu den sie betreffenden personenbezogenen Daten zu erhalten und schließlich deren Berichtigung oder Löschung zu erwirken.

(203) Schließlich ist die Kommission auf der Grundlage der verfügbaren Informationen über die US-Rechtsordnung, einschließlich der Informationen in den Anhängen VI und VII, der Auffassung, dass Eingriffe der US-Behörden in die Grundrechte von Personen, deren personenbezogene Daten nach dem Datenschutzrahmen EU-USA aus der Union in die Vereinigten Staaten übermittelt werden, im öffentlichen Interesse, insbesondere für Zwecke der Strafverfolgung und der nationalen Sicherheit, auf das zur Erreichung des betreffenden legitimen Ziels unbedingt erforderliche Maß beschränkt sind und dass ein wirksamer Rechtsschutz gegen solche Eingriffe besteht. In Anbetracht der vorstehenden Feststellungen sollte daher beschlossen werden, dass die Vereinigten Staaten ein angemessenes Schutzniveau im Sinne von Artikel 45 der Verordnung (EU) 2016/679, ausgelegt im Lichte der Charta der Grundrechte der Europäischen Union, für personenbezogene Daten gewährleisten, die aus der Europäischen Union an Organisationen übermittelt werden, die nach dem Datenschutzrahmen EU-USA zertifiziert sind.

(204) Da die in der EO 14086 vorgesehenen Einschränkungen, Garantien und Rechtsbehelfe wesentliche Elemente des Rechtsrahmens der Vereinigten Staaten sind, auf den sich die Bewertung der Kommission stützt, basiert die Annahme dieses Beschlusses insbesondere darauf, dass alle Nachrichtendienste der Vereinigten Staaten aktualisierte Strategien und Verfahren zur Umsetzung der EO 14086 annehmen und dass die Union als zugelassene Organisation für die Zwecke des Rechtsbehelfsverfahrens benannt wird, was am 3. Juli 2023 (siehe Erwägungsgrund 126) bzw. 30. Juni 2023 (siehe Erwägungsgrund 176) geschehen ist.

([403]) 5 U.S.C. § 552. Ähnliche Rechtsvorschriften existieren auf der Ebene der einzelnen Bundesstaaten.

([404]) 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). Die Kriterien für und die Dauer der Geheimhaltung sind in der Executive Order 13526 festgelegt, die als allgemeine Regel vorsieht, dass für die Freigabe auf der Grundlage des Zeitraums, während dessen die Informationen für die nationale Sicherheit sensibel sind, ein bestimmter Zeitpunkt oder ein bestimmtes Ereignis festgelegt werden muss, zu dem die Informationen automatisch freigegeben werden müssen (siehe Abschnitt 1.5 der EO 13526).

([405]) Das Gericht bestimmt de novo, ob Dokumente rechtmäßig zurückgehalten werden, und kann die Regierung anweisen, Zugang zu den Dokumenten zu gewähren (5 U.S.C. § 552(a)(4)(B)).

5. AUSWIRKUNGEN DIESES BESCHLUSSES UND MAßNAHMEN DER DATENSCHUTZBEHÖRDEN

(205) Die Mitgliedstaaten und ihre Organe müssen die notwendigen Maßnahmen treffen, um Rechtsakten der Unionsorgane nachzukommen, da für diese Rechtsakte eine Vermutung der Rechtmäßigkeit gilt, 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.

(206) Daher ist ein nach Artikel 45 Absatz 3 der Verordnung (EU) 2016/679 erlassener Angemessenheitsbeschluss der Kommission für alle Organe der Mitgliedstaaten, an die er gerichtet ist, einschließlich ihrer unabhängigen Aufsichtsbehörden, verbindlich. So können insbesondere Übermittlungen von einem Verantwortlichen oder Auftragsverarbeiter in der Union an zertifizierte Organisationen in den Vereinigten Staaten ohne weitere Genehmigung vorgenommen werden.

(207) Es sei daran erinnert, dass nach Artikel 58 Absatz 5 der Verordnung (EU) 2016/679 und wie vom Gerichtshof im Urteil in der Rechtssache Schrems ([406]) erläutert Folgendes gilt: Wenn eine nationale Datenschutzbehörde, auch auf eine Beschwerde hin, die Vereinbarkeit eines Angemessenheitsbeschlusses der Kommission mit den Grundrechten des Einzelnen auf Privatsphäre und Datenschutz infrage stellt, muss das nationale Recht Rechtsbehelfe vorsehen, die es der Datenschutzbehörde ermöglichen, diese Rügen vor einem nationalen Gericht geltend zu machen, das gegebenenfalls ein Vorabentscheidungsverfahren beim Gerichtshof einleiten muss. ([407])

6. ÜBERWACHUNG UND ÜBERPRÜFUNG DIESES BESCHLUSSES

(208) Nach der Rechtsprechung des Gerichtshofs ([408]) und Artikel 45 Absatz 4 der Verordnung (EU) 2016/679 sollte die Kommission nach Erlass eines Angemessenheitsbeschlusses die relevanten Entwicklungen in dem Drittland fortlaufend überwachen, um festzustellen, ob ein Drittland weiterhin ein im Wesentlichen gleichwertiges Schutzniveau bietet. Eine solche Kontrolle ist auf jeden Fall erforderlich, wenn der Kommission Informationen vorliegen, die Anlass zu begründeten Zweifeln geben.

(209) Daher sollte die Kommission die Situation in den Vereinigten Staaten in Bezug auf den Rechtsrahmen und die tatsächliche Praxis bei der Verarbeitung personenbezogener Daten, wie in diesem Beschluss geprüft, fortlaufend überwachen. Um diesen Prozess zu erleichtern, sollten die US-Behörden die Kommission unverzüglich über wesentliche Entwicklungen in der US-Rechtsordnung unterrichten, die sich auf den Rechtsrahmen, der Gegenstand dieses Beschlusses ist, auswirken, sowie über jede Entwicklung der in diesem Beschluss bewerteten Verfahrensweisen im Zusammenhang mit der Verarbeitung personenbezogener Daten, sowohl was die Verarbeitung personenbezogener Daten durch zertifizierte Organisationen in den Vereinigten Staaten als auch die Einschränkungen und Garantien für den Zugang der Behörden zu personenbezogenen Daten anbelangt.

(210) Damit die Kommission ihre Überwachungsfunktion wirksam ausüben kann, sollten die Mitgliedstaaten die Kommission über alle relevanten Maßnahmen der nationalen Datenschutzbehörden informieren, insbesondere über Anfragen oder Beschwerden von betroffenen EU-Bürgern in Bezug auf die Übermittlung personenbezogener Daten aus der Europäischen Union an zertifizierte Organisationen in den Vereinigten Staaten. Ferner sollte die Kommission über jegliche Hinweise darauf informiert werden, dass die Maßnahmen der US-Behörden, die für die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder für die nationale Sicherheit zuständig sind, einschließlich der Aufsichtsbehörden, nicht das erforderliche Schutzniveau gewährleisten.

([406]) Schrems, Rn. 65.

([407]) Schrems, Rn: 65: „Insoweit ist es Sache des nationalen Gesetzgebers, Rechtsbehelfe vorzusehen, die es der betreffenden nationalen Kontrollstelle ermöglichen, die von ihr für begründet erachteten Rügen vor den nationalen Gerichten geltend zu machen, damit diese, wenn sie die Zweifel der Kontrollstelle an der Gültigkeit der Entscheidung der Kommission teilen, um eine Vorabentscheidung über deren Gültigkeit ersuchen."

([408]) Schrems, Rn. 76.

(211) nach Artikel 45 Absatz 3 der Verordnung (EU) 2016/679 ([409]) sollte die Kommission nach Erlass dieses Beschlusses regelmäßig überprüfen, ob die Feststellungen zur Angemessenheit des von den Vereinigten Staaten gewährleisteten Schutzniveaus im Rahmen des Datenschutzrahmens EU-USA noch sachlich und rechtlich gerechtfertigt sind. Da insbesondere die EO 14086 und der Erlass des US-Justizministers die Schaffung neuer Mechanismen und die Umsetzung neuer Garantien erfordern, sollte dieser Beschluss innerhalb eines Jahres nach seinem Inkrafttreten einer ersten Überprüfung unterzogen werden, um festzustellen, ob alle einschlägigen Elemente vollständig umgesetzt worden sind und in der Praxis wirksam funktionieren. Nach dieser ersten Überprüfung und in Abhängigkeit von deren Ergebnissen wird die Kommission in enger Abstimmung mit dem nach Artikel 93 Absatz 1 der Verordnung (EU) 2016/679 eingesetzten Ausschuss und dem Europäischen Datenschutzausschuss über die Häufigkeit künftiger Überprüfungen entscheiden. ([410])

(212) Zur Durchführung der Überprüfungen sollte die Kommission mit dem Handelsministerium, der FTC und dem Verkehrsministerium zusammentreffen, gegebenenfalls in Begleitung anderer Abteilungen und Stellen, die an der Umsetzung des Datenschutzrahmens EU-USA beteiligt sind, sowie – bei Fragen des staatlichen Zugriffs auf Daten – mit Vertretern des Justizministeriums, des ODNI (einschließlich des CLPO), anderer Nachrichtendienste, des Datenschutzüberprüfungsgerichts und mit Spezialanwälten. Die Teilnahme an diesem Treffen sollte Vertretern der Mitglieder des Europäischen Datenschutzausschusses offenstehen.

(213) Die Überprüfung sollte sich auf alle Aspekte der Funktionsweise dieses Beschlusses in Bezug auf die Verarbeitung personenbezogener Daten in den Vereinigten Staaten erstrecken, insbesondere auf die Anwendung der Grundsätze mit besonderem Augenmerk auf den Schutz im Falle der Weiterübertragung, die einschlägigen Entwicklungen in der Rechtsprechung, die Wirksamkeit der Ausübung der Rechte des Einzelnen, die Überwachung und Durchsetzung der Einhaltung der Grundsätze sowie die Einschränkungen und Garantien in Bezug auf den staatlichen Zugriff, vor allem die Umsetzung und Anwendung der mit der EO 14086 eingeführten Garantien, unter anderem durch Strategien und Verfahren, die von Nachrichtendiensten entwickelt werden, das Zusammenspiel zwischen der EO 14086 und Abschnitt 702 FISA und der EO 12333 sowie die Wirksamkeit von Aufsichtsmechanismen und Rechtsbehelfen (einschließlich des Funktionierens der neuen Beschwerdestelle, die im Rahmen der EO 14086 eingerichtet wurde). Im Rahmen dieser Überprüfungen wird auch der Zusammenarbeit zwischen den Datenschutzbehörden und den zuständigen Behörden der Vereinigten Staaten Aufmerksamkeit geschenkt werden, unter anderem der Erarbeitung von Leitlinien und anderen Auslegungshilfen zur Anwendung der Grundsätze sowie zu anderen Aspekten der Funktionsweise des Rahmens.

(214) Auf der Grundlage der Überprüfung sollte die Kommission einen öffentlichen Bericht erstellen, der dem Europäischen Parlament und dem Rat vorgelegt wird.

7. **AUSSETZUNG, AUFHEBUNG ODER ÄNDERUNG DIESES BESCHLUSSES**

(215) Lassen verfügbare Informationen – insbesondere Informationen, die sich aus der Überwachung dieses Beschlusses ergeben oder von den US-Behörden oder der Mitgliedstaaten zur Verfügung gestellt werden – darauf schließen, dass das Schutzniveau für die nach diesem Beschluss übermittelten Daten möglicherweise nicht mehr angemessen ist, sollte die Kommission die zuständigen US-Behörden umgehend davon in Kenntnis setzen und sie ersuchen, innerhalb einer bestimmten, angemessenen Frist geeignete Maßnahmen zu treffen.

(216) Falls die zuständigen US-Behörden nach Ablauf dieser Frist keine derartigen Maßnahmen getroffen haben oder nicht auf andere Weise glaubhaft gemacht haben, dass dieser Beschluss weiterhin auf einem angemessenen Schutzniveau beruht, wird die Kommission das Verfahren nach Artikel 93 Absatz 2 der Verordnung (EU) 2016/679 einleiten, um diesen Beschluss teilweise oder vollständig auszusetzen oder aufzuheben.

(217) Alternativ wird die Kommission dieses Verfahren einleiten, um den Beschluss zu ändern, indem sie insbesondere Datenübermittlungen zusätzlichen Bedingungen unterwirft oder den Anwendungsbereich der Angemessenheitsfeststellung auf Datenübermittlungen beschränkt, für die auch weiterhin ein angemessenes Schutzniveau gewährleistet ist.

([409]) Nach Artikel 45 Absatz 3 der Verordnung (EU) 2016/679 ist „[i]n dem Durchführungsrechtsakt … ein Mechanismus für eine regelmäßige Überprüfung, … vorzusehen, bei der allen maßgeblichen Entwicklungen in dem Drittland oder bei der internationalen Organisation Rechnung getragen wird."

([410]) Nach Artikel 45 Absatz 3 der Verordnung (EU) 2016/679 muss „mindestens alle vier Jahre eine regelmäßige Überprüfung stattfinden". Siehe auch Europäischer Datenschutzausschuss, Referenzgrundlage für Angemessenheit, WP 254 Rev. 01.

(218) Die Kommission soll das Verfahren zur Aussetzung oder Aufhebung des Beschlusses insbesondere einleiten, sofern

a) es Hinweise darauf gibt, dass Organisationen, die nach diesem Beschluss personenbezogene Daten von der Union erhalten haben, die Grundsätze nicht einhalten und dass die zuständigen Aufsichts- und Strafverfolgungsbehörden nicht wirksam gegen diese Nichteinhaltung vorgehen,

b) es Hinweise darauf gibt, dass die US-Behörden die geltenden Bedingungen und Einschränkungen für den Zugang von US-Behörden zu personenbezogenen Daten, die nach dem Datenschutzrahmen EU-USA für Zwecke der Strafverfolgung und der nationalen Sicherheit übermittelt werden, nicht einhalten oder

c) Beschwerden von betroffenen Personen in der Union nicht wirksam nachgegangen wird, auch nicht durch den ODNI CLPO und/oder das Datenschutzüberprüfungsgericht.

(219) Die Kommission sollte ferner die Einleitung des Verfahrens zur Änderung, Aussetzung oder Aufhebung dieses Beschlusses in Betracht ziehen, wenn die zuständigen US-Behörden nicht die Informationen oder Erläuterungen liefern, die für die Bewertung des Schutzniveaus für personenbezogene Daten, die aus der Union an die Vereinigten Staaten übermittelt werden, oder für die Einhaltung dieses Beschlusses erforderlich sind. In diesem Zusammenhang sollte die Kommission Überlegungen dazu anstellen, inwieweit die relevanten Informationen aus anderen Quellen bezogen werden können.

(220) In hinreichend begründeten Fällen äußerster Dringlichkeit, z. B. wenn die EO 14086 oder der Erlass des US-Justizministers in einer Weise geändert würden, die das in diesem Beschluss beschriebene Schutzniveau untergräbt, oder wenn die durch den Justizminister erfolgte Benennung der Union als zugelassene Organisation für die Zwecke des Rechtsbehelfsverfahrens widerrufen wird, wird die Kommission von der Möglichkeit Gebrauch machen, nach dem in Artikel 93 Absatz 3 der Verordnung (EU) 2016/679 genannten Verfahren sofort geltende Durchführungsrechtsakte zur Aussetzung, Aufhebung oder Änderung dieses Beschlusses zu erlassen.

8. **SCHLUSSBEMERKUNGEN**

(221) Der Europäische Datenschutzausschuss hat seine Stellungnahme ([411]) veröffentlicht, der bei der Ausarbeitung dieses Beschlusses Rechnung getragen wurde.

(222) Das Europäische Parlament nahm eine Entschließung zur Angemessenheit des Datenschutzrahmens EU-USA an. ([412])

(223) Die in diesem Beschluss vorgesehenen Maßnahmen entsprechen der Stellungnahme des nach Artikel 93 Absatz 1 der Verordnung (EU) 2016/679 eingesetzten Ausschusses —

HAT FOLGENDEN BESCHLUSS ERLASSEN:

Artikel 1

Für die Zwecke des Artikels 45 der Verordnung (EU) 2016/679 gewährleisten die Vereinigten Staaten ein angemessenes Schutzniveau für personenbezogene Daten, die aus der Union an Organisationen in den Vereinigten Staaten übermittelt werden, die in der vom U.S. Department of Commerce (Handelsministerium) geführten und öffentlich zugänglichen „Data Privacy Framework List“ (Datenschutzrahmen-Liste) nach Anhang I Abschnitt I.3 aufgeführt sind.

Artikel 2

Wenn die zuständigen Behörden in den Mitgliedstaaten zum Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten ihre Befugnisse nach Artikel 58 der Verordnung (EU) 2016/679 im Hinblick auf die Übermittlung von Daten in Sinne des Artikels 1 dieses Beschlusses ausüben, unterrichtet der betreffende Mitgliedstaat unverzüglich die Kommission.

([411]) Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework vom 28. Februar 2023.

([412]) Entschließung des Europäischen Parlaments vom 11. Mai 2023 zur Angemessenheit des vom Datenschutzrahmen zwischen der EU und den USA gebotenen Schutzes (2023/2501(RSP)).

Artikel 3

(1) Die Kommission überwacht fortlaufend die Anwendung des Rechtsrahmens, der Gegenstand dieses Beschlusses ist, einschließlich der Bedingungen, unter denen Weiterübermittlungen vorgenommen werden, individuelle Rechte ausgeübt werden und die US-Behörden Zugang zu Daten haben, die auf der Grundlage dieses Beschlusses übermittelt werden, um zu prüfen, ob die Vereinigten Staaten weiter ein angemessenes Schutzniveau im Sinne des Artikels 1 gewährleisten.

(2) Die Mitgliedstaaten und die Kommission unterrichten sich gegenseitig über Fälle, in denen es Anhaltspunkte dafür gibt, dass die Einrichtungen in den Vereinigten Staaten, die zur Durchsetzung der in Anhang I dargelegten Grundsätze gesetzlich befugt sind, nicht für wirksame Verfahren zur Aufdeckung und Kontrolle sorgen, mit denen Verstöße gegen die in Anhang I aufgeführten Grundsätze in der Praxis 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 Wahrung der nationalen 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 erforderliche und angemessene Maß hinausgehen und/oder dass kein wirksamer Rechtsschutz vor derartigen Eingriffen besteht.

(4) Ein Jahr nach dem Tag der Bekanntgabe dieses Beschlusses an die Mitgliedstaaten und danach mit einer Häufigkeit, die in enger Abstimmung mit dem nach Artikel 93 Absatz 1 der Verordnung (EU) 2016/679 eingesetzten Ausschuss und dem Europäischen Datenschutzausschuss festgelegt wird, evaluiert die Kommission die Feststellung in Artikel 1 Absatz 1 auf der Grundlage aller verfügbaren Informationen, einschließlich Informationen, die bei der gemeinsam mit den zuständigen Behörden der Vereinigten Staaten durchgeführten Überprüfung gewonnen wurden.

(5) Liegen der Kommission Hinweise darauf vor, dass ein angemessenes Schutzniveau nicht länger gewährleistet ist, so unterrichtet die Kommission die zuständigen US-Behörden. Erforderlichenfalls beschließt sie nach Artikel 45 Absatz 5 der Verordnung (EU) 2016/679, diesen Beschluss auszusetzen, zu ändern oder zu widerrufen oder seinen Anwendungsbereich einzuschränken. Die Kommission kann einen solchen Beschluss auch erlassen, wenn sie aufgrund mangelnder Kooperation der US-Regierung nicht feststellen kann, ob die Vereinigten Staaten weiterhin ein angemessenes Schutzniveau gewährleisten.

Artikel 4

Dieser Beschluss ist an die Mitgliedstaaten gerichtet.

Brüssel, den 10. Juli 2023

Für die Kommission
Didier REYNDERS
Mitglied der Kommission

ANHANG I

GRUNDSÄTZE DES DATENSCHUTZRAHMENS EU-USA, HERAUSGEGEBEN VOM US-HANDELSMINISTERIUM

I. ÜBERBLICK

1. Während die Vereinigten Staaten und die Europäische Union (EU) sich gemeinsam für die Verbesserung des Schutzes der Privatsphäre und der Rechtsstaatlichkeit einsetzen und die Bedeutung des transatlantischen Datenverkehrs für unsere jeweiligen Bürger, Volkswirtschaften und Gesellschaften anerkennen, verfolgen die Vereinigten Staaten in Bezug auf den Schutz der Privatsphäre einen anderen Ansatz als die EU. Die USA verfolgen einen sektoralen Ansatz, der auf einer Mischung von Rechtsvorschriften, Verordnungen und freiwilliger Selbstkontrolle basiert. Das US-Handelsministerium („Ministerium") gibt im Rahmen seiner gesetzlichen Befugnis, den internationalen Handel zu unterstützen, zu fördern und zu entwickeln (15 U.S.C. § 1512) die Grundsätze für den Datenschutzrahmen EU-USA heraus, einschließlich der Zusatzgrundsätze (im Folgenden zusammen „Grundsätze") und des Anhangs I der Grundsätze („Anhang I"). Die Grundsätze wurden in Absprache mit der Europäischen Kommission (im Folgenden „Kommission"), den Industrievertretern und anderen Interessenträgern entwickelt, um den Handel zwischen den Vereinigten Staaten und der EU zu erleichtern. Die Grundsätze sind ein Schlüsselelement des Datenschutzrahmens EU-USA (im Folgenden „Datenschutzrahmen EU-USA") und bieten Organisationen in den USA einen verlässlichen Mechanismus für die Übermittlung personenbezogener Daten aus der EU in die USA, während gleichzeitig sichergestellt wird, dass betroffene Personen in der EU weiterhin wirksame Garantien und einen wirksamen Schutz im Einklang mit dem EU-Recht in Bezug auf die Verarbeitung ihrer personenbezogenen Daten genießen, wenn diese Daten in Nicht-EU-Staaten übermittelt werden. Die Grundsätze sind ausschließlich für den Gebrauch durch Organisationen in den Vereinigten Staaten bestimmt, die personenbezogene Daten aus der Europäischen Union erhalten, um sich für den Datenschutzrahmen zu qualifizieren und so vom Angemessenheitsbeschluss der Europäischen Kommission zu profitieren. ([1]) Die Grundsätze berühren nicht die Anwendung der Verordnung (EU) 2016/679 (im Folgenden „Datenschutz-Grundverordnung" oder „DSGVO") ([2]), die für die Verarbeitung personenbezogener Daten in den EU-Mitgliedstaaten gilt. Ebenso wenig schränken die Prinzipien ansonsten nach US-Recht geltende Datenschutzverpflichtungen ein.

2. Um sich auf den Datenschutzrahmen EU-USA zur Übermittlung personenbezogener Daten aus der EU stützen zu können, muss eine Organisation gegenüber dem Ministerium (oder einer von ihm benannten Stelle) durch Selbstzertifizierung erklären, dass sie sich an die Grundsätze hält. Obwohl Entscheidungen von Organisationen, dem Datenschutzrahmen EU-USA beizutreten, vollkommen freiwillig sind, ist die wirksame Einhaltung der Grundsätze obligatorisch: Organisationen, die sich gegenüber dem Ministerium selbst zertifizieren und öffentlich erklären, dass sie die Grundsätze befolgen, müssen diese vollständig einhalten. Um dem Datenschutzrahmen EU-USA 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 ihre Bereitschaft erklären, die Grundsätze einzuhalten, c) ihre Datenschutzbestimmungen im Einklang mit diesen Grundsätzen offenlegen und d) diese vollständig umsetzen. ([3]) Ein Verstoß der Organisation gegen diese Grundsätze ist von der FTC gemäß Abschnitt 5 des Federal Trade Commission (FTC) Act zur Verhinderung unlauterer oder irreführender Praktiken, die im Handel erfolgen oder den Handel beeinträchtigen (15 U.S.C. § 45), vom Verkehrsministerium gemäß 49 U.S.C. § 41712 zur Verhinderung unlauterer oder irreführender Praktiken im Luftverkehr oder beim Verkauf von Luftverkehrsdienstleistungen durch Luftfahrtunternehmen oder Vermittler oder nach anderen Gesetzen oder Verordnungen, die solche Handlungen verbieten, verfolgbar.

([1]) Unter der Voraussetzung, dass der Beschluss der Kommission über die Angemessenheit des Datenschutzrahmens für Island, Liechtenstein und Norwegen gilt, wird der Datenschutzrahmen sowohl für die EU als auch für diese drei Länder gelten. Demzufolge sind bei Bezugnahmen auf die EU und ihre Mitgliedstaaten auch Island, Liechtenstein und Norwegen eingeschlossen. Demzufolge sind bei Bezugnahmen auf die EU und ihre Mitgliedstaaten auch Island, Liechtenstein und Norwegen eingeschlossen.

([2]) VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).

([3]) Die Grundsätze des EU-US-Datenschutzschilds wurden in die „Grundsätze des Datenschutzrahmens EU-USA" geändert. (*Siehe* Zusatzgrundsatz „Selbstzertifizierung").

3. Das Ministerium 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 „Datenschutzrahmen-Liste"). Die Vorteile des Datenschutzrahmens EU-USA sind ab dem Datum der Aufnahme der Organisation in die Datenschutzrahmen-Liste durch das Ministerium garantiert. Das Ministerium wird eine Organisation von der Datenschutzrahmen-Liste streichen, wenn sie freiwillig aus dem Datenschutzrahmen EU-USA ausscheidet oder wenn sie es versäumt, ihre jährlich fällige Zertifizierung gegenüber dem Ministerium zu erneuern. Die Organisation muss die Grundsätze für personenbezogene Daten, die sie während der Zeit ihrer Beteiligung am Datenschutzrahmen EU-USA erhalten hat, weiter einhalten, solange sie diese Daten speichert, und gegenüber dem Ministerium jährlich die Einhaltung zusichern und einen „angemessenen" Schutz für sie bieten (z. B. durch einen Vertrag, der die Anforderungen der von der Kommission angenommenen einschlägigen Standardvertragsklauseln vollständig widerspiegelt); ansonsten muss die Organisation die Daten zurückgeben oder löschen. Das Ministerium wird die Organisationen von der Datenschutzrahmen-Liste streichen, wenn sie wiederholt gegen die Grundsätze verstoßen haben. Diese Organisationen müssen personenbezogene Daten, die sie während der Zeit ihrer Beteiligung am Datenschutzrahmen EU-USA erhalten haben, zurückgeben oder löschen. Die Streichung einer Organisation von der Datenschutzrahmen-Liste bedeutet, dass sie nicht mehr in den Genuss des Angemessenheitsbeschlusses der Kommission zum Empfang personenbezogener Daten aus der EU kommen kann.

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 Datenschutzrahmen-Liste gestrichen wurden. Das Ministerium wird deutlich darauf hinweisen, dass diese Organisationen dem Datenschutzrahmen EU-USA nicht angehören; dass die Streichung von der Datenschutzrahmen-Liste bedeutet, dass diese Organisationen nicht geltend machen können, dass sie den Datenschutzrahmen EU-USA einhalten, und sie alle Aussagen oder irreführende Praktiken vermeiden müssen, die auf ihre Beteiligung am Datenschutzrahmen EU-USA hindeuten; und dass diese Organisationen nicht mehr die sich aus dem Angemessenheitsbeschluss der Europäischen Kommission ergebenden Vorteile in Anspruch nehmen können, die ihnen den Empfang personenbezogener Daten aus der EU ermöglichen. Gegen eine Organisation, die nach ihrer Streichung von der Datenschutzrahmen-Liste weiter eine Beteiligung am Datenschutzrahmen EU-USA vorgibt oder sonstige falsche Angaben zum Datenschutzrahmen EU-USA macht, können von der FTC, vom Verkehrsministerium oder anderen Behörden entsprechende Durchsetzungsmaßnahmen eingeleitet werden.

5. Die Geltung dieser Grundsätze kann begrenzt werden a) insoweit, als sie erforderlich ist, um einer richterlichen Anordnung nachzukommen oder Erfordernissen des öffentlichen Interesses, der Strafverfolgung oder der nationalen Sicherheit gerecht zu werden, einschließlich der Fälle, in denen Gesetze oder staatliche Vorschriften entgegenstehende Verpflichtungen begründen, b) durch Gesetzesrecht, Fallrecht oder staatliche Regulierungsvorschriften, aus denen sich 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 ebendieser Ermächtigung dies erfordert, oder c) wenn die DSGVO Ausnahmeregelungen vorsieht, sofern diese Ausnahmeregelungen unter vergleichbaren Voraussetzungen getroffen werden. In diesem Zusammenhang gehören zu den im US-Recht verankerten Garantien zum Schutz der Privatsphäre und der bürgerlichen Freiheiten auch diejenigen, die in der Executive Order 14086 ([4]) unter den darin festgelegten Bedingungen (einschließlich der Anforderungen an die Notwendigkeit und Verhältnismäßigkeit) vorgeschrieben sind. Im Hinblick auf das Ziel eines wirksameren Schutzes der Privatsphäre sollen die Organisationen die Grundsätze in vollem Umfang und in transparenter Weise anwenden, indem sie sich unter anderem darum bemühen, in ihren Datenschutzbestimmungen die Fälle anzugeben, in denen Abweichungen von den unter Buchstabe b genannten Grundsätzen zulässig sind. 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 Datenschutzrahmen EU-USA auf alle personenbezogenen Daten anzuwenden, die im Vertrauen auf den Datenschutzrahmen EU-USA übermittelt werden. Eine Organisation, die sich für eine Ausdehnung der Vorteile des Datenschutzrahmens EU-USA 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.

([4]) Executive Order of October 7, 2022, „Enhancing Safeguards for United States Signals Intelligence Activities."

7. Für Fragen der Auslegung und der Einhaltung der Grundsätze sowie der einschlägigen Datenschutzbestimmungen durch Organisationen, die dem Datenschutzrahmen EU-USA angehören, gilt das US-Recht, außer 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. Für die Zwecke dieses Beschlusses gelten folgende Begriffsbestimmungen:

   a) „personenbezogene Daten" bezeichnet in beliebiger Form aufgezeichnete Daten über eine identifizierte oder identifizierbare Person, die unter die DSGVO fallen und aus der EU 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) „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 und des Anhangs I der Grundsätze ist der Tag, an dem der Angemessenheitsbeschluss der Europäischen Kommission in Kraft getreten ist.

II. GRUNDSÄTZE

1. BEKANNTMACHUNG

a) Die Organisation muss Privatpersonen über Folgendes informieren:

   i) ihre Beteiligung am Datenschutzrahmen EU-USA, einschließlich eines Links zur Datenschutzrahmen-Liste oder Internetadresse der Liste,

   ii) die Arten der erfassten personenbezogenen Daten und gegebenenfalls die US-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 Datenschutzrahmens EU-USA 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 den 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, ([5])

   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.

([5]) *Siehe z. B.* Abschnitt c des Grundsatzes des Rechtsschutzes, der Durchsetzung und der Haftung.

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 (d. h. „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 (d. h. „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 Punkt iv, sinnvolle und geeignete Schritte unternehmen, um eine unbefugte Verarbeitung zu unterbinden und 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. ([6]) 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 ([7]), wie damit ein Verarbeitungszweck im Sinne von Artikel 5(a) erfüllt wird. Diese Verpflichtung hindert Organisationen nicht daran, personenbezogene 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 des Datenschutzrahmens EU-USA. Die Organisationen sollen zur Einhaltung dieser Bestimmung angemessene und geeignete Maßnahmen ergreifen.

6. **ZUGANG**

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.

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 die Betroffenen untersucht und zügig behandelt werden und nach denen Schadensersatz 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, und

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 Datenschutzrahmen EU-USA 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.

([6]) Je nach Sachlage kommt als zulässiger Zweck für die Verarbeitung beispielsweise Folgendes infrage: 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.

([7]) 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.

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 Datenschutzrahmen angehörende Organisation für die Verarbeitung der personenbezogenen Daten, die sie im Rahmen des Datenschutzrahmens EU-USA erhält und anschließend an einen Dritten weitergibt, der in ihrem Auftrag und auf ihre Anweisung tätig ist, verantwortlich. Die dem Datenschutzrahmen 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) Wenn eine Organisation Gegenstand einer richterlichen Anordnung wegen Nichteinhaltung oder einer Anordnung einer US-Behörde (z. B. der FTC oder des Verkehrsministeriums) ist, die in den Grundsätzen oder in einem künftigen Anhang zu den Grundsätzen aufgeführt ist und auf Nichteinhaltung beruht, muss die Organisation alle relevanten Abschnitte eines dem Gericht oder der US-Behörde vorgelegten Berichts über die Einhaltung der Grundsätze oder des Datenschutzrahmens EU-USA veröffentlichen, soweit dies mit den Vertraulichkeitsanforderungen vereinbar ist. Das Ministerium hat eine spezielle Kontaktstelle eingerichtet, an die sich Datenschutzbehörden bei Compliance-Problemen von dem Datenschutzrahmen angehörenden Organisationen wenden können. Die FTC und das Verkehrsministerium werden 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 (d. h. „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 oder

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, 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 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, Telekommunikationsunternehmen und andere Organisationen sind nicht nach den Grundsätzen haftbar, wenn sie im Namen einer anderen Organisation Daten lediglich übermitteln, weiterleiten oder zwischenspeichern. Der Datenschutzrahmen EU-USA begründet 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 Datenschutzrahmen angehörender 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 Datenschutzrahmen 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 wie nachfolgend dargelegt umsetzen. Im Rahmen des Datenschutzrahmens EU-USA müssen sich in den USA ansässige Organisationen, die personenbezogene Daten aus der EU erhalten, verpflichten, wirksame Mechanismen einzusetzen, um die Einhaltung der Grundsätze zu gewährleisten. 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 Datenschutzrahmen-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 erhoben werden, und

iii) dass sie sich an die Empfehlung der entsprechenden Datenschutzbehörden hält, wenn diese der Organisation aufgeben, spezifische Maßnahmen zu treffen, um den Grundsätzen des Datenschutzrahmens 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, sodass u. a. ein einheitlicher schlüssiger Ansatz gewährleistet wird.

2. Das Gremium berät die betreffenden US-amerikanischen Organisationen bei ungeklärten Beschwerden von Privatpersonen über den Umgang mit personenbezogenen Daten, die aus der EU im Rahmen des Datenschutzrahmens EU-USA übermittelt wurden. Diese Beratung soll gewährleisten, dass die Grundsätze korrekt angewendet werden; sie schließt die Rechtsmittel für die betroffene(n) Privatperson(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 Privatpersonen gegen Organisationen, die sich auf die Grundsätze des Datenschutzrahmens EU-USA und zur Zusammenarbeit mit den Datenschutzbehörden verpflichtet haben; dabei ermutigt es die betroffenen Privatpersonen 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 FTC, 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 Ministerium, sodass die Datenschutzrahmen-Liste entsprechend geändert werden kann. Jede Unterlassung der Zusammenarbeit und jeder Verstoß gegen die Grundsätze des Datenschutzrahmens können als irreführende Praktiken gemäß Abschnitt 5 des FTC Act (15 U.S.C. § 45), 49 U.S.C. § 41712 oder den anderen vergleichbaren Gesetzen rechtlich verfolgt werden.

d) Wünscht eine Organisation, dass ihr die Vorteile des Datenschutzrahmens auch bei Personaldaten zuteilwerden, die zur Verwendung im Rahmen von Beschäftigungsverhältnissen aus der EU übermittelt werden, muss sie 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 Höhe der Gebühr wird vom Ministerium nach Anhörung der Kommission festgelegt. Die Einziehung der Gebühr kann durch einen vom Ministerium ausgewählten Dritten erfolgen, der als Verwahrer der zu diesem Zweck eingezogenen Mittel fungiert. Das Ministerium wird eng mit der Kommission und den Datenschutzbehörden zusammenarbeiten, um geeignete Verfahren für die Verteilung der durch die Gebühr eingenommenen Mittel sowie andere verfahrenstechnische und administrative Aspekte des Gremiums festzulegen. Das Ministerium und die Kommission können vereinbaren, die Häufigkeit der Erhebung der Gebühr zu ändern.

6. **Selbstzertifizierung**

a) In den Genuss der Vorteile des Datenschutzrahmens EU-USA kommt eine Organisation ab dem Datum der Aufnahme der Organisation in die Datenschutzrahmens-Liste durch das Ministerium. Das Ministerium wird eine Organisation erst dann auf die Datenschutzrahmen-Liste setzen, wenn es festgestellt hat, dass die erste Selbstzertifizierung der Organisation vollständig ist, und es wird die Organisation von dieser Liste streichen, wenn sie freiwillig ausscheidet, es versäumt, ihre jährlich fällige Zertifizierung zu erneuern oder die Grundsätze dauerhaft nicht einhält (siehe Zusatzgrundsatz „Beschwerdeverfahren und Durchsetzung")

b) Um sich erstmals für den Datenschutzrahmen EU-USA zu zertifizieren oder später erneut zu zertifizieren, muss eine Organisation jedes Mal einen Antrag an das Ministerium stellen, der von einem leitenden Mitarbeiter im Namen der Organisation, die ihre Einhaltung der Grundsätze selbst zertifiziert oder erneut zertifiziert (je nach Fall) ([8]), eingereicht wird und mindestens die folgenden Informationen enthält:

([8]) Der Antrag muss über die Website des Ministeriums zum Datenschutzrahmen von einer Person innerhalb der Organisation gestellt werden, die befugt ist, Erklärungen zur Einhaltung der Grundsätze im Namen der Organisation und aller zugehörigen Einheiten abzugeben.

i) den Namen der US-Organisation, die die Selbstzertifizierung oder die erneute Zertifizierung beantragt, sowie die Namen aller ihrer US-Einrichtungen oder US-Tochterunternehmen, die ebenfalls die Grundsätze einhalten, die die Organisation abdecken möchte,

ii) eine Beschreibung der Tätigkeit der Organisation im Zusammenhang mit personenbezogenen Daten aus der EU, die im Rahmen des Datenschutzrahmens EU-USA erhoben würden,

iii) eine Beschreibung der einschlägigen Datenschutzbestimmung(en) der Organisation die folgenden Angaben umfassen muss:

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

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

iv) die Kontaktstelle, die innerhalb der Organisation für die Bearbeitung von Beschwerden, Auskunftsersuchen und anderen Angelegenheiten der Grundsätze zuständig ist ([9]), darunter:

1. Name(n), Berufsbezeichnung(en) (falls zutreffend), E-Mail-Adresse(n) und Telefonnummer(n) der zuständigen Person(en) oder der zuständigen Kontaktstelle(n) innerhalb der Organisation und

2. die betreffende Postanschrift der Organisation in den USA,

v) 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),

vi) die Bezeichnungen aller Datenschutzprogramme, an denen die Organisation teilnimmt,

vii) die Überprüfungsmethode (d. h. Selbsteinschätzung oder externe Prüfungen der Einhaltung der Vorschriften, einschließlich des Dritten, der diese Prüfungen durchführt) ([10]) und

viii) den/die einschlägigen unabhängigen Mechanismus/Mechanismen, der/die für die Prüfung nicht erledigter Beschwerden im Zusammenhang mit den Grundsätzen zur Verfügung steht/stehen. ([11])

c) Wenn die Organisation wünscht, dass ihr die Vorteile des Datenschutzrahmens EU-USA 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 ersten Selbstzertifizierungsantrag sowie in allen Anträgen auf erneute Zertifizierung hinweisen und sich bereit erklären, gemäß den Zusatzgrundsätzen „Personaldaten“ und „Rolle der Datenschutzbehörden“, soweit anwendbar, mit den Datenschutzbehörden 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.

([9]) Die primäre „Kontaktstelle in der Organisation“ oder der „leitende Mitarbeiter in der Organisation“ darf nicht extern sein (z. B. ein externer Rechtsberater oder ein externer Berater).

([10]) *Siehe* Zusatzgrundsatz „Anlassunabhängige Kontrolle“.

([11]) *Siehe* Zusatzgrundsatz „Beschwerdeverfahren und Durchsetzung“.

d) Das Ministerium führt die Datenschutzrahmen-Liste der Organisationen, die erste Selbstzertifizierungsanträge eingereicht haben, und macht sie öffentlich zugänglich. Diese Liste wird auf der Grundlage der eingereichten Anträge auf die jährlichen erneuten Zertifizierungen sowie der Meldungen aktualisiert, die gemäß dem Zusatzgrundsatz „Beschwerdeverfahren und Durchsetzung" eingehen. Diese Selbstzertifizierungsanträge sind mindestens jährlich neu vorzulegen, andernfalls wird die Organisation von der Datenschutzrahmen-Liste gestrichen, und die Vorteile des Datenschutzrahmens EU-USA sind nicht mehr garantiert. Alle Organisationen, die vom Ministerium auf die Datenschutzrahmen-Liste aufgenommen werden, müssen über einschlägige Datenschutzbestimmungen verfügen, die mit dem Grundsatz der Informationspflicht übereinstimmen, und in diesen Datenschutzbestimmungen angeben, dass sie sich an die Grundsätze halten. ([12]) Wenn die Datenschutzbestimmungen einer Organisation online verfügbar sind, müssen sie mit einem Hyperlink zur Datenschutzrahmen-Website des Ministeriums sowie mit einem Hyperlink zur Website oder dem Beschwerdeformular der unabhängigen Beschwerdestelle versehen sein, der zur Verfügung steht, um ungelöste, mit den Grundsätzen zusammenhängende Beschwerden kostenlos für den Einzelnen zu untersuchen.

e) Die Grundsätze gelten unmittelbar vom Zeitpunkt der Selbstzertifizierung an. Dem Datenschutzrahmen angehörende Organisationen, die sich zuvor selbst nach den Grundsätzen des EU-US-Datenschutzschilds zertifiziert haben, müssen ihre Datenschutzbestimmungen aktualisieren und sich stattdessen auf die „Grundsätze des Datenschutzrahmens EU-USA" beziehen. Diese Organisationen nehmen diesen Hinweis so bald wie möglich auf, spätestens jedoch drei Monate nach Inkrafttreten der Grundsätze des Datenschutzrahmens EU-USA.

f) Eine Organisation muss alle personenbezogenen Daten, die sie aus der EU auf der Grundlage des Datenschutzrahmens EU-USA erhält, den Grundsätzen unterwerfen. Die Verpflichtung auf die Grundsätze gilt ohne zeitliche Begrenzung für personenbezogene Daten, die der Organisation übermittelt wurden, während sie in den Genuss der Vorteile des Datenschutzrahmens EU-USA 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 aus dem Datenschutzrahmen EU-USA ausscheidet. Eine Organisation, die aus dem Datenschutzrahmen EU-USA ausscheiden möchte, muss dies dem Ministerium im Voraus mitteilen. In dieser Mitteilung muss auch angegeben werden, was die Organisation mit den personenbezogenen Daten, die sie unter Berufung auf den Datenschutzrahmen EU-USA erhalten hat, zu tun gedenkt (d. h. ob sie die Daten aufbewahren, zurückgeben oder löschen wird und, falls sie die Daten aufbewahren wird, die zulässigen Mittel, mit denen sie den Schutz der Daten gewährleisten wird). Eine Organisation, die aus dem Datenschutzrahmen EU-USA ausscheidet, diese Daten aber behalten möchte, muss sich entweder dem Handelsministerium gegenüber jährlich dazu verpflichten, die Grundsätze auf die Daten 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 Kommission gebilligten einschlägigen Standardklauseln vollauf genügt); andernfalls muss die Organisation die Daten zurückgeben oder löschen. ([13]) Eine Organisation, die aus dem Datenschutzrahmen EU-USA ausscheidet, muss aus den relevanten Datenschutzbestimmungen jede Bezugnahme auf den Datenschutzrahmen EU-USA entfernen, die darauf hindeutet, dass sich die Organisationen weiterhin aktiv am Datenschutzrahmen EU-USA beteiligt und Anspruch auf die damit verbundenen Vorteile hat.

([12]) Eine Organisation, die sich zum ersten Mal selbst zertifiziert, darf in ihrer endgültigen Datenschutzerklärung erst dann auf ihre Beteiligung am Datenschutzrahmen EU-USA hinweisen, wenn das Ministerium der Organisation mitgeteilt hat, dass sie dazu berechtigt ist. Die Organisation muss dem Ministerium bei der ersten Selbstzertifizierung einen Entwurf ihrer Datenschutzerklärung vorlegen, der den Grundsätzen entspricht. Sobald das Ministerium festgestellt hat, dass die Einreichung des ersten Selbstzertifizierungsantrags der Organisation ansonsten vollständig ist, wird das Ministerium die Organisation benachrichtigen, dass sie ihre mit dem Datenschutzrahmen EU-USA konforme Datenschutzerklärung fertigstellen (z. B. gegebenenfalls veröffentlichen) sollte. Die Organisation muss das Ministerium unverzüglich benachrichtigen, sobald die entsprechende Datenschutzerklärung fertiggestellt ist. Zu diesem Zeitpunkt wird das Ministerium die Organisation auf die Datenschutzrahmen-Liste aufnehmen.

([13]) Wenn sich eine Organisation zum Zeitpunkt des Ausscheidens dafür entscheidet, personenbezogene Daten, die sie im Vertrauen auf den Datenschutzrahmen EU-USA erhalten hat, aufzubewahren und dem Ministerium jährlich zu versichern, dass sie die Grundsätze weiterhin auf diese Daten anwendet, muss die Organisation dem Ministerium nach dem Ausscheiden jährlich mitteilen (d. h. so lange, bis die Organisation einen „angemessenen" Schutz dieser Daten auf andere zulässige Weise gewährleistet oder alle diese Daten zurückgibt oder löscht und das Ministerium davon in Kenntnis setzt), was sie mit diesen personenbezogenen Daten getan hat, was sie mit allen personenbezogenen Daten zu tun gedenkt, die sie weiterhin aufbewahren wird, und wer als ständiger Ansprechpartner für Fragen zu den Grundsätzen dienen wird.

g) Eine Organisation, die aufgrund einer Änderung des Unternehmensstatus (z. B. durch Fusion, Übernahme, Konkurs oder Auflösung) ihren Status als selbstständige rechtliche Einheit verliert, muss dies dem Ministerium vorher mitteilen. In der Mitteilung sollte auch angegeben werden, ob der aus der Änderung des Unternehmensstatus hervorgehende Rechtsträger i) weiterhin am Datenschutzrahmen EU-USA durch eine bestehende Selbstzertifizierung beteiligt sein wird, ii) sich als neuer Beteiligter am Datenschutzrahmen EU-USA selbst zertifizieren wird (z. B. wenn der neue oder weiterbestehende Rechtsträger nicht bereits über eine bestehende Selbstzertifizierung verfügt, mit der er am Datenschutzrahmen EU-USA teilnehmen könnte), oder iii) andere Garantien einführen wird, z. B. eine schriftliche Vereinbarung, um sicherzustellen, dass die Grundsätze weiterhin auf alle personenbezogenen Daten angewendet werden, die die Organisation im Rahmen des Datenschutzrahmens EU-USA erhalten hat und aufbewahren wird. Ist weder i) noch ii) noch iii) der Fall, müssen personenbezogene Daten, die im Rahmen des Datenschutzrahmens erhoben wurden, unverzüglich zurückgegeben oder gelöscht werden.

h) Wenn eine Organisation aus welchem Grund auch immer den Datenschutzrahmen EU-USA verlässt, muss sie alle Erklärungen entfernen, die darauf hindeuten, dass sie sich weiter am Datenschutzrahmen EU-USA beteiligt oder Ansprüche auf die damit verbundenen Vorteile hat. Wurde das Gütesiegel des Datenschutzrahmens EU-USA verwendet, ist auch dies zu entfernen. Bei falschen Angaben über die Einhaltung der Grundsätze, die die Organisation gegenüber der Öffentlichkeit macht, können die FTC, das Verkehrsministerium 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 Datenschutzrahmens EU-USA tatsächlich besteht und dass ihre Datenschutzpolitik tatsächlich umgesetzt worden ist und den Grundsätzen 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) Bei einer Selbstzertifizierung ist nachzuweisen, dass die Bestimmungen der Organisation für den Schutz personenbezogener Daten aus der EU korrekt, umfassend und leicht zugänglich sind, den Grundsätzen entsprechen und vollständig umgesetzt werden (d. h. dass diese Regeln eingehalten werden). Die Organisation muss ferner feststellen, dass betroffene Personen über interne Beschwerdeverfahren und Beschwerdeverfahren bei unabhängigen Schiedsstellen informiert werden, dass sie ihre Arbeitnehmer 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 Privatpersonen, im Rahmen einer Untersuchung oder bei einer Beschwerde wegen Nichteinhaltung von Datenschutzvorschriften.

d) Bei einer externen anlassunabhängigen Kontrolle ist nachzuweisen, dass die Bestimmungen der Organisation für den Schutz personenbezogener Daten aus der EU korrekt, umfassend und leicht zugänglich sind, den Grundsätzen entsprechen und vollständig umgesetzt werden (d. h. dass diese Regeln eingehalten werden). Ferner ist anzugeben, dass Privatpersonen 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 Privatpersonen, im Rahmen einer Untersuchung oder bei einer Beschwerde wegen Nichteinhaltung von Datenschutzvorschriften.

e) Organisationen müssen ihre Unterlagen zur Umsetzung ihrer nach den Grundsätzen des Datenschutzrahmens EU-USA konzipierten Datenschutzbestimmungen dokumentieren und im Fall einer Untersuchung oder einer Beschwerde wegen Verletzung der Datenschutzvorschriften ihre Unterlagen der unabhängigen Beschwerdestelle übergeben, die für die Prüfung von Beschwerden zuständig ist, oder der gesetzlichen Aufsichtsbehörde, die bei unlauteren und irreführenden Geschäftspraktiken 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 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 personenbezogenen Daten der betroffenen Person verarbeitet oder nicht ([14]),

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

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.

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 Geschäftsinformationen

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.

([14]) 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) Können vertrauliche Geschäftsdaten leicht von den personenbezogenen 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 im Rahmen der Datenschutz-Grundverordnung 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 Kontaktstelle 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

i) 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

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

i) Frist für die Auskunftserteilung

i) 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 Datenschutzrahmen EU-USA

i) Übermittelt eine in der EU ansässige Organisation im Rahmen des Beschäftigungsverhältnisses erhobene personenbezogene Daten über ihre (früheren oder derzeitigen) Arbeitnehmer an eine Mutterorganisation, eine verbundene Organisation oder eine nicht verbundene Dienstleistungsorganisation in den USA, die dem Datenschutzrahmen EU-USA angehört, so fällt diese Übermittlung in den Anwendungsbereich der Grundsätze des Datenschutzrahmens EU-USA. 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 gelten nur für die Übermittlung von und den Zugriff auf Daten über identifizierte oder identifizierbare Privatpersonen. 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 Datenschutzrahmens EU-USA 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 personenbezogenen Daten erhoben wurden oder denen der Betroffene nachträglich zugestimmt hat. Macht ein Arbeitnehmer 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

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

d) Durchsetzung

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 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 dem Datenschutzrahmen EU-USA angehörende US-Organisation, die Personaldaten, die im Rahmen eines Beschäftigungsverhältnisses aus der EU übermittelt wurden, verwendet und wünscht, dass auf solche Übermittlungen die Grundsätze des Datenschutzrahmens EU-USA 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

i) Bei gelegentlichen beschäftigungsbezogenen operativen Erfordernissen der dem Datenschutzrahmen angehörenden Organisation im Hinblick auf im Rahmen des Datenschutzrahmens EU-USA 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 Datenschutzrahmen 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 Datenschutzrahmen EU-USA beigetreten ist oder nicht.

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

1. nur auf Weisung des 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 und

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 Datenschutzrahmen angehörenden Organisationen einen angemessenen Schutz gewähren, ist bei reinen Verarbeitungsverträgen mit diesen Organisationen keine vorherige Genehmigung erforderlich.

b) Datenübermittlung innerhalb einer kontrollierten Gruppe von Unternehmen

i) Werden personenbezogene 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 Datenschutzrahmen EU-USA angehörende Organisation für die Einhaltung der Grundsätze verantwortlich.

c) Datenübermittlung zwischen den Verantwortlichen

i) Bei der Übermittlung von Daten zwischen Verantwortlichen muss der Empfänger keine dem Datenschutzrahmen angehörende Organisation sein oder über eine unabhängige Beschwerdestelle verfügen. Die dem Datenschutzrahmen angehörende Organisation muss einen Vertrag mit dem empfangenden externen für die Verarbeitung Verantwortlichen schließen, der das gleiche Schutzniveau wie im Rahmen des Datenschutzrahmens EU-USA vorsieht, wobei es nicht erforderlich ist, dass der als Verantwortlicher tätige Dritte eine dem Datenschutzrahmen 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 Datenschutzrahmen EU-USA 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 diese Forderungen des Durchsetzungsgrundsatzes, indem sie i) von der Privatwirtschaft entwickelte Datenschutzprogramme befolgen, in deren Regeln die Grundsätze integriert sind und die wirksame Durchsetzungsmechanismen vorsehen, wie sie im Grundsatz des Rechtsschutzes, der Durchsetzung und der Haftung beschrieben sind, ii) sich gesetzlich oder durch Rechtsverordnung vorgesehenen Kontrollorganen unterwerfen, die Beschwerden von Privatpersonen nachgehen und Streitigkeiten schlichten, iii) 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 Abschnitt 5 FTC Act (15 U.S.C. § 45) zur Verhinderung unlauterer oder irreführender Praktiken, gemäß 49 U.S.C. § 41712 zur Verhinderung unlauterer oder irreführender Praktiken im Luftverkehr oder beim Verkauf von Luftverkehrsdienstleistungen durch Luftfahrtunternehmen oder Vermittler, oder nach anderen Gesetzen oder Verordnungen, die solche Handlungen verbieten, verfolgbar sein müssen.

c) Um die Einhaltung ihrer Verpflichtungen im Rahmen des Datenschutzrahmens zu gewährleisten und die Verwaltung des Programms zu unterstützen, müssen Organisationen sowie deren unabhängige Beschwerdestellen dem Ministerium auf Anfrage Informationen zum Datenschutzrahmen 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 Privatpersonen sollen dazu angehalten werden, Beschwerden zunächst an die Organisation zu richten, die ihre Daten verarbeitet, ehe sie eine unabhängige Beschwerdestelle anrufen. Organisationen müssen der Privatperson 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 unabhängige Beschwerdestelle muss jede von einer Privatperson vorgetragene Beschwerde prüfen, es sei denn, sie ist offensichtlich unbegründet oder nicht ernsthaft. Der Betreiber der unabhängigen 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. 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 und zu den von ihnen im Rahmen des Datenschutzrahmens EU-USA erbrachten Dienstleistungen veröffentlichen. Diese Informationen müssen Folgendes umfassen: 1) Angaben über die Anforderungen an unabhängige Beschwerdestellen in den Grundsätzen oder einen Link zu diesen Anforderungen, 2) einen Link zur Datenschutzrahmen-Website des Ministeriums, 3) einen Hinweis, dass das Beschwerdeverfahren im Rahmen des Datenschutzrahmens EU-USA für Privatpersonen kostenlos ist, 4) eine Beschreibung, wie eine Beschwerde im Zusammenhang mit den Grundsätzen eingereicht werden kann, 5) Bearbeitungsfristen für Beschwerden im Zusammenhang mit den Grundsätzen 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 Folgendes umfassen: 1) die Gesamtzahl der im Berichtsjahr eingegangen Beschwerden, die die Grundsätze betreffen, 2) die Art der eingegangenen Beschwerden, 3) die Qualität der Streitbeilegung, z. B. die Dauer der Bearbeitung von Beschwerden und 4) die Ergebnisse der eingegangenen Beschwerden, insbesondere die Anzahl und Art der auferlegten Abhilfemaßnahmen oder Sanktionen.

iv) Wie in Anlage I ausgeführt, steht Privatpersonen ein Schiedsverfahren offen, anhand dessen bei Restansprüchen festgestellt wird, ob eine dem Datenschutzrahmen 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 ([15]) oder im Hinblick auf eine Behauptung zur Angemessenheit des Datenschutzrahmens EU-USA. Im Rahmen dieses Schiedsverfahrens ist das Datenschutzrahmen-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 Datenschutzrahmen angehörende Organisationen können eine gerichtliche Überprüfung und Durchsetzung der Schiedssprüche nach US-Recht gemäß dem Federal Arbitration Act beantragen.

e) Rechtsbehelfe und Sanktionen

i) 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 infrage die öffentliche Bekanntmachung des Verstoßes, in bestimmten Fällen die Anordnung der Löschung der

([15]) Die Grundsätze, Überblick, Absatz 5.

betreffenden Daten ([16]), der vorübergehende oder dauernde Entzug eines Siegels, Entschädigungen für Personen, denen durch die Nichteinhaltung der Grundsätze ein Schaden entstanden ist, und Auflagen. Unabhängige Beschwerdestellen und Einrichtungen der freiwilligen Selbstkontrolle des privaten Sektors müssen bei Missachtung ihrer Entscheidungen die Gerichte anrufen oder die zuständige Regierungsbehörde verständigen und das Ministerium unterrichten.

f) Befassung der FTC:

i) 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 Abschnitt 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 Datenschutzrahmens EU-USA oder zur Beteiligung am Datenschutzrahmen EU-USA von Organisationen, die entweder nicht mehr auf der Datenschutzrahmen-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 mitzuteilen.

g) Fortgesetzte Missachtung der Grundsätze

i) Missachtet eine Organisation fortgesetzt die Grundsätze, kann sie die Vorteile des Datenschutzrahmens nicht mehr in Anspruch nehmen. Organisationen, die fortwährend gegen die Grundsätze verstoßen haben, werden vom Ministerium von der Datenschutzrahmen-Liste gestrichen und müssen die im Rahmen des Datenschutzrahmens EU-USA 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, einschließlich des Ministeriums, festgestellt wird, dass die Organisation so häufig gegen die Grundsätze verstößt, die es einzuhalten vorgibt, dass diese Behauptung nicht mehr glaubwürdig ist. In Fällen, in denen eine solche Entscheidung von einer anderen Stelle als dem Ministerium getroffen wird, muss die Organisation das Ministerium unverzüglich über diese Tatsachen informieren. 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 der fortgesetzten Missachtung der Grundsätze wird das Ministerium die betreffende Organisation von der Datenschutzrahmen-Liste streichen, auch als Reaktion auf eine Mitteilung der Missachtung durch die Organisation selbst, durch eine Einrichtung der freiwilligen Selbstkontrolle für den Datenschutz bzw. eine andere unabhängige Beschwerdestelle oder durch ein staatliches Kontrollorgan. Das geschieht jedoch erst, nachdem die 30-tägige Frist abgelaufen ist, in der die betroffene Organisation Gelegenheit hat zu reagieren. ([17]) Aus der Datenschutzrahmen-Liste des Ministeriums lässt sich also ersehen, welche Organisationen als dem Datenschutzrahmen EU-USA angehörig anerkannt sind und welche diese Anerkennung verloren haben.

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

([16]) Unabhängige 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 in eklatanter Weise verletzt hat.

([17]) Das Ministerium gibt in der Mitteilung die Frist an, die der Organisation zur Verfügung steht, um auf die Mitteilung zu reagieren; diese Frist beträgt in der Regel weniger als 30 Tage.

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. 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 Direktmarketings 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 der DSGVO können personenbezogene Daten in Ermangelung eines Angemessenheitsbeschlusses in ein Drittland übermittelt werden, wenn angemessene Datenschutzgarantien gemäß Artikel 46 DSGVO vorgesehen sind oder in bestimmten Situationen eine der Bedingungen von Artikel 49 DSGVO erfüllt ist (z. B. wenn die betroffene Person der Übermittlung ausdrücklich zugestimmt hat). US-Organisationen, die sich dem Datenschutzrahmen angeschlossen haben, bieten ein angemessenes Schutzniveau für personenbezogene Daten und können daher Datenübermittlungen aus der EU auf der Grundlage von Artikel 45 DSGVO erhalten, ohne ein Übermittlungsinstrument gemäß Artikel 46 DSGVO einrichten oder die Bedingungen von Artikel 49 DSGVO erfüllen zu müssen. Da das Konzept des Datenschutzrahmens EU-USA 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 dem Datenschutzrahmen angehören. 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

i) Das Recht der EU/Mitgliedstaaten gilt für die Erhebung der personenbezogenen Daten und für ihre Verarbeitung vor der Übermittlung in die USA. Die Grundsätze 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 Datenschutzrahmen angehörende 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

i) 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

i) 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. Dies würde die Aussagefähigkeit der Ergebnisse infrage 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

i) 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 Datenschutzrahmen 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 Medizinprodukteherstellern an Behörden wie die amerikanische Food and Drug Administration.

g) Verschlüsselte Daten

i) 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, sodass er unter bestimmten Umständen (z. B. wenn eine nachträgliche medizinische Überwachung notwendig ist) einzelne Versuchspersonen identifizieren kann. Die Übermittlung derart verschlüsselter Daten von der EU in die USA, bei denen es sich nach EU-Recht um personenbezogene Daten handelt, würde unter die Grundsätze fallen.

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

a) Eine Organisation muss die 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 offenstehen).

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 Verwendungen 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 obigen Grundsätze absichtlich personenbezogene Daten offengelegt hat, sodass diese Ausnahme von der Regel für die Organisation selbst oder aber für andere von Nutzen ist, verliert sie die Vorteile aus dem Datenschutzrahmen EU-USA.

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 Informationen 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 rechtmäßigen Anträgen von Behörden auf Zugang zu personenbezogenen Daten zu sorgen, können die dem Datenschutzrahmen angehörenden 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 regelmäßige Überprüfung der Funktionsweise des Datenschutzrahmens EU-USA 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.

ANHANG I SCHIEDSMODELL

In diesem Anhang I sind die Bedingungen aufgeführt, unter denen dem Datenschutzrahmen EU-USA 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 Datenschutzrahmen EU-USA 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 Datenschutzrahmens EU-USA geklärt werden konnten.

A. **Anwendungsbereich**

Mit dem Schiedsverfahren können Privatpersonen bei Restansprüchen feststellen lassen, ob eine dem Datenschutzrahmen 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 Datenschutzrahmens EU-USA.

B. **Verfügbare Abhilfemaßnahmen**

Im Rahmen dieses Schiedsverfahrens ist das Datenschutzrahmen-Panel (das Schiedsforum, das aus einem oder drei von den Parteien ausgewählten Schiedsrichtern besteht) 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. Dies sind die einzigen Befugnisse des Datenschutzrahmen-Panels in Bezug auf Abhilfemaßnahmen. Bei der Prüfung von Abhilfemaßnahmen muss das Datenschutzrahmen-Panel andere bereits von anderen Mechanismen im Rahmen des Datenschutzrahmens EU-USA verhängte Abhilfemaßnahmen berücksichtigen. Schadensersatz, 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 d)i) des Zusatzgrundsatzes „Beschwerdeverfahren und Durchsetzung" 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 Ministerium zuleiten und dem Ministerium 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 diese Option nicht in Anspruch genommen werden, wenn eine Datenschutzbehörde 1) nach dem Zusatzgrundsatz „Rolle der Datenschutzbehörden" oder dem Zusatzgrundsatz „Personaldaten" 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 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 Privatperson, 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]) Die Grundsätze, Überblick, Absatz 5.

E. **Überprüfung und Durchsetzung**

Privatpersonen und dem Datenschutzrahmen angehörende Organisationen können eine gerichtliche Überprüfung und Durchsetzung der Schiedssprüche nach US-Recht gemäß dem Federal Arbitration Act ([2]) beantragen. Derartige Fälle müssen bei dem Bundesbezirksgericht eingereicht werden, dessen territoriale Zuständigkeit sich auf den Hauptgeschäftsort der dem Datenschutzrahmen angehörenden Organisation erstreckt.

Mit diesem Schiedsverfahren sollen individuelle Streitigkeiten geklärt werden, und die Schiedssprüche 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 für das Datenschutzrahmen-Panel aus dem im Folgenden erörterten Verzeichnis der Schiedsrichter aus.

Im Einklang mit dem geltenden Recht erstellen das Ministerium und die Kommission ein Verzeichnis mit mindestens 10 Schiedsrichtern, die aufgrund ihrer Unabhängigkeit, Integrität und Sachkenntnis ausgewählt werden. Dafür gilt Folgendes:

Die Schiedsrichter

1) verbleiben für einen Zeitraum von drei Jahren in dem Verzeichnis, sofern keine außergewöhnlichen Umstände oder wichtigen Gründe für die Streichung vorliegen; dieser Zeitraum kann vom Ministerium nach vorheriger Mitteilung an die Kommission um weitere drei Jahre verlängert werden,

2) sind gegenüber einer der Parteien oder einer dem Datenschutzrahmen angehörenden Organisation bzw. gegenüber den USA, der EU oder einem EU-Mitgliedstaat oder einer anderen Regierungsbehörde, öffentlichen Stelle oder Strafverfolgungsbehörde weder weisungsgebunden noch anderweitig verpflichtet und

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

([2]) 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 [Abschnitt 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 Schiedsspruchs 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 Abschnitt 10 und 11 des [FAA] aufgegeben, geändert oder korrigiert wird." *Ebenda*. § 9.

G. **Schiedsverfahren**

Das Ministerium und die Kommission haben sich im Einklang mit dem geltenden Recht auf die Annahme einer Schiedsgerichtsordnung geeinigt, die die Verfahren vor dem Datenschutzrahmen-Panel regelt. ([3]) Für den Fall, dass die für das Verfahren geltenden Regeln geändert werden müssen, vereinbaren das Ministerium und die Kommission, diese Regeln zu ändern oder ein anderes bestehendes, gut etabliertes US-Schiedsverfahren zu übernehmen, vorbehaltlich der folgenden Erwägungen:

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.

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 Datenschutzbehörden Hilfe ausschließlich bei der Erstellung 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 Datenschutzrahmen-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.

([3]) Das International Centre for Dispute Resolution (ICDR), die internationale Abteilung der American Arbitration Association (AAA) (im Folgenden zusammen „ICDR-AAA"), wurde vom Handelsministerium mit der Durchführung von Schiedsverfahren gemäß den Grundsätzen und der Verwaltung des in Anhang I der Grundsätze genannten Schiedsfonds beauftragt. Am 15. September 2017 einigten sich das Ministerium und die Kommission auf die Annahme einer Reihe von Schiedsregeln, mit denen die in Anhang I der Grundsätze beschriebenen verbindlichen Schiedsverfahren geregelt werden, sowie auf einen Verhaltenskodex für Schiedsrichter, der den allgemein anerkannten ethischen Standards für Handelsschiedsrichter und Anhang I der Grundsätze entspricht. Das Ministerium und die Kommission haben vereinbart, die Schiedsregeln und den Verhaltenskodex an die Aktualisierungen des Datenschutzrahmens EU-USA anzupassen, und das Ministerium wird mit dem ICDR-AAA zusammenarbeiten, um diese Aktualisierungen vorzunehmen.

H. **Kosten**

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

Das Ministerium ermöglicht im Einklang mit dem geltenden Recht die Aufrechterhaltung eines Fonds, in den die dem Datenschutzrahmen angehörenden Organisationen einen Beitrag 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 dem Ministerium regelmäßig über die Tätigkeit des Fonds Bericht erstattet. Das Ministerium arbeitet mit dem Dritten zusammen, um die Tätigkeit des Fonds regelmäßig zu überprüfen, einschließlich der Notwendigkeit einer Anpassung des Beitrags oder der Obergrenze für die Schiedskosten, und prüft unter anderem die Anzahl der Schiedsverfahren sowie deren Kosten und Dauer, und zwar im Einvernehmen, dass den dem Datenschutzrahmen angehörenden Organisationen keine übermäßige finanzielle Belastung auferlegt wird. Das Ministerium wird die Kommission über das Ergebnis dieser Überprüfungen mit dem Dritten unterrichten und die Kommission im Voraus über etwaige Anpassungen der Höhe der Beiträge informieren. Rechtsanwaltsgebühren sind von dieser Bestimmung oder einem anderen Fonds im Rahmen dieser Bestimmung nicht erfasst.

ANHANG II

UNITED STATES DEPARTMENT OF COMMERCE
Secretary of Commerce
Washington, D.C. 20230

6. Juli 2023

Herrn Didier Reynders
Kommissar für Justiz
Europäische Kommission
Rue de la Loi/Wetstraat 200
1049 Brüssel
Belgien

Sehr geehrter Herr Reynders,

es ist mir eine große Freude, Ihnen im Namen der Vereinigten Staaten mit diesem Schreiben eine Materialsammlung zum Datenschutzrahmen EU-USA zukommen zu lassen, die in Verbindung mit der Executive Order 14086 mit dem Titel „Enhancing Safeguards for United States Signals Intelligence Activities" und Titel 28 CFR Teil 201 zur Änderung der Vorschriften des Justizministeriums zur Einrichtung des „Data Protection Review Court" wichtige und detaillierte Verhandlungen zur Stärkung des Schutzes der Privatsphäre und der bürgerlichen Freiheiten widerspiegelt. Diese Verhandlungen haben zu neuen Garantien geführt, mit denen sichergestellt werden soll, dass die Tätigkeiten der USA im Bereich der Signalaufklärung zur Verfolgung bestimmter nationaler Sicherheitsziele notwendig und verhältnismäßig sind, sowie zu einem neuen Mechanismus, der es Privatpersonen in der Europäischen Union ermöglicht, Rechtsbehelfe einzulegen, wenn sie der Auffassung sind, dass sie unrechtmäßig Ziel von Signalaufklärungsmaßnahmen geworden sind, wodurch der Schutz personenbezogener Daten in der EU gewährleistet wird. Der Datenschutzrahmen EU-USA wird die Grundlage für eine integrative und wettbewerbsfähige digitale Wirtschaft bilden. Wir sollten beide stolz auf die Verbesserungen sein, die sich in diesem Rahmenwerk widerspiegeln und die den Schutz der Privatsphäre weltweit verbessern werden. In Kombination mit der Executive Order, den Regelungen und anderen öffentlich zugänglichen Materialien bietet diese Sammlung der Kommission eine fundierte Grundlage, um eine aktuelle Angemessenheitsfeststellung vorzunehmen. ([1])

Folgende Unterlagen werden beigefügt:

— Die Grundsätze des Datenschutzrahmens EU-USA, einschließlich der Zusatzgrundsätze (zusammen „die Grundsätze") und Anhang I der Grundsätze (d. h. ein Anhang, in dem die Bedingungen festgelegt sind, unter denen die dem Datenschutzrahmen angehörenden Organisationen verpflichtet sind, bestimmte Restansprüche in Bezug auf personenbezogene Daten, die unter die Grundsätze fallen, in einem Schiedsverfahren zu entscheiden),

— ein Schreiben der International Trade Administration des Ministeriums, die das Datenschutzrahmen-Programm verwaltet, in dem die Verpflichtungen beschrieben werden, die unser Ministerium eingegangen ist, um sicherzustellen, dass der Datenschutzrahmen EU-USA wirksam funktioniert,

— ein Schreiben der Federal Trade Commission zur internen Durchsetzung der Grundsätze,

— ein Schreiben des Verkehrsministeriums zur internen Durchsetzung der Grundsätze,

— ein Schreiben des Office of the Director of National Intelligence zu den für die nationalen Sicherheitsbehörden in den USA geltenden Garantien und Beschränkungen 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.

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

Das vollständige Paket des Datenschutzrahmens EU-USA wird auf der Datenschutzrahmen-Website des Ministeriums veröffentlicht, und die Grundsätze und Anhang I der Grundsätze werden am Tag des Inkrafttretens des Angemessenheitsbeschlusses der Europäischen Kommission in Kraft treten.

Seien Sie versichert, dass die USA diese Zusagen sehr ernst nehmen. Wir freuen uns auf unsere Zusammenarbeit bei der Umsetzung des Datenschutzrahmens EU-USA und der Einleitung der nächsten Phase in diesem Prozess.

Mit freundlichen Grüßen

Gina M. RAIMONDO

ANHANG III

UNITED STATES DEPARTMENT OF COMMERCE
International Trade Administration
Washington, D C 20230

12. Dezember 2022

Herr Didier Reynders
Kommissar für Justiz
Europäische Kommission
Rue de la Loi/Wetstraat 200
1049 Brüssel
Belgien

Sehr geehrter Herr Reynders,

im Namen der International Trade Administration („ITA“) darf ich Ihnen mitteilen, welche Verpflichtungen das Handelsministerium („Ministerium“) eingegangen ist, um den Schutz personenbezogener Daten durch die Verwaltung und Überwachung des Datenschutzrahmen-Programms zu gewährleisten. Der Abschluss des Datenschutzrahmens EU-USA („Datenschutzrahmen“) ist ein großer Erfolg für den Datenschutz und die Unternehmen auf beiden Seiten des Atlantiks, da er den EU-Bürgern die Gewissheit bieten wird, dass ihre Daten geschützt werden und sie bei etwaigen Bedenken über Rechtsmittel verfügen, und er wird es Tausenden von Unternehmen ermöglichen, weiterhin Investitionen zu tätigen und sich anderweitig am transatlantischen Handel zu beteiligen, was unseren jeweiligen Volkswirtschaften und Bürgern zugutekommt. Der Datenschutzrahmen EU-USA ist das Ergebnis langjähriger harter Arbeit und Kooperation mit Ihnen und Ihren Kolleginnen und Kollegen in der Europäischen Kommission („Kommission“). Wir freuen uns, unsere Kooperation mit der Kommission im Sinne eines wirksamen Funktionierens dieser Zusammenarbeit fortzusetzen.

Mit dem Datenschutzrahmen sind grundlegende Vorteile sowohl für Privatpersonen als auch für Unternehmen verbunden. Erstens beinhaltet es einen umfassenden Katalog von Schutzbestimmungen für die Daten von EU-Bürgern, die in die Vereinigten Staaten übermittelt werden. Dem Datenschutzrahmen angehörende US-Organisationen müssen an der Entwicklung einer einheitlichen Datenschutzstrategie mitwirken, sich öffentlich zur Einhaltung der „Grundsätze des Datenschutzrahmens EU-USA“, einschließlich der Zusatzgrundsätze (zusammen „Grundsätze“), und des Anhangs I der Grundsätze (d. h. eines Anhangs, in dem die Bedingungen festgelegt sind, unter denen dem Datenschutzrahmen EU-USA angehörende Organisationen verpflichtet sind, bestimmte Restansprüche in Bezug auf personenbezogene Daten, die unter die Grundsätze fallen, in einem Schiedsverfahren zu klären) verpflichten, damit diese Verpflichtung nach US-Recht durchsetzbar wird, ([1]) die Einhaltung beim Ministerium jährlich neu zertifizieren, EU-Bürgern eine kostenfreie unabhängige Streitbeilegung ermöglichen und sich der Zuständigkeit einer in den Grundsätzen aufgeführten US-Behörde (z. B. der Federal Trade Commission („FTC“), dem Verkehrsministerium) oder einer in einem künftigen Anhang zu den Grundsätzen aufgeführten US-Behörde unterstellen. Die Entscheidung einer Organisation, sich selbst zu zertifizieren, ist zwar freiwillig, aber sobald sich eine Organisation öffentlich zur Einhaltung der Grundsätze des Datenschutzrahmens EU-USA verpflichtet, kann ihre Verpflichtung nach US-Recht von der FTC, dem Verkehrsministerium oder einer anderen US-Behörde durchgesetzt werden, je nachdem, welche Behörde für die betreffende Organisation zuständig ist. Zweitens bietet der Datenschutzrahmen EU-USA Unternehmen in den USA sowie Tochtergesellschaften europäischer Unternehmen

([1]) Organisationen, die ihre Verpflichtung zur Einhaltung der Grundsätze des EU-US-Datenschutzschilds selbst zertifiziert haben und die Vorteile der Beteiligung am Datenschutzrahmen EU-USA genießen möchten, müssen die „Grundsätze des Datenschutzrahmens EU-USA“ einhalten. Diese Verpflichtung zur Einhaltung der „Grundsätze des Datenschutzrahmens EU-USA“ muss sich so bald wie möglich, spätestens jedoch drei Monate nach Inkrafttreten der „Grundsätze des Datenschutzrahmens EU-USA“ in den Datenschutzbestimmungen dieser beteiligten Organisationen niederschlagen. (*Siehe* Abschnitt e des Zusatzgrundsatzes „Selbstzertifizierung“).

in den USA die Möglichkeit, personenbezogene Daten aus der Europäischen Union zu empfangen, was den Datenfluss im Sinne des transatlantischen Handels erleichtert. Die Datenflüsse zwischen den Vereinigten Staaten und der Europäischen Union sind die größten der Welt und unterstützen die 7,1 Billionen USD schweren Wirtschaftsbeziehungen zwischen den USA und der EU, die Millionen von Arbeitsplätzen auf beiden Seiten des Atlantiks sichern. 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. Dank des transatlantischen Datenverkehrs können US-Organisationen Daten verarbeiten, die erforderlich sind, um EU-Bürgern Waren, Dienstleistungen und Beschäftigungsmöglichkeiten anzubieten.

Das Ministerium ist bestrebt, eng und produktiv mit unseren Kolleginnen und Kollegen in der EU zusammenzuarbeiten, um das Datenschutzrahmen-Programm wirksam zu verwalten und zu überwachen. Dieses Engagement zeigt sich in der Entwicklung und kontinuierlichen Optimierung eines breiten Spektrums von Ressourcen durch das Ministerium, um Organisationen bei der Selbstzertifizierung zu unterstützen, in der Einrichtung einer Website mit gezielten Informationen für interessierte Kreise, in der Zusammenarbeit mit der Kommission und den europäischen Datenschutzbehörden bei der Entwicklung von Leitlinien zur Klärung wichtiger Elemente des Datenschutzrahmens EU-USA, in der Öffentlichkeitsarbeit zur Förderung des Verständnisses der Datenschutzverpflichtungen von Organisationen und in der Überwachung und Kontrolle der Einhaltung der Anforderungen des Programms durch die Organisationen.

Unsere kontinuierliche Zusammenarbeit mit unseren geschätzten Kolleginnen und Kollegen in der EU wird es dem Ministerium ermöglichen, sicherzustellen, dass der Datenschutzrahmen EU-USA wirksam funktioniert. Die Regierung der Vereinigten Staaten arbeitet seit Langem mit der Kommission zusammen, um gemeinsame Datenschutzgrundsätze zu fördern, die Unterschiede in unseren jeweiligen rechtlichen Ansätzen zu überbrücken und gleichzeitig den Handel und das Wirtschaftswachstum in der Europäischen Union und den Vereinigten Staaten zu fördern. Wir glauben, dass der Datenschutzrahmen EU-USA, der ein Beispiel für diese Zusammenarbeit ist, es der Kommission ermöglichen wird, einen neuen Angemessenheitsbeschluss zu erlassen, der es Organisationen erlaubt, den Datenschutzrahmen EU-USA zu nutzen, um personenbezogene Daten aus der Europäischen Union in die Vereinigten Staaten im Einklang mit dem EU-Recht zu übermitteln.

Verwaltung und Überwachung des Datenschutzrahmen-Programms durch das Handelsministerium

Das Ministerium ist fest entschlossen, das Datenschutzrahmen-Programm wirksam zu verwalten und zu überwachen, und wird angemessene Anstrengungen unternehmen und Ressourcen bereitstellen, um dies zu gewährleisten. Das Ministerium 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 („Datenschutzrahmen-Liste“). Diese Liste wird auf der Grundlage der jährlichen Anträge auf erneute Zertifizierung durch die dem Datenschutzrahmen angehörenden Organisationen und durch die Streichung von Organisationen aktualisiert, wenn diese sich freiwillig zurückziehen, die jährliche erneute Zertifizierung nicht in Übereinstimmung mit den Verfahren des Ministeriums durchführen oder wenn festgestellt wird, dass sie die Grundsätze dauerhaft nicht einhalten. Das Ministerium wird außerdem ein amtliches Verzeichnis der US-Organisationen führen, die von der Liste gestrichen wurden, und wird es der Öffentlichkeit zugänglich machen, wobei in jedem Falle die Gründe für die Streichung einzelner Organisationen angegeben werden. Die vorgenannte amtliche Liste und das Verzeichnis werden auf der Datenschutzrahmen-Website des Ministeriums öffentlich zugänglich bleiben. Die Website zum Datenschutzrahmen wird eine deutlich sichtbare Erklärung enthalten, dass jede Organisation, die von der Datenschutzrahmen-Liste gestrichen wird, nicht mehr behaupten darf, dass sie sich am Datenschutzrahmen EU-USA beteiligt oder ihn einhält, und dass sie unter dem Datenschutzrahmen EU-USA personenbezogene Daten erhalten kann. Eine solche Organisation muss jedoch weiterhin die Grundsätze auf die personenbezogenen Daten anwenden, die sie während ihrer Beteiligung am Datenschutzrahmen erhalten hat, solange sie diese Daten aufbewahrt. Das Ministerium verpflichtet sich im Rahmen seines übergreifenden, kontinuierlichen Engagements für die wirksame Verwaltung und Überwachung des Datenschutzrahmen-Programms insbesondere zu Folgendem:

Prüfung der Selbstzertifizierungs-Anforderungen

— Bevor das Ministerium die erste Selbstzertifizierung oder die jährliche erneute Zertifizierung einer Organisation (zusammen „Selbstzertifizierung“) abschließt und eine Organisation in die Datenschutzrahmen-Liste aufnimmt bzw. darin belässt, prüft es, ob die Organisation zumindest die einschlägigen Anforderungen des Zusatzgrundsatzes zur Selbstzertifizierung in Bezug auf die Informationen erfüllt, die eine Organisation dem Ministerium im Rahmen ihrer Selbstzertifizierung übermitteln muss, und ob sie rechtzeitig einschlägige Datenschutzbestimmungen vorgelegt hat, die Privatpersonen über alle 13 im Grundsatz der Informationspflicht aufgeführten Punkte informieren. Das Ministerium wird überprüfen, ob die Organisation

— die Organisation identifiziert hat, die ihre Selbstzertifizierung beantragt, sowie alle US-Einrichtungen oder US-Tochterunternehmen der selbstzertifizierenden Organisation, die sich ebenfalls an die Grundsätze halten, die die Organisation durch ihre Selbstzertifizierung abgedeckt haben möchte,

— die erforderlichen Kontaktinformationen bereitgestellt hat (z. B. Kontaktinformationen für bestimmte Personen und/oder Stellen innerhalb der selbstzertifizierenden Organisation, die für die Bearbeitung von Beschwerden, Auskunftsbegehren und anderen Fragen im Zusammenhang mit dem Datenschutzrahmen EU-USA zuständig sind),

— den/die Zweck(e) beschrieben hat, für den/die die Organisation die von der Europäischen Union erhaltenen personenbezogenen Daten erhebt und verwendet,

— angegeben hat, welche personenbezogenen Daten aus der Europäischen Union unter Berufung auf den Datenschutzrahmen EU-USA übermittelt werden und daher von ihrer Selbstzertifizierung erfasst sind,

— falls die Organisation über eine öffentlich zugängliche Website verfügt, die Internetadresse, unter der die einschlägigen Datenschutzbestimmungen auf dieser Website leicht zugänglich sind, oder, falls die Organisation über keine öffentlich zugängliche Website verfügt, eine Kopie der einschlägigen Datenschutzbestimmungen und den Ort, an dem die Datenschutzbestimmungen von den betroffenen Personen eingesehen werden können (d. h. von den betroffenen Mitarbeitern, wenn es sich um Datenschutzbestimmungen für Personaldaten handelt, oder von der Öffentlichkeit, wenn es sich bei den einschlägigen Datenschutzbestimmungen nicht um Datenschutzbestimmungen der Personalabteilung handelt) angegeben hat,

— zu gegebener Zeit (d. h. zunächst nur in einem mit dem Antrag eingereichten Entwurf der Datenschutzerklärung, wenn es sich um eine erste Selbstzertifizierung handelt; andernfalls in einer endgültigen Datenschutzerklärung, die gegebenenfalls veröffentlicht wird) eine Erklärung über die Einhaltung der Grundsätze sowie einen Hyperlink oder die Internetadresse der Datenschutzrahmen-Website des Ministeriums (z. B. die Homepage oder die Website mit der Datenschutzrahmen-Liste), angegeben hat,

— zu gegebener Zeit alle anderen zwölf im Grundsatz der Informationspflicht aufgeführten Punkte (z. B. die Möglichkeit für den betroffene EU-Bürger, unter bestimmten Bedingungen ein bindendes Schiedsverfahren in Anspruch zu nehmen; die Bestimmung, personenbezogene Daten auf rechtmäßige Anfrage von Behörden offenzulegen, um Erfordernissen der nationalen Sicherheit oder der Strafverfolgung nachzukommen und die Haftung der Organisation bei Weitergabe an Dritte) in ihre einschlägigen Datenschutzbestimmungen aufgenommen 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),

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

— festgelegt hat, ob es sich bei der relevanten Methode (d. h. bei den von ihr bereitzustellenden Folgeverfahren) zur Überprüfung der Einhaltung der Grundsätze um eine „Selbstbewertung“ (d. h. eine interne Überprüfung) oder um eine „externe Überprüfung“ (d. h. eine Überprüfung durch Dritte) handelt, und, falls es sich bei der relevanten Methode um eine externe Überprüfung handelt, auch den Dritten genannt hat, der die Überprüfung durchgeführt hat,

— die angemessene unabhängige Beschwerdestelle bestimmt hat, die für die Behandlung von Beschwerden im Zusammenhang mit den Grundsätzen zur Verfügung steht, und der betroffenen Person kostenlos einen geeigneten Rechtsbehelf gewährt.

  — Hat sich die Organisation für eine unabhängige Beschwerdestelle entschieden, die von einer privaten Stelle zur alternativen Streitbeilegung angeboten wird, so hat sie in ihren einschlägigen Datenschutzbestimmungen einen Hyperlink oder die Internetadresse der entsprechenden Website oder des entsprechenden Beschwerdeformulars anzugeben, die bzw. das für die Untersuchung ungelöster Beschwerden im Rahmen der Grundsätze zur Verfügung steht.

  — Wenn die Organisation entweder dazu verpflichtet ist (z. B. in Bezug auf Personaldaten, die im Rahmen eines Arbeitsverhältnisses aus der Europäischen Union übermittelt werden) oder sich dafür entschieden hat, mit den zuständigen Datenschutzbehörden bei der Untersuchung und Beilegung von Beschwerden im Zusammenhang mit den Grundsätzen zusammenzuarbeiten, hat sie sich verpflichtet, im Rahmen dieser Zusammenarbeit mit den Datenschutzbehörden und der Befolgung ihrer diesbezüglichen Empfehlungen spezifische Maßnahmen zur Einhaltung der Grundsätze zu ergreifen.

— Das Ministerium wird auch prüfen, ob die von der Organisation vorgelegte Selbstzertifizierung den einschlägigen Datenschutzbestimmungen entspricht. Wenn eine selbstzertifizierende Organisation ihre US-Einrichtungen oder US-Tochterunternehmen einbeziehen möchte, die über eigene einschlägige Datenschutzbestimmungen verfügen, wird das Ministerium auch die einschlägigen Datenschutzbestimmungen dieser einbezogenen Einrichtungen oder Tochterunternehmen überprüfen, um sicherzustellen, dass sie alle im Grundsatz der Informationspflicht geforderten Aspekte enthalten.

— Das Ministerium wird mit den Behörden (z. B. der FTC und dem Verkehrsministerium) zusammenarbeiten, um zu überprüfen, ob die Organisationen in den Zuständigkeitsbereich der in der Selbstzertifizierung angegebenen Behörde fallen, wenn das Ministerium Grund hat, daran zu zweifeln.

— Das Ministerium wird mit privaten Stellen für alternative Streitbeilegung zusammenarbeiten, um zu überprüfen, ob die Organisationen aktiv bei den unabhängigen Beschwerdestellen registriert sind, wie in der Selbstzertifizierung angegeben, und ob die Organisationen aktiv für die in der Selbstzertifizierung angegebene externe Überprüfung der Einhaltung der Grundsätze registriert sind, wenn diese Stellen beide Arten von Dienstleistungen anbieten können.

— Das Ministerium wird mit dem vom Ministerium ausgewählten Dritten zusammenarbeiten, der als Verwahrer der durch die Gebühr für das Gremium der Datenschutzbehörden (d. h. die jährliche Gebühr zur Deckung der Betriebskosten des Gremiums der Datenschutzbehörden) eingenommenen Mittel fungiert, um zu überprüfen, ob die Organisationen diese Gebühr für das betreffende Jahr gezahlt haben, sofern die Organisationen die Datenschutzbehörden als die einschlägigen unabhängigen Beschwerdestellen angegeben haben.

— Das Ministerium wird mit dem Dritten zusammenarbeiten, der vom Ministerium für die Durchführung der Schiedsverfahren gemäß den Grundsätzen und die Verwaltung des in Anhang I der Grundsätze genannten Schiedsfonds ausgewählt wurde, um zu überprüfen, ob die Organisationen einen Beitrag zu diesem Schiedsfonds geleistet haben.

— Stellt das Ministerium bei der Prüfung der von den Organisationen eingereichten Anträge auf Selbstzertifizierung Mängel fest, wird es diesen Organisationen mitteilen, dass sie diese Mängel innerhalb der vom Ministerium festgesetzten Frist beheben müssen. ([2]) Das Ministerium wird sie auch darauf hinweisen, dass eine Nichtbeantwortung innerhalb der vom Ministerium gesetzten Frist oder ein Versäumnis, die Selbstzertifizierung in Übereinstimmung mit den Verfahren des Ministeriums abzuschließen, dazu führt, dass diese Selbstzertifizierungsanträge als aufgegeben betrachtet werden, und dass jede falsche Darstellung hinsichtlich der Beteiligung einer Organisation am Datenschutzrahmen oder der Einhaltung dieses Rahmens durch die FTC, das Verkehrsministerium oder eine andere zuständige Regierungsbehörde zu Durchsetzungsmaßnahmen führen kann. Das Ministerium wird die Organisationen über die Kontaktkanäle informieren, die die Organisationen dem Ministerium mitgeteilt haben.

Erleichterung der Zusammenarbeit mit Stellen zur alternativen Streitbeilegung, die mit den Grundsätzen zusammenhängende Dienstleistungen erbringen

— Das Ministerium wird mit privaten Stellen zur alternativen Streitbeilegung zusammenarbeiten, die unabhängige Beschwerdeverfahren zur Verfügung stellen und ungelöste Beschwerden im Zusammenhang mit den Grundsätzen daraufhin untersuchen können, ob sie zumindest die Anforderungen des Zusatzgrundsatzes „Beschwerdeverfahren und Durchsetzung“ erfüllen. Das Ministerium wird überprüfen, ob sie

  — auf ihren öffentlichen Websites Informationen über die Grundsätze und die Dienstleistungen, die sie im Rahmen des Datenschutzrahmens EU-USA erbringen, bereitstellen, die Folgendes umfassen müssen: 1) Angaben über die Anforderungen an unabhängige Beschwerdestellen in den Grundsätzen oder einen Link zu diesen Anforderungen, 2) einen Hyperlink zur Website des Ministeriums zum Datenschutzrahmen, 3) einen Hinweis, dass das Beschwerdeverfahren im Rahmen des Datenschutzrahmens EU-USA für Privatpersonen kostenlos ist, 4) eine Beschreibung, wie eine Beschwerde im Zusammenhang mit den Grundsätzen eingereicht werden kann, 5) Bearbeitungsfristen für Beschwerden im Zusammenhang mit den Grundsätzen 6) eine Beschreibung der Palette möglicher Abhilfemaßnahmen. Das Ministerium wird die Beschwerdestellen rechtzeitig über wesentliche Änderungen bei der Überwachung und Verwaltung des Datenschutzrahmen-Programms durch das Ministerium informieren, wenn solche Änderungen bevorstehen oder bereits vorgenommen wurden und diese Änderungen für die Rolle der Stellen im Rahmen des Datenschutzrahmens EU-USA relevant sind,

([2]) Im Hinblick auf die erneute Zertifizierung wird von den Organisationen erwartet, dass sie diese Fragen innerhalb von 45 Tagen klären; vorbehaltlich der Festlegung einer anderen angemessenen Frist durch das Ministerium.

— jährlich einen Bericht mit zusammengefassten statistischen Angaben zu ihren Dienstleistungen vorlegen, der Folgendes beinhaltet: 1) die Gesamtzahl der im Berichtsjahr eingegangen Beschwerden, die die Grundsätze betreffen, 2) die Art der eingegangenen Beschwerden, 3) die Qualität der Streitbeilegung, z. B. die Dauer der Bearbeitung von Beschwerden und 4) die Ergebnisse der eingegangenen Beschwerden, insbesondere die Anzahl und Art der auferlegten Abhilfemaßnahmen oder Sanktionen. Das Ministerium wird den Stellen spezifische zusätzliche Leitlinien zu den Informationen zur Verfügung stellen, die in diesen Jahresberichten enthalten sein sollten, und diese Anforderungen näher erläutern (z. B. eine Liste der spezifischen Kriterien, die eine Beschwerde erfüllen muss, damit sie für die Zwecke des Jahresberichts als Beschwerde im Zusammenhang mit den Grundsätzen betrachtet werden kann), sowie andere Arten von Informationen, die die Stellen zur Verfügung stellen sollten (z. B. eine Beschreibung, wie die Stelle tatsächliche oder potenzielle Interessenkonflikte in Situationen vermeidet, in denen sie für eine Organisation sowohl Überprüfungsdienste als auch Streitbeilegungsdienste erbringt, wenn die Stelle auch eine Dienstleistung im Zusammenhang mit den Grundsätzen erbringt). In den zusätzlichen Leitlinien des Ministeriums ist auch das Datum angegeben, bis zu dem die Jahresberichte der Stellen für den betreffenden Berichtszeitraum veröffentlicht werden müssen.

Weiterbehandlung der Fälle von Organisationen, die die Streichung von der Datenschutzrahmen-Liste beantragt haben oder von dieser Liste gestrichen wurden

— Wenn eine Organisation aus dem Datenschutzrahmen EU-USA ausscheiden möchte, verlangt das Ministerium, dass die Organisation alle Verweise auf den Datenschutzrahmen EU-USA aus allen relevanten Datenschutzbestimmungen entfernt, die implizieren, dass die Organisation weiterhin dem Datenschutzrahmen EU-USA angehört und personenbezogene Daten im Rahmen des Datenschutzrahmens EU-USA erhalten kann (siehe Beschreibung der Verpflichtung des Ministeriums, nach falschen Angaben über die Beteiligung zu suchen). Das Ministerium verlangt außerdem, dass die Organisation einen entsprechenden Fragebogen ausfüllt und dem Ministerium vorlegt, damit Folgendes überprüft werden kann:

  — ihren Wunsch, aus dem Datenschutzrahmen auszuscheiden,

  — Informationen darüber, was sie mit den personenbezogenen Daten zu tun gedenkt, die sie während ihrer Beteiligung am Datenschutzrahmen EU-USA unter Berufung auf den Datenschutzrahmen EU-USA erhalten hat, d. h. ob sie a) diese Daten aufbewahren, die Grundsätze weiterhin auf diese Daten anwenden und gegenüber dem Ministerium jährlich ihre Verpflichtung zur Anwendung der Grundsätze auf diese Daten bestätigen wird, b) diese Daten aufbewahren und einen „angemessenen“ Schutz dieser Daten durch andere zulässige Mittel gewährleisten wird oder c) alle diese Daten innerhalb einer bestimmten Frist zurückgibt oder löscht sowie

  — wer innerhalb der Organisation als ständige Kontaktperson für Fragen im Zusammenhang mit den Grundsätzen fungieren wird.

— Wenn sich eine Organisation für Option a, wie oben beschrieben, entscheidet, wird das Ministerium auch verlangen, dass die Organisation jedes Jahr nach ihrem Ausscheiden (d. h. bis zum ersten Jahrestag ihres Ausscheidens und bis zu jedem weiteren Jahrestag, es sei denn, die Organisation gewährleistet einen „angemessenen“ Schutz dieser Daten durch andere zulässige Mittel oder sie gibt alle diese Daten zurück oder löscht sie und teilt dies dem Ministerium mit) einen entsprechenden Fragebogen ausfüllt und dem Ministerium vorlegt, um zu überprüfen, was sie mit diesen personenbezogenen Daten getan hat, was sie mit allen personenbezogenen Daten zu tun gedenkt, die sie weiterhin aufbewahren wird, und wer innerhalb der Organisation als ständige Kontaktperson für Fragen im Zusammenhang mit den Grundsätzen fungieren wird.

— Wenn die Selbstzertifizierung einer Organisation abgelaufen ist (d. h. die Organisation hat weder die jährliche erneute Zertifizierung ihrer Einhaltung der Grundsätze abgeschlossen noch wurde sie aus einem anderen Grund von der Datenschutzrahmen-Liste gestrichen, wie z. B. Ausscheiden), wird das Ministerium die Organisation auffordern, einen entsprechenden Fragebogen auszufüllen und dem Ministerium vorzulegen, um zu prüfen, ob die Organisation ausscheiden oder sich erneut zertifiziert werden möchte.

  — Wenn sie ausscheiden möchte, muss sie auch nachweisen, was sie mit den personenbezogenen Daten zu tun gedenkt, die sie unter Berufung auf den Datenschutzrahmen EU-USA erhalten hat, während sie am Datenschutzrahmen EU-USA beteiligt war (siehe die vorstehende Beschreibung dessen, was eine Organisation nachweisen muss, wenn sie aus dem Datenschutzrahmen ausscheiden möchte).

  — Wenn sie eine erneute Zertifizierung anstrebt, muss sie auch nachweisen, dass sie während der Zeit, in der ihr Zertifizierungsstatus abgelaufen ist, die Grundsätze auf personenbezogene Daten angewandt hat, die sie im Rahmen des Datenschutzrahmens EU-USA erhalten hat, und angeben, welche Schritte sie unternehmen wird, um die noch offenen Fragen zu klären, die ihre erneute Zertifizierung verzögert haben.

— Wenn eine Organisation aus einem der folgenden Gründe von der Datenschutzrahmen-Liste gestrichen wird: a) Ausscheiden aus dem Datenschutzrahmen EU-USA, b) Versäumnis, die jährliche erneute Zertifizierung ihrer Einhaltung der Grundsätze abzuschließen (d. h. entweder hat die Organisation das jährliche Verfahren zur erneuten Zertifizierung begonnen, aber nicht rechtzeitig abgeschlossen, oder sie hat das jährliche Verfahren zur erneuten Zertifizierung überhaupt nicht begonnen) oder c) „fortgesetzte Missachtung der Grundsätze", wird das Ministerium eine Mitteilung an die im Antrag der Organisation auf Selbstzertifizierung angegebene(n) Kontaktperson(en) senden, in der der Grund für die Streichung angegeben wird und in der erklärt wird, dass die Organisation nicht länger ausdrücklich oder stillschweigend behaupten darf, dass sie dem Datenschutzrahmen EU-USA angehört oder die Grundsätze einhält, oder dass sie berechtigt ist, personenbezogene Daten gemäß dem Datenschutzrahmen EU-USA zu erhalten. In der Mitteilung, die auch andere Inhalte enthalten kann, die auf den Grund der Streichung zugeschnitten sind, wird darauf hingewiesen, dass Organisationen, die ihre Beteiligung am Datenschutzrahmen EU-USA oder ihre Einhaltung der Grundsätze falsch darstellen, einschließlich der Fälle, in denen sie nach der Streichung von der Datenschutzrahmen-Liste behaupten, am Datenschutzrahmen EU-USA beteiligt zu sein, Gegenstand von Durchsetzungsmaßnahmen der FTC, des Verkehrsministeriums oder anderer zuständiger Regierungsstellen sein können.

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

— Wenn eine Organisation a) aus dem Datenschutzrahmen EU-USA ausscheidet, b) die jährliche erneute Zertifizierung ihrer Einhaltung der Grundsätze nicht abschließt (d. h. entweder das jährliche Verfahren zur erneuten Zertifizierung begonnen, aber nicht rechtzeitig abgeschlossen hat, oder sie hat das jährliche Verfahren zur erneuten Zertifizierung überhaupt nicht begonnen), c) aus dem Datenschutzrahmen EU-USA gestrichen wird, insbesondere wegen „fortgesetzter Missachtung der Grundsätze", oder d) eine erste Selbstzertifizierung ihrer Einhaltung der Grundsätze nicht abschließt (d. h. begonnen, aber nicht rechtzeitig abgeschlossen hat), wird das Ministerium von Amts wegen überprüfen, dass alle einschlägigen veröffentlichten Datenschutzbestimmungen der Organisation keine Verweise auf den Datenschutzrahmen EU-USA enthalten, die implizieren, dass die Organisation dem Datenschutzrahmen EU-USA angehört und berechtigt ist, personenbezogene Daten gemäß dem Datenschutzrahmen EU-USA zu erhalten. Stellt das Ministerium solche Verweise fest, wird es die Organisation darüber informieren, dass es die Angelegenheit gegebenenfalls an die zuständige Behörde weiterleiten wird, um mögliche Durchsetzungsmaßnahmen einzuleiten, falls die Organisation weiterhin falsche Angaben zu ihrer Beteiligung am Datenschutzrahmen macht. Das Ministerium informiert die Organisation mittels der Kontaktkanäle, die die Organisation dem Ministerium zur Verfügung gestellt hat, oder gegebenenfalls auf andere geeignete Weise. Wenn die Organisation weder die Verweise entfernt noch ihre Einhaltung der Grundsätze des Datenschutzrahmens EU-USA gemäß den Verfahren des Ministeriums selbst zertifiziert, wird das Ministerium die Angelegenheit von Amts wegen an die FTC, das Verkehrsministerium oder eine andere zuständige Behörde verweisen oder andere geeignete Maßnahmen ergreifen, um die ordnungsgemäße Verwendung des Datenschutzrahmens EU-USA sicherzustellen.

— Das Ministerium wird weitere Anstrengungen unternehmen, um falsche Behauptungen über die Beteiligung am Datenschutzrahmen EU-USA und die missbräuchliche Verwendung des Gütesiegels für den Datenschutzrahmen EU-USA aufzudecken, auch durch Organisationen, die im Gegensatz zu den vorstehend beschriebenen Organisationen noch nicht einmal mit dem Selbstzertifizierungsprozess begonnen haben (z. B. durch Durchführung geeigneter Internetrecherchen, um Verweise auf den Datenschutzrahmen EU-USA in den Datenschutzbestimmungen von Organisationen zu finden). Wenn das Ministerium durch diese Bemühungen falsche Behauptungen über die Beteiligung am Datenschutzrahmen EU-USA und die missbräuchliche Verwendung des Gütesiegels des Datenschutzrahmens EU-USA feststellt, wird es die Organisation darüber informieren, dass es die Angelegenheit gegebenenfalls an die zuständige Behörde weiterleiten wird, um mögliche Durchsetzungsmaßnahmen einzuleiten, falls die Organisation weiterhin falsche Angaben zu ihrer Beteiligung am Datenschutzrahmen EU-USA macht. Das Ministerium informiert die Organisation mittels der Kontaktkanäle, die die Organisation dem Ministerium gegebenenfalls zur Verfügung gestellt hat, oder erforderlichenfalls auf andere geeignete Weise. Wenn die Organisation weder die Verweise entfernt noch ihre Einhaltung der Grundsätze des Datenschutzrahmens EU-USA gemäß den Verfahren des Ministeriums selbst zertifiziert, wird das Ministerium die Angelegenheit von Amts wegen an die FTC, das Verkehrsministerium oder eine andere zuständige Behörde verweisen oder andere geeignete Maßnahmen ergreifen, um die ordnungsgemäße Verwendung des Datenschutzrahmens EU-USA sicherzustellen.

— Das Ministerium prüft und bearbeitet unverzüglich konkrete und ernst gemeinte Beschwerden über falsche Behauptungen im Zusammenhang mit dem Datenschutzrahmen EU-USA, die beim Ministerium eingehen (z. B. Beschwerden von Datenschutzbehörden, unabhängigen Beschwerdestellen, die im Rahmen von alternativen Streitbeilegungsverfahren des Privatsektors angeboten werden, von betroffenen Personen, Unternehmen aus der EU und den USA und anderen Dritten).

— Das Ministerium kann auch andere geeignete Abhilfemaßnahmen ergreifen. Falsche Angaben gegenüber dem Ministerium unterliegen dem False Statements Act (18 U.S.C. § 1001).

Regelmäßige Durchführung der von Amts wegen vorgenommenen Kontrollen der Einhaltung und Bewertungen des Datenschutzrahmens

— Das Ministerium wird die Einhaltung der Grundsätze durch Organisationen, die dem Datenschutzrahmen EU-USA angehören, fortlaufend überwachen, um Probleme zu ermitteln, die Folgemaßnahmen rechtfertigen könnten. Insbesondere wird das Ministerium von Amts wegen routinemäßige Stichprobenkontrollen bei nach dem Zufallsprinzip ausgewählten Organisationen, die dem Datenschutzrahmen EU-USA angehören, sowie Ad-hoc-Stichprobenkontrollen bei bestimmten Organisationen, die dem Datenschutzrahmen EU-USA angehören, durchführen, wenn potenzielle Mängel bei der Einhaltung der Grundsätze festgestellt werden (z. B. potenzielle Mängel bei der Einhaltung der Grundsätze, die dem Ministerium von Dritten zur Kenntnis gebracht werden), um zu überprüfen, dass a) die zuständige(n) Kontaktstelle(n) für die Bearbeitung von Beschwerden, Auskunftsbegehren und anderen Fragen im Zusammenhang mit dem Datenschutzrahmen EU-USA vorhanden ist (sind), b) gegebenenfalls die öffentlich zugänglichen Datenschutzbestimmungen der Organisation sowohl auf der öffentlichen Website der Organisation als auch über einen Hyperlink auf der Datenschutzrahmen-Liste öffentlich einsehbar sind, c) die Datenschutzbestimmungen der Organisation weiterhin die in den Grundsätzen beschriebenen Anforderungen an die Selbstzertifizierung erfüllen und d) die von der Organisation benannte unabhängige Beschwerdestelle für die Behandlung von Beschwerden im Rahmen des Datenschutzrahmens EU-USA zur Verfügung steht. Das Ministerium wird auch aktiv die Medien auf Berichte hin überwachen, die glaubwürdige Beweise für die Nichteinhaltung der Grundsätze durch Organisationen enthalten, die dem Datenschutzrahmen EU-USA angehören.

— Im Rahmen der Überprüfung der Einhaltung der Grundsätze wird das Ministerium eine Organisation, die dem Datenschutzrahmen EU-USA angehört, auffordern, einen detaillierten Fragebogen auszufüllen und dem Ministerium zu übermitteln, wenn a) dem Ministerium ernst gemeinte Beschwerden über die Einhaltung der Grundsätze durch eine Organisation zugegangen sind, b) die Organisation keine zufriedenstellende Antwort auf eine mit dem Datenschutzrahmen EU-USA verbundene Anfrage des Ministeriums übermittelt oder c) deutliche Anhaltspunkte darauf schließen lassen, dass eine Organisation ihren Zusagen im Zusammenhang mit dem Datenschutzrahmen EU-USA nicht nachkommt. Hat das Ministerium einen solchen detaillierten Fragebogen an eine Organisation geschickt und die Organisation antwortet nicht zufriedenstellend auf den Fragebogen, informiert das Ministerium die Organisation darüber, dass das Ministerium die Angelegenheit gegebenenfalls an die zuständige Behörde für mögliche Durchsetzungsmaßnahmen verweist, wenn das Ministerium keine rechtzeitige und zufriedenstellende Antwort von der Organisation erhält. Das Ministerium informiert die Organisation mittels der Kontaktkanäle, die die Organisation dem Ministerium zur Verfügung gestellt hat, oder gegebenenfalls auf andere geeignete Weise. Wenn die Organisation nicht rechtzeitig und zufriedenstellend antwortet, wird das Ministerium die Sache von Amts wegen an die FTC, das Verkehrsministerium oder eine andere zuständige Vollzugsbehörde weiterleiten oder andere angemessene Maßnahmen ergreifen, um die Einhaltung der Vorschriften sicherzustellen. Das Ministerium stimmt diese Einhaltungskontrollen bei Bedarf mit den zuständigen Datenschutzbehörden ab und

— bewertet regelmäßig die Verwaltung und Überwachung des Datenschutzrahmen-Programms, um sicherzustellen, dass die Kontrollbemühungen, einschließlich der Bemühungen durch den Einsatz von Suchwerkzeugen (z. B. zur Überprüfung fehlerhafter Links zu Datenschutzbestimmungen von Organisationen, die dem Datenschutzrahmen EU-USA angehören), für bestehende und neue Problemfelder angemessen sind.

Überarbeitung der Website zum Datenschutzrahmen mit Blick auf ausgewählte Zielgruppen

Das Ministerium überarbeitet die Website zum Datenschutzrahmen, um sie auf folgende Zielgruppen auszurichten: EU-Bürger, EU-Unternehmen, US-Unternehmen und Datenschutzbehörden. Durch die Aufnahme von speziell auf EU-Bürger und EU-Unternehmen zugeschnittenen Materialien kann die Transparenz auf vielfältige Weise gesteigert werden. In Bezug auf EU-Bürger wird auf der Website Folgendes klar erläutert: 1) die Rechte, die im Datenschutzrahmen EU-USA für EU-Bürger vorgesehen sind, 2) die Rechtsbehelfe, die EU-Bürgern zur Verfügung stehen, wenn sie der Ansicht sind, dass eine Organisation gegen ihre Verpflichtung zur Einhaltung der Grundsätze verstoßen hat und 3) Hinweise zur Selbstzertifizierung eines Unternehmens im Rahmen des Datenschutzrahmens EU-USA. Im Hinblick auf EU-Unternehmen wird die Überprüfung der folgenden Aspekte erleichtert: 1) ob eine Organisation dem Datenschutzrahmen EU-USA angehört, 2) welche Informationen von der Selbstzertifizierung einer Organisation im Rahmen des Datenschutzrahmens EU-USA abgedeckt werden, 3) welche Datenschutzbestimmungen auf diese Informationen zur Anwendung kommen und 4) anhand welcher Methoden eine Organisation die Einhaltung der Grundsätze prüft. Im Hinblick auf US-Unternehmen werden folgende Punkte klar erläutert: 1) die Vorteile der Beteiligung am Datenschutzrahmen EU-USA, 2) die Modalitäten für den Beitritt zum Datenschutzrahmen EU-USA sowie für die erneute Zertifizierung und das Ausscheiden aus dem Datenschutzrahmen EU-USA, und 3) die Verwaltung und Durchsetzung des Datenschutzrahmens EU-USA durch die Vereinigten Staaten. Die Aufnahme von speziell an die Datenschutzbehörden gerichteten Materialien (z. B. Informationen über die spezielle Kontaktstelle des Ministeriums für Datenschutzbehörden und ein Hyperlink zu Inhalten im Zusammenhang mit den Grundsätzen auf der FTC-Website) wird sowohl die Zusammenarbeit als auch die Transparenz erleichtern. Das Ministerium wird außerdem auf Ad-hoc-Basis mit der Kommission und dem Europäischen Datenschutzausschuss („EDSA“) zusammenarbeiten, um zusätzliches, aktuelles Material (z. B. Antworten auf häufig gestellte Fragen) für die Website zum Datenschutzrahmen zu entwickeln, wenn solche Informationen die effiziente Verwaltung und Überwachung des Datenschutzrahmen-Programms erleichtern würden.

Erleichterung der Zusammenarbeit mit den Datenschutzbehörden

Für den Ausbau der Kooperationsmöglichkeiten mit den Datenschutzbehörden unterhält das Ministerium eine spezielle Kontaktstelle, 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. Nach Eingang ist das Ministerium nach besten Kräften um eine Klärung der Beschwerde mit der dem Datenschutzrahmen EU-USA angehörenden Organisation bemüht. Innerhalb von 90 Tagen nach Eingang der Beschwerde unterrichtet das Ministerium die Datenschutzbehörde über den aktuellen Sachstand. Die spezielle Kontaktstelle wird auch Hinweise auf Organisationen entgegennehmen, die fälschlicherweise behaupten, am Datenschutzrahmen EU-USA beteiligt zu sein. In der speziellen Kontaktstelle werden alle von den Datenschutzbehörden an das Ministerium übermittelten Fälle erfasst, und das Ministerium erstellt bei der gemeinsamen Überprüfung einen Bericht, der in aggregierter Form die im Laufe des Jahres bei ihm eingegangenen Beschwerden enthält. Die spezielle Kontaktstelle unterstützt Datenschutzbehörden bei der Erfassung von Informationen zur Selbstzertifizierung oder zum bisherigen Beitritt einer Organisation zum Datenschutzrahmen EU-USA und beantwortet Anfragen der Datenschutzbehörden zur Umsetzung der spezifischen Anforderungen des Datenschutzrahmens EU-USA. Das Ministerium wird auch mit der Kommission und dem EDSA in Bezug auf verfahrenstechnische und administrative Aspekte des Gremiums der Datenschutzbehörden zusammenarbeiten, einschließlich der Festlegung geeigneter Verfahren für die Verteilung der Mittel, die durch die Gebühren des Gremiums der Datenschutzbehörden eingenommen werden. Wir hoffen, dass die Kommission mit dem Ministerium zusammenarbeiten wird, um die Lösung von Problemen zu erleichtern, die im Zusammenhang mit diesen Verfahren auftreten können. Darüber hinaus stellt das Ministerium den Datenschutzbehörden Material zum Datenschutzrahmen EU-USA 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 Datenschutzrahmen und die damit verbundenen Rechte und Pflichten kann die Erkennung von Problemen unmittelbar nach ihrem Auftreten begünstigen und die Einleitung geeigneter Abhilfemaßnahmen begünstigen.

Erfüllung der in Anhang I der Grundsätze eingegangenen Verpflichtungen

Das Ministerium wird seinen Verpflichtungen gemäß Anhang I der Grundsätze nachkommen und unter anderem eine Liste von Schiedsrichtern führen, die gemeinsam mit der Kommission auf der Grundlage ihrer Unabhängigkeit, Integrität und Sachkenntnis ausgewählt werden, und gegebenenfalls den vom Ministerium ausgewählten Dritten unterstützen, der die Schiedsverfahren gemäß Anhang I der Grundsätze durchführt und den dort genannten Schiedsfonds verwaltet. ([3]) Das Ministerium wird mit dem Dritten zusammenarbeiten, um unter anderem zu überprüfen, ob der Dritte eine Website mit Informationen über das Schiedsverfahren unterhält, darunter die Informationen über 1) die Einleitung des Verfahrens und die Einreichung von Unterlagen, 2) die vom Ministerium verwaltete Liste der Schiedsrichter und wie die Schiedsrichter aus dieser Liste auszuwählen sind, 3) die anwendbaren Schiedsverfahren und den Verhaltenskodex für Schiedsrichter, die vom Ministerium und der Kommission angenommen wurden ([4]) und (4) die Erhebung und Zahlung der Schiedsrichtergebühren. Darüber hinaus wird das Ministerium mit dem Dritten zusammenarbeiten, um die Tätigkeit des Schiedsfonds regelmäßig zu überprüfen, einschließlich der Notwendigkeit einer Anpassung des Beitrags oder die Obergrenzen (d. h. Höchstbeträge) für die Schiedskosten, und unter anderem die Anzahl der Schiedsverfahren sowie deren Kosten und Dauer prüfen, und zwar im Einvernehmen, dass den dem Datenschutzrahmen EU-USA angehörenden Organisationen keine übermäßige finanzielle Belastung auferlegt wird. Das Ministerium wird die Kommission über das Ergebnis dieser Überprüfungen mit dem Dritten unterrichten und die Kommission im Voraus über etwaige Anpassungen der Höhe der Beiträge informieren.

Durchführung gemeinsamer Überprüfungen der Funktionsweise des Datenschutzrahmens EU-USA

Das Ministerium und andere Stellen werden in regelmäßigen Abständen Sitzungen mit der Kommission, interessierten Datenschutzbehörden und geeigneten Vertretern des EDSA abhalten, bei denen das Ministerium über den aktuellen Stand des Datenschutzrahmens EU-USA berichten wird. Auf den Sitzungen werden aktuelle Fragen im Zusammenhang mit der Funktionsweise, Umsetzung, Überwachung und Durchsetzung des Datenschutzrahmen-Programms erörtert. Gegebenenfalls können bei den Sitzungen auch verwandte Themen erörtert werden, z. B. andere Datenübermittlungsmechanismen, die von den Garantien des Datenschutzrahmens EU-USA profitieren.

([3]) Das International Centre for Dispute Resolution (ICDR), die internationale Abteilung der American Arbitration Association (AAA) (zusammen „ICDR-AAA“), wurde vom Handelsministerium mit der Durchführung von Schiedsverfahren gemäß den Grundsätzen und der Verwaltung des in Anhang I der Grundsätze genannten Schiedsfonds beauftragt.

([4]) Am 15. September 2017 einigten sich das Ministerium und die Kommission auf die Annahme einer Reihe von Schiedsregeln, mit denen die in Anhang I der Grundsätze beschriebenen verbindlichen Schiedsverfahren geregelt werden, sowie auf einen Verhaltenskodex für Schiedsrichter, der den allgemein anerkannten ethischen Standards für Handelsschiedsrichter und Anhang I der Grundsätze entspricht. Das Ministerium und die Kommission haben vereinbart, die Schiedsregeln und den Verhaltenskodex an die Aktualisierungen des Datenschutzrahmens EU-USA anzupassen, und das Ministerium wird mit dem ICDR-AAA zusammenarbeiten, um diese Aktualisierungen vorzunehmen.

Aktualisierung von Gesetzen

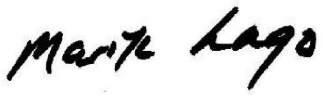
Das Ministerium wird die Kommission in angemessener Weise über wesentliche Änderungen des Rechts der Vereinigten Staaten unterrichten, wenn sie für den Datenschutzrahmen EU-USA relevant sind und den Datenschutz sowie die Beschränkungen und Schutzvorkehrungen für den Zugriff staatlicher Behörden auf personenbezogene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

Staatlicher Zugriff auf personenbezogene Daten

Die Vereinigten Staaten haben die Executive Order 14086 mit dem Titel „Enhancing Safeguards for United States Signals Intelligence Activities" und Titel 28 CFR Teil 201 zur Änderung der Vorschriften des Justizministeriums erlassen, um das Datenschutzüberprüfungsgericht (Data Protection Review Court, „DPRC") einzurichten, die einen starken Schutz personenbezogener Daten im Hinblick auf den staatlichen Zugriff auf Daten für Zwecke der nationalen Sicherheit bieten. Der vorgesehene Schutz umfasst die Stärkung des Schutzes der Privatsphäre und der bürgerlichen Freiheiten, um sicherzustellen, dass die Maßnahmen im Zusammenhang mit der US-Signalaufklärung zur Verfolgung bestimmter nationaler Sicherheitsziele notwendig und verhältnismäßig sind, die Einrichtung einer neuen Beschwerdestelle mit unabhängigen und verbindlichen Befugnissen und Stärkung der bestehenden strengen und mehrstufigen Aufsicht über die US-Signalaufklärung. Dieser Schutz bietet EU-Bürgern einen neuen, mehrstufigen Rechtsbehelfsmechanismus, der auch ein unabhängiges DPRC umfasst, das sich aus Personen zusammensetzt, die nicht der US-Regierung angehören und die uneingeschränkte Befugnis haben, über Beschwerden zu entscheiden und gegebenenfalls Abhilfemaßnahmen anzuordnen. Das Ministerium führt eine Liste der EU-Bürger, die eine qualifizierte Beschwerde gemäß Executive Order 14086 und Titel 28 CFR Teil 201 eingereicht haben. Fünf Jahre nach dem Datum dieses Schreibens und danach alle fünf Jahre wird sich das Ministerium mit den zuständigen Stellen in Verbindung setzen, um festzustellen, ob die Informationen über die Überprüfung qualifizierter Beschwerden oder die Überprüfung von Anträgen auf Überprüfung, die dem DPRC vorgelegt wurden, freigegeben wurden. Wenn solche Informationen freigegeben werden, wird das Ministerium mit der zuständigen Datenschutzbehörde zusammenarbeiten, um die EU-Bürger zu informieren. Diese Verbesserungen bestätigen, dass personenbezogene Daten aus der EU, die in die Vereinigten Staaten übermittelt werden, in einer Weise verarbeitet werden, die den rechtlichen Anforderungen der EU in Bezug auf den Zugang von Behörden zu Daten entspricht.

Ausgehend von den Grundsätzen, der Executive Order 14086, dem Titel 28 CFR Teil 201 und den Begleitschreiben und -materialien, einschließlich der Zusagen des Ministeriums zur Verwaltung und Überwachung des Datenschutzrahmen-Programms, rechnen wir damit, dass die Kommission den Datenschutzrahmen EU-USA als ausreichend erachtet, um einen Schutz im Sinne der EU-Rechtsvorschriften zu gewährleisten, und dass Daten weiterhin an Organisationen übermittelt werden, die dem Datenschutzrahmen EU-USA angehören. Wir gehen auch davon aus, dass Übermittlungen an US-Organisationen, die auf der Grundlage von EU-Standardvertragsklauseln oder verbindlichen unternehmensinternen Vorschriften der EU erfolgen, durch die Bedingungen dieser Vereinbarungen weiter erleichtert werden.

Mit freundlichen Grüßen



Marisa LAGO

ANHANG IV

UNITED STATES OF AMERICA
Federal Trade Commission
WASHINGTON, D.C. 20580

Office of the Chair

9. Juni 2023

Didier Reynders
Kommissar für Justiz
Europäische Kommission
Rue de la Loi / Wetstraat 200
1049 Brüssel
Belgien

Sehr geehrter Herr Reynders,

die Federal Trade Commission der Vereinigten Staaten („FTC“) begrüßt die Gelegenheit, ihre Rolle bei der Durchsetzung der Grundsätze des Datenschutzrahmens EU-USA („Datenschutzrahmen EU-USA“) zu erläutern. Die FTC setzt sich seit Langem für den grenzüberschreitenden Schutz der Verbraucher und der Privatsphäre ein, und wir sind entschlossen, die Aspekte dieses Rahmens für den gewerblichen Sektor durchzusetzen. Die FTC hat eine solche Rolle seit dem Jahr 2000 im Zusammenhang mit der Safe Harbor-Regelung zwischen den USA und der EU und zuletzt seit 2016 im Zusammenhang mit dem EU-US-Datenschutzschild übernommen. ([1]) Am 16. Juli 2020 erklärte der Gerichtshof der Europäischen Union („EuGH“) den Angemessenheitsbeschluss der Europäischen Kommission, der dem EU-US-Datenschutzschild zugrunde liegt, aus anderen Gründen als den von der FTC durchgesetzten Handelsgrundsätzen für ungültig. Seitdem haben die USA und die Europäische Kommission den Datenschutzrahmen EU-USA ausgehandelt, um dem EuGH-Urteil Rechnung zu tragen.

Mit diesem Schreiben bekräftige ich das Engagement der FTC für eine konsequente Durchsetzung der Grundsätze des Datenschutzrahmens EU-USA. Insbesondere bekräftigen wir unser Engagement in drei Schlüsselbereichen: 1) der vorrangigen Behandlung von überwiesenen Fällen und Ermittlungen, 2) der Erwirkung und Überwachung von Anordnungen und 3) der Zusammenarbeit mit den EU-Datenschutzbehörden bei der Durchsetzung.

I. **Einleitung**

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 Rechtsvorschriften Geltung und sorgt damit für den Schutz und die Sicherheit von Verbrauchern und Verbraucherdaten. Das wichtigste von ihr durchzusetzende Gesetz, der FTC Act, untersagt „unlautere“ oder

([1]) Schreiben der Vorsitzenden Edith Ramirez an Věra Jourová, Kommissarin für Justiz, Verbraucher und Gleichstellung der Europäischen Kommission, über die Durchsetzung des neuen EU-US-Datenschutzschilds durch die Federal Trade Commission (29. Februar 2016), *abrufbar unter* https://www.ftc.gov/legal-library/browse/cases-proceedings/public-statements/letter-chairwoman-edith-ramirez-vera-jourova-commissioner-justice-consumers-gender-equality-european. Die FTC hat sich bereits in der Vergangenheit verpflichtet, die Safe-Harbor-Regelung zwischen den USA und der EU durchzusetzen. Schreiben von Robert Pitofsky, Vorsitzender der FTC, an John Mogg, Direktor der GD Binnenmarkt, Europäische Kommission (14. Juli 2000), *abrufbar unter* https://www.federalregister.gov/documents/2000/07/24/00-18489/issuance-of-safe-harbor-principles-and-transmission-to-european-commission. Das vorliegende Schreiben ersetzt diese früheren Verpflichtungen.

„irreführende" Handlungen oder Praktiken, die den Geschäftsverkehr betreffen oder sich darauf auswirken. ([2]) 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. ([3])

Die FTC hat in letzter Zeit auch eine Reihe von Initiativen zur Verstärkung ihrer Arbeit im Bereich des Schutzes der Privatsphäre ergriffen. Im August 2022 kündigte die FTC an, dass sie Regeln zur Bekämpfung schädlicher kommerzieller Überwachung und unzureichender Datensicherheit erwäge. ([4]) Ziel des Projekts ist es, eine fundierte öffentliche Dokumentation zu erstellen, die Aufschluss darüber gibt, ob die FTC Regeln zu kommerziellen Überwachungs- und Datensicherheitspraktiken erlassen sollte und wie solche Regeln gegebenenfalls aussehen sollten. Wir freuen uns über Anmerkungen von EU-Interessenträgern zu dieser und anderen Initiativen.

Unsere „PrivacyCon"-Konferenzen bringen weiterhin führende Wissenschaftler zusammen, um die neuesten Forschungsergebnisse und Trends im Zusammenhang mit dem Schutz der Privatsphäre der Verbraucher und der Datensicherheit zu erörtern. Wir haben auch die Fähigkeit der FTC verbessert, mit den technologischen Entwicklungen Schritt zu halten, die im Mittelpunkt unserer Arbeit zum Schutz der Privatsphäre stehen, indem wir ein wachsendes Team von Technologen und interdisziplinären Forschern aufgebaut haben. Wie Sie wissen, haben wir auch einen gemeinsamen Dialog mit Ihnen und Ihren Kolleginnen und Kollegen in der Europäischen Kommission über datenschutzrelevante Themen wie dunkle Muster und Geschäftsmodelle, die durch eine allgegenwärtige Datenerfassung gekennzeichnet sind, angekündigt. ([5]) Darüber hinaus haben wir vor Kurzem einen Bericht an den Kongress herausgegeben, in dem wir vor den Gefahren warnen, die mit dem Einsatz künstlicher Intelligenz („KI") zur Bekämpfung der vom Kongress identifizierten Online-Bedrohungen verbunden sind. In dem Bericht wurden Bedenken hinsichtlich Ungenauigkeit, Voreingenommenheit, Diskriminierung und heimlicher kommerzieller Überwachung geäußert. ([6])

b) **US-Rechtsschutz zugunsten der EU-Verbraucher**

Der Datenschutzrahmen EU-USA ist im Gesamtzusammenhang des US-Datenschutzes zu sehen, der auch EU-Verbraucher auf verschiedene Weise schützt. 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, die zum Schutz inländischer Verbraucher zur Verfügung stehen. ([7])

Die FTC setzt ferner weitere zielgerichtete Gesetze durch, die Bestimmungen zum Schutz von Verbrauchern außerhalb der USA beinhalten, darunter das 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 Kindern unter 13 Jahren erfassen, die Eltern davon in Kenntnis setzen und deren nachprüfbare Zustimmung einholen müssen. In den USA betriebene Websites und Dienste, die dem COPPA

([2]) 15 U.S.C. § 45(a). Die FTC ist nicht für Fragen der Strafverfolgung oder der nationalen Sicherheit zuständig. 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. In einigen Fällen deckt sich die Zuständigkeit der FTC mit der 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.

([3]) *Siehe* FTC, Datenschutz und Sicherheit, https://www.ftc.gov/business-guidance/privacy-security.

([4]) *Siehe* Pressemitteilung, Federal Trade Commission, FTC Explores Rules Cracking Down on Commercial Surveillance and Lax Data Security Practices (11. August 2022), https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-explores-rules-cracking-down-commercial-surveillance-lax-data-security-practices.

([5]) *Siehe* Gemeinsame Presseerklärung von Didier Reynders, Kommissar für Justiz der Europäischen Kommission, und Lina Khan, Vorsitzende der Federal Trade Commission der Vereinigten Staaten (30. März 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/Joint%20FTC-EC%20Statement%20informal%20dialogue%20consumer%20protection%20issues.pdf.

([6]) *Siehe* Pressemitteilung, Federal Trade Commission, FTC Report Warns About Using Artificial Intelligence to Combat Online Problems (16. Juni 2022), https://www.ftc.gov/news-events/news/press-releases/2022/06/ftc-report-warns-about-using-artificial-intelligence-combat-online-problems.

([7]) 15 U.S.C. § 45(a)(4)(B). Darüber hinaus umfassen „unlautere oder irreführende Handlungen oder Praktiken" solche Handlungen oder Praktiken, die den Außenhandel betreffen und i) tatsächlich oder wahrscheinlich einen nach vernünftigem Ermessen vorhersehbaren Schaden in den Vereinigten Staaten bewirken oder ii) bei denen entscheidungserhebliches Verhalten in den Vereinigten Staaten eine Rolle spielt. 15 U.S.C. § 45(a)(4)(A).

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. 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) **FTC-Durchsetzungsmaßnahmen**

Die FTC hat sowohl Verfahren nach der Safe-Harbor-Regelung als auch nach dem EU-US-Datenschutzschild eingeleitet und den EU-Datenschutzschild auch nach der Aufhebung des Angemessenheitsbeschlusses, auf den sich der EU-US-Datenschutzschild stützt, durch den EuGH weiter durchgesetzt. ([8]) Mehrere der jüngsten Beschwerden der FTC enthielten Vorwürfe, dass Unternehmen gegen die Bestimmungen des EU-US-Datenschutzschilds verstoßen hätten, darunter die Verfahren gegen Twitter ([9]), CafePress ([10]) und Flo. ([11]) Im Rahmen der Zwangsvollstreckung gegen Twitter verhängte die FTC eine Geldbuße in Höhe von 150 Mio. USD gegen Twitter, weil das Unternehmen mit seinen Praktiken, von denen mehr als 140 Mio. Kunden betroffen waren, gegen eine frühere FTC-Verfügung verstoßen hatte, darunter auch gegen Grundsatz 5 des EU-US-Datenschutzschilds (Datenintegrität und Zweckbindung). Darüber hinaus verlangt die FTC, dass Twitter seinen Nutzern die Nutzung sicherer Multi-Faktor-Authentifizierungsmethoden ermöglicht, bei denen die Nutzer ihre Telefonnummer nicht angeben müssen.

In der Rechtssache CafePress warf die FTC dem Unternehmen vor, sensible Verbraucherdaten nicht zu schützen, eine schwerwiegende Verletzung des Schutzes personenbezogener Daten zu verschleiern und gegen die Grundsätze 2 (Wahlmöglichkeit), 4 (Sicherheit) und 6 (Auskunftsrecht) des EU-US-Datenschutzschilds zu verstoßen. Gemäß der Anordnung der FTC muss das Unternehmen die unzureichenden Authentifizierungsmaßnahmen durch eine Multi-Faktor-Authentifizierung ersetzen, die Menge der erhobenen und gespeicherten Daten erheblich einschränken, die Sozialversicherungsnummern verschlüsseln und die Informationssicherheitsprogramme durch einen Dritten bewerten lassen und der FTC eine Kopie zur Veröffentlichung vorlegen.

In der Rechtssache Flo behauptete die FTC, dass die Fruchtbarkeits-App Gesundheitsinformationen der Nutzer an Drittanbieter von Datenanalysen weitergegeben habe, obwohl sie sich zur Geheimhaltung dieser Informationen verpflichtet hatte. Die Beschwerde der FTC bezog sich insbesondere auf die Interaktionen des Unternehmens mit EU-Verbrauchern und darauf, dass Flo gegen die Grundsätze 1 (Informationspflicht), 2 (Wahlmöglichkeit), 3 (Verantwortlichkeit für die Weitergabe) und 5 (Datenintegrität und Zweckbindung) des EU-US-Datenschutzschilds verstoßen habe. Gemäß der FTC-Verfügung ist Flo unter anderem verpflichtet, die betroffenen Nutzer über die Weitergabe ihrer personenbezogenen Daten zu informieren und Dritte, die Gesundheitsdaten der Nutzer erhalten haben, anzuweisen, diese Daten zu vernichten. Die Verfügungen der FTC schützen alle Verbraucher weltweit, die Kunden eines US-Unternehmens sind, und nicht nur jene unter ihnen, die Beschwerden eingereicht haben.

Viele frühere Fälle der Durchsetzung der Safe-Harbor-Regelung und des EU-US-Datenschutzschilds betrafen Organisationen, die eine erste Selbstzertifizierung durch das Handelsministerium abgeschlossen hatten, es aber versäumt hatten, ihre jährliche Selbstzertifizierung aufrechtzuerhalten, während sie sich weiterhin als aktuelle Beteiligte ausgaben. Andere Fälle betrafen falsche Behauptungen über die Beteiligung von Organisationen, die nie eine erste Selbstzertifizierung durch das Handelsministerium abgeschlossen hatten. Auch in Zukunft werden wir unsere proaktiven Durchsetzungsbemühungen auf die Arten von Verstößen gegen den Datenschutzrahmen konzentrieren, die in Fällen wie Twitter, CafePress und Flo geltend gemacht wurden. Inzwischen verwaltet und überwacht das Handelsministerium den Selbstzertifizierungsprozess, führt die einschlägige Liste der Organisationen, die dem Datenschutzrahmen EU-USA angehören, und befasst sich mit anderen Fragen im Zusammenhang mit der Beteiligung an dem Programm. ([12]) Wichtig ist, dass Organisationen, die sich auf die Beteiligung am Datenschutzrahmen EU-USA berufen, auch dann der materiellen Durchsetzung der Grundsätze des Datenschutzrahmens unterliegen können, wenn sie keine Selbstzertifizierung durch das Handelsministerium vornehmen oder aufrechterhalten.

([8]) *Siehe* Anlage A mit einer Liste der Fälle der FTC im Zusammenhang mit der Safe-Harbor-Regelung und dem Datenschutzschild.

([9]) *Siehe* Pressemitteilung, Federal Trade Commission, FTC Charges Twitter with Deceptively Using Account Security Data to Sell Targeted Ads (25. Mai 2022), https://www.ftc.gov/news-events/news/press-releases/2022/05/ftc-charges-twitter-deceptively-using-account-security-data-sell-targeted-ads.

([10]) *Siehe* Pressemitteilung, Federal Trade Commission, FTC Takes Action Against CafePress for Data Breach Cover Up (15. März 2022), https://www.ftc.gov/news-events/news/press-releases/2022/03/ftc-takes-action-against-cafepress-data-breach-cover.

([11]) *Siehe* Pressemitteilung, Federal Trade Commission, FTC Finalizes Order with Flo Health, a Fertility-Tracking App that Shared Sensitive Health Data with Facebook, Google, and Others (22. Juni 2021), https://www.ftc.gov/news-events/news/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared-sensitive-health-data-facebook-google.

([12]) Schreiben von Marisa Lago, geschäftsführender Staatssekretärin für internationalen Handel, an Herrn Didier Reynders, Kommissar für Justiz, Europäische Kommission (12. Dezember 2022).

II. **Die vorrangige Behandlung von überwiesenen Fällen und Ermittlungen**

Wie bereits im Rahmen der US-EU-Safe-Harbor-Regelung und des EU-US-Datenschutzschilds verpflichtet sich die FTC, überwiesene Fälle des Handelsministeriums und der EU-Mitgliedstaaten im Zusammenhang mit den Grundsätzen des Datenschutzrahmens EU-USA vorrangig zu behandeln. Wir werden auch Fällen Vorrang einräumen, die uns von Selbstregulierungsorganisationen für den Datenschutz und anderen unabhängigen Streitbeilegungsgremien wegen Nichteinhaltung der Grundsätze des Datenschutzrahmens EU-USA überwiesen werden.

Um im Rahmen des Datenschutzrahmens EU-USA die Zuleitung von Fällen aus den EU-Mitgliedstaaten zu erleichtern, hat die FTC ein standardisiertes Verweisungsverfahren eingerichtet und den EU-Mitgliedstaaten eine Anleitung dazu gegeben, welche Art von Informationen für die FTC bei den Ermittlungen zu einem ihr zugeleiteten Fall besonders hilfreich ist. Zu diesem Zweck hat die FTC innerhalb der Behörde eine Kontaktstelle für aus den EU-Mitgliedstaaten weitergeleitete Fälle benannt. 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 das Handelsministerium, ein EU-Mitgliedstaat, eine Selbstregulierungsorganisation oder eine andere unabhängige Beschwerdestelle die FTC mit einer Sache befasst, kann diese eine Reihe von Maßnahmen ergreifen, um die aufgeworfenen Fragen zu klären. Beispielsweise können wir die Datenschutzpolitik der Organisation überprüfen; zusätzliche Informationen direkt bei der Organisation 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 zusätzliche Bemühungen zur Unterrichtung der Marktteilnehmer hilfreich wären; und gegebenenfalls ein Verfahren einleiten.

Neben der vorrangigen Behandlung von Fällen, die vom Handelsministerium, von EU-Mitgliedstaaten, von Selbstregulierungsorganisationen für den Datenschutz oder von anderen unabhängigen Streitbeilegungsgremien ([13]) an die FTC weitergeleitet werden, wird die FTC auch weiterhin auf eigene Initiative erhebliche Verstöße gegen den Datenschutzrahmen EU-USA untersuchen und dabei eine Reihe von Instrumenten einsetzen. Im Rahmen des FTC-Programms zur Untersuchung von Datenschutz- und Sicherheitsproblemen, an denen kommerzielle Organisationen beteiligt sind, hat die Behörde routinemäßig überprüft, ob das betreffende Unternehmen Angaben über seine Beteiligung am EU-US-Datenschutzschild gemacht hat. Wenn dies der Fall war, die Ermittlungen aber offensichtliche Verstöße gegen die Grundsätze des EU-US-Datenschutzschilds erkennen ließen, berücksichtigte die FTC das mutmaßliche Fehlverhalten bei ihren Durchsetzungsmaßnahmen. Wir werden bei der neuen Regelung an diesem offensiven Vorgehen festhalten.

III. **Erwirkung und Überwachung von Anordnungen**

Die FTC bekräftigt zudem die von ihr eingegangene Verpflichtung, die Befolgung von Anordnungen zu erwirken und zu überwachen, um die Einhaltung der Grundsätze des Datenschutzrahmens zu gewährleisten. Wir werden in künftigen die Grundsätze des Datenschutzrahmens EU-USA betreffenden FTC-Verfügungen durch eine Vielzahl geeigneter vorläufiger Anordnungen auf die Einhaltung der Grundsätze hinwirken. Die Nichtbefolgung von Verfügungen der FTC kann zur Folge haben, dass je Verstoß ein Bußgeld von bis zu 50 120 USD und bei anhaltenden Verstößen von 50 120 USD je Tag verhängt wird. ([14]) Wenn sich die Praktiken auf zahlreiche Verbraucher auswirken, kann sich die Summe schnell auf mehrere Millionen 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 allen ihren Verfügungen überwacht die FTC systematisch die Einhaltung der bestehenden Verfügungen, die die Grundsätze des EU-US-Datenschutzschilds betreffen, und erhebt bei Bedarf Klagen zu deren Durchsetzung. ([15]) 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. Schließlich wird die FTC eine Online-Liste der Unternehmen führen, die Verfügungen im Zusammenhang mit der Durchsetzung der Grundsätze des Datenschutzrahmens unterliegen. ([16])

([13]) Auch wenn die FTC keinen Beschwerden einzelner Verbraucher nachgeht oder dabei vermittelt, wird sie Fälle, die ihr von EU-Datenschutzbehörden im Zusammenhang mit den Grundsätzen des Datenschutzrahmens EU-USA 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-Verbrauchern zur Verfügung steht, für eine Beschwerde an die FTC unter https://reportfraud.ftc.gov/ nutzen. Bei Individualbeschwerden, die die Grundsätze des Datenschutzrahmens EU-USA betreffen, ist es aber für EU-Bürger am zweckmäßigsten, wenn sie ihre Beschwerde bei einer Datenschutzbehörde ihres Mitgliedstaats oder einer unabhängigen Beschwerdestelle einreichen.

([14]) 15 U.S.C. § 45(m); 16 C.F.R. § 1.98. Dieser Betrag wird regelmäßig an die Inflation angepasst.

([15]) Im vergangenen Jahr hat die FTC beschlossen, das Verfahren zur Ermittlung von Wiederholungstätern zu straffen. *Siehe* Pressemitteilung, Federal Trade Commission, FTC Authorizes Investigations into Key Enforcement Priorities (1. Juli 2021), https://www.ftc.gov/news-events/news/press-releases/2021/07/ftc-authorizes-investigations-key-enforcement-priorities.

([16]) *Siehe* FTC, Privacy Shield, https://www.ftc.gov/business-guidance/privacy-security/privacy-shield.

IV. **Durchsetzung der Zusammenarbeit mit den EU-Datenschutzbehörden**

Die FTC erkennt die wichtige Rolle an, die Datenschutzbehörden der EU bei der Einhaltung der Grundsätze des Datenschutzrahmens spielen kann, und befürwortet verstärkte Konsultationen und eine engere Zusammenarbeit bei der Durchsetzung. Ein koordinierter Ansatz zur Bewältigung der Herausforderungen, die sich aus den aktuellen digitalen Marktentwicklungen und datenintensiven Geschäftsmodellen ergeben, wird immer wichtiger. Die FTC wird auch mit den vorlegenden Durchsetzungsinstanzen Informationen über die ihr zugeleiteten Sachen austauschen, 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, 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 ([17]). 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.

Über Rücksprachen mit vorlegenden EU-Datenschutzbehörden zu fallspezifischen Fragen hinaus wird die FTC an regelmäßigen Zusammenkünften mit dazu benannten Vertretern des Europäischen Datenschutzausschusses („EDSA“) teilnehmen, um in allgemeiner Form darüber zu diskutieren, wie sich die Zusammenarbeit bei der Durchsetzung verbessern lässt. Die FTC wird sich zudem gemeinsam mit dem Handelsministerium, der Europäischen Kommission und Vertretern des EDSA der regelmäßigen Überprüfung des Datenschutzrahmens EU-USA 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. Die FTC freut sich, ihr Engagement für die Durchsetzung der kommerziellen Aspekte des Datenschutzrahmens EU-USA zu bekräftigen. Wir betrachten unsere Partnerschaft mit unseren Kolleginnen und Kollegen in der EU als ein wesentliches Element des Datenschutzes für die US- und EU-Bürger.

Mit freundlichen Grüßen

Lina Khan

Lina M. KHAN
Vorsitzende, Federal Trade Commission

([17]) 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.

Anlage A

Durchsetzung von dem Datenschutzschild und der Safe-Harbor-Regelung

	Aktenzeichen/FTC-Fall Nr.	Rechtssache	Link
1	FTC-Fall Nr. 2023062 Rechtssache Nr. 3:22-cv-03070 (N. D. Cal.)	US v. **Twitter, Inc.**	Twitter
2	FTC-Fall Nr. 192 3209	In Sachen Residual Pumpkin Entity, LLC, vormals d/b/a **CafePress**, und PlanetArt, LLC, d/b/a **CafePress**	CafePress
3	FTC-Fall Nr. 192 3133 Aktenzeichen C-4747	In der Sache **Flo Health, Inc.**	Flo Health
4	FTC-Fall Nr. 192 3050 Aktenzeichen C-4723	In der Sache **Ortho-Clinical Diagnostics, Inc.**	Ortho-Clinical
5	FTC-Fall Nr. 192 3092 Aktenzeichen C-4709	In der Sache **T&M Protection, LLC**	T&M Protection
6	FTC-Fall Nr. 192 3084 Aktenzeichen C-4704	In der Sache **TDARX, Inc.**	TDARX
7	FTC-Fall Nr. 192 3093 Aktenzeichen C-4706	In der Sache **Global Data Vault, LLC**	Global Data
8	FTC-Fall Nr. 192 3078 Aktenzeichen C-4703	In der Sache **Incentive Services, Inc.**	Incentive Services
9	FTC-Fall Nr. 192 3090 Aktenzeichen C-4705	In der Sache **Click Labs, Inc.**	Click Labs
10	FTC-Fall Nr. 182 3192 Aktenzeichen C-4697	In der Sache **Medable, Inc.**	Medable
11	FTC-Fall Nr. 182 3189 Aktenzeichen 9386	In der Sache NTT Global Data Centers Americas, Inc. als Rechtsnachfolger von **RagingWire Data Centers, Inc.**	RagingWire
12	FTC-Fall Nr. 182 3196 Aktenzeichen C-4702	In der Sache **Thru, Inc.**	Thru
13	FTC-Fall Nr. 182 3188 Aktenzeichen C-4698	In der Sache **DCR Workforce, Inc.**	DCR Workforce
14	FTC-Fall Nr. 182 3194 Aktenzeichen C-4700	In der Sache **LotaData, Inc.**	LotaData
15	FTC-Fall Nr. 182 3195 Aktenzeichen C-4701	In der Sache **EmpiriStat, Inc.**	EmpiriStat

16	FTC-Fall Nr. 182 3193 Aktenzeichen C-4699	In der Sache 214 Technologies, Inc. auch d/b/a **Trueface.ai**	Trueface.ai
17	FTC-Fall Nr. 182 3107 Aktenzeichen 9383	In der Sache **Cambridge Analytica, LLC**	Cambridge Analytica
18	FTC-Fall Nr. 182 3152 Aktenzeichen C-4685	In der Sache **SecureTest, Inc.**	SecurTest
19	FTC-Fall Nr. 182 3144 Aktenzeichen C-4664	In der Sache **VenPath, Inc.**	VenPath
20	FTC-Fall Nr. 182 3154 Aktenzeichen C-4666	In der Sache **SmartStart Employment Screening, Inc.**	SmartStart
21	FTC-Fall Nr. 182 3143 Aktenzeichen C-4663	In der Sache **mResourceLLC**, d/b/a Loop Works LLC	mResource
22	FTC-Fall Nr. 182 3150 Aktenzeichen C-4665	In der Sache **Idmission LLC**	IDmission
23	FTC-Fall Nr. 182 3100 Aktenzeichen C-4659	In der Sache **ReadyTech Corporation**	ReadyTech
24	FTC-Fall Nr. 172 3173 Aktenzeichen C-4630	In der Sache **Decusoft, LLC**	Decusoft
25	FTC-Fall Nr. 172 3171 Aktenzeichen C-4628	In der Sache **Tru Communication, Inc.**	Tru
26	FTC-Fall Nr. 172 3172 Aktenzeichen C-4629	In der Sache **Md7, LLC**	Md7
30	FTC-Fall Nr. 152 3198 Aktenzeichen C-4543	In der Sache **Jhayrmaine Daniels (d/b/a California Skate-Line)**	Jhayrmaine Daniels
31	FTC-Fall Nr. 152 3190 Aktenzeichen C-4545	In der Sache **Dale Jarrett Racing Adventure, Inc.**	Dale Jarrett
32	FTC-Fall Nr. 152 3141 Aktenzeichen C-4540	In der Sache **Golf Connect, LLC**	Golf Connect
33	FTC-Fall Nr. 152 3202 Aktenzeichen C-4546	In der Sache **Inbox Group, LLC**	Inbox Group
34	Aktenzeichen 152 3187 Aktenzeichen C-4542	In der Sache **IOActive, Inc.**	IOActive
35	FTC-Fall Nr. 152 3140 Aktenzeichen C-4549	In der Sache **Jubilant Clinsys, Inc.**	Jubilant
36	FTC-Fall Nr. 152 3199 Aktenzeichen C-4547	In der Sache **Just Bagels Manufacturing, Inc.**	Just Bagels

37	FTC-Fall Nr. 152 3138 Aktenzeichen C-4548	In der Sache **NAICS Association, LLC**	NAICS
38	FTC-Fall Nr. 152 3201 Aktenzeichen C-4544	In der Sache **One Industries Corp.**	One Industries
39	FTC-Fall Nr. 152 3137 Aktenzeichen C-4550	In der Sache **Pinger, Inc.**	Pinger
40	FTC-Fall Nr. 152 3193 Aktenzeichen C-4552	In der Sache **SteriMed Medical Waste Solutions**	SteriMed
41	FTC-Fall Nr. 152 3184 Aktenzeichen C-4541	In der Sache **Contract Logix, LLC**	Contract Logix
42	FTC-Fall Nr. 152 3185 Aktenzeichen C-4551	In der Sache **Forensics Consulting Solutions, LLC**	Forensics Consulting
43	FTC-Fall Nr. 152 3051 Aktenzeichen C-4526	In der Sache **American Int'l Mailing, Inc.**	AIM
44	FTC-Fall Nr. 152 3015 Aktenzeichen C-4525	In der Sache **TES Franchising, LLC**	TES
45	FTC-Fall Nr. 142 3036 Aktenzeichen C-4459	In der Sache **American Apparel, Inc.**	American Apparel
46	FTC-Fall Nr. 142 3026 Aktenzeichen C-4469	In der Sache **Fantage.com, Inc.**	Fantage
47	FTC-Fall Nr. 142 3017 Aktenzeichen C-4461	In der Sache **Apperian, Inc.**	Apperian
48	FTC-Fall Nr. 142 3018 Aktenzeichen C-4462	In der Sache **Atlanta Falcons Football Club, LLC**	Atlanta Falcons
49	FTC-Fall Nr. 142 3019 Aktenzeichen C-4463	In der Sache **Baker Tilly Virchow Krause, LLP**	Baker Tilly
50	FTC-Fall Nr. 142 3020 Aktenzeichen C-4464	In der Sache **BitTorrent, Inc.**	BitTorrent
51	FTC-Fall Nr. 142 3022 Aktenzeichen C-4465	In der Sache **Charles River Laboratories, Int'l**	Charles River
52	FTC-Fall Nr. 142 3023 Aktenzeichen C-4466	In der Sache **DataMotion, Inc.**	DataMotion
53	FTC-Fall Nr. 142 3024 Aktenzeichen C-4467	In der Sache **DDC Laboratories, Inc**., d/b/a DNA Diagnostics Center	DDC
54	FTC-Fall Nr. 142 3028 Aktenzeichen C-4470	In der Sache **Level 3 Communications, LLC**	Level 3

55	FTC-Fall Nr. 142 3025 Aktenzeichen C-4468	In der Sache **PDB Sports, Ltd.**, d/b/a the Denver Broncos Football Club, LLP	Broncos
56	FTC-Fall Nr. 142 3030 Aktenzeichen C-4471	In der Sache **Reynolds Consumer Products, Inc.**	Reynolds
57	FTC-Fall Nr. 142 3031 Aktenzeichen C-4472	In der Sache **Receivable Management Services Corporation**	Receivable Mgmt
58	FTC-Fall Nr. 142 3032 Aktenzeichen C-4473	In der Sache **Tennessee Football, Inc.**	Tennessee Football
59	FTC-Fall Nr. 102 3058 Aktenzeichen C-4369	In der Sache **Myspace LLC**	Myspace
60	FTC-Fall Nr. 092 3184 Aktenzeichen C-4365	In der Sache **Facebook, Inc.**	Facebook
61	FTC-Fall Nr. 092 3081 Civil Action No. 09-CV-5276 (C.D. Cal.)	FTC v. Javian Karnani, und **Balls of Kryptonite, LLC**, d/b/a Bite Size Deals, LLC, and Best Priced Brands, LLC	Balls of Kryptonite
62	FTC-Fall Nr. 102 3136 Aktenzeichen C-4336	In der Sache **Google, Inc.**	Google
63	FTC-Fall Nr. 092 3137 Aktenzeichen C-4282	In der Sache **Myspace LLC**	World Innovators
64	FTC-Fall Nr. 092 3141 Aktenzeichen C-4271	In der Sache **Progressive Gaitways LLC**	Progressive Gaitways
65	FTC-Fall Nr. 092 3139 Aktenzeichen C-4270	In der Sache **Onyx Graphics, LLC**	Onyx Graphics
66	FTC-Fall Nr. 092 3138 Aktenzeichen C-4269	In der Sache **ExpatEdge Partners, LLC**	ExpatEdge
67	FTC-Fall Nr. 092 3140 Aktenzeichen C-4281	In der Sache **Directors Desk LLC**	Directors Desk
68	FTC-Fall Nr. 092 3142 Aktenzeichen C-4272	In der Sache **Collectify LLC**	Collectify

ANHANG V

THE SECRETARY OF TRANSPORTATION
WASHINGTON, DC 20590

6. Juli 2023

Kommissar Didier Reynders
Europäische Kommission
Rue de la Loi / Wetstraat 200
1049 Brüssel
Belgien

Sehr geehrter Herr Reynders,

das US-Verkehrsministerium („Ministerium") freut sich über diese Gelegenheit, näher auf seine Rolle bei der Umsetzung der Grundsätze des Datenschutzrahmens EU-USA („Datenschutzrahmen EU-USA") eingehen zu können. Der Datenschutzrahmen EU-USA wird einen wesentlichen Beitrag zum Schutz personenbezogener Daten, die im Geschäftsverkehr in einer zunehmend vernetzten Welt zur Verfügung gestellt werden, leisten. Er 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.

Das Ministerium hat seine Verpflichtung zur Durchsetzung der Safe-Harbor-Regelung zwischen den USA und der EU erstmals vor über 22 Jahren in einem Schreiben an die Europäische Kommission öffentlich zum Ausdruck gebracht; diese Verpflichtungen wurden in einem Schreiben aus dem Jahr 2016 in Bezug auf den EU-US-Datenschutzschild wiederholt und erweitert. In diesem Schreiben verpflichtete sich das Ministerium, die Grundsätze der Safe-Harbor-Regelung zwischen den USA und der EU und anschließend die Grundsätze des Datenschutzschilds zwischen der EU und den USA mit Nachdruck geltend zu machen. Das Ministerium dehnt diese Verpflichtung auf die Grundsätze des Datenschutzrahmens EU-USA aus, und dieses Schreiben erinnert an diese Verpflichtung.

Insbesondere bestätigt das Ministerium seine Verpflichtung in den folgenden Schlüsselbereichen: 1) vorrangige Behandlung von Ermittlungen bei mutmaßlichen Verstößen gegen die Grundsätze des Datenschutzrahmens EU-USA, 2) angemessene Durchsetzungsmaßnahmen gegen Organisationen, die falsche oder irreführende Behauptungen über die Beteiligung am Datenschutzrahmen EU-USA aufstellen, und 3) Überwachung und Veröffentlichung von Durchsetzungsmaßnahmen im Zusammenhang mit Verstößen gegen die Grundsätze des Datenschutzrahmens EU-USA. 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 Grundsätze des Datenschutzrahmens liefern, um den notwendigen Kontext herzustellen.

1. **Hintergrund**

A. Datenschutzabteilung im Ministerium

Das Ministerium setzt sich konsequent dafür ein, die Geheimhaltung personenbezogener Daten, die Verbraucher den Luftverkehrsgesellschaften oder den Inhabern von Kartenverkaufsstellen überlassen, zu gewährleisten.

Die Handlungsbefugnisse des Ministeriums auf diesem Gebiet ergeben sich aus 49 U.S.C. 41712, zur Verhinderung unlauterer oder irreführender Praktiken im Luftverkehr oder beim Verkauf von Luftverkehrsdienstleistungen durch Luftfahrtunternehmen oder Vermittler. Abschnitt 41712 ist nach dem Vorbild von Abschnitt 5 des Federal Trade Commission (FTC) Act (15 U.S.C. 45) aufgebaut.

Vor Kurzem hat das Verkehrsministerium Vorschriften zur Definition unlauterer und irreführender Praktiken erlassen, die im Einklang mit der Entscheidungspraxis des Verkehrsministeriums und der FTC stehen (Titel 14 CFR § 399.79). 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.

Eine Praxis ist für den Verbraucher „irreführend“, wenn sie geeignet ist, einen unter den gegebenen Umständen vernünftig handelnden Verbraucher in Bezug auf einen wesentlichen Punkt zu täuschen. Ein Sachverhalt ist wesentlich, wenn er das Verhalten oder die Entscheidung des Verbrauchers in Bezug auf ein Produkt oder eine Dienstleistung beeinflusst haben könnte. Abgesehen von diesen allgemeinen Grundsätzen legt das Verkehrsministerium Abschnitt 41712 speziell dahin gehend aus, dass es Beförderern und Fahrkartenverkäufern untersagt ist, 1) gegen die eigenen Datenschutzbestimmungen zu verstoßen, 2) gegen eine vom Ministerium verabschiedete Regel zu verstoßen, wonach bestimmte Datenschutzpraktiken als unlauter oder irreführend eingestuft werden oder 3) den Children's Online Privacy Protection Act (COPPA) oder FTC-Bestimmungen zu seiner Umsetzung zu verletzen oder 4) als Beteiligter am Datenschutzrahmen EU-USA die Grundsätze des Datenschutzrahmens EU-USA nicht einzuhalten. ([1])

Wie oben ausgeführt, verfügt das Ministerium gemäß Bundesgesetz 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 Grundsätzen des Datenschutzrahmens EU-USA bekennt, kann das Ministerium daher von den rechtlichen Befugnissen gemäß Abschnitt 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 Grundsätze des Datenschutzrahmens EU-USA verpflichtet haben, dann würde ein Verstoß gegen diese Grundsätze eine Verletzung der Bestimmungen des Abschnitts 41712 darstellen.

B. Durchsetzungsmaßnahmen

Die Dienststelle des Ministeriums für den Verbraucherschutz in der Luftfahrt (Office of Aviation Consumer Protection, „OACP“) ([2]) untersucht und verfolgt Fälle, nach 49 U.S.C. § 41712. Sie setzt das gesetzliche Verbot unlauterer und irreführender Praktiken gemäß Abschnitt 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. ([3])

Sollte in einem Fall keine angemessene und geeignete Vereinbarung erzielt werden können, ist die OACP 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 Abschnitts 41712 kann Unterlassungsanordnungen nach sich ziehen; der Verstoß gegen diese Anordnungen kann zivilrechtliche Sanktionen in Höhe von bis zu 37 377 USD für jeden Verstoß gegen Abschnitt 41712 zur Folge haben.

Das Ministerium hat nicht das Recht, beschwerdeführenden Privatpersonen Schadensersatz oder finanzielle Entschädigungen zuzuerkennen. Es kann allerdings Vereinbarungen genehmigen, die sich aus von der OACP 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 Grundsätzen des Datenschutzrahmens EU-USA weiterhin so gehandhabt werden, falls die Umstände dies erfordern. Sollte eine Luftverkehrsgesellschaft die Bestimmungen des Abschnitts 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 Abschnitt 41712 gilt das Verbot unlauterer und irreführender Praktiken im Luftverkehr oder beim Verkauf von Flugtickets für amerikanische oder ausländische Luftverkehrsgesellschaften oder Inhaber von Kartenverkaufsstellen. Das Ministerium geht häufig gegen amerikanische und ausländische Luftverkehrsgesellschaften 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.

([1]) https://www.transportation.gov/individuals/aviation-consumer-protection/privacy.

([2]) Ehemals bekannt als Office of Aviation Enforcement and Proceedings (Dienststelle für Rechtsdurchsetzung und Verfahren im Luftverkehr).

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

Im Zusammenhang mit Luftverkehrsgesellschaften setzt das Ministerium darüber hinaus weitere zielgerichtete Gesetze durch, die Bestimmungen zum Schutz von Verbrauchern außerhalb der USA beinhalten, darunter das Children's Online Privacy Act (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 Luftverkehrsgesellschaften, die in den USA geschäftlich tätig sind, gegen das COPPA verstoßen, ist das Ministerium zur Einleitung von Durchsetzungsmaßnahmen befugt.

II. **Durchsetzung der Grundsätze des Datenschutzrahmens EU-USA**

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

A. Vorrangige Ermittlung bei mutmaßlichen Verstößen

Die OACP des Ministeriums prüft alle Beschwerden wegen mutmaßlicher Verstöße gegen den Datenschutzrahmen EU-USA, dazu gehören auch Beschwerden von EU-Datenschutzbehörden und leitet Durchsetzungsmaßnahmen ein, sofern es Anzeichen für einen Verstoß gibt.

Darüber hinaus arbeitet die OACP mit der FTC und dem Handelsministerium zusammen und befasst sich vorrangig mit Beschwerden über den Verstoß beaufsichtigter Unternehmen gegen im Rahmen des Datenschutzrahmens EU-USA eingegangenen Datenschutzverpflichtungen.

Nach Eingang einer Beschwerde über einen mutmaßlichen Verstoß gegen die Grundsätze des Datenschutzrahmens kann die OACP 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 Datenschutzrahmen EU-USA durch die Inhaber von Kartenverkaufsstellen erlangen, 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 Datenschutzrahmens EU-USA.

B. Vorgehen bei falschen oder irreführenden Angaben zur Beteiligung

Das Ministerium bekräftigt seine Zusage, im Falle von Verstößen gegen die Grundsätze des Datenschutzrahmens EU-USA, die auch falsche oder irreführende Angaben zur Beteiligung am Datenschutzrahmen EU-USA 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 Datenschutzrahmens EU-USA bezeichnen oder das Gütesiegel des Datenschutzrahmens EU-USA ohne Genehmigung verwenden.

Wenn im Übrigen eine Organisation in ihren Datenschutzbestimmungen zusichert, dass sie sich an die Grundsätze des Datenschutzrahmens EU-USA hält, reicht die bloße Tatsache, dass sie sich beim Handelsministerium nicht selbst zertifiziert oder ihre Selbstzertifizierung nicht verlängert, nicht aus, um sich der Durchsetzung dieser Zusicherungen durch das Handelsministerium zu entziehen.

C. Überwachung von Durchsetzungsmaßnahmen bei Verstößen gegen den Datenschutzrahmen EU-USA und Unterrichtung der Öffentlichkeit darüber

Darüber hinaus bekräftigt die OACP des Ministeriums ihr Engagement für die Überwachung möglicher Durchsetzungsmaßnahmen, die zur Gewährleistung der Einhaltung der Grundsätze des Datenschutzrahmens EU-USA erforderlich sein können. Insbesondere wenn die Dienststelle eine Anordnung an eine Luftverkehrsgesellschaft oder einen Inhaber einer Kartenverkaufsstelle erlässt, in der künftige Verstöße gegen den Datenschutzrahmen EU-USA und gegen Abschnitt 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 Datenschutzrahmen EU-USA 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 Datenschutzrahmen EU-USA 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.

Mit freundlichen Grüßen

Pete BUTTIGIEG

ANHANG VI

US-Justizministerium

Abteilung für Strafsachen

Amt des stellvertretenden Justizministers WASHINGTON, D.C. 20530

23. Juni 2023

Ana Gallego Torres
Generaldirektorin für Justiz und Verbraucher
Europäische Kommission
Rue Montoyer/Montoyerstraat 59
1049 Brüssel
Belgien

Sehr geehrte Frau Generaldirektorin Gallego Torres,

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]) Alle in diesem Schreiben beschriebenen rechtlichen Verfahren 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 Datenschutzrahmen EU-USA vornehmen, unabhängig von der Staatsangehörigkeit oder dem Wohnort 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.“ Verfassung der Vereinigten Staaten, Zusatzartikel IV. 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 Privatpersonen vor willkürlichen Eingriffen durch Regierungsbeamte.“ 388 U.S. 41, 53 (1967) (unter Berufung auf Camara v. 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

([1]) In diesem Überblick geht es nicht um die Instrumente, die die Strafverfolgungsbehörden beispielsweise bei Ermittlungen im Zusammenhang mit Terrorismus oder Fragen der nationalen Sicherheit nutzen, z. B. National Security Letters (NSLs) für bestimmte Aufzeichnungen zu Kreditdaten, Finanzdaten und elektronischen Teilnehmer- und Transaktionsdaten, 12 U.S.C. § 3414; 15 U.S. C. § 1681u; 15 U.S.C. § 1681v; 18 U.S.C. § 2709, 50 U.S.C. § 3162, und nicht um die elektronische Überwachung, Durchsuchungsbefehle, Geschäftsunterlagen und die anderweitige Erfassung von Daten gemäß dem Foreign Intelligence Surveillance Act, 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 oder Gesetze der Bundesstaaten ein zusätzliches Rechtsschutzniveau vorsehen, das über jenes der Verfassung der USA hinausgeht. Der von den Bundesstaaten gewährte Rechtsschutz muss mindestens dem der US-Verfassung – insbesondere dem vierten Zusatzartikel, aber nicht darauf beschränkt – entsprechen.

Durchführung einer Haussuchung ein gerichtlicher Hausdurchsuchungsbefehl vorliegen muss. Siehe Katz v. United States, 389 U.S. 347, 357 (1967). Die Standards für den Erlass von Anordnungen, wie das Erfordernis eines hinreichenden Verdachts und das Erfordernis der Spezifizität, gelten sowohl für physische Durchsuchungs- und Beschlagnahmeanordnungen als auch für Anordnungen in Bezug auf gespeicherte Inhalte elektronischer Kommunikation gemäß dem Stored Communications Act (siehe unten). In Fällen, in denen diese Vorschrift nicht gilt, unterliegt das Eingreifen des Staates immer noch einer Prüfung der „Zumutbarkeit". Somit gewährleistet also die Verfassung selbst, dass die Regierung der Vereinigten Staaten nicht uneingeschränkt oder willkürlich private Informationen beschlagnahmen darf. ([3])

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 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 einberufen 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 Fed. R. Crim. P. 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, regeln zusätzliche Vorschriften den Zugriff des Staates auf Teilnehmerdaten, Verkehrsdaten und bei Internetdienstanbietern von Telefongesellschaften und anderen dritten Dienstanbietern gespeicherte Kommunikationsinhalte (18 U.S.C. §§ 2701–2712). 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, Internet-Protokoll-Adressen (IP-Adressen) und dazugehörigen Zeitstempel und Rechnungsinformationen einholen zu

([3]) Im Hinblick auf die vorstehend erörterten Grundsätze des vierten Zusatzartikels zum Schutz der Privatsphäre und der Sicherheitsinteressen wenden die US-Gerichte diese Grundsätze regelmäßig auf neue Arten von Ermittlungsinstrumenten der Strafverfolgungsbehörden an, die durch technologische Entwicklungen ermöglicht werden. So entschied der Oberste Gerichtshof im Jahr 2018, dass der Erwerb historischer Standortdaten eines Mobilfunkunternehmens durch die Regierung im Rahmen einer strafrechtlichen Untersuchung über einen längeren Zeitraum eine „Durchsuchung" darstellt, die nach dem vierten Zusatzartikel einer richterlichen Anordnung bedarf. Carpenter v. United States, 138 S. Ct. 2206 (2018).

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. ([4])

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. §§ 2510-2523. Dies kann nur auf richterliche 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 – Fed. R. Crim. P. 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. Eine Person, die einer Durchsuchung unterzogen wird oder deren Eigentum durchsucht wird, kann die Beseitigung von Beweismitteln verlangen, die bei einer rechtswidrigen Durchsuchung erlangt wurden, wenn diese Beweismittel in einem Strafverfahren gegen diese Person verwendet werden. Siehe Mapp v. Ohio, 367 U.S. 643 (1961). Wird ein Dateninhaber aufgrund eines Durchsuchungsbefehls zur Offenlegung von Daten verpflichtet, kann die verpflichtete Partei die Verpflichtung zur Offenlegung als unverhältnismäßige Belastung anfechten. Siehe die Rechtssache In re Application of United States, 610 F.2d 1148, 1157 (3d Cir. 1979) (in der festgestellt wird, dass „ein ordnungsgemäßes Verfahren eine Anhörung zur Frage der Aufwendigkeit erfordert, bevor eine Telefongesellschaft zur Unterstützung eines Durchsuchungsbefehls verpflichtet werden kann") und die Rechtssache In re Application of United States, 616 F.2d 1122 (9th Cir. 1980) (mit der gleichen Schlussfolgerung aufgrund der Aufsichtsbefugnis des Gerichts).

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 (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 (DIOG) (abrufbar unter https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29), eines umfassenden Handbuchs mit detaillierten Erläuterungen zu den Grenzen der Anwendung von Ermittlungsinstrumenten und entsprechenden Hilfestellungen zur Gewährleistung des Schutzes von Bürgerrechten und der Privatsphäre bei sämtlichen Ermittlungen. Weitere Regeln und Richtlinien, die die Ermittlungsaktivitäten von Bundesstaatsanwälten einschränken, sind im Justice Manual niedergelegt, abrufbar unter https://www.justice.gov/jm/justicemanual.

Zivil- und Aufsichtsbehörden (öffentliches Interesse):

([4]) Darüber hinaus ist die Regierung nach Abschnitt 2705(b) des SCA befugt, auf der Grundlage eines nachgewiesenen Bedürfnisses nach Schutz vor Offenlegung eine richterliche Anordnung zu erwirken, die es einem Anbieter von Kommunikationsdiensten untersagt, seine Nutzer freiwillig über den Eingang eines Gerichtsverfahrens nach dem SCA zu informieren. Im Oktober 2017 gab der stellvertretende Justizminister Rod Rosenstein ein Memorandum an Rechtsanwälte und Mitarbeiter des Justizministeriums heraus, das Leitlinien enthält, mit denen sichergestellt werden soll, dass Anträge auf solche Schutzanordnungen auf die spezifischen Fakten und Bedenken einer Ermittlung zugeschnitten sind, und in dem eine allgemeine Obergrenze von einem Jahr für den Zeitraum festgelegt wird, für den ein Antrag die Veröffentlichung verzögern kann. Im Mai 2022 gab die stellvertretende Justizministerin Lisa Monaco zusätzliche Leitlinien zu diesem Thema heraus, die unter anderem interne Genehmigungserfordernisse des Justizministeriums für Anträge auf Verlängerung einer Schutzanordnung über den ursprünglichen Zeitraum von einem Jahr hinaus und die Beendigung von Schutzanordnungen nach Abschluss der Ermittlungen vorsehen.

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. Fed. R. Civ. P. 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. 31 U.S.C. § 5318; 31 C.F.R. Kapitel X. Andere Unternehmen wiederum können sich auf das Fair Credit Reporting Act (Gesetz zur Regelung des Datenschutzes bei Konsumentenkrediten), 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. §§ 3401-3423. 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).

Schlussfolgerung:

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.

Bruce C. Swartz
Deputy Assistant Attorney General and
Counselor for International Affairs

ANHANG VII

AMT DES DIRECTOR OF NATIONAL INTELLIGENCE AMT DES GENERAL COUNSEL

WASHINGTON, DC 20511

9: Dezember 2022

Leslie B. Kiernan
General Counsel
US-Justizministerium
1401 Constitution
Ave., NW Washington, DC 20230

Sehr geehrte Frau Kiernan,

am 7. Oktober 2022 unterzeichnete Präsident Biden die Executive Order 14086 mit dem Titel „Enhancing Safeguards for United States Signals Intelligence Activities", mit der die strengen Datenschutz- und Bürgerrechtsgarantien, die für US-Signalaufklärung gelten, verstärkt werden. Zu diesen Garantien zählen: die Anforderung, dass signalerfassende Aufklärungstätigkeiten aufgezählten legitimen Zielen dienen müssen, das ausdrückliche Verbot derartiger Tätigkeiten zur Verfolgung bestimmter verbotener Ziele, die Einführung innovativer Verfahren, die sicherstellen, dass die signalerfassende Aufklärung diesen legitimen Zielen dient und nicht verbotene Ziele fördert, die Verpflichtung, dass signalerfassende Aufklärungstätigkeiten nur dann durchgeführt werden, wenn auf der Grundlage einer angemessenen Abwägung aller relevanten Faktoren festgestellt wurde, dass sie zur Förderung einer validierten Aufklärungspriorität notwendig sind, und nur in dem Umfang und auf die Art und Weise, die der validierten Aufklärungspriorität, für die sie genehmigt wurden, angemessen sind und die Anweisung an die Nachrichtendienste, ihre Strategien und Verfahren zu aktualisieren, um den in der Executive Order geforderten Garantien im Bereich der Signalaufklärung Rechnung zu tragen. Von besonderer Bedeutung ist, dass mit der Executive Order auch eine unabhängige und verbindliche Beschwerdestelle eingerichtet wird, die es Personen aus den in der Executive Order genannten „qualifizierenden Staaten" ermöglicht, Rechtsbehelfe einzulegen, wenn sie der Auffassung sind, dass sie rechtswidriger signalerfassender Aufklärung der USA ausgesetzt waren, einschließlich Tätigkeiten, die gegen die in der Executive Order enthaltenen Schutzbestimmungen verstoßen.

Die von Präsident Biden erlassene Executive Order 14086 ist das Ergebnis von mehr als einem Jahr dauernden ausführlichen Verhandlungen zwischen Vertretern der Europäischen Kommission („Kommission") und den Vereinigten Staaten; sie enthält die Maßnahmen, die die Vereinigten Staaten ergreifen werden, um ihren Verpflichtungen aus dem Datenschutzrahmen EU-USA nachzukommen. Im Geiste der Zusammenarbeit, die zu diesem Rahmenprogramm geführt hat, gehe ich davon aus, dass Sie von der Kommission zwei Fragenkomplexe erhalten haben, die die Umsetzung der Executive Order durch die Nachrichtendienste betreffen. Gerne beantworte ich diese Fragen mit diesem Schreiben.

Abschnitt 702 des Foreign Intelligence Surveillance Act von 1978 („Abschnitt 702 des FISA")

Der erste Fragenkomplex betrifft Abschnitt 702 des FISA, nachdem es möglich ist, Auslandsaufklärungsdaten durch die gezielte Überwachung von Nicht-US-Bürgern zu sammeln, von denen vermutet wird, dass sie sich außerhalb der Vereinigten Staaten aufhalten, wobei amerikanische Anbieter elektronischer Kommunikationsdienste zur Unterstützung verpflichtet sind. Die Fragen beziehen sich insbesondere auf die Wechselwirkung zwischen dieser Bestimmung und der Executive Order 14086 sowie auf die anderen Garantien, die für Tätigkeiten nach Abschnitt 702 des FISA gelten.

Zunächst können wir bestätigen, dass die Nachrichtendienste die in der Executive Order 14086 festgelegten Garantien auf Tätigkeiten nach Abschnitt 702 des FISA anwenden werden.

Darüber hinaus unterliegt die Anwendung von Abschnitt 702 des FISA durch die Regierung zahlreichen weiteren Garantien. So müssen beispielsweise alle Zertifizierungen nach Abschnitt 702 des FISA sowohl vom Justizminister als auch vom Direktor der Nationalen Nachrichtendienste unterzeichnet werden, und die Regierung muss alle diese Zertifizierungen dem Foreign Intelligence Surveillance Court (Gericht der Vereinigten Staaten betreffend die Überwachung der Auslandsgeheimdienste, „FISC") zur Genehmigung vorlegen, der sich aus unabhängigen Richtern zusammensetzt, die auf Lebenszeit ernannt werden und eine nicht verlängerbare Amtszeit von sieben Jahren haben. Die Zertifizierungen definieren Kategorien von ausländischen Signalaufklärungsdaten, die der gesetzlichen Definition von Daten zur Auslandsaufklärung entsprechen müssen, indem sie auf Nicht-US-Bürger abzielen, von denen angenommen wird, dass sie sich außerhalb der Vereinigten Staaten aufhalten. Die Zertifizierungen umfassten Informationen über den internationalen Terrorismus und andere Themen wie die Beschaffung von Informationen über Massenvernichtungswaffen. Jede jährliche Zertifizierung muss dem FISC in einem Zertifizierungsantragspaket zur Genehmigung vorgelegt werden, das die Zertifizierungen des Justizministers und des Direktors des Nationalen Nachrichtendienstes, eidesstattliche Erklärungen bestimmter Leiter von Nachrichtendiensten sowie für die Regierung verbindliche Verfahren für die zielgenaue Erfassung, Minimierung und Abfrage enthält. Die Verfahren zur zielgenauen Erfassung erfordern unter anderem, dass die Nachrichtendienste auf der Grundlage der Gesamtumstände vernünftigerweise davon ausgehen können, dass die gezielte Datenerhebung wahrscheinlich zur Erhebung der in einer Zertifizierung nach Abschnitt 702 des FISA aufgeführten Daten zur Auslandsaufklärung führen wird.

Darüber hinaus muss der Nachrichtendienst bei der Erhebung von Daten nach Abschnitt 702 des FISA eine schriftliche Erläuterung der Grundlage für seine Einschätzung zum Zeitpunkt der Zielauswahl vorlegen, dass die Zielperson wahrscheinlich über Daten zur Auslandsaufklärung verfügt, die in einer Zertifizierung nach Abschnitt 702 des FISA aufgeführt sind, diese erhält oder weitergibt, bestätigen, dass der in den Verfahren zur zielgenauen Erfassung nach Abschnitt 702 des FISA festgelegte Standard weiterhin erfüllt ist und die Erhebung einstellen, wenn der Standard nicht mehr erfüllt ist. Siehe U.S. Government Submission to Foreign Intelligence Surveillance Court, 2015 Summary of Notable Section 702 Requirements, S. 2–3 (15. Juli 2015).

Die Anforderung an die Nachrichtendienste, ihre Einschätzung, dass die zielgenaue Erfassung nach Abschnitt 702 des FISA den geltenden Standards entspricht, schriftlich festzuhalten und regelmäßig zu bestätigen, erleichtert dem FISC die Aufsicht über die zielgenaue Erfassung. Alle aufgezeichneten Bewertungen und Begründungen der zielgenauen Erfassung werden alle zwei Monate von den Anwälten der Nachrichtenaufsichtsabteilung des Justizministeriums überprüft, die diese Aufsichtsfunktion unabhängig von den Operationen der Auslandsaufklärungsdienste ausüben. Die Abteilung des Justizministeriums, die diese Funktion ausübt, ist dann gemäß einer seit Langem bestehenden Regel des FISC dafür verantwortlich, dem FISC alle Verstöße gegen die geltenden Verfahren zu melden. Diese Dokumentation und die regelmäßigen Treffen zwischen dem FISC und dieser Abteilung des Justizministeriums zur Überwachung der zielgenauen Erfassung nach Abschnitt 702 des FISA ermöglichen es dem FISC, die Einhaltung der Verfahren für zielgenaue Erfassung nach Abschnitt 702 des FISA und anderer Verfahren durchzusetzen und auf andere Weise sicherzustellen, dass die Handlungen der Regierung rechtmäßig sind. Das FISC kann dies auf verschiedene Weise tun, unter anderem durch den Erlass verbindlicher Beschlüsse über Abhilfemaßnahmen, mit denen die Befugnis der Regierung zur zielgenauen Erfassung aufgehoben oder die Datenerhebung nach Abschnitt 702 des FISA geändert oder aufgeschoben wird. Das FISC kann die Regierung auch auffordern, weitere Berichte oder Informationen über die Einhaltung der Verfahren zur zielgenauen Erfassung und anderer Verfahren vorzulegen oder Änderungen an diesen Verfahren zu verlangen.

Die „Sammelerhebung" von Signalaufklärungsdaten

Der zweite Fragenkomplex betrifft die „Sammelerhebung" von Signalaufklärungsdaten, die in der Executive Order 14086 als „die genehmigte Erhebung großer Mengen von Signalaufklärungsdaten aus technischen oder operativen Gründen ohne Verwendung von Unterscheidungsmerkmalen (z. B. ohne Verwendung spezifischer Identifikatoren oder Suchbegriffe definiert wird)".

Zu diesen Fragen ist zunächst festzustellen: Eine Sammelerhebung ist weder nach dem FISA noch nach den National Security Letters zulässig. In Bezug auf die FISA:

— Nach Titel I und III des FISA, durch die elektronische Überwachung und Durchsuchung genehmigt werden, ist (mit wenigen Ausnahmen, z. B. Notfällen) eine richterliche Anordnung erforderlich und es muss in jedem Falle hinreichend Anlass zu der Vermutung bestehen, dass die Zielperson eine ausländische Macht oder ein Vertreter einer ausländischen Macht ist. Siehe 50 U.S.C. §§ 1805-1824.

— Mit dem USA FREEDOM Act von 2015 wurde Titel IV des FISA, der den Einsatz von Geräten zur Rufnummernerfassung aufgrund einer richterlichen Anordnung (außer in Notfällen) erlaubt, dahin gehend geändert, dass die Regierung Anfragen anhand eines „konkreten Suchbegriffs" stellen muss. Siehe 50 U.S.C. § 1842(c)(3).

— Titel V des FISA, der es dem Federal Bureau of Investigation (FBI) erlaubt, bestimmte Arten von Geschäftsunterlagen zu erhalten, erfordert eine richterliche Anordnung auf der Grundlage eines Antrags, in dem dargelegt wird, dass „konkrete und nachvollziehbare Tatsachen vorliegen, die die Annahme rechtfertigen, dass es sich bei der Person, auf die sich die Unterlagen beziehen, um eine ausländische Macht oder einen Vertreter einer ausländischen Macht handelt". Siehe 50 U.S.C. § 1862(b)(2)(B) ([1]).

— Schließlich gestattet Abschnitt 702 des FISA „die gezielte Überwachung von Personen, die sich mit hinreichender Bestimmtheit außerhalb der Vereinigten Staaten aufhalten, um Auslandsaufklärungsdaten zu erlangen". Siehe 50 U.S.C. § 188la(a). Wie das Privacy and Civil Liberties Oversight Board (Stelle zur Überwachung des Schutzes der Privatsphäre und der bürgerlichen Freiheiten) feststellte, besteht die Datenerhebung durch die Regierung gemäß Abschnitt 702 des FISA „ausschließlich darin, einzelne Personen ins Visier zu nehmen und die mit diesen Personen verbundene Kommunikation zu erfassen, von der die Regierung Grund zu der Annahme hat, dass sie bestimmte Arten von Auslandsinformationen erhalten wird", weshalb „das Programm nicht durch die Erfassung einer großen Menge von Kommunikationen funktioniert". Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act,* S. 103 (2. Juli 2014) ([2]).

In Bezug auf die National Security Letters schreibt der USA FREEDOM Act von 2015 einen „konkreten Suchbegriff" für die Verwendung solcher Letters vor. Siehe 12 U.S.C. § 3414(a)(2); 15 U.S.C. § 1681u; 15 U.S.C. § 1681v(a); 18 U.S.C. § 2709(b).

Darüber hinaus bestimmt die Executive Order 14086, dass „[d]ie zielgenaue Erhebung Vorrang haben muss" und dass „eine Sammelerhebung nur dann zulässig ist, wenn die für die Förderung einer validierten Aufklärungspriorität erforderlichen Informationen nicht in angemessener Weise durch eine zielgenaue Erhebung gewonnen werden können." *Siehe* Executive Order 14086, § 2(c)(ii)(A).

Wenn die Nachrichtendienste feststellen, dass die Sammelerhebung diesen Standards entspricht, sieht die Executive Order 14086 zusätzliche Garantien vor. Insbesondere verlangt die Executive Order, dass die Nachrichtendienste bei der Durchführung von Sammelerhebungen „angemessene Methoden und technische Maßnahmen anwenden, um die gesammelten Daten auf das zu beschränken, was für die Förderung einer validierten Aufklärungspriorität erforderlich ist, und um die Erhebung irrelevanter Informationen so gering wie möglich zu halten". *Siehe ebd.* In der Executive Order heißt es außerdem, dass „Tätigkeiten im Rahmen der Signalaufklärung", „zu denen auch die Abfrage von durch Sammelerhebungen gewonnenen Signalen gehört, … nur dann durchgeführt werden, wenn auf der Grundlage einer angemessenen Abwägung aller relevanten Faktoren festgestellt wurde, dass sie zur Förderung einer validierten Aufklärungspriorität notwendig sind." *Siehe ebd.* § 2(a)(ii)(A). In der Executive Order wird dieser Grundsatz weiter konkretisiert, indem festgelegt wird, dass die Nachrichtendienste nur nicht-minimierte Signalaufklärungsdaten abfragen dürfen, die durch eine Sammelerhebung im Rahmen der Verfolgung von sechs zulässigen Zielen und „in Übereinstimmung mit Strategien und Verfahren, die den Auswirkungen der Abfragen auf die Privatsphäre und die bürgerlichen Freiheiten aller Personen, unabhängig von ihrer Staatsangehörigkeit oder ihrem Wohnort", gewonnen wurden. *Siehe ebd.* § 2(c)(iii)(D). Schließlich werden in der Executive Order auch der Umgang mit den erhobenen Daten, ihre Sicherheit und die Zugangskontrolle zu den Daten geregelt. *Siehe ebd.*§ 2(c)(iii)(A) und § 2(c)(iii)(B).

* * * * *

Wir hoffen, Ihnen mit diesen Erläuterungen gedient zu haben. Sollten Sie weitere Fragen zur Umsetzung der Executive Order 14086 durch die US-Nachrichtendienste haben, stehen wir Ihnen gerne zur Verfügung.

([1]) Von 2001 bis 2020 erlaubte Titel V des FISA dem FBI, bei der FISC die Genehmigung zu beantragen, „materielle Objekte" zu erhalten, die für bestimmte genehmigte Ermittlungen relevant sind. *Siehe* USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272, § 215 (2001). Diese Formulierung, die inzwischen nicht mehr benutzt wird und somit keine Gesetzeskraft mehr hat, war die Grundlage dafür, dass die Regierung einst in großem Umfang Metadaten über Telefongespräche sammeln konnte. Noch bevor die Bestimmung außer Kraft trat, wurde sie jedoch durch den USA FREEDOM Act dahin gehend geändert, dass die Regierung verpflichtet ist, einen Antrag an das FISC auf einen „konkreten Suchbegriff" zu stützen. *Siehe* USA FREEDOM Act, Pub. L. No. 114-23, 129 Stat. 268, § I 03 (2015).

([2]) Gemäß den Abschnitten 703 und 704, die es den Nachrichtendiensten gestatten, sich im Ausland aufhaltende US-Bürger zu überwachen, ist (außer in Notfällen) eine richterliche Anordnung erforderlich, und es müssen stets hinreichende Gründe für die Annahme vorliegen, dass die Zielperson eine ausländische Macht, ein Vertreter einer ausländischen Macht oder ein Beamter oder Angestellter einer ausländischen Macht ist. Siehe 50 U.S.C. §§ 1881b, 1881c.

Sincerely,

Christopher C. FONZONE
General Counsel

ANHANG VIII

Abkürzungsverzeichnis

In diesem Beschluss werden die folgenden Abkürzungen verwendet:

AAA	American Arbitration Association (Amerikanischer Verband für Schiedsgerichtsbarkeit)
AGG-DOM	Attorney General Guidelines for Domestic FBI Operations (Leitlinien des Justizministers für Inlandseinsätze des FBI)
APA	Administrative Procedure Act (Verwaltungsverfahrensgesetz)
Beschluss	Durchführungsbeschluss der Kommission gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates über die Angemessenheit des Schutzniveaus für personenbezogene Daten nach dem Datenschutzrahmen EU-USA
CIA	Central Intelligence Agency (Zentraler Nachrichtendienst)
CNSS	Committee on National Security Systems (Ausschuss für nationale Sicherheitssysteme)
DNI	Director of National Intelligence (Direktor des Nationalen Nachrichtendienstes)
DoJ	Department of Justice (Justizministerium)
DPRC	Data Protection Review Court (Datenschutzüberprüfungsgericht)
ECOA	Equal Credit Opportunity Act (Gesetz über die Chancengleichheit bei der Kreditvergabe)
ECPA	Electronic Communications Privacy Act (Gesetz zum Datenschutz in der elektronischen Kommunikation)
EWR	Europäischer Wirtschaftsraum
EO 12333	Executive Order 12333 'United States Intelligence Activities' (Durchführungsverordnung 12333 „Aufklärung durch die USA")
EO 14086, EO	Executive Order 14086 'Enhancing Safeguards for US Signals Intelligence Activities' (Durchführungsverordnung 14086 „Verbesserung der Garantien für signalerfassende Aufklärung durch die USA")
FBI	Federal Bureau of Investigation (Strafverfolgungsbehörde innerhalb des Justizministeriums)
FCRA	Fair Credit Reporting Act (Gesetz zur Regelung des Datenschutzes bei Konsumentenkrediten)
FISA	Foreign Intelligence Surveillance Act (Gesetz über die Überwachung der Auslandsgeheimdienste)
FISC	Foreign Intelligence Surveillance Court (Gericht zur Überwachung der Auslandsgeheimdienste)
FISCR	Foreign Intelligence Surveillance Court of Review (Rechtsmittelgericht für Entscheidungen im Bereich der Überwachung der Auslandsgeheimdienste)
FOIA	Freedom of Information Act (Gesetz über die Informationsfreiheit)
FRA	Federal Records Act

FTC	Federal Trade Commission (Wettbewerbsbehörde)
Gerichtshof	Gerichtshof der Europäischen Union
Grundsätze	Grundsätze des Datenschutzrahmens EU-USA
HIPAA	Health Insurance Portability and Accountability Act (Gesetz über die Übertragbarkeit und Rechenschaftspflicht der Krankenversicherung)
ICDR	International Centre for Dispute Resolution (internationale Abteilung der American Arbitration Association (AAA))
IOB	Intelligence Oversight Board (Nachrichtendienstaufsichtsgremium)
NIST	National Institute for Standards and Technology (Normeninstitut)
NSA	National Security Agency (Nachrichtendienst)
NSL	National Security Letter(s)
ODNI	Office of the Director of National Intelligence (Büro des Direktors des Nationalen Nachrichtendienstes)
ODNI CLPO, CLPO	Civil Liberties Protection Officer of the Director of National Intelligence (Bürgerrechtsbeauftragter des Büros des Direktors des Nationalen Nachrichtendienstes)
OMB	Office of Management and Budget
OPCL	Office of Privacy and Civil Liberties of the Department of Justice (Büro für Datenschutz und Bürgerrechte des Justizministeriums)
PCLOB	Privacy and Civil Liberties Oversight Board (Stelle zur Überwachung des Schutzes der Privatsphäre und der bürgerlichen Freiheiten)
PIAB	President's Intelligence Advisory Board (Beratungsgremium des Präsidenten für Nachrichtendienste)
PPD 28	Presidential Policy Directive 28
Verordnung (EU) 2016/679	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
US	Vereinigte Staaten
Union	Europäische Union