EUROPÄISCHE
KOMMISSION

Brüssel, 10.7.2023
K(2023) 4745 endgültig

**DURCHFÜHRUNGSBESCHLUSS 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 EU-US-Datenschutzrahmen**

(Text mit Bedeutung für den EWR)

[Vollmer: Dies ist eine inoffizielle Übersetzung durch www.DeepL.com, weshalb der Seitenumfang von 137 auf 256 Seiten angewachsen ist. Eine offizielle Übersetzung ins Deutsche wird sicherlich bald erfolgen.]

**DURCHFÜHRUNGSBESCHLUSS 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 EU-US-Datenschutzrahmen**

(Text mit 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 und 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. EINFÜHRUNG

(1) Die Verordnung (EU) 2016/679[2] regelt die Übermittlung personenbezogener Daten von für die Verarbeitung Verantwortlichen oder Auftragsverarbeitern in der Union an Drittländer und internationale Organisationen, soweit diese Übermittlungen in den Anwendungsbereich der Verordnung fallen. Die Vorschriften für internationale Datenübermittlungen sind in Kapitel V der genannten Verordnung festgelegt. Während der Fluss personenbezogener Daten in und aus Ländern außerhalb der Europäischen Union für die Ausweitung des grenzüberschreitenden Handels und der internationalen Zusammenarbeit von wesentlicher Bedeutung ist, darf das Schutzniveau personenbezogener Daten in der Union nicht durch Übermittlungen an Drittländer oder internationale Organisationen untergraben werden[3] .

(2) Gemäß Artikel 45 Absatz 3 der Verordnung (EU) 2016/679 kann die Kommission im Wege eines Durchführungsrechtsakts beschließen, dass ein Drittland, ein Gebiet oder ein oder mehrere bestimmte Sektoren innerhalb eines Drittlands ein angemessenes Schutzniveau gewährleisten. Unter dieser Voraussetzung können Übermittlungen personenbezogener Daten in ein Drittland erfolgen, ohne dass eine weitere Genehmigung gemäß Artikel 45 Absatz 1 und Erwägungsgrund 103 der Verordnung (EU) 2016/679 eingeholt werden muss.

(3) Gemäß Artikel 45 Absatz 2 der Verordnung (EU) 2016/679 muss sich der Erlass eines Angemessenheitsbeschlusses auf eine umfassende Analyse der Rechtsordnung des Drittlands stützen, die sowohl die für Datenimporteure geltenden Vorschriften als auch die Beschränkungen und Garantien in Bezug auf den Zugang der Behörden zu personenbezogenen Daten umfasst. Bei ihrer Bewertung muss die Kommission feststellen, ob das betreffende Drittland ein Schutzniveau gewährleistet, das dem in der Union gewährleisteten Schutz "im Wesentlichen gleichwertig" ist (Erwägungsgrund

[1] ABl. L 119 vom 4.5.2016, S. 1.

[2] Der Einfachheit halber ist ein Verzeichnis der in dieser Entscheidung verwendeten Abkürzungen in Anhang VIII enthalten.

[3] Siehe Erwägungsgrund 101 der Verordnung (EU) 2016/679.

104 der Verordnung (EU) 2016/679). Ob dies der Fall ist, ist anhand des Unionsrechts, insbesondere der Verordnung (EU) 2016/679, sowie der Rechtsprechung des Gerichtshofs der Europäischen Union (EuGH)[4] zu beurteilen.

(4) Wie der Gerichtshof in seinem Urteil vom 6. Oktober 2015 in der Rechtssache C-362/14, *Maximillian Schrems* gegen den *Datenschutzbeauftragten*[5] *(Schrems),* klargestellt hat, ist es nicht erforderlich, ein identisches Schutzniveau zu finden. Insbesondere können die Mittel, auf die das betreffende Drittland zum Schutz personenbezogener Daten zurückgreift, von den in der Union eingesetzten Mitteln abweichen, solange sie sich in der Praxis als wirksam erweisen, um ein angemessenes Schutzniveau zu gewährleisten[6] . Die Angemessenheitsnorm verlangt also keine Punkt-zu-Punkt-Übernahme der Unionsvorschriften. Vielmehr ist zu prüfen, ob das ausländische System insgesamt durch den Inhalt der Datenschutzrechte und ihre wirksame Umsetzung, Überwachung und Durchsetzung das erforderliche Schutzniveau gewährleistet[7] . Darüber hinaus sollte die Kommission nach diesem Urteil bei der Anwendung dieses Maßstabs insbesondere prüfen, ob der Rechtsrahmen des betreffenden Drittlands Vorschriften vorsieht, die Eingriffe in die Grundrechte der Personen, deren Daten aus der Union übermittelt werden, begrenzen sollen, zu denen die staatlichen Stellen dieses Landes befugt wären, wenn sie legitime Ziele wie die nationale Sicherheit verfolgen, und ob er einen wirksamen Rechtsschutz gegen Eingriffe dieser Art bietet[8] . Das "Angemessenheitsreferat" des Europäischen Datenschutzausschusses, das diesen Standard weiter präzisieren soll, bietet ebenfalls Orientierungshilfe in dieser Hinsicht[9] .

(5) Der anwendbare Standard in Bezug auf solche Eingriffe in die Grundrechte auf Schutz der Privatsphäre und Datenschutz wurde vom Gerichtshof in seinem Urteil vom 16. Juli 2020 in der Rechtssache C-311/18, *Datenschutzbeauftragter gegen Facebook Ireland Limited und Maximillian Schrems (Schrems II),* weiter präzisiert, mit dem der Durchführungsbeschluss (EU) 2016/1250[10] der Kommission zu einem früheren transatlantischen Rahmen für den Datenverkehr, dem EU-US-Datenschutzschild (Privacy Shield), für ungültig erklärt wurde. Der Gerichtshof vertrat die Auffassung, dass die Beschränkungen des Schutzes personenbezogener Daten, die sich aus
Das innerstaatliche Recht der USA über den Zugang zu und die Verwendung von Daten, die von der Union an die Vereinigten Staaten zu Zwecken der nationalen Sicherheit übermittelt wurden, durch US-Behörden war nicht in einer Weise geregelt, die den Anforderungen genügt, die im Hinblick auf die Notwendigkeit und Verhältnismäßigkeit solcher Eingriffe in das Recht auf Datenschutz im Wesentlichen denen des Unionsrechts entsprechen[11] . Der Gerichtshof vertrat ferner die Auffassung, dass kein Rechtsbehelf bei einer Einrichtung möglich ist, die den Personen, deren Daten an die Vereinigten Staaten übermittelt wurden, Garantien bietet, die den in Artikel 47 der Charta über das Recht auf einen wirksamen Rechtsbehelf geforderten Garantien im Wesentlichen gleichwertig sind[12] .

---

4 Siehe zuletzt die Rechtssache C-311/18, *Facebook Ireland und Schrems* (*Schrems II*) ECLI:EU:C:2020:559.

5 Rechtssache C-362/14, *Maximilian Schrems v. Daten Schutz Kommissar* (*Schrems*), ECLI:EU:C:2015:650, Randnr. 73.

6 *Schrems*, Ziffer 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. 6-7.

8 *Schrems*, Ziffer 88-89.

9 Europäischer Datenschutzausschuss, Referent für Angemessenheit, WP 254 rev. 01. verfügbar 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 von der Europäischen Union gewährleisteten Schutzes - U.S. Privacy Shield (ABl. L 207 vom 1.8.2016, S. 1).

[11] *Schrems II*, Ziffer 185.

[12] *Schrems II*, Ziffer 197.

(6) Nach dem Urteil in der Rechtssache *Schrems II* nahm die Kommission Gespräche mit der US-Regierung im Hinblick auf einen möglichen neuen Angemessenheitsbeschluss auf, der die Anforderungen von Artikel 45 Absatz 2 der Verordnung (EU) 2016/679 in der Auslegung des Gerichtshofs erfüllen würde. Als Ergebnis dieser Gespräche verabschiedeten die Vereinigten Staaten am 7. Oktober 2022 die Executive Order 14086 "Enhancing Safeguards for US Signals Intelligence Activities" (EO 14086), die durch eine Verordnung des U.S. Attorney General (AG Regulation)[13] über den Data Protection Review Court ergänzt wird. Darüber hinaus wurde der Rahmen, der für gewerbliche Einrichtungen gilt, die im Rahmen dieses Beschlusses aus der Union übermittelte Daten verarbeiten - der "EU-US-Datenschutzrahmen" (EU-U.S. DPF oder DPF) - aktualisiert.

(7) Die Kommission hat das US-Recht und die US-Praxis, einschließlich EO 14086 und der AG-Verordnung, sorgfältig geprüft. Auf der Grundlage der in den Erwägungsgründen 9-200 dargelegten Feststellungen kommt die Kommission zu dem Schluss, dass die Vereinigten Staaten ein angemessenes Schutzniveau für personenbezogene Daten gewährleisten, die im Rahmen der EU-US-DSGVO von einem für die Verarbeitung Verantwortlichen oder einem Auftragsverarbeiter in der Union[14] an zertifizierte Organisationen in den Vereinigten Staaten übermittelt werden.

(8) Dieser Beschluss hat zur Folge, dass Übermittlungen personenbezogener Daten von für die Verarbeitung Verantwortlichen und Auftragsverarbeitern in der Union[15] an zertifizierte Organisationen in den Vereinigten Staaten stattfinden können, ohne dass eine weitere Genehmigung eingeholt werden muss. Er berührt nicht die unmittelbare Anwendung der Verordnung (EU) 2016/679 auf solche Organisationen, wenn die in Artikel 3 der Verordnung festgelegten Bedingungen für den territorialen Anwendungsbereich der Verordnung erfüllt sind.

## 2. DER EU-US-DATENSCHUTZRAHMEN

### 2.1 Persönlicher und materieller Geltungsbereich

#### *2.1.1 Zertifizierte Organisationen*

(9) Die EU-US-DSGVO basiert auf einem Zertifizierungssystem, mit dem sich US-Organisationen zu einer Reihe von Datenschutzgrundsätzen - den "EU-US-Datenschutzrahmengrundsätzen", einschließlich der ergänzenden Grundsätze (zusammen: die Grundsätze) - verpflichten, die vom US-Handelsministerium (DoC) herausgegeben werden und in Anhang I dieser Entscheidung enthalten sind[16] . Um für eine Zertifizierung nach dem EU-U.S. DPF in Frage zu kommen, muss eine Organisation den Ermittlungs- und Durchsetzungsbefugnissen der Federal Trade Commission (FTC) oder des U.S. Department of Transportation (DoT)[17] unterliegen. Die Grundsätze

---

13 28 CFR Teil 302.

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

15 Dieser Beschluss berührt nicht die Anforderungen der Verordnung (EU) 2016/679, die für die Stellen (für die Verarbeitung Verantwortliche und Auftragsverarbeiter) in der Union gelten, die die Daten übermitteln, z. B. in Bezug auf Zweckbindung, Datenminimierung, Transparenz und Datensicherheit

(siehe auch Artikel 44 der Verordnung (EU) 2016/679).

16 Siehe hierzu *Schrems*, Randnummer 81, in der der Gerichtshof bestätigt, dass ein System der Selbstzertifizierung ein angemessenes Schutzniveau gewährleisten kann.

17 Anhang I, Abschnitt I.2. Die FTC hat eine weitreichende Zuständigkeit für kommerzielle Aktivitäten, mit einigen Ausnahmen,

z. B. in Bezug auf Banken, Fluggesellschaften, das Versicherungsgeschäft und die Common-Carrier-Aktivitäten von Telekommunikationsdienstleistern (obwohl das Urteil des U.S. Court of Appeals for the Ninth Circuit vom 26. Februar 2018 in der Rechtssache FTC gegen AT&T bestätigt hat, dass die FTC auch für nicht

gelten unmittelbar nach der Zertifizierung. Wie in den Erwägungsgründen 48-52 näher erläutert, müssen die DPF-Organisationen der EU und der USA ihre Einhaltung der Grundsätze jährlich neu bescheinigen[18] .

### *2.1.2 Definition der personenbezogenen Daten und der Begriffe "für die Verarbeitung Verantwortlicher" und "Beauftragter*

(10) Der im Rahmen der EU-US-DSGVO gewährte Schutz gilt für alle personenbezogenen Daten, die aus der Union an Organisationen in den USA übermittelt werden, die ihre Einhaltung der Grundsätze gegenüber dem DoC bestätigt haben, mit Ausnahme von Daten, die für die Veröffentlichung, Ausstrahlung oder andere Formen der öffentlichen Wiedergabe von journalistischem Material und Informationen in zuvor veröffentlichtem Material aus Medienarchiven[19] erhoben werden. Solche Informationen können daher nicht auf der Grundlage der EU-Grundsätze übermittelt werden.
U.S. DPF.

(11) Die Grundsätze definieren personenbezogene Daten/persönliche Informationen in der gleichen Weise wie die Verordnung (EU) 2016/679, d. h. als "Daten über eine bestimmte oder bestimmbare Person, die in den Anwendungsbereich der Datenschutz-Grundverordnung fallen und von einer Organisation in den Vereinigten Staaten aus der EU empfangen und in beliebiger Form gespeichert werden"[20] . Dementsprechend umfassen sie auch pseudonymisierte (oder "verschlüsselte") Forschungsdaten (auch wenn der Schlüssel nicht an die empfangende US-Organisation weitergegeben wird)[21] . In ähnlicher Weise wird der Begriff der Verarbeitung definiert als "jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte 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 Verbreitung sowie das Löschen oder Vernichten"[22] .

(12) Die EU-US-DSGVO gilt für Organisationen in den USA, die als für die Verarbeitung Verantwortliche (d. h. als 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 Namen eines für die Verarbeitung Verantwortlichen handeln)[24] gelten. US-Auftragsverarbeiter müssen vertraglich verpflichtet werden, nur auf Weisung des für die Verarbeitung Verantwortlichen in der EU zu handeln und diesen bei der Wahrnehmung seiner Rechte nach den Grundsätzen[25] zu unterstützen. Darüber hinaus muss ein Auftragsverarbeiter im Falle einer Unterauftragsverarbeitung einen Vertrag mit dem Unterauftragsverarbeiter schließen, der dasselbe Schutzniveau wie die Grundsätze garantiert, und Maßnahmen ergreifen, um deren ordnungsgemäße Umsetzung zu gewährleisten[26] .

## 2.2 EU-US-Datenschutzrahmenprinzipien

### *2.2.1 Zweckbindung und Auswahl*

---

Gemeinsame Beförderungstätigkeiten solcher Einrichtungen). Siehe auch Anhang IV, Fußnote 2. Das DoT ist für die Durchsetzung der Einhaltung der Vorschriften durch Luftfahrtunternehmen und Flugscheinverkaufsstellen (im Luftverkehr) 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 Namen eines für die Verarbeitung Verantwortlichen handeln, vorbehaltlich der Anweisungen des letzteren und im Rahmen spezifischer vertraglicher Verpflichtungen.

[25] Anhang I, Abschnitt III.10.a. Siehe auch die vom DoC in Absprache mit dem Europäischen Datenschutzausschuss im Rahmen des Privacy Shield erstellten Leitlinien, in denen die Pflichten von US-Verarbeitern, die personenbezogene Daten aus der Union erhalten, im Rahmen des Privacy Shield geklärt werden. Da sich diese Vorschriften nicht geändert haben, bleibt dieser Leitfaden/FAQ weiterhin relevant unter der EU-U.S. DPF (https://www.privacyshield.gov/article?id=Processing-FAQs).

[26] Anhang I, Abschnitt II.3.b.

(13) Personenbezogene Daten sollten rechtmäßig und nach Treu und Glauben verarbeitet werden. Sie sollten für einen bestimmten Zweck erhoben und anschließend nur insoweit verwendet werden, als dies mit dem Zweck der Verarbeitung nicht unvereinbar ist.

(14) Im Rahmen der EU-US-DSGVO 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 Zweck, für den sie ursprünglich erhoben oder später von der betroffenen Person genehmigt wurden, unvereinbar ist[27] .

(15) Zweitens muss die Organisation, bevor sie personenbezogene Daten für einen neuen (geänderten) Zweck verwendet, der sich zwar wesentlich von dem ursprünglichen Zweck unterscheidet, aber immer noch mit diesem vereinbar ist, oder sie an einen Dritten weitergibt, den betroffenen Personen die Möglichkeit geben, gemäß dem *Grundsatz der Wahlfreiheit (Choice Principle)*[28] über einen klaren, auffälligen und leicht zugänglichen Mechanismus Widerspruch einzulegen (Opt-out). Wichtig ist, dass dieser Grundsatz nicht das ausdrückliche Verbot einer unvereinbaren Verarbeitung[29] ersetzt.

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

(16) Für die Verarbeitung "besonderer Kategorien" von Daten sollten besondere Garantien gelten.

(17) Im Einklang mit dem *Grundsatz der Wahlfreiheit* gelten besondere Garantien für die Verarbeitung "sensibler Informationen", d. h . personenbezogener Daten mit Angaben zu medizinischen oder gesundheitlichen Bedingungen,

---

[27] Anhang I, Abschnitt II.5.a. Zu den kompatiblen Zwecken können Rechnungsprüfung, Betrugsprävention oder andere Zwecke gehören, die mit den Erwartungen einer vernünftigen Person angesichts des Kontextes der Sammlung übereinstimmen (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 in ihrem Namen und nach ihren Anweisungen handelt (Anhang I, Abschnitt II.2.b). In diesem Fall muss die Organisation jedoch einen Vertrag abschließen und die Einhaltung des Grundsatzes der *Rechenschaftspflicht bei der Weitergabe* sicherstellen, wie in Erwägungsgrund 43 näher beschrieben. Darüber hinaus kann der Grundsatz der *Wahlmöglichkeit* (ebenso wie der Grundsatz der *Benachrichtigung*) eingeschränkt werden, wenn personenbezogene Daten im Rahmen von Due-Diligence-Prüfungen (als Teil einer potenziellen Fusion oder Übernahme) oder Audits verarbeitet werden, und zwar in dem Umfang und so lange, wie dies zur Erfüllung gesetzlicher oder im öffentlichen Interesse liegender Anforderungen erforderlich ist, oder in dem Umfang und so lange, wie die Anwendung dieser Grundsätze die berechtigten Interessen der Organisation im spezifischen Kontext von Due-Diligence-Prüfungen oder Audits beeinträchtigen würde (Anhang I, Abschnitt III.4). Ergänzungsgrundsatz 15 (Anhang I, Abschnitt III.15.a und b) sieht ebenfalls eine Ausnahme vom Grundsatz der *Wahlmöglichkeit* (sowie von den Grundsätzen der *Benachrichtigung* und der *Rechenschaftspflicht bei der Weitergabe*) für personenbezogene Daten aus öffentlich zugänglichen Quellen (es sei denn, der EU-Datenexporteur weist darauf hin, dass die Informationen Beschränkungen unterliegen, die die Anwendung dieser Grundsätze erfordern) oder für personenbezogene Daten vor, die aus Aufzeichnungen stammen, die der allgemeinen Öffentlichkeit zur Einsichtnahme zugänglich sind (solange sie nicht mit nicht-öffentlichen Informationen aus Aufzeichnungen kombiniert werden und alle Bedingungen für die Einsichtnahme eingehalten werden). In ähnlicher Weise sieht der ergänzende Grundsatz 14 (Anhang I, Abschnitt III.14.f) eine Ausnahme vom Grundsatz der *Wahlmöglichkeit* (sowie von den Grundsätzen der *Benachrichtigung* und der *Rechenschaftspflicht bei der Weitergabe*) für die Verarbeitung personenbezogener Daten durch ein pharmazeutisches Unternehmen oder ein Unternehmen für Medizinprodukte zur Überwachung der Produktsicherheit und -wirksamkeit vor, sofern die Einhaltung der Grundsätze die Einhaltung der gesetzlichen Vorschriften beeinträchtigt.

[29] Dies gilt für alle Datenübermittlungen im Rahmen der EU-US-DSGVO, auch wenn es sich um Daten handelt, die im Zusammenhang mit dem Beschäftigungsverhältnis erhoben wurden. Während eine

zertifizierte US-Organisation also grundsätzlich Personaldaten für andere, nicht beschäftigungsbezogene Zwecke (z. B. bestimmte Marketingmitteilungen) verwenden darf, muss sie das Verbot der unvereinbaren Verarbeitung beachten und darf dies außerdem nur im Einklang mit den Grundsätzen der *Benachrichtigung* und der *Wahlmöglichkeit* tun. Ausnahmsweise kann eine Organisation personenbezogene Daten für einen zusätzlichen, mit dem Verbot vereinbaren Zweck verwenden, ohne dass eine *Benachrichtigung* und eine *Wahlmöglichkeit* vorgesehen sind, jedoch nur in dem Umfang und für den Zeitraum, die erforderlich sind, um die Fähigkeit der Organisation zu vermeiden, Beförderungen, Ernennungen oder andere ähnliche Beschäftigungsentscheidungen zu treffen (siehe Anhang I, Abschnitt III.9.b.(iv)). Das Verbot für die US-Organisation, Strafmaßnahmen gegen den Arbeitnehmer zu ergreifen, wenn er eine solche Entscheidung trifft, einschließlich der Einschränkung von Beschäftigungsmöglichkeiten, stellt sicher, dass der Arbeitnehmer trotz des Unterordnungsverhältnisses und der ihm innewohnenden Abhängigkeit frei von Druck ist und somit eine wirklich freie Entscheidung treffen kann. Siehe Anhang I, Abschnitt III.9.b.(i).

rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Informationen über das Sexualleben der Person oder andere von Dritten erhaltene Informationen, die von dieser Partei als sensibel identifiziert und behandelt werden[30] . Das bedeutet, dass alle Daten, die nach dem Datenschutzrecht der Union als sensibel gelten (einschließlich Daten über die sexuelle Ausrichtung, genetische Daten und biometrische Daten), von den zertifizierten Organisationen nach der EU-US-DSGVO als sensibel behandelt werden.

(18) In der Regel müssen Organisationen die ausdrückliche Zustimmung (d. h. Opt-in) von Einzelpersonen einholen, wenn sie sensible Daten für andere Zwecke verwenden wollen als die, für die sie ursprünglich erhoben oder nachträglich von der Person (durch Opt-in) genehmigt wurden, oder wenn sie sie an Dritte weitergeben wollen[31] .

(19) Eine solche Einwilligung muss in begrenzten Fällen nicht eingeholt werden, ähnlich wie bei vergleichbaren Ausnahmen nach dem Unionsrecht zum Datenschutz, z. B. wenn die Verarbeitung sensibler Daten im lebenswichtigen Interesse einer Person liegt, für die Geltendmachung von Rechtsansprüchen erforderlich ist oder für die medizinische Versorgung oder Diagnose erforderlich ist[32] .

### *2.2.3 Datengenauigkeit, -minimierung und -sicherheit*

(20) Die Daten sollten sachlich richtig und, soweit erforderlich, auf dem neuesten Stand sein. Sie sollten ferner den Zwecken entsprechen, für die sie verarbeitet werden, dafür erheblich sein und nicht darüber hinausgehen; sie sollten grundsätzlich nicht länger aufbewahrt werden, als es für die Zwecke, für die die personenbezogenen Daten verarbeitet werden, erforderlich ist.

(21) Nach dem *Grundsatz der Datenintegrität und Zweckbindung*[33] müssen personenbezogene Daten auf das beschränkt werden, was für den Zweck der Verarbeitung relevant ist. Darüber hinaus müssen Organisationen, soweit dies für die Zwecke der Verarbeitung erforderlich ist, angemessene Maßnahmen ergreifen, um sicherzustellen, dass personenbezogene Daten für den vorgesehenen Verwendungszweck zuverlässig, richtig, vollständig und aktuell sind.

(22) Darüber hinaus dürfen personenbezogene Informationen in einer Form, die eine Person identifiziert oder identifizierbar macht (und somit in Form von personenbezogenen Daten)[34] nur so lange aufbewahrt werden, wie sie dem Zweck bzw. den Zwecken dienen, für den bzw. die sie ursprünglich erhoben wurden oder für den bzw. die die Person gemäß dem *Grundsatz der Wahlfreiheit* ihre Einwilligung erteilt hat. Diese Verpflichtung hindert Organisationen nicht daran, personenbezogene Daten über längere Zeiträume weiter zu verarbeiten, jedoch nur so lange und in dem Umfang, wie diese Verarbeitung vernünftigerweise einem der folgenden spezifischen Zwecke dient, die vergleichbaren Ausnahmen im 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 aufbewahrt, so unterliegt ihre Verarbeitung den in den Grundsätzen[36] vorgesehenen Garantien.

(23) Personenbezogene Daten sollten auch in einer Weise verarbeitet werden, die ihre Sicherheit gewährleistet, einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Verarbeitung und vor zufälligem Verlust,

---

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, wenn eine Organisation oder ein Dritter diese Person unter Berücksichtigung der wahrscheinlich verwendeten Identifizierungsmittel (u. a. unter Berücksichtigung der Kosten und des Zeitaufwands für die Identifizierung und der zum Zeitpunkt der Verarbeitung verfügbaren Technologie) vernünftigerweise identifizieren könnte.

[35] Anhang I, Abschnitt II.5.b.

[36] *Ebd*.

Zerstörung oder Beschädigung. Zu diesem Zweck sollten die für die Verarbeitung Verantwortlichen und die Auftragsverarbeiter geeignete technische oder organisatorische Maßnahmen ergreifen, um personenbezogene Daten vor möglichen Bedrohungen zu schützen. Diese Maßnahmen sollten unter Berücksichtigung des Stands der Technik, der damit verbundenen Kosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Risiken für die Rechte natürlicher Personen bewertet werden.

(24) Im Rahmen der EU-US-DSGVO wird dies durch den *Sicherheitsgrundsatz* gewährleistet, der ähnlich wie in Artikel 32 der Verordnung (EU) 2016/679 verlangt, angemessene und geeignete Sicherheitsmaßnahmen zu ergreifen, die den mit der Verarbeitung verbundenen Risiken und der Art der Daten Rechnung tragen[37] .

### *2.2.4 Transparenz*

(25) Die betroffenen Personen sollten über die wichtigsten Merkmale der Verarbeitung ihrer personenbezogenen Daten informiert werden.

(26) Dies wird durch den *Benachrichtigungsgrundsatz*[38] sichergestellt, der ähnlich wie die Transparenzanforderungen gemäß der Verordnung (EU) 2016/679 von den Organisationen verlangt, die betroffenen Personen unter anderem über (i) die Teilnahme der Organisation an der DPF, (ii) die Art der erhobenen Daten, (iii) den Zweck der Verarbeitung, (iv) die Art oder Identität der Dritten, an die personenbezogene Daten weitergegeben werden können, und die Zwecke dafür zu informieren,
(v) ihre individuellen Rechte, (vi) wie sie sich mit der Organisation in Verbindung setzen können und (vii) welche Rechtsmittel zur Verfügung stehen.

(27) Dieser Hinweis muss in klarer und auffälliger Sprache erfolgen, wenn die Personen zum ersten Mal aufgefordert werden, personenbezogene Daten bereitzustellen, oder so bald wie möglich danach, auf jeden Fall aber bevor die Daten für einen wesentlich anderen (aber kompatiblen) Zweck verwendet werden als den, für den sie erhoben wurden, oder bevor sie an Dritte weitergegeben werden[39] .

(28) Darüber hinaus müssen die Organisationen ihre Datenschutzrichtlinien, die die Grundsätze widerspiegeln, veröffentlichen (oder im Falle von Personaldaten den betroffenen Personen leicht zugänglich machen) und Links zur Website des DoC (mit weiteren Einzelheiten zur Zertifizierung, den Rechten der betroffenen Personen und den verfügbaren Rechtsbehelfsmechanismen), zur Datenschutz-Rahmenliste (DPF-Liste) der teilnehmenden Organisationen und zur Website eines geeigneten alternativen Streitbeilegungsanbieters[40] bereitstellen.

### *2.2.5 Individuelle Rechte*

---

37 Anhang I, Abschnitt II.4.a. Was die Personaldaten anbelangt, schreibt die EU-US-DSGVO den Arbeitgebern außerdem vor, die Datenschutzpräferenzen der Arbeitnehmer zu berücksichtigen, indem sie den Zugang zu den personenbezogenen Daten beschränken, bestimmte Daten anonymisieren oder Codes oder Pseudonyme zuweisen (Anhang I, Abschnitt III.9.b.(iii)).

38 Anhang I, Abschnitt II.1.

39 Anhang I, Abschnitt II.1.b. Der ergänzende Grundsatz 14 (Anhang I, Abschnitt III.14.b und c) enthält besondere Bestimmungen für die Verarbeitung personenbezogener Daten im Rahmen von Gesundheitsforschung und klinischen Prüfungen. Insbesondere erlaubt dieser Grundsatz den Organisationen, Daten aus klinischen Prüfungen auch dann zu verarbeiten, wenn eine Person von der Prüfung zurückgetreten ist, sofern dies in der Mitteilung, die der Person bei ihrer Zustimmung zur Teilnahme ausgehändigt wurde, deutlich gemacht wurde. Ebenso darf eine EU-US-DSGVO-Organisation, die personenbezogene Daten für Zwecke der Gesundheitsforschung erhält, diese nur für eine neue Forschungstätigkeit in Übereinstimmung mit den Grundsätzen der *Benachrichtigung* und der *Wahlmöglichkeit* verwenden. In diesem Fall sollte die Mitteilung an die betroffene Person grundsätzlich

Informationen über künftige spezifische Verwendungen der Daten (z. B. für verwandte Studien) enthalten. Ist es nicht möglich, von vornherein alle künftigen Verwendungszwecke der Daten anzugeben (weil sich aus neuen Erkenntnissen oder Entwicklungen in der Medizin/Forschung ein neuer Verwendungszweck ergeben könnte), muss eine Erklärung enthalten sein, dass die Daten in künftigen, nicht vorhersehbaren medizinischen und pharmazeutischen Forschungsaktivitäten verwendet werden können. Wenn eine solche Weiterverwendung nicht mit den allgemeinen Forschungszwecken, für die die Daten erhoben wurden, vereinbar ist (d. h. wenn die neuen Zwecke zwar wesentlich anders sind, aber immer noch mit dem ursprünglichen Zweck vereinbar sind, siehe Erwägungsgründe 14-15), muss eine neue Einwilligung (d. h. Opt-in) eingeholt werden. Siehe darüber hinaus die in Fußnote 28 beschriebenen spezifischen Einschränkungen/Ausnahmen vom Grundsatz der *Benachrichtigung*.

[40] Anhang I, Abschnitt III.6.d.

(29) Die betroffenen Personen sollten bestimmte Rechte haben, die sie gegenüber dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter geltend machen können, insbesondere das Recht auf Zugang zu den Daten, das Recht auf Widerspruch gegen die Verarbeitung und das Recht auf Berichtigung und Löschung der Daten.

(30) Das *Auskunftsrecht*[41] der EU-US-DSGVO räumt dem Einzelnen solche Rechte ein. Insbesondere haben betroffene Personen das Recht, ohne Angabe von Gründen von einer Organisation eine Bestätigung darüber zu erhalten, ob sie sie betreffende personenbezogene Daten verarbeitet; sie haben das Recht, dass ihnen die Daten mitgeteilt werden; und sie haben das Recht, Informationen über den Zweck der Verarbeitung, die Kategorien von personenbezogenen Daten, die verarbeitet werden, und die (Kategorien von) Empfänger(n), an die die Daten weitergegeben werden, zu erhalten[42] . Organisationen sind verpflichtet, Auskunftsersuchen innerhalb einer angemessenen Frist zu beantworten[43] . Eine Organisation kann die Anzahl der Beantwortungen von Auskunftsersuchen einer bestimmten Person innerhalb eines bestimmten Zeitraums angemessen begrenzen und eine Gebühr erheben, die nicht übermäßig hoch ist, z. B. wenn die Ersuchen offensichtlich übermäßig hoch sind, insbesondere aufgrund ihres wiederholten Charakters[44] .

(31) Das Auskunftsrecht darf nur unter außergewöhnlichen Umständen eingeschränkt werden, die denen des Unionsrechts zum Datenschutz ähneln, insbesondere wenn die legitimen Rechte anderer verletzt würden; wenn die Belastung oder die Kosten für die Gewährung der Auskunft unter den gegebenen Umständen in keinem Verhältnis zu den Risiken für die Privatsphäre des Einzelnen stehen würden (obwohl Kosten und Belastung keine ausschlaggebenden Faktoren für die Entscheidung sind, ob die Gewährung der Auskunft angemessen ist); in dem Maße, in dem die Offenlegung wahrscheinlich die Wahrung wichtiger, entgegenstehender öffentlicher Interessen wie die nationale Sicherheit, die öffentliche Sicherheit oder die Verteidigung beeinträchtigen würde; die Informationen vertrauliche Geschäftsinformationen enthalten; oder die Informationen ausschließlich zu Forschungs- oder statistischen Zwecken verarbeitet werden[45] . Jede Verweigerung oder Einschränkung eines Rechts muss notwendig und hinreichend begründet sein, wobei die Organisation die Beweislast dafür trägt, dass diese Anforderungen erfüllt sind[46] . Bei dieser Beurteilung muss die Organisation insbesondere die Interessen des Einzelnen berücksichtigen[47] . Wenn es möglich ist, Informationen von anderen Daten zu trennen, für die eine Einschränkung gilt, muss die Organisation die geschützten Informationen unkenntlich machen und die verbleibenden Informationen offenlegen[48] .

(32) Darüber hinaus haben die betroffenen Personen das Recht, die Berichtigung oder Änderung unrichtiger Daten sowie die Löschung von Daten zu verlangen, die unter Verstoß gegen die Grundsätze verarbeitet wurden[49] . Wie in Erwägungsgrund 15 erläutert, haben die betroffenen Personen darüber hinaus das Recht, der Verarbeitung ihrer Daten für wesentlich andere (aber vereinbare) Zwecke als die, für die die Daten erhoben wurden, zu widersprechen bzw. diese abzulehnen, sowie der Weitergabe ihrer Daten an Dritte. Werden personenbezogene Daten für Zwecke des Direktmarketings verwendet, haben Personen ein allgemeines Recht, der Verarbeitung jederzeit zu widersprechen[50] .

(33) In den Grundsätzen wird nicht speziell auf Entscheidungen eingegangen, die die betroffene Person betreffen und ausschließlich auf der automatisierten Verarbeitung personenbezogener Daten beruhen. Da jedoch

---

41 Siehe auch den ergänzenden Grundsatz zum Thema "Zugang" (Anhang I, Abschnitt III.8).

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

43 Anhang I, Abschnitt III.8.i.

[44] Anhang I, Abschnitt III.8.f.(i)-(ii) und g.
[45] Anhang I, Abschnitt III.4; 8.b, c, e; 14.e, f und 15.d.
[46] Anhang I, Abschnitt III.8.e.(ii). Die Organisation muss die betreffende Person über die Gründe für die Verweigerung/Einschränkung informieren und eine Kontaktstelle für etwaige 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 III.8.a.(i).
[50] Anhang I, Abschnitt III.8.12.

In Bezug auf personenbezogene Daten, die in der Union erhoben wurden, wird jede Entscheidung, die auf einer automatisierten Verarbeitung beruht, in der Regel von dem für die Verarbeitung Verantwortlichen in der Union getroffen (der in einer direkten Beziehung zu der betroffenen Person steht) und unterliegt somit unmittelbar der Verordnung (EU) 2016/679[51] . Dies gilt auch für Übermittlungsszenarien, bei denen die Verarbeitung von einem ausländischen (z. B. US-amerikanischen) Unternehmen durchgeführt wird, das als Beauftragter (Auftragsverarbeiter) im Namen des für die Verarbeitung Verantwortlichen in der Union handelt (oder als Unterauftragsverarbeiter, der im Namen des für die Verarbeitung Verantwortlichen in der Union handelt, nachdem er die Daten von einem für die Verarbeitung Verantwortlichen in der Union erhalten hat, der sie erhoben hat), der auf dieser Grundlage dann die Entscheidung trifft.

(34) Dies wurde durch eine Studie bestätigt, die die Kommission 2018 im Rahmen der zweiten jährlichen Überprüfung der Funktionsweise des Privacy Shield[52] in Auftrag gegeben hatte und die zu dem Schluss kam, dass es zum damaligen Zeitpunkt keine Anhaltspunkte dafür gab, dass die Privacy-Shield-Organisationen in der Regel automatisierte Entscheidungen auf der Grundlage der im Rahmen des Privacy Shields übermittelten personenbezogenen Daten treffen.

(35) In den Bereichen, in denen Unternehmen am ehesten auf die automatisierte Verarbeitung personenbezogener Daten zurückgreifen, um Entscheidungen zu treffen, die den Einzelnen betreffen (z. B. Kreditvergabe, Hypothekenangebote, Beschäftigung, Wohnungswesen und Versicherungen), bietet das US-Recht auf jeden Fall einen besonderen Schutz gegen nachteilige Entscheidungen[53] . Diese Gesetze sehen in der Regel vor, dass der Einzelne das Recht hat, über die spezifischen Gründe für die Entscheidung (z. B. die Ablehnung eines Kredits) informiert zu werden, unvollständige oder ungenaue Informationen (sowie die Berufung auf unrechtmäßige Faktoren) anzufechten und Rechtsmittel einzulegen. Im Bereich des Verbraucherkredits enthalten der Fair Credit Reporting Act (FCRA) und der Equal Credit Opportunity Act (ECOA) Schutzbestimmungen, die den Verbrauchern in irgendeiner Form ein Recht auf Erklärung und Anfechtung der Entscheidung einräumen. Diese Gesetze sind in einer Vielzahl von Bereichen von Bedeutung, u. a. bei Krediten, Beschäftigung, Wohnraum und Versicherungen. Darüber hinaus bieten bestimmte Antidiskriminierungsgesetze wie Titel VII des Civil Rights Act und der Fair Housing Act dem Einzelnen Schutz in Bezug auf Modelle, die bei der automatisierten Entscheidungsfindung verwendet werden und zu einer Diskriminierung aufgrund bestimmter Merkmale führen könnten, und gewähren ihm das Recht, solche Entscheidungen, auch automatisierte, anzufechten. In Bezug auf Gesundheitsinformationen sieht der Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule bestimmte Rechte vor, die denen der Verordnung (EU) 2016/679 in Bezug auf den Zugang zu persönlichen Gesundheitsinformationen ähneln. Darüber hinaus verlangen die US-Behörden in ihren Leitlinien, dass medizinische Dienstleister Informationen erhalten

---

[51] Im Ausnahmefall, in dem die US-Organisation eine direkte Beziehung zu der betroffenen Person in der Union unterhält, ist dies in der Regel die Folge davon, dass sie die Person in der Union angesprochen hat, indem sie ihr Waren oder Dienstleistungen angeboten oder ihr Verhalten überwacht hat. In diesem Fall fällt die US-Organisation selbst in den Anwendungsbereich der Verordnung (EU) 2016/679 (Artikel 3 Absatz 2) und muss somit unmittelbar das Datenschutzrecht der Union einhalten.

[52] SWD(2018)497endg., Abschnitt 4.1.5. Die Studie konzentrierte sich auf i) das Ausmaß, in dem Privacy-Shield-Organisationen in den USA auf der Grundlage der automatisierten Verarbeitung personenbezogener Daten, die von Unternehmen in der EU im Rahmen des Privacy Sh ields übermittelt wurden, Entscheidungen treffen, die sich auf Einzelpersonen auswirken, und ii) die Garantien für Einzelpersonen, die das US-Bundesrecht für diese Art von Situationen vorsieht, sowie die Bedingungen für die Anwendung dieser Garantien.

[53] Siehe z.B. den Equal Credit Opportunity Act (15 U.S.C. 1691 et seq.), den Fair Credit Reporting Act (15 USC § 1681 et seq.) oder das Gesetz über fairen Wohnraum (42 U.S.C. 3601 et seq.). Darüber hinaus haben sich die Vereinigten Staaten den Grundsätzen der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung für künstliche Intelligenz angeschlossen, die unter anderem Grundsätze zu Transparenz, Erklärungsfähigkeit, Sicherheit und Rechenschaftspflicht enthalten.

die es ihnen ermöglichen, Personen über automatisierte Entscheidungsfindungssysteme zu informieren, die im medizinischen Bereich eingesetzt werden[54] .

(36) Daher bieten diese Vorschriften einen ähnlichen Schutz wie das Datenschutzrecht der Union in dem unwahrscheinlichen Fall, dass automatisierte Entscheidungen von der DPF-Organisation EU-USA selbst getroffen werden.

### *2.2.6 Beschränkungen bei Weiterüberweisungen*

(37) Das Schutzniveau für personenbezogene Daten, die von der Union an Organisationen in den Vereinigten Staaten übermittelt werden, darf durch die Weiterübermittlung dieser Daten an einen Empfänger in den Vereinigten Staaten oder einem anderen Drittland nicht untergraben werden.

(38) Nach dem *Grundsatz der Rechenschaftspflicht bei der Weiterübermittlung*[55] gelten besondere Regeln für so genannte "Weiterübermittlungen", d. h. Übermittlungen personenbezogener Daten von einer EU-US-DSGVOrganisation an einen dritten für die Verarbeitung Verantwortlichen oder einen Auftragsverarbeiter, unabhängig davon, ob sich letzterer in den Vereinigten Staaten oder in einem Drittland außerhalb der Vereinigten Staaten (und der Union) befindet. Jede Weiterübermittlung darf nur (i) für begrenzte und festgelegte Zwecke erfolgen,
(ii) auf der Grundlage eines Vertrags zwischen der EU-U.S.-amerikanischen DPF-Organisation und dem Dritten[56] (oder einer vergleichbaren Vereinbarung innerhalb einer Unternehmensgruppe[57] ) und (iii) nur dann, wenn dieser Vertrag den Dritten dazu verpflichtet, das gleiche Schutzniveau zu bieten, wie es durch die Grundsätze garantiert wird.

(39) Diese Verpflichtung, das gleiche Schutzniveau zu gewährleisten, wie es durch die Grundsätze garantiert wird, 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 mit den Zwecken, für die sie erhoben wurden oder für die die betroffene Person nachträglich ihre Einwilligung erteilt hat (gemäß dem *Grundsatz der Wahlfreiheit*), nicht unvereinbar sind.

(40) Der *Grundsatz der Rechenschaftspflicht bei der Weiterübermittlung* sollte auch in Verbindung mit dem *Grundsatz der Benachrichtigung* und - im Falle einer Weiterübermittlung an einen dritten für die Verarbeitung Verantwortlichen[58] - mit dem *Grundsatz der Wahlmöglichkeit* gelesen werden, demzufolge die betroffenen Personen (unter anderem) über die Art/Identität eines dritten Empfängers, den Zweck der Weiterübermittlung und die angebotene Wahlmöglichkeit informiert werden müssen und der Weiterübermittlung widersprechen können (Opt-out) oder - im Falle sensibler Daten - eine "bestätigende ausdrückliche Einwilligung" (Opt-in) geben müssen.

---

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 den ergänzenden Grundsatz "Obligatorische Verträge bei Weitergabe" (Anhang I, Abschnitt III.10).

56 Als Ausnahme von diesem allgemeinen Grundsatz kann eine Organisation personenbezogene Daten einer kleinen Zahl von Mitarbeitern weiterleiten, ohne einen Vertrag mit dem Empfänger zu schließen, wenn dies für gelegentliche beschäftigungsbezogene betriebliche Erfordernisse erforderlich ist, z. B. für die Buchung eines Flugs, eines Hotelzimmers oder eines Versicherungsschutzes. Allerdings muss die Organisation auch in diesem Fall die Grundsätze der *Benachrichtigung* und der *Wahlmöglichkeit einhalten* (siehe Anhang I, Abschnitt III.9.e).

57 Siehe den ergänzenden Grundsatz "Obligatorische Verträge für Weiterübermittlungen" (Anhang I, Abschnitt III.10.b). Dieser Grundsatz lässt zwar Übermittlungen zu, die auch auf nichtvertraglichen

Instrumenten beruhen (z. B. gruppeninterne Compliance- und Kontrollprogramme), doch stellt der Text klar, dass diese Instrumente stets "die Kontinuität des Schutzes personenbezogener Daten nach den Grundsätzen gewährleisten" müssen. Da die zertifizierte US-Organisation für die Einhaltung der Grundsätze verantwortlich bleibt, besteht für sie ein starker Anreiz, Instrumente zu verwenden, die in der Praxis tatsächlich wirksam sind.

[58] Der Einzelne hat kein Widerspruchsrecht, wenn die personenbezogenen Daten an einen Dritten übermittelt werden, der als Beauftragter Aufgaben im Namen und auf Anweisung der US-Organisation wahrnimmt. Dazu ist jedoch ein Vertrag mit dem Beauftragten erforderlich, und die US-Organisation trägt die Verantwortung dafür, dass der in den Grundsätzen vorgesehene Schutz durch die Ausübung ihrer Weisungsbefugnisse gewährleistet wird.

(41) Die Verpflichtung, das gleiche Schutzniveau wie in den Grundsätzen vorgesehen zu gewährleisten, gilt für alle Dritten, die an der Verarbeitung der übermittelten Daten beteiligt sind, unabhängig von ihrem Standort (in den USA oder in einem anderen Drittland) sowie für den Fall, dass der ursprüngliche Drittempfänger diese Daten selbst an einen anderen Drittempfänger weitergibt, z. B. zur Weiterverarbeitung.

(42) In jedem Fall muss der Vertrag mit dem dritten Empfänger vorsehen, dass dieser die DPF-Organisation EU-USA benachrichtigt, wenn er feststellt, dass er seiner Verpflichtung nicht mehr nachkommen kann. Wenn eine solche Feststellung getroffen wird, muss die Verarbeitung durch den Dritten eingestellt werden oder es müssen andere angemessene und geeignete Schritte unternommen werden, um die Situation zu bereinigen[59] .

(43) Zusätzliche Schutzvorkehrungen gelten im Falle einer Weitergabe an einen Dritten (d. h. einen Auftragsverarbeiter). In einem solchen Fall muss die US-Organisation sicherstellen, dass der Beauftragte nur auf ihre Anweisungen hin handelt und angemessene und geeignete Maßnahmen ergreift, (i) um sicherzustellen, dass der Beauftragte die übermittelten personenbezogenen Daten tatsächlich in einer Weise verarbeitet, die mit den Verpflichtungen der Organisation nach den Grundsätzen im Einklang steht, und (ii) um eine unbefugte Verarbeitung zu stoppen und zu berichtigen, sobald sie benachrichtigt wird[60] . Die Organisation kann von der DoC aufgefordert werden, eine Zusammenfassung oder ein repräsentatives Exemplar der Datenschutzbestimmungen des Vertrags vorzulegen[61] . Treten in einer (Teil-)Verarbeitungskette Probleme bei der Einhaltung der Vorschriften auf, so haftet grundsätzlich die Organisation, die für die Verarbeitung der personenbezogenen Daten verantwortlich ist, wie im *Grundsatz "Rückgriff, Durchsetzung und Haftung"* dargelegt, es sei denn, sie weist nach, dass sie für das Ereignis, das den Schaden verursacht hat, nicht verantwortlich ist[62] .

### *2.2.7 Rechenschaftspflicht*

(44) Nach dem Grundsatz der Rechenschaftspflicht müssen Einrichtungen, die Daten verarbeiten, geeignete technische und organisatorische Maßnahmen ergreifen, um ihren Datenschutzverpflichtungen tatsächlich nachzukommen, und in der Lage sein, dies insbesondere gegenüber der zuständigen Aufsichtsbehörde nachzuweisen.

(45) Sobald sich eine Organisation freiwillig dazu entschlossen hat,[63] im Rahmen der EU-US-DSGVO zu zertifizieren, ist ihre tatsächliche Einhaltung der Grundsätze obligatorisch und durchsetzbar. Gemäß dem *Grundsatz*[64] müssen die Organisationen der EU-US-DSGVO wirksame Mechanismen bereitstellen, um die Einhaltung der Grundsätze zu gewährleisten. Die Organisationen müssen auch Maßnahmen ergreifen, um[65] zu überprüfen, ob ihre Datenschutzrichtlinien mit den Grundsätzen übereinstimmen und tatsächlich befolgt werden. Dies kann entweder durch ein System der Selbstbeurteilung geschehen, zu dem auch interne Verfahren gehören müssen, die sicherstellen, dass die Mitarbeiter in der Umsetzung der Datenschutzpolitik der Organisation geschult werden und dass die Einhaltung regelmäßig objektiv überprüft wird, oder durch externe Überprüfungen der Einhaltung der Grundsätze, zu deren Methoden Audits, stichprobenartige Kontrollen oder der Einsatz technologischer Hilfsmittel gehören können.

---

[59] Die Situation ist unterschiedlich, je nachdem, ob der Dritte ein für die Verarbeitung Verantwortlicher oder ein Auftragsverarbeiter (Agent) ist. Im ersten Fall muss der Vertrag mit dem Dritten vorsehen, dass dieser die Verarbeitung einstellt oder andere angemessene und geeignete Maßnahmen ergreift, um die Situation zu bereinigen. Im zweiten Fall ist es Sache der EU-U.S. DPF-Organisation - als diejenige, die die Verarbeitung kontrolliert und auf deren Anweisung der

Beauftragte arbeitet - diese Maßnahmen zu ergreifen. 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 den ergänzenden Grundsatz "Selbstzertifizierung" (Anhang I, Abschnitt III.6).

64 Siehe auch den ergänzenden Grundsatz "Streitbeilegung und Vollstreckung" (Anhang I, Abschnitt III.11).

65 Siehe auch den ergänzenden Grundsatz "Verifizierung" (Anhang I, Abschnitt III.7).

(46) Darüber hinaus müssen die Organisationen Aufzeichnungen über die Umsetzung ihrer EU-US-DSGVO-Praktiken aufbewahren und diese auf Anfrage im Rahmen einer Untersuchung oder einer Beschwerde über die Nichteinhaltung einer unabhängigen Streitbeilegungsstelle oder einer zuständigen Durchsetzungsbehörde zur Verfügung stellen[66] .

### 2.3 Verwaltung, Beaufsichtigung und Durchsetzung

(47) Die EU-U.S. DPF wird vom DoC verwaltet und überwacht. Der Rahmen sieht Aufsichts- und Durchsetzungsmechanismen vor, um zu überprüfen und sicherzustellen, dass die Organisationen der EU-US-DPF die Grundsätze einhalten und dass gegen Verstöße vorgegangen wird. Diese Mechanismen sind in den Grundsätzen (Anhang I) und den vom DoC (Anhang III), der FTC (Anhang IV) und dem DoT (Anhang V) eingegangenen Verpflichtungen dargelegt.

#### *2.3.1 (Re-)Zertifizierung*

(48) Um sich im Rahmen der EU-US-DSGVO zu zertifizieren (bzw. jährlich neu zu zertifizieren), müssen die Organisationen öffentlich erklären, dass sie sich zur Einhaltung der Grundsätze verpflichten, ihre Datenschutzrichtlinien zur Verfügung stellen und diese vollständig umsetzen[67] . Als Teil ihrer (Re-)Zertifizierung )müssen die Organisationen dem DoC unter anderem den Namen der betreffenden Organisation, eine Beschreibung der Zwecke, für die die Organisation personenbezogene Daten verarbeitet, die personenbezogenen Daten, die von der Zertifizierung erfasst werden, sowie die gewählte Überprüfungsmethode, den entsprechenden unabhängigen Rechtsbehelfsmechanismus und die gesetzliche Stelle, die für die Durchsetzung der Einhaltung der Grundsätze zuständig ist, mitteilen[68] .

(49) Organisationen können personenbezogene Daten auf der Grundlage der EU-US-DSGVO ab dem Datum erhalten, an dem sie vom DoC in die Liste der DPR aufgenommen wurden. Um Rechtssicherheit zu gewährleisten und "falsche Behauptungen" zu vermeiden, dürfen Organisationen, die sich zum ersten Mal zertifizieren, nicht öffentlich auf ihre Einhaltung der Grundsätze verweisen, bevor die Datenschutzbehörde festgestellt hat, dass der Zertifizierungsantrag der Organisation vollständig ist, und die Organisation in die DPF-Liste[69] aufgenommen hat. Um sich weiterhin auf die EU-US-DSGVO berufen zu können, um personenbezogene Daten aus der Union zu erhalten, müssen diese Organisationen ihre Teilnahme an dem Rahmenwerk jährlich neu zertifizieren. Wenn eine Organisation aus irgendeinem Grund aus der EU-US-DSGVO ausscheidet, muss sie alle Erklärungen entfernen, die darauf hindeuten, dass die Organisation weiterhin an der Rahmenregelung teilnimmt[70] .

(50) Wie in den Verpflichtungen in Anhang III dargelegt, wird das DoC überprüfen, ob die Organisationen alle Zertifizierungsanforderungen erfüllen und eine (öffentliche) Datenschutzpolitik mit den gemäß dem *Grundsatz der Bekanntmachung*[71] erforderlichen Informationen eingeführt haben. Aufbauend auf den Erfahrungen mit dem (Re-)Zertifizierungsprozess im Rahmen des Privacy Shield wird das DoC eine Reihe von Überprüfungen durchführen, einschließlich der Überprüfung, ob die Datenschutzrichtlinien der Organisationen einen Hyperlink zum korrekten Beschwerdeformular auf der Website des entsprechenden Streitbeilegungsmechanismus enthalten, und, wenn mehrere Einheiten und Tochtergesellschaften einer Organisation in einem Zertifizierungsantrag enthalten sind, ob die Datenschutzrichtlinien jeder dieser Einheiten die Zertifizierungsanforderungen erfüllen und leicht zugänglich sind

66 Anhang I, Abschnitt III.7.

[67] Anhang I, Abschnitt I. 2.

[68] Anhang I, Abschnitt III.6.b und Anhang III, siehe Abschnitt "Überprüfung der Selbstzertifizierungsanforderungen".

[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 "Anforderungen an die Selbstzertifizierung überprüfen".

die den betroffenen Personen zur Verfügung stehen[72] . Darüber hinaus wird das DoC erforderlichenfalls Gegenkontrollen mit der FTC und dem DoT durchführen, um zu überprüfen, ob die Organisationen der in ihren (Re-)Zertifizierungsanträgen angegebenen Aufsichtsstelle unterliegen, und mit alternativen Streitbeilegungsstellen zusammenarbeiten, um zu überprüfen, ob die Organisationen für den in ihrem (Re-)Zertifizierungsantrag angegebenen unabhängigen Rechtsbehelfsmechanismus registriert sind[73] .

(51) Das DoC wird die Organisationen darüber informieren, dass sie alle bei der Überprüfung festgestellten Probleme angehen müssen, um die (Re-)Zertifizierung abschließen zu können. Reagiert eine Organisation nicht innerhalb des vom DoC gesetzten Zeitrahmens (bei der Rezertifizierung wird beispielsweise erwartet, dass der Prozess innerhalb von 45 Tagen abgeschlossen wird)[74] oder schließt sie ihre Zertifizierung anderweitig nicht ab, wird der Antrag als aufgegeben betrachtet. In diesem Fall können falsche Angaben über die Teilnahme oder die Einhaltung der EU-U.S. DPF von der FTC oder dem DoT[75] verfolgt werden.

(52) Um die ordnungsgemäße Anwendung der EU-US-DSGVO zu gewährleisten, müssen interessierte Parteien wie betroffene Personen, Datenexporteure und die nationalen Datenschutzbehörden in der Lage sein, die Organisationen zu identifizieren, die sich an die Grundsätze halten. Um diese Transparenz am "Eintrittspunkt" zu gewährleisten, hat sich das DoC verpflichtet, eine Liste der Organisationen zu führen und der Öffentlichkeit zugänglich zu machen, die ihre Einhaltung der Grundsätze zertifiziert haben und in den Zuständigkeitsbereich mindestens einer der in den Anhängen IV und V dieses Beschlusses genannten Durchsetzungsbehörden fallen[76] . Das DoC wird die Liste auf der Grundlage der jährlichen Neuzertifizierung einer Organisation sowie immer dann aktualisieren, wenn eine Organisation aus der DPF EU-USA austritt oder gestrichen wird. Um auch beim "Ausstieg" Transparenz zu gewährleisten, wird das DoC ein Verzeichnis der Organisationen führen, die von der Liste gestrichen wurden, und es der Öffentlichkeit zugänglich machen, wobei in jedem Fall der Grund für die Streichung angegeben wird[77] . Schließlich wird das DoC einen Link zur Webseite der FTC über die DPF EU-USA bereitstellen, auf der die Durchsetzungsmaßnahmen der FTC gemäß dem Rahmenwerk aufgeführt sind[78] .

### *2.3.2 Überwachung der Einhaltung*

(53) Das DoC wird die tatsächliche Einhaltung der Grundsätze durch die DPF-Organisationen aus der EU und den USA mit Hilfe verschiedener Mechanismen kontinuierlich überwachen[79] . Insbesondere wird es "Stichproben" bei zufällig ausgewählten Organisationen sowie Ad-hoc-Kontrollen bei bestimmten Organisationen durchführen, wenn potenzielle Probleme bei der Einhaltung der Grundsätze festgestellt werden (z. B. wenn sie dem DoC von Dritten gemeldet werden), um zu überprüfen, ob (i) Kontaktstellen für die Bearbeitung von Beschwerden und Anfragen der betroffenen Personen verfügbar sind und auf diese reagieren;
(ii) die Datenschutzpolitik der Organisation ist sowohl auf der Website als auch über ein Internetportal leicht zugänglich.

---

72 Anhang III, Abschnitt "Überprüfung der Anforderungen an die Selbstzertifizierung".

73 In ähnlicher Weise wird das DoC mit der dritten Partei zusammenarbeiten, die als Verwahrer der Gelder dient, die durch eine Gebühr für das DPA-Panel (siehe Erwägungsgrund 73) eingenommen werden, um zu überprüfen, ob Organisationen, die die DPAs als ihren unabhängigen Regressmechanismus gewählt haben, die Gebühr für das betreffende Jahr bezahlt haben. Siehe Anhang III, Abschnitt "Überprüfung der Selbstzertifizierungsanforderungen".

74 Anhang III, Fußnote 2.

[75] Siehe Anhang III, Abschnitt "Anforderungen an die Selbstzertifizierung überprüfen".

[76] Informationen über die Verwaltung der DPF-Liste finden sich in Anhang III (siehe die Einleitung unter "Verwaltung und Überwachung des Data Privacy Framework Program durch das Handelsministerium") und Anhang I (Abschnitt I.3, Abschnitt I.4, III.6.d und Abschnitt III.11.g).

[77] Anhang III, siehe die Einleitung unter "Verwaltung und Überwachung des Datenschutz-Rahmenprogramms durch das Handelsministerium".

[78] Siehe Anhang III, Abschnitt "Die Datenschutzrahmen-Website auf die Zielgruppen zuschneiden".

[79] Siehe Anhang III, Abschnitt "Regelmäßige von Amts wegen durchgeführte Überprüfungen und Bewertungen des Datenschutz-Rahmenprogramms".

(iii) die Datenschutzpolitik der Organisation weiterhin den Zertifizierungsanforderungen entspricht und (iv) das von der Organisation gewählte unabhängige Streitbeilegungsverfahren für die Bearbeitung von Beschwerden zur Verfügung steht[80] .

(54) Wenn es glaubwürdige Hinweise darauf gibt, dass eine Organisation ihre Verpflichtungen im Rahmen der EU-US-DSGVO nicht einhält (auch wenn das DoC Beschwerden erhält oder die Organisation nicht zufriedenstellend auf Anfragen des DoC antwortet), wird das DoC die Organisation auffordern, einen detaillierten Fragebogen auszufüllen und einzureichen[81] . Eine Organisation, die den Fragebogen nicht zufriedenstellend und rechtzeitig beantwortet, wird an die zuständige Behörde (die FTC oder das DoT) verwiesen, damit diese möglicherweise Durchsetzungsmaßnahmen ergreift[82] . Im Rahmen der Überwachung der Einhaltung des Datenschutzschildes führte das DoC regelmäßig die in Erwägungsgrund 53 erwähnten Stichproben durch und verfolgte kontinuierlich die öffentlichen Berichte, was es ihm ermöglichte, Probleme bei der Einhaltung der Vorschriften zu erkennen, anzugehen und zu lösen[83] . Organisationen, die die Grundsätze dauerhaft nicht einhalten, werden von der DPF-Liste gestrichen und müssen die im Rahmen des Rahmens erhaltenen personenbezogenen Daten zurückgeben oder löschen[84] .

(55) In anderen Fällen der Löschung, wie dem freiwilligen Rückzug von der Teilnahme oder der Nichtrezertifizierung, muss die Organisation die Daten entweder löschen oder zurückgeben oder kann sie aufbewahren, vorausgesetzt, sie bestätigt dem DoC jährlich ihre Verpflichtung, die Grundsätze weiterhin anzuwenden, oder sie gewährleistet einen angemessenen Schutz der personenbezogenen Daten auf andere zulässige Weise (z. B. durch die Verwendung eines Vertrags, der die Anforderungen der von der Kommission genehmigten einschlägigen Standardvertragsklauseln vollständig widerspiegelt)[85] . In diesem Fall muss eine Organisation auch eine Kontaktstelle innerhalb der Organisation für alle Fragen im Zusammenhang mit der EU-US-DSGVO benennen.

### *2.3.3 Erkennen und Angehen falscher Teilnahmeanträge*

(56) Das DoC wird sowohl von Amts wegen als auch auf der Grundlage von Beschwerden (z. B. von den Datenschutzbehörden) jede falsche Behauptung über die Teilnahme an der EU-US-DPF oder die missbräuchliche Verwendung der EU-US-DPF-Zertifizierungsmarke überwachen[86] . Insbesondere wird das DoC fortlaufend überprüfen, ob Organisationen, die (i) von der Teilnahme an der EU-US-DPF zurücktreten, (ii) die jährliche Re-Zertifizierung nicht abschließen (d. h. entweder begonnen, aber nicht rechtzeitig abgeschlossen haben oder gar nicht erst begonnen haben), die Zertifizierungsmarke nicht verwenden.

---

80 Im Rahmen seiner Überwachungsaktivitäten kann das DoC verschiedene Instrumente einsetzen, z. B. um nach defekten Links zu Datenschutzrichtlinien zu suchen oder die Nachrichten aktiv nach Berichten zu durchsuchen, die glaubwürdige Beweise für die Nichteinhaltung von Vorschriften liefern.

81 Siehe Anhang III, Abschnitt "Regelmäßige von Amts wegen durchgeführte Überprüfungen und Bewertungen des Datenschutz-Rahmenprogramms".

82 Siehe Anhang III, Abschnitt "Regelmäßige von Amts wegen durchgeführte Überprüfungen und Bewertungen des Datenschutz-Rahmenprogramms".

83 Bei der zweiten jährlichen Überprüfung des Privacy Shield teilte das DoC mit, dass es bei 100 Organisationen Stichprobenkontrollen durchgeführt und in 21 Fällen Fragebögen zur Einhaltung der Vorschriften versandt hatte (woraufhin die festgestellten Probleme behoben wurden), siehe SWD (2018) 497 final der Kommission, S. 9. In ähnlicher Weise berichtete das DoC bei der dritten jährlichen Überprüfung des Privacy Shield, dass es drei Vorfälle durch die Überwachung öffentlicher Berichte aufgedeckt und die Praxis eingeführt hat, jeden Monat Stichproben bei 30 Unternehmen durchzuführen, was in 28 % der Fälle zu Folgemaßnahmen mit Fragebögen zur Einhaltung der Vorschriften führte

(woraufhin die aufgedeckten Probleme sofort behoben oder in drei Fällen nach einem Mahnschreiben gelöst wurden), siehe Commission SWD (2019) 495 final, S. 8.

84 Anhang I Abschnitt III.11.g. Eine anhaltende Nichteinhaltung liegt insbesondere dann vor, wenn sich eine Organisation weigert, einer endgültigen Entscheidung einer Selbstregulierungs-, unabhängigen Streitbeilegungs- oder Durchsetzungsbehörde für den Datenschutz nachzukommen.

85 Anhang I, Abschnitt III.6.f.

86 Anhang III, Abschnitt "Suche nach und Umgang mit falschen Angaben zur Beteiligung".

(iii) als Teilnehmer gestrichen werden, insbesondere wegen "andauernder Nichteinhaltung", oder (iv) eine Erstzertifizierung nicht abschließen (d. h. begonnen haben, aber den Erstzertifizierungsprozess nicht rechtzeitig abgeschlossen haben), aus allen relevanten veröffentlichten Datenschutzrichtlinien Verweise auf die EU-US-DSGVO entfernen, die implizieren, dass die Organisation aktiv an der Rahmenrichtlinie teilnimmt[87] . Das DoC wird auch Internetrecherchen durchführen, um Verweise auf die EU-US-DSGVO in den Datenschutzrichtlinien von Organisationen zu ermitteln, auch um falsche Behauptungen von Organisationen zu identifizieren, die nie an der EU-US-DSGVO teilgenommen haben[88] .

(57) Stellt das DoC fest, dass Verweise auf die EU-U.S. DPF nicht entfernt wurden oder missbräuchlich verwendet werden, wird es die Organisation über eine mögliche Verweisung an die FTC/DoT[89] informieren. Reagiert eine Organisation nicht in zufriedenstellender Weise, wird das DoC die Angelegenheit an die zuständige Behörde weiterleiten, damit diese möglicherweise Durchsetzungsmaßnahmen ergreift[90] . Jede Falschdarstellung gegenüber der Öffentlichkeit durch eine Organisation in Bezug auf die Einhaltung der Grundsätze in Form von irreführenden Aussagen oder Praktiken kann von der FTC, dem DoT oder anderen zuständigen US-Durchsetzungsbehörden verfolgt werden. Falsche Darstellungen gegenüber dem DoC sind nach dem False Statements Act (18 U.S.C. § 1001) durchsetzbar.

### *2.3.4 Vollstreckung*

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

(59) DPF-Organisationen aus der EU und den USA müssen der Rechtsprechung der zuständigen US-Behörden - der FTC und des DoT - unterliegen, 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 Ineffizienz, Pflichtverletzung oder Amtsmissbrauchs abgesetzt werden. Der FTC dürfen nicht mehr als drei Kommissionsmitglieder derselben politischen Partei angehören, und die Kommissionsmitglieder dürfen während ihrer Amtszeit keine anderen Geschäfte, Berufe oder Beschäftigungen ausüben.

(61) Die FTC kann die Einhaltung der Grundsätze sowie falsche Behauptungen über die Einhaltung der Grundsätze oder die Teilnahme an der EU-U.S. DPF durch Organisationen untersuchen, die entweder nicht mehr auf der DPF-Liste stehen oder nie zertifiziert wurden[93] . Die FTC kann

---

87 *Ebd*.

88 *Ebd*.

89 *Ebd*.

90 Im Rahmen des Privacy Shield berichtete das DoC bei der dritten jährlichen Überprüfung des Rahmens, dass es 669 Fälle falscher Teilnahmeanträge (zwischen Oktober 2018 und Oktober 2019) festgestellt hat, von denen die meisten nach dem Warnschreiben des DoC beigelegt wurden, wobei 143 Fälle an die FTC weitergeleitet wurden (siehe Erwägungsgrund 62 unten). Siehe SWD (2019) 495 final der Kommission, S. 10.

91 Eine DPF-Organisation aus der EU und den USA muss sich öffentlich zur Einhaltung der Grundsätze

verpflichten, ihre Datenschutzpolitik im Einklang mit diesen Grundsätzen offenlegen und sie vollständig umsetzen. Die Nichteinhaltung der Grundsätze kann gemäß Abschnitt 5 des FTC-Gesetzes zum Verbot unlauterer und irreführender Handlungen im oder mit Bezug auf den Handel (15 U.S.C. §45) und gemäß 49 U.S.C. §41712 durchgesetzt werden, der Luftfahrtunternehmen oder Flugscheinvermittlern unlautere oder irreführende Praktiken im Luftverkehr oder beim Verkauf von Luftverkehrsleistungen untersagt.

92 15 U.S.C. § 41.

93 Anhang IV.

die Einhaltung der Vorschriften durchsetzen, indem sie behördliche oder bundesgerichtliche Anordnungen (einschließlich der durch Vergleiche erzielten "consent orders")[94] für einstweilige oder dauerhafte Verfügungen oder andere Rechtsbehelfe erwirkt, und wird die Einhaltung solcher Anordnungen systematisch überwachen[95] . Kommen Unternehmen solchen Anordnungen nicht nach, kann die FTC zivilrechtliche Strafen und andere Abhilfemaßnahmen fordern, auch für Schäden, die durch das rechtswidrige Verhalten entstanden sind. Jede an eine DPF-Organisation in der EU oder in den USA ergangene Zustimmungsanordnung wird Bestimmungen zur Selbstauskunft enthalten[96] , und die Organisationen werden verpflichtet sein, alle relevanten Abschnitte eines der FTC vorgelegten Berichts über die Einhaltung der Vorschriften oder die Bewertung der DPF in der EU oder in den USA zu veröffentlichen. Schließlich wird die FTC eine Online-Liste der Organisationen führen, gegen die FTC- oder Gerichtsbeschlüsse in EU-US-DSGVO-Fällen ergangen sind[97] .

(62) In Bezug auf das Privacy Shield hat die FTC in etwa 22 Fällen Durchsetzungsmaßnahmen ergriffen, und zwar sowohl im Hinblick auf Verstöße gegen spezifische Anforderungen des Rahmenwerks (z. B. Versäumnis, dem DoC zu bestätigen, dass die Organisation den Schutz des Privacy Shield auch nach dem Ausscheiden aus dem Rahmenwerk weiterhin anwendet, Versäumnis, durch eine Selbstbewertung oder eine externe Überprüfung der Einhaltung zu überprüfen, dass die Organisation das Rahmenwerk einhält)[98] als auch im Hinblick auf falsche Behauptungen über die Teilnahme am Rahmenwerk (z. B. durch Organisationen, die es versäumt haben, die notwendigen Schritte für eine Zertifizierung zu unternehmen oder die Zertifizierung auslaufen ließen, aber fälschlicherweise die weitere Teilnahme an dem Rahmenwerk angaben).z. B. durch Organisationen, die es versäumt haben, die für die Zertifizierung erforderlichen Schritte zu unternehmen, oder die ihre Zertifizierung auslaufen ließen, aber ihre weitere Teilnahme falsch darstellten)[99] . Diese Durchsetzungsmaßnahmen resultierten unter anderem aus dem proaktiven Einsatz von Verwaltungsvorladungen, um von bestimmten Teilnehmern am Privacy Shield Material zu erhalten, um zu prüfen, ob wesentliche Verstöße gegen die Verpflichtungen des Privacy Shield vorliegen[100] .

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

---

94 Nach Angaben der FTC ist sie nicht befugt, im Bereich des Datenschutzes Vor-Ort-Kontrollen durchzuführen. Sie ist jedoch befugt, Organisationen zur Vorlage von Dokumenten und zur Abgabe von Zeugenaussagen zu zwingen (siehe Abschnitt 20 des FTC-Gesetzes), und kann solche Anordnungen im Falle der Nichteinhaltung gerichtlich durchsetzen.

95 Siehe Anhang IV, Abschnitt "Beschaffungs- und Überwachungsaufträge".

96 Die FTC oder gerichtliche Anordnungen können Unternehmen dazu verpflichten, Datenschutzprogramme einzuführen und der FTC regelmäßig Berichte über die Einhaltung der Vorschriften oder Bewertungen dieser Programme durch unabhängige Dritte zur Verfügung zu stellen.

97 Anhang IV, Abschnitt "Aufforderung zur Einreichung von Vorschlägen und Überwachung von Aufträgen".

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

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

100 Siehe z. B. die vorbereiteten Bemerkungen des Vorsitzenden Joseph Simons bei der zweiten jährlichen

Überprüfung des Datenschutzschildes (ftc.gov).

101 Siehe z. B. die Anordnung der FTC in der Rechtssache Drizly, LLC, in der das Unternehmen u. a. aufgefordert wird, (1) alle von ihm gesammelten personenbezogenen Daten zu vernichten, die nicht für die Bereitstellung von Produkten oder Dienstleistungen für Verbraucher erforderlich sind, (2) die Erhebung oder Speicherung personenbezogener Daten zu unterlassen, sofern sie nicht für bestimmte, in einem Aufbewahrungszeitplan festgelegte Zwecke erforderlich sind.

102 Siehe z. B. die FTC-Anordnung in der Sache CafePress (24. März 2022), in der u. a. gefordert wird, die Menge der erhobenen Daten zu minimieren.

103 Siehe z. B. die Durchsetzungsmaßnahmen der FTC in den Fällen Drizzly, LLC und CafePress, in denen sie die betreffenden Unternehmen aufforderte, ein spezielles Sicherheitsprogramm oder spezifische Sicherheitsmaßnahmen einzuführen. Was Datenschutzverletzungen betrifft, siehe auch die FTC-Verfügung vom 27. Januar 2023 in der Sache Chegg, den 2019 mit Equifax geschlossenen Vergleich (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. den Fall RealPage, Inc. (16. Oktober 2018), in dem die FTC auf der Grundlage des FCRA Durchsetzungsmaßnahmen gegen ein Mieter-Screening-Unternehmen ergriff, das Hintergrundberichte über Einzelpersonen für Immobilien

(64) Das DoT hat die ausschließliche Befugnis, die Datenschutzpraktiken von Fluggesellschaften zu regeln, und teilt sich die Zuständigkeit mit der FTC in Bezug auf die Datenschutzpraktiken von Flugscheinvermittlern beim Verkauf von Flugreisen. Die Beamten des DoT versuchen zunächst, eine Einigung zu erzielen, und wenn dies nicht möglich ist, können sie ein Durchsetzungsverfahren mit einer Beweisanhörung vor einem Verwaltungsrichter des DoT einleiten, der befugt ist, Unterlassungsanordnungen und zivilrechtliche Sanktionen zu erlassen[105] . Verwaltungsrichter genießen nach dem Verwaltungsverfahrensgesetz (Administrative Procedure Act - APA) mehrere Schutzmaßnahmen, um ihre Unabhängigkeit und Unparteilichkeit zu gewährleisten. So können sie beispielsweise nur aus triftigen Gründen entlassen werden; sie werden nach dem Rotationsprinzip mit Fällen betraut; sie dürfen keine Aufgaben wahrnehmen, die mit ihren Pflichten und Verantwortlichkeiten als Verwaltungsrichter unvereinbar sind; sie unterliegen nicht der Aufsicht durch das Untersuchungsteam der Behörde, bei der sie angestellt sind (in diesem Fall das DoT); und sie müssen ihre Funktion als Richter bzw. Vollstrecker unparteiisch ausüben[106] . Das DoT hat sich verpflichtet, Vollstreckungstitel zu überwachen und sicherzustellen, dass Anordnungen, die aus EU-U.S. DPF-Fälle sind auf der Website[107] verfügbar.

### 2.4 Abhilfe

(65) Um einen angemessenen Schutz und insbesondere die Durchsetzung der Rechte des Einzelnen zu gewährleisten, sollte der betroffenen Person ein wirksamer administrativer und gerichtlicher Rechtsbehelf zur Verfügung stehen.

(66) Die EU-US-DSGVO verlangt von den Organisationen durch den *Grundsatz des Rückgriffs, der Durchsetzung und der Haftung,* dass sie Rechtsmittel für Personen vorsehen, die von der Nichteinhaltung der Vorschriften betroffen sind, und somit den betroffenen Personen in der Union die Möglichkeit geben, Beschwerden über die Nichteinhaltung der Vorschriften durch die EU-US-DSGVO einzureichen und diese Beschwerden erforderlichenfalls durch eine Entscheidung, die einen wirksamen Rechtsbehelf vorsieht, beheben zu lassen[108] . Im Rahmen ihrer Zertifizierung müssen die Organisationen die Anforderungen dieses Grundsatzes erfüllen, indem sie wirksame und leicht zugängliche unabhängige Rechtsbehelfsmechanismen vorsehen, mit denen die Beschwerden und Streitigkeiten jeder einzelnen Person untersucht und zügig und ohne Kosten für die betroffene Person beigelegt werden können[109] .

(67) Organisationen können sich für unabhängige Rechtsbehelfsmechanismen in der Union oder in den Vereinigten Staaten entscheiden. Wie in Erwägungsgrund 73 näher erläutert, beinhaltet dies die Möglichkeit, sich freiwillig zur Zusammenarbeit mit den EU-Datenschutzbehörden zu verpflichten. Wenn Organisationen Personaldaten verarbeiten, ist eine solche Verpflichtung zur Zusammenarbeit mit den EU-DSGVOs obligatorisch. Andere Alternativen sind unabhängige alternative Streitbeilegungsverfahren oder von der Privatwirtschaft entwickelte Datenschutzprogramme, die die Grundsätze in ihre Vorschriften aufnehmen. Letztere müssen wirksame Durchsetzungsmechanismen in Übereinstimmung mit den Anforderungen des *Grundsatzes "Rückgriff, Durchsetzung und Haftung"* umfassen.

(68) Folglich bietet die EU-US-DSGVO den betroffenen Personen eine Reihe von Möglichkeiten, ihre Rechte geltend zu machen, Beschwerden über die Nichteinhaltung der Vorschriften durch EU-US-Organisationen einzureichen und eine Lösung für ihre Beschwerden zu finden, gegebenenfalls durch eine Entscheidung

---

Die FTC stellte fest, dass das Unternehmen keine angemessenen Maßnahmen ergriff, um die Richtigkeit der Informationen zu gewährleisten, die es auf der Grundlage seines automatischen Entscheidungstools

zur Verfügung stellte. Die FTC stellte fest, dass das Unternehmen keine angemessenen Maßnahmen ergriffen hat, um die Richtigkeit der Informationen zu gewährleisten, die es auf der Grundlage seines automatischen Entscheidungstools bereitstellt.

105 Siehe Anhang V, Abschnitt "Durchsetzungspraktiken".

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

107 Anhang V, siehe Abschnitt "Überwachung und öffentliche Durchsetzungsanordnungen bei Verstößen gegen die EU-US-DSGVO".

108 Anhang I, Abschnitt II.7.

109 Anhang I, Abschnitt III.11.

Bereitstellung eines wirksamen Rechtsbehelfs. Einzelpersonen können eine Beschwerde direkt bei einer Organisation, bei einer von der Organisation benannten unabhängigen Streitbeilegungsstelle, bei den nationalen Datenschutzbehörden, beim DoC oder bei der FTC einreichen. In Fällen, in denen ihre Beschwerden durch keinen dieser Rechtsbehelfs- oder Durchsetzungsmechanismen gelöst werden konnten, haben Einzelpersonen auch das Recht, ein verbindliches Schiedsverfahren in Anspruch zu nehmen (Anhang I zu diesem Beschluss). Mit Ausnahme des Schiedspanels, das erst nach Ausschöpfung bestimmter Rechtsbehelfe angerufen werden kann, steht es den Betroffenen frei, einen oder alle Rechtsbehelfe ihrer Wahl in Anspruch zu nehmen, und sie sind nicht verpflichtet, einen Rechtsbehelf dem anderen vorzuziehen oder eine bestimmte Reihenfolge einzuhalten.

(69) Erstens können die betroffenen Personen in der Union Fälle der Nichteinhaltung der Grundsätze durch direkte Kontakte mit den EU-US-DSGVOrganisationen[110] verfolgen. Um eine Lösung zu erleichtern, muss die Organisation einen wirksamen Rechtsbehelfsmechanismus einrichten, um solche Beschwerden zu bearbeiten. Die Datenschutzpolitik einer Organisation muss daher den Einzelnen eindeutig über eine Kontaktstelle innerhalb oder außerhalb der Organisation informieren, die für die Bearbeitung von Beschwerden zuständig ist (einschließlich aller einschlägigen Einrichtungen in der Union, die auf Anfragen oder Beschwerden reagieren können), sowie über die benannte unabhängige Streitbeilegungsstelle (siehe Erwägungsgrund 70). Nach Eingang der Beschwerde einer betroffenen Person, entweder direkt von der betroffenen Person oder über die Beschwerdestelle nach Verweisung durch eine Datenschutzbehörde, muss die Organisation der betroffenen Person in der Union innerhalb von 45 Tagen eine Antwort zukommen lassen[111] . Ebenso sind Organisationen verpflichtet, auf Anfragen und andere Informationsersuchen der Datenschutzbehörde oder einer Datenschutzbehörde[112] (wenn die Organisation sich zur Zusammenarbeit mit der Datenschutzbehörde verpflichtet hat) bezüglich der Einhaltung der Grundsätze unverzüglich zu antworten.

(70) Zweitens können Einzelpersonen auch direkt eine Beschwerde bei einer unabhängigen Streitbeilegungsstelle (entweder in den Vereinigten Staaten oder in der Union) einreichen, die von einer Organisation benannt wurde, um individuelle Beschwerden zu untersuchen und zu lösen (es sei denn, sie sind offensichtlich unbegründet oder leichtfertig) und der Einzelperson kostenlos angemessene Rechtsmittel zur Verfügung zu stellen[113] . Die von einer solchen Stelle verhängten Sanktionen und Rechtsbehelfe müssen streng genug sein, um die Einhaltung der Grundsätze durch die Organisationen zu gewährleisten, und sollten eine Rückgängigmachung oder Korrektur der Auswirkungen der Nichteinhaltung durch die Organisation und je nach den Umständen die Beendigung der weiteren Verarbeitung der betreffenden personenbezogenen Daten und/oder deren Löschung sowie eine öffentliche Bekanntmachung der Nichteinhaltung vorsehen[114] . Unabhängige Streitbeilegungsstellen, die von einer Organisation benannt werden, sind verpflichtet, auf ihren öffentlichen Websites einschlägige Informationen über die EU-US-DSGVO und die von ihnen im Rahmen der DSGVO erbrachten Dienstleistungen zu veröffentlichen[115] . Jedes Jahr müssen sie einen Jahresbericht mit Gesamtstatistiken über diese Dienste veröffentlichen[116] .

(71) Im Rahmen ihrer Verfahren zur Überprüfung der Einhaltung der Vorschriften kann das DoC überprüfen, ob die EU-US-DPF-Organisationen tatsächlich bei den unabhängigen Regressmechanismen registriert sind, die sie

110 Anhang I, Abschnitt III.11.d.(i).

111 Anhang I, Abschnitt III.11.d.(i).

112 Dabei handelt es sich um die von dem Gremium der Datenschutzbehörden gemäß dem ergänzenden

Grundsatz "Die Rolle der Datenschutzbehörden" (Anhang I, Abschnitt III.5) benannte Bearbeitungsbehörde.

113 Anhang I, Abschnitt III.11.d.

114 Anhang I, Abschnitt II.7 und III.11.e.

115 Anhang I, Abschnitt III.11.d.(ii).

116 Der Jahresbericht muss enthalten: (1) die Gesamtzahl der im Berichtsjahr eingegangenen Beschwerden im Zusammenhang mit der EU-US-Drogenbekämpfungsbehörde; (2) die Art der eingegangenen Beschwerden; (3) Qualitätsmaßstäbe für die Streitbeilegung, z. B. die Dauer der Beschwerdebearbeitung; und (4) die Ergebnisse der eingegangenen Beschwerden, insbesondere die Anzahl und Art der verhängten Abhilfemaßnahmen oder Sanktionen.

behaupten, dass sie bei[117] registriert sind. Sowohl die Organisationen als auch die zuständigen unabhängigen Rückgriffsmechanismen sind verpflichtet, unverzüglich auf Anfragen und Ersuchen des DoC um Informationen im Zusammenhang mit der EU-U.S. DPF zu reagieren. Das DoC wird mit den unabhängigen Rückgriffsmechanismen zusammenarbeiten, um zu überprüfen, ob sie auf ihren Websites Informationen über die Grundsätze und die Dienstleistungen, die sie im Rahmen der EU-U.S.-Entscheidungsinitiative anbieten, bereitstellen und ob sie Jahresberichte veröffentlichen[118] .

(72) Kommt die Organisation der Entscheidung einer Streitbeilegungs- oder Selbstregulierungsstelle nicht nach, muss diese das DoC und die FTC (oder eine andere US-Behörde, die für die Untersuchung der Nichteinhaltung durch die Organisation zuständig ist) oder ein zuständiges Gericht[119] über die Nichteinhaltung informieren. Weigert sich eine Organisation, einer endgültigen Entscheidung einer Selbstregulierungsstelle für den Datenschutz, einer unabhängigen Streitbeilegungsstelle oder einer staatlichen Stelle nachzukommen, oder stellt eine solche Stelle fest, dass eine Organisation die Grundsätze häufig nicht einhält, kann dies als anhaltende Nichteinhaltung angesehen werden, so dass das DoC die Organisation, die die Grundsätze nicht einhält, nach einer ersten 30-tägigen Benachrichtigung und einer Gelegenheit zur Stellungnahme von der DPF-Liste streichen wird[120] . Wenn die Organisation nach der Streichung von der Liste weiterhin die EU-US-DPF-Zertifizierung beansprucht, wird das DoC sie an die FTC oder eine andere Durchsetzungsbehörde verweisen[121] .

(73) Drittens können Einzelpersonen ihre Beschwerden auch bei einer nationalen Datenschutzbehörde in der Union einreichen, die von ihren Untersuchungs- und Abhilfebefugnissen gemäß der Verordnung (EU) 2016/679 Gebrauch machen kann. Organisationen sind verpflichtet, bei der Untersuchung und Beilegung einer Beschwerde durch eine Datenschutzbehörde zu kooperieren, entweder wenn es um die Verarbeitung von Personaldaten geht, die im Rahmen eines Beschäftigungsverhältnisses erhoben wurden, oder wenn sich die jeweilige Organisation freiwillig der Aufsicht durch die Datenschutzbehörden unterworfen hat[122] . Insbesondere müssen die Organisationen auf Anfragen reagieren, den Ratschlägen der Datenschutzbehörde Folge leisten, auch in Bezug auf Abhilfe- oder Ausgleichsmaßnahmen, und der Datenschutzbehörde schriftlich bestätigen, dass diese Maßnahmen ergriffen wurden[123] . Bei Nichteinhaltung der von der Datenschutzbehörde erteilten Ratschläge verweist die Datenschutzbehörde solche Fälle an das US-Handelsministerium (das Organisationen von der EU-US-DSGVO-Liste streichen kann) oder, im Hinblick auf mögliche Durchsetzungsmaßnahmen, an die FTC oder das US-Handelsministerium (die Nichtzusammenarbeit mit den Datenschutzbehörden oder die Nichteinhaltung der Grundsätze ist nach US-Recht strafbar)[124] .

(74) Um die Zusammenarbeit bei der effektiven Bearbeitung von Beschwerden zu erleichtern, haben sowohl das DoC als auch die FTC eine spezielle Kontaktstelle eingerichtet, die für die direkte Verbindung mit den Datenschutzbehörden zuständig ist[125] . Diese Kontaktstellen helfen bei Anfragen der Datenschutzbehörden bezüglich der Einhaltung der Grundsätze durch eine Organisation.

[117] Anhang I, Abschnitt "Überprüfung der Anforderungen an die Selbstzertifizierung".

118 Siehe Anhang III, Abschnitt "Erleichterung der Zusammenarbeit mit alternativen Streitbeilegungsstellen, die prinzipienbezogene 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 die Ziffern ii und iii.

121 Siehe Anhang III, Abschnitt "Suche nach und Umgang mit falschen Angaben zur Beteiligung".

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 "Verweisungspriorisierung und Untersuchung" und "Durchsetzungszusammenarbeit mit den EU-Datenschutzbehörden").

(75) Der Ratschlag der Datenschutzbehörden[126] wird erteilt, nachdem beide Streitparteien ausreichend Gelegenheit hatten, sich zu äußern und alle gewünschten Beweise vorzulegen. Das Gremium kann den Rat so schnell erteilen, wie es das Erfordernis eines ordnungsgemäßen Verfahrens zulässt, in der Regel jedoch innerhalb von 60 Tagen nach Eingang einer Beschwerde[127] . Kommt eine Organisation der Aufforderung nicht innerhalb von 25 Tagen nach Zustellung des Gutachtens nach und bietet sie keine zufriedenstellende Erklärung für die Verzögerung, kann das Gremium seine Absicht bekannt geben, entweder die Angelegenheit der FTC (oder einer anderen zuständigen US-Durchsetzungsbehörde) zu unterbreiten oder zu dem Schluss zu kommen, dass die Verpflichtung zur Zusammenarbeit ernsthaft verletzt wurde. In der ersten Alternative kann dies zu Durchsetzungsmaßnahmen auf der Grundlage von Abschnitt 5 des FTC Act (oder eines ähnlichen Gesetzes)[128] führen. In der zweiten Alternative informiert das Gremium das DoC, das die Weigerung der Organisation, den Ratschlägen des DPA-Gremiums nachzukommen, als anhaltende Nichterfüllung betrachtet, die zur Streichung der Organisation von der DPF-Liste führt.

(76) Wenn die Datenschutzbehörde, an die die Beschwerde gerichtet wurde, keine oder nur unzureichende Maßnahmen ergriffen hat, um einer Beschwerde nachzugehen, hat der einzelne Beschwerdeführer die Möglichkeit, diese (Un-)Maßnahmen vor den nationalen Gerichten des jeweiligen EU-Mitgliedstaats anzufechten.

(77) Einzelpersonen können sich auch dann mit Beschwerden an die Datenschutzbehörden wenden, wenn das Gremium der Datenschutzbehörde nicht als Streitbeilegungsstelle einer Organisation benannt worden ist. In diesen Fällen kann die DPA solche Beschwerden entweder an das DoC oder die FTC weiterleiten. Zur Erleichterung und Verstärkung der Zusammenarbeit in Angelegenheiten, die einzelne Beschwerden und die Nichteinhaltung der Grundsätze durch die DPF-Organisationen der EU und der USA betreffen, wird das DoC eine spezielle Kontaktstelle einrichten, die als Verbindungsstelle fungiert und bei Anfragen der DPA bezüglich der Einhaltung der Grundsätze durch eine Organisation behilflich ist[129] . Auch die FTC hat sich verpflichtet, eine eigene Kontaktstelle einzurichten[130] .

(78) Viertens hat sich das DoC verpflichtet, Beschwerden über die Nichteinhaltung der Grundsätze durch eine Organisation entgegenzunehmen, zu prüfen und sich nach besten Kräften um eine Lösung zu bemühen[131] . Zu diesem Zweck sieht das DoC spezielle Verfahren für die Datenschutzbehörden vor, um Beschwerden an eine spezielle Kontaktstelle weiterzuleiten, sie zu verfolgen und mit den Organisationen Kontakt aufzunehmen, um die Lösung zu erleichtern[132] . Um die Bearbeitung einzelner Beschwerden zu beschleunigen, steht die Kontaktstelle in Fragen der Einhaltung der Grundsätze direkt mit der jeweiligen Datenschutzbehörde in Verbindung und informiert sie insbesondere innerhalb von höchstens 90 Tagen nach der Weiterleitung über den Stand der Beschwerden[133] . Auf diese Weise können betroffene Personen Beschwerden über die Nichteinhaltung der Vorschriften durch EU-US-DSGVO-Organisationen direkt bei ihrer nationalen Datenschutzbehörde einreichen und sie an das DoC als US-Behörde weiterleiten, die die EU-US-DSGVO verwaltet.

(79) Kommt die Aufsichtsbehörde aufgrund von Überprüfungen von Amts wegen, Beschwerden oder anderen Informationen zu dem Schluss, dass eine Organisation die Grundsätze dauerhaft nicht eingehalten hat, kann sie diese Organisation von der DPF-Liste streichen[134] . Verweigerung der Befolgung einer endgültigen Entscheidung einer Selbstregulierungsorganisation für den Datenschutz, eines unabhängigen Schiedsgerichts

[126] Die Geschäftsordnung des informellen Gremiums der Datenschutzbehörden sollte von den

Datenschutzbehörden auf der Grundlage ihrer Kompetenz zur Organisation ihrer Arbeit und zur Zusammenarbeit untereinander festgelegt werden.

127 Anhang I, Abschnitt III.5.c.(i).

128 Anhang I, Abschnitt III.5.c.(ii).

129 Siehe Anhang III, Abschnitt "Erleichterung der Zusammenarbeit mit den Datenschutzbehörden".

130 Siehe Anhang IV, Abschnitte "Verweisungsprioritäten und Ermittlungen" und "Zusammenarbeit mit den EU-Datenschutzbehörden".

131 Anhang III, siehe z. B. den 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.

oder einer staatlichen Stelle, einschließlich einer Datenschutzbehörde, wird als anhaltende Nichteinhaltung angesehen[135] .

(80) Fünftens muss eine DPF-Organisation aus der EU und den USA der Rechtsprechung der US-Behörden unterliegen, insbesondere der FTC[136] , die über die notwendigen Ermittlungs- und Durchsetzungsbefugnisse verfügen, um die Einhaltung der Grundsätze wirksam sicherzustellen. Die FTC prüft vorrangig Hinweise auf die Nichteinhaltung der Grundsätze, die von unabhängigen Streitbeilegungs- oder Selbstregulierungsgremien, dem DoC und den DPAs (auf eigene Initiative oder aufgrund von Beschwerden) eingehen, um festzustellen, ob ein Verstoß gegen Abschnitt 5 des FTC Act vorliegt[137] . Die FTC hat sich verpflichtet, ein standardisiertes Verweisungsverfahren einzurichten, eine Kontaktstelle in der Behörde für die Verweisung von DPAs zu benennen und Informationen über Verweisungen auszutauschen. Darüber hinaus kann sie Beschwerden von Einzelpersonen direkt entgegennehmen und auf eigene Initiative Untersuchungen der Datenschutzbehörden der EU und der USA durchführen, insbesondere im Rahmen ihrer umfassenderen Untersuchung von Datenschutzfragen.

(81) Sechstens kann die betroffene Person in der Union als "letztes Mittel" für den Fall, dass keiner der anderen verfügbaren Rechtsbehelfe die Beschwerde einer Person zufriedenstellend gelöst hat, ein verbindliches Schiedsverfahren durch das "EU-U.S. Data Privacy Framework Panel" (EU-U.S. DPF Panel)[138] in Anspruch nehmen. Die Organisationen müssen die betroffenen Personen über die Möglichkeit, ein verbindliches Schiedsverfahren in Anspruch zu nehmen, informieren und sind verpflichtet, darauf zu reagieren, sobald eine betroffene Person diese Möglichkeit in Anspruch genommen hat, indem sie der betreffenden Organisation eine Mitteilung zukommen lassen[139] .

(82) Dieses EU-US-DSGVO-Panel besteht aus einem Pool von mindestens zehn Schiedsrichtern, die vom DoC und der Kommission aufgrund ihrer Unabhängigkeit und Integrität sowie ihrer Erfahrung mit dem US-amerikanischen Datenschutzrecht und dem Datenschutzrecht der Union benannt werden. Für jede einzelne Streitigkeit wählen die Parteien aus diesem Pool ein Panel mit einem oder drei Schiedsrichtern aus[140] .

(83) Das Internationale Zentrum für Streitbeilegung (ICDR), die internationale Abteilung der American Arbitration Association (AAA), wurde vom DoC mit der Durchführung der Schiedsverfahren beauftragt. Die Verfahren vor dem DPF-Panel EU-USA werden durch eine Reihe von vereinbarten Schiedsregeln und einen Verhaltenskodex für die ernannten Schiedsrichter geregelt. Die Website der IKSR und der AAA bietet klare und präzise Informationen über das Schiedsverfahren und das Verfahren zur Beantragung eines Schiedsverfahrens.

(84) Die zwischen dem DoC und der Kommission vereinbarte Schlichtungsregelung ergänzt die EU-U.S. Diese enthält mehrere Merkmale, die die Zugänglichkeit dieses Verfahrens für die betroffenen Personen in der Union verbessern: (i) Bei der Vorbereitung einer Klage vor dem Schiedsgericht kann die betroffene Person von ihrer nationalen Datenschutzbehörde unterstützt werden; (ii) das Schiedsverfahren findet zwar in den Vereinigten Staaten statt, aber die betroffenen Personen in der Union können sich für eine Teilnahme per Video- oder Telefonkonferenz entscheiden, die für die betroffene Person kostenlos ist; (iii) das Schiedsverfahren wird in der Regel in englischer Sprache abgehalten, aber ein Dolmetscher bei der Schiedsanhörung und eine Übersetzung werden grundsätzlich auf begründeten Antrag und ohne Kosten für die betroffene Person zur Verfügung gestellt; (iv) und schließlich muss zwar jede Partei ihre eigenen Kosten tragen.

135 Anhang I, Abschnitt III.11.g.

136 Eine DPF-Organisation aus der EU und den USA muss sich öffentlich zur Einhaltung der Grundsätze verpflichten, ihre Datenschutzpolitik im Einklang mit diesen Grundsätzen öffentlich bekannt geben und sie vollständig umsetzen. Die Nichteinhaltung kann gemäß Abschnitt 5 des FTC Acts, der unlautere und irreführende Handlungen im oder auf den Handel verbietet, durchgesetzt werden.

137 Siehe auch die vom DoT eingegangenen ähnlichen Verpflichtungen, Anhang V.

138 Siehe Anhang I, Anhang I "Schiedsgerichtsmodell".

139 Siehe Anhang I, Abschnitt II.1.a.(xi) und II.7.c.

140 Die Anzahl der Schiedsrichter im Gremium muss von den Parteien vereinbart werden.

Anwaltskosten, wenn sie sich vor dem Panel von einem Anwalt vertreten lassen, wird das DoC einen Fonds unterhalten, der mit jährlichen Beiträgen der DPF-Organisationen der EU und der USA gespeist wird, die die Kosten des Schiedsverfahrens bis zu einem von den US-Behörden in Absprache mit der Kommission[141] festzulegenden Höchstbetrag decken sollen.

(85) Das EU-U.S. DPF-Panel ist befugt, individuelle, nicht-monetäre Rechtsmittel[142] zu verhängen, die notwendig sind, um die Nichteinhaltung der Grundsätze zu beheben. Das Gremium berücksichtigt bei seiner Entscheidung auch andere Rechtsbehelfe, die bereits durch andere EU-US-DSGVO-Mechanismen erlangt wurden, doch können Betroffene immer noch ein Schiedsverfahren in Anspruch nehmen, wenn sie diese anderen Rechtsbehelfe für unzureichend halten. So können betroffene Personen in der Union in allen Fällen, in denen die Maßnahmen oder die Untätigkeit von EU-US-DSGVOrganisationen, unabhängigen Rechtsbehelfsmechanismen oder den zuständigen US-Behörden (z. B. der FTC) ihre Beschwerden nicht zufriedenstellend gelöst haben, ein Schiedsverfahren anrufen. Ein Schiedsverfahren kann nicht in Anspruch genommen werden, wenn eine Datenschutzbehörde rechtlich befugt ist, die betreffende Forderung gegenüber der EU-US-DSGVO zu klären, d. h. in den Fällen, in denen die Organisation entweder verpflichtet ist, mit den Datenschutzbehörden zusammenzuarbeiten und deren Ratschläge in Bezug auf die Verarbeitung von im Beschäftigungskontext erhobenen Personaldaten zu befolgen, oder sich freiwillig dazu verpflichtet hat. Einzelpersonen können den Schiedsspruch bei der
US-Gerichte im Rahmen des Federal Arbitration Act, wodurch ein Rechtsbehelf für den Fall gewährleistet ist, dass eine Organisation die Vorschriften nicht einhält.

(86) Siebtens: Wenn eine Organisation ihrer Verpflichtung zur Einhaltung der Grundsätze und der veröffentlichten Datenschutzrichtlinien nicht nachkommt, stehen nach amerikanischem Recht zusätzliche Rechtsmittel zur Verfügung, darunter auch Schadensersatz. So können Einzelpersonen unter bestimmten Bedingungen im Rahmen der Verbraucherschutzgesetze der Bundesstaaten bei betrügerischen Falschdarstellungen, unlauteren oder irreführenden Handlungen oder Praktiken[143] und im Rahmen des Deliktsrechts (insbesondere im Rahmen der Delikte des Eindringens in die Privatsphäre[144] , der Aneignung des Namens oder des Bildes[145] und der öffentlichen Bekanntgabe privater Tatsachen[146] ) gerichtlichen Rechtsschutz (einschließlich Schadensersatz) erhalten.

(87) Die oben beschriebenen Rechtsbehelfe stellen sicher, dass jede Beschwerde über die Nichteinhaltung der EU-U.S. DSGVO durch zertifizierte Organisationen wirksam entschieden und behoben wird.

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

141 Anhang I von Anhang I, Abschnitt G.6.

142 Einzelpersonen können in einem Schiedsverfahren keine Schadensersatzansprüche geltend machen, aber die Inanspruchnahme eines Schiedsverfahrens schließt nicht die Möglichkeit aus, vor den ordentlichen US-Gerichten Schadensersatz zu fordern.

143 Siehe z.B. die staatlichen 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) Unfaire Geschäftspraktiken und Verbraucherschutzgesetz).

144 D.h. im Falle einer vorsätzlichen Einmischung in die privaten Angelegenheiten oder Belange einer

Person in einer Weise, die für eine vernünftige Person höchst beleidigend wäre (Restatement (2nd) of Torts, § 652(b)).

145 Diese unerlaubte Handlung kommt in der Regel bei der Aneignung und Verwendung des Namens oder Bildes einer Person zur Werbung für ein Unternehmen oder ein Produkt oder für einen ähnlichen kommerziellen Zweck zur Anwendung (siehe Restatement (2nd) of Torts, § 652C).

146 D.h. wenn Informationen über das Privatleben einer Person öffentlich gemacht werden, wenn dies für eine vernünftige Person höchst beleidigend ist und die Informationen nicht von legitimem Interesse für die Öffentlichkeit sind (Restatement (2nd) of Torts, §652D).

(88) Die Kommission bewertete auch die Beschränkungen und Garantien, einschließlich der Aufsicht und der individuellen Rechtsbehelfsmechanismen, die im Recht der Vereinigten Staaten in Bezug auf die Erhebung und anschließende Verwendung personenbezogener Daten, die an für die Verarbeitung Verantwortliche und Auftragsverarbeiter in den USA im öffentlichen Interesse übermittelt wurden, insbesondere für Zwecke der Strafverfolgung und der nationalen Sicherheit, durch US-Behörden zur Verfügung stehen (Zugang der Regierung)[147] . Bei der Bewertung der Frage, ob die Bedingungen für den staatlichen Zugang zu Daten, die gemäß diesem Beschluss an die Vereinigten Staaten übermittelt werden, die Prüfung der "wesentlichen Gleichwertigkeit" gemäß 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 Rechtsgrundlage, die den Eingriff in ein solches Recht erlaubt, muss selbst den Umfang der Einschränkung der Ausübung des betreffenden Rechts festlegen[148] . Um dem Erfordernis der Verhältnismäßigkeit zu genügen, wonach Ausnahmen und Beschränkungen des Schutzes personenbezogener Daten nur insoweit gelten dürfen, als dies in einer demokratischen Gesellschaft zur Erreichung bestimmter Ziele von allgemeinem Interesse, die den von der Union anerkannten Zielen gleichwertig sind, unbedingt erforderlich ist, muss diese Rechtsgrundlage außerdem klare und präzise Regeln für den Anwendungsbereich und die Anwendung der betreffenden Maßnahmen festlegen und Mindestgarantien vorsehen, damit die Personen, deren Daten übermittelt wurden, über ausreichende Garantien verfügen, um ihre personenbezogenen Daten wirksam gegen die Gefahr des Missbrauchs zu schützen[149] . Darüber hinaus müssen diese Vorschriften und Garantien rechtsverbindlich sein und von den Betroffenen durchgesetzt werden können[150] . Insbesondere müssen die betroffenen Personen die Möglichkeit haben, vor einem unabhängigen und unparteiischen Gericht Klage zu erheben, um Zugang zu ihren personenbezogenen Daten zu erhalten oder die Berichtigung oder Löschung dieser Daten zu erwirken[151] .

### 3.1 Zugang und Verwendung durch US-Behörden für Zwecke der Strafverfolgung

(90) Was den Eingriff in personenbezogene Daten betrifft, die im Rahmen der EU-US-DSGVO zu Strafverfolgungszwecken übermittelt werden, so sieht das Recht der Vereinigten Staaten eine Reihe von Beschränkungen für den Zugang zu und die Verwendung von personenbezogenen Daten vor und bietet Überwachungs- und Rechtsbehelfsmechanismen, die den in Erwägungsgrund 89 dieses Beschlusses genannten Anforderungen entsprechen. Die Bedingungen, unter denen ein solcher Zugang erfolgen kann, und die Garantien, die

---

147 Dies ist auch im Lichte von Abschnitt I.5 von Anhang I relevant. Gemäß diesem Abschnitt und ähnlich wie in der Datenschutz-Grundverordnung kann die Einhaltung der Datenschutzanforderungen und -rechte, die Teil der Datenschutzgrundsätze sind, Einschränkungen unterliegen. Solche Einschränkungen sind jedoch nicht absolut, sondern können nur unter bestimmten Bedingungen geltend gemacht werden, beispielsweise in dem Maße, in dem sie erforderlich sind, um einer gerichtlichen Anordnung nachzukommen oder Anforderungen des öffentlichen Interesses, der Strafverfolgung oder der nationalen Sicherheit zu erfüllen. In diesem Zusammenhang und aus Gründen der Klarheit bezieht sich dieser Abschnitt auch auf die in EO 14086 festgelegten Bedingungen, die unter anderem in den Erwägungsgründen 127-141 bewertet werden.

148 Siehe *Schrems II*, Randnrn. 174-175 und die dort zitierte Rechtsprechung. Siehe auch, was den Zugang von Behörden der Mitgliedstaaten betrifft, Rechtssache C-623/17, *Privacy International,* ECLI:EU:C:2020:790, Randnr. 65, und verbundene Rechtssachen C-511/18, C-512/18 und C-520/18, *La Quadrature du Net u. a.,* ECLI:EU:C:2020:791, Randnr. 175.

149 Siehe *Schrems II*, Randnrn. 176 und 181, sowie die zitierte Rechtsprechung. Zum Zugang der Behörden

der Mitgliedstaaten siehe auch *Privacy International*, Randnr. 68, und *La Quadrature du Net u. a.*, Randnr. 132.

150 Siehe *Schrems II*, Randnrn. 181-182.

151 Vgl. Urteile *Schrems I*, Randnr. 95, und *Schrems II*, Randnr. 194. In diesem Zusammenhang hat der EuGH insbesondere hervorgehoben, dass die Einhaltung von Artikel 47 der Charta der Grundrechte, der das Recht auf einen wirksamen Rechtsbehelf bei einem unabhängigen und unparteiischen Gericht garantiert, "zum erforderlichen Schutzniveau in der Europäischen Union beiträgt [und] von der Kommission festgestellt werden muss, bevor sie einen Angemessenheitsbeschluss gemäß Artikel 45 Absatz 1 der Verordnung (EU) 2016/679 erlässt" (*Schrems II*, Randnr. 186).

die für die Ausübung dieser Befugnisse gelten, werden in den folgenden Abschnitten eingehend geprüft. In diesem Zusammenhang hat die US-Regierung (über das Justizministerium) auch Zusicherungen zu den geltenden Beschränkungen und Garantien gegeben (Anhang VI zu diesem Beschluss).

### *3.1.1 Rechtsgrundlagen, Einschränkungen und Garantien*

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

(91) Auf personenbezogene Daten, die von zertifizierten US-Organisationen verarbeitet und auf der Grundlage der EU-US-DSGVO aus der Union übermittelt werden, können US-Bundesstaatsanwälte und Bundesermittlungsbeamte zu Strafverfolgungszwecken nach verschiedenen Verfahren zugreifen, die in den Erwägungsgründen 92-99 näher erläutert werden. Diese Verfahren gelten in gleicher Weise, wenn Informationen von einer beliebigen US-Organisation eingeholt werden, unabhängig von der Staatsangehörigkeit oder dem Wohnsitz der betroffenen Personen[152] .

(92) Erstens kann ein Richter auf Antrag eines Strafverfolgungsbeamten des Bundes oder eines Anwalts der Regierung einen Durchsuchungs- oder Beschlagnahmebeschluss (einschließlich elektronisch gespeicherter Informationen)[153] erlassen. Ein solcher Durchsuchungs- oder Beschlagnahmebeschluss darf nur ausgestellt werden, wenn ein "wahrscheinlicher Grund"[154] vorliegt, dass "beschlagnahmbare Gegenstände" (Beweise für eine Straftat, illegal besessene Gegenstände oder Gegenstände, die für die Begehung einer Straftat bestimmt sind oder verwendet werden) an dem in dem Beschluss angegebenen Ort gefunden werden können. Der Durchsuchungsbefehl muss die zu beschlagnahmenden Gegenstände bezeichnen und den Richter benennen, an den der Durchsuchungsbefehl zurückgegeben werden muss. Eine Person, die von einer Durchsuchung betroffen ist oder deren Eigentum von einer Durchsuchung betroffen ist, kann die Unterdrückung von Beweisen beantragen, die durch eine unrechtmäßige Durchsuchung erlangt wurden oder daraus hervorgegangen sind, wenn diese Beweise in einem Strafverfahren gegen diese Person eingeführt werden[155] . Wenn ein Dateninhaber (z. B. ein Unternehmen) aufgrund einer Anordnung zur Offenlegung von Daten verpflichtet ist, kann er insbesondere die Verpflichtung zur Offenlegung als unangemessenen Aufwand anfechten[156] .

(93) Zweitens kann eine Vorladung durch ein Geschworenengericht (eine von einem Richter oder Staatsanwalt eingesetzte Ermittlungsinstanz) im Rahmen von Ermittlungen in bestimmten schwerwiegenden Fällen erlassen werden.

---

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 95-98) , *Suzlon Energy Ltd. gegen Microsoft Corp.*

153 Federal Rules of Criminal Procedure, 41. In einem Urteil aus dem Jahr 2018 bestätigte der Oberste Gerichtshof, dass ein Durchsuchungsbefehl oder eine Ausnahme von der Durchsuchungsbefugnis auch für Strafverfolgungsbehörden erforderlich ist, um auf historische Standortdaten von Mobilfunkanbietern zuzugreifen, die einen umfassenden Überblick über die Bewegungen eines Nutzers bieten, und dass der Nutzer eine angemessene Erwartung an die Privatsphäre in Bezug auf solche Informationen haben kann (*Timothy Ivory Carpenter gegen Vereinigte Staaten von Amerika*, Nr. 16-402, 585 U.S. (2018)). Infolgedessen können solche Daten in der Regel nicht auf der Grundlage eines Gerichtsbeschlusses von einem Mobilfunkunternehmen eingeholt werden, wenn berechtigte Gründe für die Annahme bestehen, dass die Informationen für eine laufende strafrechtliche Untersuchung relevant und wesentlich sind, sondern es muss ein hinreichender Verdacht nachgewiesen werden, wenn ein Haftbefehl verwendet wird.

154 Dem Obersten Gerichtshof zufolge ist der "hinreichende Verdacht" ein "praktischer, nichttechnischer"

Standard, der sich auf die "faktischen und praktischen Erwägungen des täglichen Lebens stützt, nach denen vernünftige und umsichtige Menschen [...] handeln" (*Illinois v. Gates*, 462 U.S. 213, 232 (1983)). Was Durchsuchungsbefehle betrifft, so liegt ein hinreichender Verdacht vor, wenn eine Durchsuchung mit an Sicherheit grenzender Wahrscheinlichkeit zur Entdeckung von Beweisen für eine Straftat führen wird (id).

155 *Mapp vs. Ohio*, 367 U.S. 643 (1961).

156 Siehe *In re Application of United States*, 610 F.2d 1148, 1157 (3d Cir. 1979) (mit der Feststellung, dass "ein ordnungsgemäßes Verfahren eine Anhörung zur Frage der Erschwernis erfordert, bevor eine Telefongesellschaft gezwungen wird, Unterstützung bei einem Durchsuchungsbefehl zu leisten") und *In re Application of United States*, 616 F.2d 1122 (9th Cir. 1980).

Straftaten[157] , in der Regel auf Antrag eines Bundesstaatsanwalts, um von jemandem die Vorlage oder Bereitstellung von Geschäftsunterlagen, elektronisch gespeicherten Informationen oder anderen materiellen Gegenständen zu verlangen. Darüber hinaus erlauben verschiedene Gesetze die Verwendung von Verwaltungsvorladungen zur Vorlage oder Bereitstellung von Geschäftsunterlagen, elektronisch gespeicherten Informationen oder anderen materiellen Gegenständen bei Ermittlungen im Zusammenhang mit Betrug im Gesundheitswesen, Kindesmissbrauch, Geheimdienstschutz, Fällen von kontrollierten Substanzen und Untersuchungen der Generalinspektion[158] . In beiden Fällen müssen die Informationen für die Untersuchung relevant sein, und die Vorladung darf nicht unangemessen, d. h. zu weit gefasst, erdrückend oder beschwerlich sein (und kann vom Empfänger der Vorladung aus diesen Gründen angefochten werden)[159] .

(94) Sehr ähnliche Bedingungen gelten für administrative Vorladungen, die ausgestellt werden, um Zugang zu Daten zu erhalten, die sich im Besitz von Unternehmen in den USA zu zivilen oder regulatorischen Zwecken ("öffentliches Interesse") befinden. Die Befugnis der Behörden mit zivil- und aufsichtsrechtlichen Zuständigkeiten, solche administrativen Vorladungen zu erlassen, muss in einem Gesetz festgelegt werden. Die Verwendung einer behördlichen Vorladung unterliegt einer "Angemessenheitsprüfung", die voraussetzt, dass die Untersuchung zu einem legitimen Zweck durchgeführt wird, dass die mit der Vorladung angeforderten Informationen für diesen Zweck relevant sind, dass die Behörde nicht bereits über die Informationen verfügt, die sie mit der Vorladung anfordert, und dass die für die Ausstellung der Vorladung erforderlichen Verwaltungsschritte eingehalten wurden[160] . Die Rechtsprechung des Obersten Gerichtshofs hat auch klargestellt, dass die Bedeutung des öffentlichen Interesses an den angeforderten Informationen mit der Bedeutung der persönlichen und organisatorischen Datenschutzinteressen abgewogen werden muss[161] . Während die Verwendung einer behördlichen Vorladung nicht der vorherigen gerichtlichen Genehmigung unterliegt, wird sie im Falle einer Anfechtung durch den Empfänger aus den oben genannten Gründen oder wenn die ausstellende Behörde versucht, die Vorladung vor Gericht durchzusetzen, einer gerichtlichen Überprüfung unterzogen[162] . Zusätzlich zu diesen allgemeinen, übergreifenden Beschränkungen können sich aus einzelnen Gesetzen spezifische (strengere) Anforderungen ergeben[163] .

(95) Drittens gibt es mehrere Rechtsgrundlagen, die es den Strafverfolgungsbehörden ermöglichen, Zugang zu Kommunikationsdaten zu erhalten. Ein Gericht kann eine Anordnung erlassen, die die Erhebung

---

157 Der fünfte Zusatzartikel der US-Verfassung schreibt vor, dass bei "Kapital- oder anderen berüchtigten Verbrechen" eine Anklage vor einem Geschworenengericht erhoben werden muss. 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, Vorladungen zu erlassen.

158 Siehe Anhang VI.

159 Federal Rules of Criminal Procedure, 17.

160 *Vereinigte Staaten gegen 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 Falle einer Anfechtung einer behördlichen Vorladung prüfen muss, ob (1) die Untersuchung einem rechtmäßig genehmigten Zweck dient, (2) die fragliche Vorladungsbefugnis in der Anordnungsbefugnis des Kongresses liegt und (3) die "angeforderten Dokumente für die Untersuchung relevant sind". Das Gericht stellte auch fest, dass ein behördliches Vorladungsersuchen "angemessen" sein muss, d.h. es muss eine "angemessene, aber nicht übermäßige Spezifizierung der vorzulegenden Dokumente für die Zwecke der betreffenden Untersuchung" erfordern, einschließlich "einer genauen Beschreibung des Ortes, der durchsucht werden soll, und der Personen oder Dinge, die beschlagnahmt werden sollen."

163 Das Gesetz zum Schutz der Privatsphäre in Finanzangelegenheiten (Right to Financial Privacy Act) ermächtigt eine Regierungsbehörde beispielsweise nur dann , die Finanzunterlagen eines Finanzinstituts im Rahmen einer behördlichen Vorladung anzufordern, wenn (1) Grund zu der Annahme besteht, dass die angeforderten Aufzeichnungen für eine rechtmäßige Untersuchung der Strafverfolgungsbehörden relevant sind und (2) dem Kunden eine Kopie der Vorladung oder Vorladung zusammen mit einer Mitteilung zugestellt wurde, in der die Art der Untersuchung mit angemessener Genauigkeit angegeben ist (12 U.S.C. §3405). Ein weiteres Beispiel ist der Fair Credit Reporting Act, der es Verbraucherauskunfteien verbietet, Verbraucherberichte auf behördliche Vorladungen hin offenzulegen (und es ihnen nur erlaubt, auf Vorladungen von Geschworenengerichten oder gerichtliche Anordnungen zu antworten, 15 U.S.C. §1681 et seq.). Was den Zugang zu Kommunikationsdaten betrifft, so gelten die besonderen Anforderungen des Stored Communications Act, auch im Hinblick auf die Möglichkeit, behördliche Vorladungen zu verwenden (siehe Erwägungsgründe 96-97 für einen detaillierten Überblick).

von inhaltsunabhängigen Echtzeit-Wahl-, Leitweg-, Adressierungs- und Signalisierungsinformationen über eine Telefonnummer oder eine E-Mail (durch den Einsatz eines Pen-Registers oder eines Trap-and-Trace-Geräts), wenn sie feststellt, dass die Behörde bescheinigt hat, dass die wahrscheinlich zu erlangenden Informationen für eine laufende strafrechtliche Ermittlung relevant sind[164] . Die Anordnung muss unter anderem die Identität des Verdächtigen, sofern bekannt, die Merkmale der Kommunikation, auf die sie sich bezieht, und die Straftat, auf die sich die zu erhebenden Informationen beziehen, angeben. Die Verwendung eines Pen-Registers oder eines Trap-and-Trace-Geräts kann für einen Zeitraum von höchstens sechzig Tagen genehmigt werden, der nur durch einen neuen Gerichtsbeschluss verlängert werden kann.

(96) Darüber hinaus kann der Zugang zu Teilnehmerinformationen, Verkehrsdaten und gespeicherten Kommunikationsinhalten, die sich im Besitz von Internet-Diensteanbietern, Telefongesellschaften und anderen Drittanbietern befinden, zu Strafverfolgungszwecken auf der Grundlage des Stored Communications Act[165] gewährt werden. Um den gespeicherten Inhalt elektronischer Kommunikation zu erhalten, müssen die Strafverfolgungsbehörden grundsätzlich eine richterliche Anordnung einholen, die sich auf wahrscheinliche Gründe für die Annahme stützt, dass das betreffende Konto Beweise für eine Straftat enthält[166] . Für Informationen zur Teilnehmerregistrierung, IP-Adressen und zugehörige Zeitstempel sowie Rechnungsinformationen können die Strafverfolgungsbehörden eine Vorladung verwenden. Für die meisten anderen gespeicherten Informationen, die nicht zum Inhalt gehören, wie z. B. E-Mail-Kopfzeilen ohne Betreffzeile, muss eine Strafverfolgungsbehörde einen Gerichtsbeschluss einholen, der ausgestellt wird, wenn der Richter davon überzeugt ist, dass es hinreichende Gründe für die Annahme gibt, dass die angeforderten Informationen für eine laufende strafrechtliche Untersuchung relevant und wesentlich sind.

(97) Anbieter, die Anfragen nach dem Stored Communications Act erhalten, können einen Kunden oder Teilnehmer, dessen Informationen angefordert werden, freiwillig benachrichtigen, es sei denn, die zuständige Strafverfolgungsbehörde erwirkt eine Schutzanordnung, die eine solche Benachrichtigung untersagt[167] . Bei einer solchen Schutzanordnung handelt es sich um eine gerichtliche Verfügung, die einen Anbieter von elektronischen Kommunikationsdiensten oder Ferncomputerdiensten, an den ein Haftbefehl, eine Vorladung oder eine gerichtliche Anordnung gerichtet ist, verpflichtet, solange das Gericht es für angemessen hält, keine anderen Personen über die Existenz des Haftbefehls, der Vorladung oder der gerichtlichen Anordnung zu informieren. Schutzanordnungen werden gewährt, wenn ein Gericht feststellt, dass Grund zu der Annahme besteht, dass eine Benachrichtigung die Ermittlungen ernsthaft gefährden oder das Verfahren unangemessen verzögern würde, z. B. weil dadurch das Leben oder die körperliche Unversehrtheit einer Person gefährdet würde, die Flucht vor der Strafverfolgung, die Einschüchterung potenzieller Zeugen, usw. Ein Memorandum des stellvertretenden Generalstaatsanwalts (das für alle Staatsanwälte und Bediensteten des Justizministeriums verbindlich ist) verlangt von den Staatsanwälten, dass sie eine detaillierte Entscheidung über die Notwendigkeit einer Schutzanordnung treffen und dem Gericht eine Begründung vorlegen, wie die gesetzlichen Kriterien für die Erlangung einer

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 Abonnent oder Kunde benachrichtigt wird (entweder im Voraus oder unter bestimmten Umständen durch eine verzögerte Benachrichtigung), können die länger als 180 Tage gespeicherten Inhaltsinformationen auch auf der Grundlage einer behördlichen Vorladung oder einer Vorladung durch die Grand Jury (18 U.S.C. §§ 2701(b)(1)(B)) oder einer gerichtlichen Anordnung (wenn es vernünftige Gründe für die Annahme gibt, dass die Informationen für eine laufende strafrechtliche Untersuchung relevant und wesentlich sind (18 U.S.C. §§ 2701(d)), eingeholt werden. Nach einem Urteil eines Bundesberufungsgerichts erhalten staatliche Ermittler jedoch in der Regel Durchsuchungsbefehle von Richtern, um den Inhalt privater Kommunikation oder gespeicherter Daten von einem kommerziellen Kommunikationsdienstleister zu erfassen. *Vereinigte Staaten gegen Warshak*, 631 F.3d 266 (6th Cir. 2010).

167 18 U.S.C. § 2705(b).

Schutzanordnung im konkreten Fall erfüllt sind[168] . Das Memorandum schreibt auch vor, dass Anträge auf Schutzanordnungen im Allgemeinen nicht darauf abzielen dürfen, die Zustellung um mehr als ein Jahr zu verzögern. Wenn unter außergewöhnlichen Umständen Anordnungen von längerer Dauer erforderlich sein könnten, dürfen solche Anordnungen nur mit schriftlicher Zustimmung eines vom US-Staatsanwalt oder dem zuständigen stellvertretenden Generalstaatsanwalt benannten Vorgesetzten beantragt werden. Darüber hinaus muss ein Staatsanwalt bei Abschluss der Ermittlungen unverzüglich prüfen, ob es eine Grundlage für die Aufrechterhaltung ausstehender Schutzanordnungen gibt, und, falls dies nicht der Fall ist, die Schutzanordnung aufheben und sicherstellen, dass der Diensteanbieter darüber informiert wird[169] .

(98) Strafverfolgungsbehörden können auch drahtgebundene, mündliche oder elektronische Kommunikation in Echtzeit auf der Grundlage eines Gerichtsbeschlusses abhören, in dem ein Richter unter anderem feststellt, dass es wahrscheinliche Gründe für die Annahme gibt, dass das Abhören oder die elektronische Überwachung Beweise für ein Bundesverbrechen oder den Aufenthaltsort eines Flüchtigen, der vor der Strafverfolgung flieht, erbringen wird[170] .

(99) Weitere Schutzmaßnahmen sind in verschiedenen Politiken und Richtlinien des Justizministeriums enthalten, darunter die Richtlinien des Generalstaatsanwalts für inländische FBI-Operationen (AGG-DOM), die unter anderem vorschreiben, dass das Federal Bureau of Investigation (FBI) unter Berücksichtigung der Auswirkungen auf die Privatsphäre und die bürgerlichen Freiheiten die am wenigsten einschneidenden Ermittlungsmethoden einsetzt[171] .

(100) Den Zusicherungen der US-Regierung zufolge gelten für die Ermittlungen der Strafverfolgungsbehörden auf bundesstaatlicher Ebene (in Bezug auf Ermittlungen, die nach bundesstaatlichen Gesetzen durchgeführt werden) dieselben oder höhere Schutzbestimmungen[172] . Insbesondere bekräftigen verfassungsrechtliche Bestimmungen sowie Gesetze und Rechtsprechung auf bundesstaatlicher Ebene den oben genannten Schutz vor unangemessenen Durchsuchungen und Beschlagnahmen, indem sie die Ausstellung eines Durchsuchungsbefehls vorschreiben[173] . Ähnlich wie die auf Bundesebene gewährten Schutzmaßnahmen

---

168 Siehe das Memorandum des stellvertretenden Generalstaatsanwalts Rod Rosenstein vom 19. Oktober 2017 über eine restriktivere Politik bei Anträgen auf Schutzanordnungen (oder Geheimhaltungsvereinbarungen), abrufbar unter https://www.justice.gov/criminal-ccips/page/file/1005791/download.

169 Memorandum der stellvertretenden Generalstaatsanwältin Lisa Moncao vom 27. Mai 2022 über eine ergänzende Richtlinie für Anträge auf Schutzanordnungen gemäß 18 U.S.C. §2705(b).

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 Regeln und Richtlinien, die Einschränkungen für die Ermittlungstätigkeit von Bundesstaatsanwälten vorsehen, sind im Handbuch der US-Staatsanwälte (United States Attorneys' Manual) enthalten, das unter http://www.justice.gov/usam/united-states-attorneys- abrufbar ist. Abweichungen von diesen Richtlinien bedürfen der vorherigen Genehmigung des Direktors, des stellvertretenden Direktors oder des vom Direktor benannten stellvertretenden Exekutivdirektors des FBI, es sei denn, eine solche Genehmigung kann wegen der Unmittelbarkeit oder Schwere einer Bedrohung der Sicherheit von Personen oder Gütern oder der nationalen Sicherheit nicht eingeholt werden (in diesem Fall muss der Direktor oder eine andere befugte Person so bald wie möglich benachrichtigt werden). Werden die Leitlinien nicht befolgt, muss das FBI das Justizministerium davon in Kenntnis setzen, das wiederum den Generalstaatsanwalt und den stellvertretenden Generalstaatsanwalt unterrichtet.

172 Anhang VI, Fußnote 2. Siehe auch z. B. *Arnold gegen die Stadt Cleveland*, 67 Ohio St.3d 35, 616 N.E.2d 163, 169 (1993) ("In den Bereichen der individuellen Rechte und der bürgerlichen Freiheiten bietet die Verfassung der Vereinigten Staaten, soweit sie auf die Staaten anwendbar ist, eine

Untergrenze, unter die staatliche Gerichtsentscheidungen nicht fallen dürfen"); *Cooper gegen Kalifornien*, 386 U.S. 58, 62, 87 S.Ct. 788, 17 L.Ed.2d 730 (1967) ("Unsere Entscheidung berührt natürlich nicht die Befugnis des Staates, höhere Standards für Durchsuchungen und Beschlagnahmungen festzulegen, als die Bundesverfassung vorschreibt, wenn er 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 Beschlagnahmungen vorschreiben kann als die Bundesverfassung, können die Gerichte von Arizona keinen geringeren Schutz bieten als der vierte Verfassungszusatz").

173 Die meisten Staaten haben den Schutz des Vierten Verfassungszusatzes in ihre Verfassungen übernommen. Siehe Alabama Const. art. I, § 5); Alaska Const. art. I, § 14; 1; Arkansas Const. art. II, § 15; Kalifornien

Durchsuchungsbefehle dürfen nur bei Vorliegen eines hinreichenden Verdachts ausgestellt werden und müssen den zu durchsuchenden Ort und die zu beschlagnahmende Person oder Sache beschreiben[174] .

*3.1.1.2 Weiterverwendung der gesammelten Informationen*

(101) Für die Weiterverwendung von Daten, die von den Strafverfolgungsbehörden des Bundes erhoben wurden, schreiben verschiedene Gesetze, Richtlinien und Standards spezifische Schutzmaßnahmen vor. 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 generell für die Weiterverwendung von Daten durch alle Bundesbehörden, einschließlich der Daten, auf die für zivile oder regulatorische Zwecke zugegriffen wird. Dazu gehören auch die Anforderungen, die sich aus den Memos/Verordnungen des Office of Management and Budget, dem Federal Information Security Management Modernization Act, dem E-Government Act und dem Federal Records Act ergeben.

(102) In Übereinstimmung mit den Befugnissen des Clinger-Cohen Act (P.L. 104-106, Division E) und des Computer Security Act of 1987 (P.L. 100-235) hat das Office of Management and Budget (OMB) das Rundschreiben Nr. A-130 herausgegeben, um allgemeine verbindliche Richtlinien zu erstellen, die für alle Bundesbehörden (einschließlich der Strafverfolgungsbehörden) gelten, wenn sie mit personenbezogenen Daten umgehen[175] . Das Rundschreiben verlangt insbesondere von allen Bundesbehörden, "die Erstellung, Sammlung, Verwendung, Verarbeitung, Speicherung, Pflege, Verbreitung und Offenlegung personenbezogener Daten auf das rechtlich zulässige, relevante und vernünftigerweise als notwendig erachtete Maß für die ordnungsgemäße Erfüllung der autorisierten Aufgaben der Behörde zu beschränken"[176] . Darüber hinaus müssen die Bundesbehörden, soweit dies vernünftigerweise praktikabel ist, sicherstellen, dass personenbezogene

---

Const. art. I, § 13; Colorado Const. art. II, § 7; Conneticut Const. art. I, § 7; Delaware Const. art. I, § 6; Florida. Const. art. I, § 12; Georgia Const. art. I, § I, para. XIII; Hawai 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; Nevad 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 Länder (z. B. Maryland, North Carolina und Virginia) haben in ihren Verfassungen spezielle Bestimmungen über Durchsuchungsbefehle verankert, die von der Rechtsprechung so ausgelegt wurden, dass sie einen ähnlichen oder höheren Schutz bieten als der Vierte Verfassungszusatz (siehe Maryland. Decl. of Rts. art. 26; North Carolina Const. art. I, § 20; Virginia Const. art. I, § 10, und einschlägiges Fallrecht, 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 Verfassungsbestimmungen, die die Privatsphäre allgemeiner schützen (Arizona Const. art. 2, § 8; Washington Const. art. I, § 7), die von Gerichten so ausgelegt wurden, dass sie mehr Schutz bieten als der Vierte Verfassungszusatz (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.

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 verknüpft sind oder verknüpft werden können", siehe OMB-Rundschreiben Nr. A-130, S. 33 (Definition von "personenbezogenen Daten").

176 OMB Circular No. A-130, Managing Information as a Strategic Resource, Appendix II, Responsibilities for Managing Personally Identifiable Information, 81 Fed. Reg. 49.689 (28. Juli 2016), S. 17.

identifizierbare Informationen korrekt, relevant, zeitnah und vollständig sind und auf das Minimum reduziert werden, das für die ordnungsgemäße Erfüllung der Aufgaben einer Behörde erforderlich ist. Ganz allgemein müssen Bundesbehörden ein umfassendes Datenschutzprogramm einrichten, um die Einhaltung der geltenden Datenschutzanforderungen zu gewährleisten, Datenschutzrichtlinien zu entwickeln und zu bewerten und Datenschutzrisiken zu bewältigen; Verfahren zur Aufdeckung, Dokumentation und Meldung von Vorfällen im Zusammenhang mit der Einhaltung von Datenschutzbestimmungen einrichten; Programme zur Sensibilisierung für den Datenschutz und zur Schulung von Mitarbeitern und Auftragnehmern entwickeln und Richtlinien und Verfahren einführen, um sicherzustellen, dass das Personal für die Einhaltung der Datenschutzanforderungen und -richtlinien verantwortlich gemacht wird[177] .

(103) Darüber hinaus verpflichtet der E-Government Act[178] alle Bundesbehörden (einschließlich der Strafverfolgungsbehörden), Schutzmaßnahmen für die Informationssicherheit zu ergreifen, die dem Risiko und dem Ausmaß des Schadens angemessen sind, der sich aus einem unbefugten Zugriff, einer unbefugten Nutzung, Offenlegung, Störung, Änderung oder Zerstörung ergeben würde; einen Chief Information Officer zu haben, der die Einhaltung der Anforderungen an die Informationssicherheit sicherstellt, und eine jährliche unabhängige Bewertung (z. B. durch einen Generalinspektor, siehe Erwägungsgrund 109) ihres Informationssicherheitsprogramms und ihrer Praktiken vorzunehmen[179] . In ähnlicher Weise verlangen der Federal Records Act (FRA)[180] und ergänzende Verordnungen[181] , dass Informationen, die sich im Besitz von Bundesbehörden befinden, Sicherheitsvorkehrungen 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 die die Mindestanforderungen an die Informationssicherheit weiter spezifizieren, die eingeführt werden müssen, einschließlich Zugangskontrollen, Sensibilisierung und Schulung, Notfallplanung, Reaktion auf Vorfälle, Prüfungs- und Rechenschaftsinstrumente, Gewährleistung der System- und Informationsintegrität, Durchführung von Datenschutz- und Sicherheitsrisikobewertungen usw.[182] . Darüber hinaus müssen alle Bundesbehörden (einschließlich der Strafverfolgungsbehörden) in Übereinstimmung mit den Richtlinien des OMB einen Plan für den Umgang mit Datenschutzverletzungen aufrechterhalten und umsetzen, auch wenn es um die Reaktion auf solche Verletzungen und die Bewertung der Schadensrisiken geht[183] .

(105) Was die Datenaufbewahrung betrifft, so schreibt die FRA[184] den US-Bundesbehörden (einschließlich der Strafverfolgungsbehörden) vor, Aufbewahrungsfristen für ihre Aufzeichnungen festzulegen (nach deren Ablauf diese Aufzeichnungen entsorgt werden müssen), die von der Nationalen

177 Anhang 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 Anhang 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.

183 Memorandum 17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information", verfügbar 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 et seq.

Archive und Aktenverwaltung[185] . Die Länge dieser Aufbewahrungsfristen wird unter Berücksichtigung verschiedener Faktoren festgelegt, wie z. B. der Art der Untersuchung, ob das Beweismaterial noch für die Untersuchung relevant ist usw. In Bezug auf das FBI sieht das AGG-DOM vor, dass das FBI über einen solchen Plan zur Aufbewahrung von Unterlagen verfügen und ein System unterhalten muss, mit dem der Stand und die Grundlage von Ermittlungen umgehend abgerufen werden können.

(106) Schließlich enthält auch das OMB-Rundschreiben Nr. A-130 bestimmte Anforderungen an die Verbreitung personenbezogener Daten. Grundsätzlich muss die Verbreitung und Offenlegung personenbezogener Daten auf das beschränkt werden, was rechtlich zulässig, relevant und vernünftigerweise für die ordnungsgemäße Erfüllung der Aufgaben einer Behörde erforderlich ist[186] . Bei der Weitergabe personenbezogener Daten an andere Regierungsstellen müssen die US-Bundesbehörden gegebenenfalls Bedingungen (einschließlich der Durchführung spezifischer Sicherheits- und Datenschutzkontrollen) festlegen, die die Verarbeitung der Daten durch schriftliche Vereinbarungen (einschließlich Verträgen, Vereinbarungen über die Datennutzung, Vereinbarungen über den Informationsaustausch und Absichtserklärungen) regeln[187] . Hinsichtlich der Gründe, aus denen Informationen weitergegeben werden dürfen, sehen das AGG-DOM und der FBI Domestic Investigations and Operations Guide[188] beispielsweise vor, dass das FBI dazu gesetzlich verpflichtet sein kann (z. B. aufgrund eines internationalen Abkommens) oder unter bestimmten Umständen Informationen weitergeben darf, z. B. an andere US-Behörden. an andere US-Behörden, wenn die Weitergabe mit dem Zweck, für den die Informationen gesammelt wurden, vereinbar ist und mit deren Zuständigkeiten zusammenhängt; an Kongressausschüsse; an ausländische Behörden, wenn die Informationen mit deren Zuständigkeiten zusammenhängen und die Weitergabe mit den Interessen der Vereinigten Staaten vereinbar ist; wenn die Weitergabe in besonderem Maße notwendig ist, um die Sicherheit von Personen oder Gütern zu schützen oder um vor einem Verbrechen oder einer Bedrohung der nationalen Sicherheit zu schützen oder ein solches zu verhindern, und wenn die Weitergabe mit dem Zweck, für den die Informationen gesammelt wurden, vereinbar ist[189] .

### *3.1.2 Beaufsichtigung*

(107) Die Tätigkeit der Strafverfolgungsbehörden des Bundes unterliegt der Kontrolle durch verschiedene Organe[190] . Wie in den Erwägungsgründen 92-99 erläutert, umfasst dies in den meisten Fällen eine vorherige Kontrolle durch die Justiz, die einzelne Erhebungsmaßnahmen genehmigen muss, bevor sie eingesetzt werden können. Darüber hinaus beaufsichtigen andere Stellen verschiedene Phasen der Tätigkeit der Strafverfolgungsbehörden, einschließlich der Erhebung und

---

185 Die National Archives and Record Administration (Nationale Archiv- und Aktenverwaltung) ist befugt, die Praktiken der Behörden bei der Verwaltung von Unterlagen zu bewerten und kann entscheiden, ob die weitere Aufbewahrung bestimmter Unterlagen gerechtfertigt ist (44 U.S.C. §§ 2904(c), 2906).

186 OMB-Rundschreiben Nr. A-130, Abschnitt 5.f.1.(d)

187 OMB-Rundschreiben Nr. A-130, Anhang I §3(d).

188 Siehe auch FBI-Leitfaden für inländische Ermittlungen und Operationen (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 Mechanismen gelten auch für die Erhebung und Verwendung von Daten durch Bundesbehörden für zivile und regulatorische Zwecke. Bundesbehörden für zivile und regulatorische Zwecke unterliegen der Kontrolle durch ihre jeweiligen Generalinspektoren und der Aufsicht durch den Kongress, einschließlich des Government Accountability Office, der Prüfungs- und

Untersuchungsbehörde des Kongresses. Sofern die Behörde nicht über einen Datenschutzbeauftragten verfügt - eine Position, die typischerweise in Behörden wie dem Justizministerium und dem Ministerium für Innere Sicherheit (DHS) aufgrund ihrer Zuständigkeiten für die Strafverfolgung und die nationale Sicherheit zu finden ist - fallen diese Aufgaben in den Zuständigkeitsbereich des Senior Agency Official for Privacy (SAOP) der Behörde. Alle Bundesbehörden sind gesetzlich verpflichtet, einen SAOP zu benennen, der die Verantwortung für die Einhaltung der Datenschutzgesetze durch die Behörde und die Überwachung der damit verbundenen Angelegenheiten trägt. Siehe z. B. OMB M-16-24, Role and Designation of Senior Agency Officials for Privacy (2016).

Verarbeitung von personenbezogenen Daten. Zusammen gewährleisten diese gerichtlichen und außergerichtlichen Stellen, dass die Strafverfolgungsbehörden einer unabhängigen Aufsicht unterliegen.

(108) Erstens gibt es in verschiedenen Abteilungen, die für die Strafverfolgung zuständig sind, Beauftragte für den Schutz der Privatsphäre und der bürgerlichen Freiheiten[191] . Während die spezifischen Befugnisse dieser Beauftragten je nach Ermächtigungsgesetz etwas variieren können, umfassen sie in der Regel die Überwachung von Verfahren, um sicherzustellen, dass die jeweilige Abteilung/Behörde die Belange des Schutzes der Privatsphäre und der bürgerlichen Freiheiten angemessen berücksichtigt und angemessene Verfahren zur Behandlung von Beschwerden von Personen eingerichtet hat, die der Ansicht sind, dass ihre Privatsphäre oder bürgerlichen Freiheiten verletzt worden sind. Die Leiter der einzelnen Abteilungen oder Behörden müssen sicherstellen, dass die Beauftragten für den Schutz der Privatsphäre und die Wahrung der bürgerlichen Freiheiten über das Material und die Ressourcen verfügen, die sie zur Erfüllung ihres Mandats benötigen, dass sie Zugang zu dem für die Wahrnehmung ihrer Aufgaben erforderlichen Material und Personal erhalten und dass sie über vorgeschlagene Änderungen der Politik informiert und dazu konsultiert werden[192] . Die Beauftragten für den Schutz der Privatsphäre und der bürgerlichen Freiheiten erstatten dem Kongress regelmäßig Bericht, u. a. über die Anzahl und Art der bei der Abteilung/Behörde eingegangenen Beschwerden und eine Zusammenfassung der Bearbeitung dieser Beschwerden, der durchgeführten Überprüfungen und Untersuchungen sowie der Auswirkungen der von den Beauftragten durchgeführten Tätigkeiten[193] .

(109) Zweitens beaufsichtigt ein unabhängiger Generalinspektor die Aktivitäten des Justizministeriums, einschließlich des FBI[194] . Die Generalinspekteure sind gesetzlich unabhängig[195] und für die Durchführung unabhängiger Untersuchungen, Prüfungen und Inspektionen der Programme und Tätigkeiten des Ministeriums zuständig. Sie haben Zugang zu allen Aufzeichnungen, Berichten, Audits, Überprüfungen, Dokumenten, Papieren, Empfehlungen oder anderem relevanten Material, erforderlichenfalls durch Vorladung, und können Zeugenaussagen machen[196] . Die Generalinspektoren geben zwar unverbindliche Empfehlungen für Abhilfemaßnahmen ab, doch werden ihre Berichte, einschließlich der Berichte über Folgemaßnahmen (oder das Fehlen solcher Maßnahmen)[197] , in der Regel veröffentlicht und dem Kongress übermittelt, der auf dieser Grundlage seine Aufsichtsfunktion wahrnehmen kann (siehe Erwägungsgrund 111)[198] .

---

191 Siehe 42 U.S.C. § 2000ee-1. Dazu gehören zum Beispiel das Justizministerium, das Ministerium für Innere Sicherheit und das FBI. Im DHS ist zusätzlich ein Chief Privacy Officer für die Wahrung und Verbesserung des Schutzes der Privatsphäre und die Förderung der Transparenz innerhalb des Ministeriums verantwortlich (6 U.S.C. 142, Abschnitt 222). Alle DHS-Systeme, -Technologien, -Formulare und -Programme, die personenbezogene Daten erheben oder Auswirkungen auf die Privatsphäre haben, unterliegen der Aufsicht des Chief Privacy Officer, der Zugang zu allen Aufzeichnungen, Berichten, Audits, Überprüfungen, Dokumenten, Papieren, Empfehlungen und anderen Materialien hat, die dem Ministerium zur Verfügung stehen, ggf. auch durch Vorladung. Der Datenschutzbeauftragte muss dem Kongress jährlich über Aktivitäten des Ministeriums berichten, die sich auf den Datenschutz auswirken, einschließlich Beschwerden über Datenschutzverletzungen.

192 42 U.S.C. § 2000ee-1(d).

193 Siehe 42 U.S.C. §§ 2000ee-1 (f)(1)-(2). Aus dem Bericht des Chief Privacy and Civil Liberties Officer des DOJ und des Office of Privacy and Civil Liberties für den Zeitraum Oktober 2020 bis März 2021 geht beispielsweise hervor, dass 389 Überprüfungen zum Schutz der Privatsphäre 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 Office of Inspector General im

Department of Homeland Security eingerichtet.

195 Generalinspektoren haben eine sichere Amtszeit und können nur vom Präsidenten abgesetzt werden, der dem Kongress die Gründe für eine solche Absetzung schriftlich mitteilen muss.

196 Siehe Generalinspektionsgesetz von 1978, § 6.

197 Siehe hierzu beispielsweise die vom DoJ Office of the Inspector General erstellte Übersicht über die von ihm ausgesprochenen Empfehlungen und das Ausmaß, in dem sie durch Folgemaßnahmen der Abteilung und der Agentur umgesetzt wurden, https://oig.justice.gov/sites/default/files/reports/22-043.pdf.

198 Siehe Inspector General Act of 1978, §§ 4(5), 5. Beispielsweise hat das Office of the Inspector General des Justizministeriums vor kurzem 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 DOJ gibt. Diese Aktivitäten

(110) Drittens unterliegen die für die Strafverfolgung zuständigen Dienststellen in dem Maße, in dem sie Maßnahmen zur Terrorismusbekämpfung durchführen, der Aufsicht des Privacy and Civil Liberties Oversight Board (PCLOB), einer unabhängigen Behörde innerhalb der Exekutive, die sich aus einem parteiübergreifenden, fünfköpfigen Gremium zusammensetzt, das vom Präsidenten mit Zustimmung des Senats für eine feste Amtszeit von sechs Jahren ernannt wird[199] . Gemäß ihrem Gründungsstatut ist die PCLOB mit Aufgaben im Bereich der Terrorismusbekämpfung und deren Umsetzung betraut, wobei der Schutz der Privatsphäre und der bürgerlichen Freiheiten im Vordergrund steht. Im Rahmen seiner Überprüfung kann er auf alle relevanten Unterlagen, Berichte, Prüfungen, Überprüfungen, Dokumente, Papiere und Empfehlungen, einschließlich Verschlusssachen, zugreifen, Interviews durchführen und Zeugenaussagen hören[200] . Er erhält Berichte von den Beauftragten für bürgerliche Freiheiten und Datenschutz mehrerer Bundesministerien/Bundesbehörden[201] , kann Empfehlungen an die Regierung und die Strafverfolgungsbehörden aussprechen und erstattet den Ausschüssen des Kongresses und dem Präsidenten regelmäßig Bericht[202] . Die Berichte des Ausschusses, einschließlich der Berichte an den Kongress, müssen so weit wie möglich öffentlich zugänglich gemacht werden[203] .

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

### *3.1.3 Abhilfe*

(112) Wie bereits erwähnt, müssen die Strafverfolgungsbehörden in den meisten Fällen eine vorherige richterliche Genehmigung für die Erhebung personenbezogener Daten einholen. Obwohl dies für administrative Vorladungen nicht erforderlich ist, sind diese auf bestimmte Situationen beschränkt und unterliegen einer unabhängigen gerichtlichen Überprüfung, zumindest wenn die Regierung eine gerichtliche Durchsetzung anstrebt. Insbesondere können Empfänger von behördlichen Vorladungen diese vor Gericht mit der Begründung anfechten, sie seien unangemessen, d. h. zu weit gefasst, erdrückend oder belastend[205] .

---

Dazu gehörte auch die Untersuchung eines ehemaligen Auftragnehmers im Zusammenhang mit der unrechtmäßigen Weitergabe elektronischer Überwachungsdaten (Abhören einer Person) im Rahmen einer laufenden Untersuchung, die zur Verurteilung des Auftragnehmers führte. Das Office of the Inspector General führte auch eine Untersuchung der Informationssicherheitsprogramme und -praktiken der DOJ-Behörden durch, bei der die Wirksamkeit der Informationssicherheitsstrategien, -verfahren und -praktiken einer repräsentativen Untergruppe der Systeme der Behörde geprüft wurde.

199 Die Mitglieder des Beirats werden ausschließlich auf der Grundlage ihrer beruflichen Qualifikation, ihrer Leistungen, ihres öffentlichen Ansehens, ihres Fachwissens im Bereich der bürgerlichen Freiheiten und des Schutzes der Privatsphäre sowie ihrer einschlägigen Erfahrungen und ohne Rücksicht auf ihre politische Zugehörigkeit ausgewählt. Es dürfen auf keinen Fall mehr als drei Mitglieder des Ausschusses derselben politischen Partei angehören. Eine Person, die in den Ausschuss berufen wird, darf während ihrer Tätigkeit im Ausschuss kein gewählter Beamter, Angestellter oder Angestellter der Bundesregierung sein, außer in ihrer Eigenschaft als Mitglied des Ausschusses. 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 gehören mindestens das Justizministerium, das Verteidigungsministerium, das Ministerium für Innere Sicherheit sowie jedes andere Ministerium, jede andere Behörde oder jedes andere Element der Exekutive, das vom PCLOB als geeignet für die Erfassung eingestuft wird.

202 42 U.S.C. §2000ee, (e).

[203] 42 U.S.C. § 2000ee (f).

[204] So veranstalten die Ausschüsse beispielsweise thematische Anhörungen (siehe z . B. eine kürzlich durchgeführte Anhörung des Justizausschusses des Repräsentantenhauses Ausschusses zu "digitale Rasterfahndung", https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4983) sowie regelmäßige Anhörungen zur Aufsicht, z. B. über das FBI und das DoJ, siehe 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.

(113) Einzelpersonen können zunächst bei den Strafverfolgungsbehörden Anträge oder Beschwerden über den Umgang mit ihren personenbezogenen Daten einreichen. Dazu gehört auch die Möglichkeit, Zugang zu personenbezogenen Daten und deren Berichtigung zu verlangen[206] . In Bezug auf Aktivitäten im Zusammenhang mit der Terrorismusbekämpfung können Einzelpersonen auch eine Beschwerde bei den Datenschutzbeauftragten (oder anderen Datenschutzbeauftragten) der Strafverfolgungsbehörden einreichen[207] .

(114) Darüber hinaus sieht das US-Recht eine Reihe von Rechtsbehelfen für Einzelpersonen vor, die sich gegen eine Behörde oder einen ihrer Beamten wenden, wenn diese Behörden personenbezogene Daten verarbeiten[208] . Diese Rechtsmittel, zu denen insbesondere das APA, der Freedom of Information Act (FOIA) und der Electronic Communications Privacy Act (ECPA) gehören, stehen allen Personen unabhängig von ihrer Nationalität offen, sofern die entsprechenden Bedingungen erfüllt sind.

(115) Nach den Bestimmungen über die gerichtliche Überprüfung des APA[209] ist im Allgemeinen "jede Person, die durch eine Maßnahme der Behörde ein rechtliches Unrecht erleidet oder durch eine Maßnahme der Behörde nachteilig beeinflusst oder geschädigt wird", berechtigt, eine gerichtliche Überprüfung zu beantragen[210] . Dies schließt die Möglichkeit ein, das Gericht aufzufordern, "Maßnahmen, Feststellungen und Schlussfolgerungen der Behörde für rechtswidrig zu erklären und aufzuheben, die [...] willkürlich, willkürlich, ermessensmissbräuchlich oder anderweitig nicht im Einklang mit dem Gesetz sind"[211] .

(116) Im Einzelnen legt Titel II des ECPA[212] ein System gesetzlicher Datenschutzrechte fest und regelt als solches den Zugriff der Strafverfolgungsbehörden auf den Inhalt drahtgebundener, mündlicher oder elektronischer Kommunikation, die von Drittanbietern gespeichert wird[213] . Er kriminalisiert den rechtswidrigen (d. h. nicht gerichtlich genehmigten oder anderweitig zulässigen) Zugang zu solchen Kommunikationen und bietet einer betroffenen Person die Möglichkeit, vor einem US-Bundesgericht eine Zivilklage auf tatsächlichen Schadenersatz und Strafschadensersatz sowie Billigkeits- oder Feststellungsklagen gegen einen Regierungsbeamten, der vorsätzlich solche rechtswidrigen Handlungen begangen hat, oder gegen die Vereinigten Staaten einzureichen.

(117) Darüber hinaus räumen mehrere andere Gesetze Einzelpersonen das Recht ein, Klage gegen eine
US-Behörden oder -Beamte in Bezug auf die Verarbeitung ihrer personenbezogenen Daten, wie z. B. der Wiretap Act[214] , der Computer Fraud and Abuse Act[215] , der Federal Torts

---

206 OMB-Rundschreiben Nr. A-130, Anhang II, Abschnitt 3(a) und (f), das von den Bundesbehörden verlangt, einen angemessenen Zugang und Korrekturen auf Anfrage von Einzelpersonen zu gewährleisten und Verfahren für die Entgegennahme und Bearbeitung von Beschwerden und Anfragen im Zusammenhang mit der Privatsphäre einzurichten.

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

208 Die in diesem Abschnitt genannten Rechtsbehelfe gelten auch für die Erhebung und Verwendung von Daten durch Bundesbehörden für zivil- und ordnungsrechtliche Zwecke.

209 5 U.S.C. § 702.

210 Im Allgemeinen unterliegen nur "endgültige" Maßnahmen der Behörde - und nicht "vorläufige, verfahrenstechnische oder Zwischenmaßnahmen" der Behörde - der gerichtlichen Überprüfung. 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 die Kommunikation von zwei bestimmten Kategorien von Netzbetreibern, nämlich von Anbietern von (i) elektronische Kommunikationsdienste, z. B. Telefonie oder E-Mail; (ii) Ferninformatikdienste wie Computerspeicher- oder -verarbeitungsdienste.

214 18 U.S.C. §§ 2510 et seq. Nach dem Wiretap Act (18 U.S.C. § 2520) kann eine Person, deren drahtgebundene, mündliche oder elektronische Kommunikation abgefangen, offengelegt oder absichtlich verwendet wird, eine Zivilklage wegen Verletzung des Wiretap Act einreichen, unter bestimmten Umständen auch gegen einen einzelnen Regierungsbeamten oder die Vereinigten Staaten. Für die Erfassung von Informationen, die nicht den Inhalt betreffen (z. B. IP-Adresse, E-Mail-An-/Abgangsadresse), siehe auch das Kapitel Pen Registers and Trap and Trace Devices in Titel 18 (18 U.S.C.
§§ 3121-3127 und, für zivilrechtliche Klagen, § 2707).

Claim Act[216] , dem Right to Financial Privacy Act[217] , und dem Fair Credit Reporting Act[218] .

(118) Auch nach dem FOIA[219] , 5 U.S.C. § 552, hat jede Person das Recht, Zugang zu Unterlagen von Bundesbehörden zu erhalten, auch wenn diese personenbezogene Daten der Person enthalten. Nach Ausschöpfung der verwaltungsrechtlichen Rechtsmittel kann eine Person dieses Recht auf Zugang vor Gericht geltend machen, es sei denn, die betreffenden Unterlagen sind durch eine Ausnahmeregelung oder einen speziellen Ausschluss für die Strafverfolgung vor der Veröffentlichung geschützt[220] . In diesem Fall prüft das Gericht, ob eine Ausnahmeregelung gilt oder von der betreffenden Behörde rechtmäßig in Anspruch genommen wurde.

### 3.2 Zugang und Nutzung durch US-Behörden für Zwecke der nationalen Sicherheit

(119) Das Recht der Vereinigten Staaten enthält verschiedene Beschränkungen und Garantien in Bezug auf den Zugang zu und die Verwendung von personenbezogenen Daten für Zwecke der nationalen Sicherheit und sieht Aufsichts- und Rechtsbehelfsmechanismen vor, die mit den in Erwägungsgrund 89 dieses Beschlusses genannten Anforderungen im Einklang stehen. Die Bedingungen, unter denen ein solcher Zugriff erfolgen kann, und

---

215 18 U.S.C. § 1030. Nach dem Computer Fraud and Abuse Act kann eine Person jede Person wegen vorsätzlichen unbefugten Zugriffs (oder Überschreitung der Zugriffsberechtigung) zur Erlangung von Informationen aus einem Finanzinstitut, einem Computersystem der US-Regierung oder einem anderen bestimmten Computer verklagen, unter bestimmten Umständen auch einen einzelnen Regierungsbeamten.

216 28 U.S.C. §§ 2671 et seq. Nach dem Federal Tort Claims Act kann eine Person unter bestimmten Umständen eine Klage gegen die Vereinigten Staaten wegen "fahrlässiger oder unrechtmäßiger Handlungen oder Unterlassungen eines Mitarbeiters der Regierung, der im Rahmen seines Amtes oder seiner Beschäftigung handelt", einreichen.

217 12 U.S.C. §§ 3401 et seq. Nach dem Right to Financial Privacy Act kann eine Person unter bestimmten Umständen Klage gegen die Vereinigten Staaten erheben, wenn sie geschützte Finanzunterlagen unter Verstoß gegen das Gesetz erhalten oder offengelegt hat. Der Zugang der Regierung zu geschützten Finanzunterlagen ist im Allgemeinen verboten, es sei denn, die Regierung stellt den Antrag auf der Grundlage einer rechtmäßigen Vorladung oder eines Durchsuchungsbefehls oder, mit Einschränkungen, eines formellen schriftlichen Antrags, und die Person, deren Informationen gesucht werden, erhält eine Benachrichtigung über einen solchen Antrag.

218 15 U.S.C. §§ 1681-1681x. Nach dem Fair Credit Reporting Act kann eine Person gegen jede Person klagen, die die Anforderungen (insbesondere die Notwendigkeit einer rechtmäßigen Genehmigung) hinsichtlich der Sammlung, Verbreitung und Verwendung von Verbraucherkreditberichten nicht einhält, oder unter bestimmten Umständen gegen eine Regierungsbehörde.

219 5 U.S.C. § 552.

220 Diese Ausnahmen sind jedoch nur ein Rahmen. Zum Beispiel sind nach 5 U.S.C. § 552 (b)(7) sind FOIA-Rechte für "Aufzeichnungen oder Informationen, die für Strafverfolgungszwecke zusammengestellt wurden, ausgeschlossen, jedoch nur insoweit, als die Vorlage solcher Strafverfolgungsaufzeichnungen oder -informationen (A) vernünftigerweise erwartet werden könnte, dass sie Vollstreckungsverfahren beeinträchtigt, (B) einer Person das Recht auf ein faires Verfahren oder eine unparteiische Entscheidung vorenthalten würde, (C) nach vernünftigem Ermessen einen ungerechtfertigten Eingriff in die Privatsphäre darstellen könnte, (D) nach vernünftigem Ermessen erwartet werden könnte, dass die Identität einer vertraulichen Quelle, einschließlich einer staatlichen, lokalen oder ausländischen Agentur oder Behörde oder einer privaten Institution, die Informationen auf vertraulicher Basis geliefert hat, offengelegt wird, und, im Falle einer Aufzeichnung oder von Informationen, die von einer Strafverfolgungsbehörde im Rahmen einer strafrechtlichen Untersuchung oder von einer Behörde, die eine rechtmäßige nachrichtendienstliche Untersuchung im Bereich der nationalen Sicherheit durchführt, von einer vertraulichen Quelle zur Verfügung gestellte Informationen, (E) Techniken und Verfahren für Ermittlungen oder Strafverfolgungsmaßnahmen der Strafverfolgungsbehörden oder Leitlinien für Ermittlungen oder Strafverfolgungsmaßnahmen der Strafverfolgungsbehörden offenlegen würde, wenn vernünftigerweise davon auszugehen ist, dass eine solche Offenlegung die Gefahr einer Umgehung des Gesetzes birgt, oder (F) vernünftigerweise davon

auszugehen ist, dass das Leben oder die körperliche Sicherheit einer Person gefährdet wird." Außerdem "[w]enn ein Ersuchen gestellt wird, das den Zugang zu Aufzeichnungen betrifft [von deren Vorlage vernünftigerweise erwartet werden könnte, dass sie ein Vollstreckungsverfahren beeinträchtigen] und- (A) die Untersuchung oder das Verfahren einen möglichen Verstoß gegen das Strafrecht beinhaltet; und (B) Grund zu der Annahme besteht, dass (i) die Person, die Gegenstand der Ermittlungen oder des Verfahrens ist, nichts von deren Anhängigkeit weiß und (ii) vernünftigerweise zu erwarten ist, dass die Offenlegung des Vorhandenseins der Unterlagen das Vollstreckungsverfahren beeinträchtigen könnte, kann die Behörde die Unterlagen nur so lange als nicht den Anforderungen dieses Abschnitts unterliegend behandeln, wie dieser Umstand andauert." (5 U.S.C. § 552 (c)(1)).

Die für die Ausübung dieser Befugnisse geltenden Schutzklauseln werden in den folgenden Abschnitten eingehend bewertet.

### *3.2.1 Rechtsgrundlagen, Einschränkungen und Garantien*

#### *3.2.1.1 Geltender Rechtsrahmen*

(120) Personenbezogene Daten, die von der Union an die DPF-Organisationen der EU und der USA übermittelt werden, können von den 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,
Die US-Geheimdienste dürfen den Zugang zu solchen Daten für Zwecke der nationalen Sicherheit nur beantragen, wenn sie gesetzlich dazu ermächtigt sind, insbesondere nach dem Foreign Intelligence Surveillance Act (FISA) oder nach gesetzlichen Bestimmungen, die den Zugang durch National Security Letters (NSL) genehmigen[221] . Das FISA enthält mehrere Rechtsgrundlagen, die für die Erhebung (und anschließende Verarbeitung) personenbezogener Daten von betroffenen Personen aus der Union, die im Rahmen der EU-US-DSGVO übermittelt werden, genutzt werden können (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 142-152 ausführlicher beschrieben.

(122) Die US-Nachrichtendienste haben auch die Möglichkeit, personenbezogene Daten außerhalb der Vereinigten Staaten zu erheben, wozu auch personenbezogene Daten im Transit zwischen der Union und den Vereinigten Staaten gehören können. Die Erhebung außerhalb der Vereinigten Staaten stützt sich auf die Executive Order 12333 (EO 12333)[227] , die vom Präsidenten[228] erlassen wurde.

(123) Die Sammlung von Signalen ist die Form der nachrichtendienstlichen Sammlung, die für die vorliegende Angemessenheitsfeststellung am relevantesten ist, da sie die Sammlung von elektronischer Kommunikation und Daten aus Informationssystemen betrifft. Eine solche Sammlung kann von den US-Nachrichtendiensten sowohl innerhalb der Vereinigten Staaten (auf der Grundlage des FISA) als auch während des Transits von Daten in die Vereinigten Staaten (auf der Grundlage der EO 12333) durchgeführt werden.

(124) Am 7. Oktober 2022 erließ der US-Präsident die EO 14086 über die Verbesserung der Sicherheitsvorkehrungen für den US-Signalnachrichtendienst, in der Beschränkungen und Sicherheitsvorkehrungen für alle Aktivitäten des US-Signalnachrichtendienstes festgelegt sind. Dieser Erlass ersetzt die Presidential Policy Directive (PPD-28)

---

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, der die traditionelle individualisierte elektronische Überwachung betrifft.

223 50 U.S.C. §1822, der körperliche Durchsuchungen zu Zwecken der Auslandsaufklärung betrifft.

224 50 U.S.C. § 1842 mit § 1841(2) und Abschnitt 3127 von Titel 18, der die Installation von Pen-Registern oder Trap-and-Trace-Geräten betrifft.

225 50 U.S.C. § 1861, der es dem FBI erlaubt, "einen Antrag auf eine Anordnung zu stellen, die einen gewöhnlichen Spediteur, eine öffentliche Einrichtung, ein physisches Lager oder eine Fahrzeugvermietungseinrichtung ermächtigt, Aufzeichnungen, die sich in ihrem Besitz befinden, für eine Untersuchung zur Sammlung ausländischer nachrichtendienstlicher Informationen oder eine Untersuchung zum internationalen Terrorismus freizugeben".

226 50 U.S. Code § 1881a, der es Elementen des US-Geheimdienstes erlaubt, Zugang zu Informationen, einschließlich des Inhalts von Internet-Kommunikation, von US-Unternehmen zu erhalten, wobei

bestimmte Nicht-US-Personen außerhalb der Vereinigten Staaten mit der gesetzlich vorgeschriebenen Unterstützung von Anbietern elektronischer Kommunikation ins Visier genommen werden.

227 EO 12333: United States Intelligence Activities, Federal Register Vol. 40, No 235 (8. Dezember 1981, geändert am 30. Juli 2008). EO 12333 definiert allgemein die Ziele, Richtungen, Aufgaben und Zuständigkeiten der nachrichtendienstlichen Bemühungen der USA (einschließlich der Rolle der verschiedenen Elemente der Intelligence Community) und legt die allgemeinen Parameter für die Durchführung nachrichtendienstlicher Tätigkeiten fest.

228 Nach Artikel II der US-Verfassung ist der Präsident als Oberbefehlshaber der Streitkräfte für die Gewährleistung der nationalen Sicherheit und insbesondere für die Sammlung ausländischer Informationen zuständig.

weitgehend[229] , stärkt die Bedingungen, Beschränkungen und Schutzmaßnahmen, die für alle nachrichtendienstlichen Tätigkeiten (d. h. auf der Grundlage von FISA und EO 12333) gelten, unabhängig davon, wo sie stattfinden[230] , und führt einen neuen Rechtsbehelfsmechanismus ein, durch den diese Schutzmaßnahmen von Einzelpersonen geltend gemacht und durchgesetzt werden können[231] (siehe im Einzelnen Erwägungsgründe 176-194). Damit wird das Ergebnis der Gespräche zwischen der EU und den USA, die nach der Aufhebung des Angemessenheitsbeschlusses der Kommission zum Privacy Shield durch den Gerichtshof stattfanden (siehe Erwägungsgrund 6), in amerikanisches Recht umgesetzt. Er ist daher ein besonders wichtiges Element des in diesem Beschluss bewerteten Rechtsrahmens.

(125) Die durch EO 14086 eingeführten Beschränkungen und Schutzmaßnahmen ergänzen die in Abschnitt 702 FISA und EO 12333 vorgesehenen. Die nachstehend (in den Abschnitten 3.2.1.2 und 3.2.1.3) beschriebenen Anforderungen müssen von den Nachrichtendiensten bei der Durchführung von Signals Intelligence-Aktivitäten gemäß Abschnitt 702 FISA und EO 12333 angewandt werden, z. B. bei der Auswahl/Ermittlung von Kategorien ausländischer nachrichtendienstlicher Informationen, die gemäß Abschnitt 702 FISA zu beschaffen sind, bei der Erhebung ausländischer nachrichtendienstlicher Informationen oder bei der Spionageabwehr gemäß EO 12333 und bei der Entscheidung über einzelne Zielpersonen gemäß Abschnitt 702 FISA und EO 12333.

(126) Die in dieser vom Präsidenten erlassenen Exekutivanordnung festgelegten Anforderungen sind für die gesamte Intelligence Community verbindlich. Sie müssen durch Strategien und Verfahren der Agenturen umgesetzt werden, die sie in konkrete Anweisungen für den täglichen Betrieb umsetzen. In dieser Hinsicht räumt 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 sie mit den Anforderungen der EO in Einklang zu bringen. Diese aktualisierten Strategien und Verfahren müssen in Absprache mit dem Generalstaatsanwalt, dem Beauftragten für den Schutz der bürgerlichen Freiheiten beim Direktor der nationalen Nachrichtendienste (ODNI CLPO) und dem PCLOB - einem unabhängigen Aufsichtsgremium, das befugt ist, die Strategien der Exekutive und ihre 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 öffentlich zugänglich gemacht werden[232] . Sobald die aktualisierten Strategien und Verfahren in Kraft sind, wird das PCLOB außerdem eine Überprüfung durchführen, um sicherzustellen, dass sie mit dem EB übereinstimmen. Innerhalb von 180 Tagen nach Abschluss einer solchen Überprüfung durch den PCLOB muss jeder Nachrichtendienst sorgfältig prüfen und umsetzen oder

---

229 EO 14086 ersetzt eine frühere Präsidentenrichtlinie, PPD 28, mit Ausnahme ihres Abschnitts 3 und eines ergänzenden Anhangs (der von den Nachrichtendiensten verlangt, ihre Prioritäten und Anforderungen im Bereich der Signalaufklärung jährlich zu überprüfen, wobei der Nutzen von Signalaufklärungstätigkeiten für die nationalen Interessen der USA sowie das Risiko, das von diesen Tätigkeiten ausgeht, zu berücksichtigen sind).Mit Ausnahme von Abschnitt 3 und dem ergänzenden Anhang (der die Nachrichtendienste dazu verpflichtet, ihre Prioritäten und Anforderungen im Bereich der Signalaufklärung jährlich zu überprüfen, wobei der Nutzen der Signalaufklärung für die nationalen Interessen der USA sowie das Risiko, das von diesen Aktivitäten ausgeht, zu berücksichtigen sind) und Abschnitt 6 (der allgemeine Bestimmungen enthält), siehe das 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 laut Fußnote 3 für nachrichtendienstliche Tätigkeiten zur Sammlung von Nachrichten oder Informationen über Nachrichten gilt, mit Ausnahme nachrichtendienstlicher Tätigkeiten zur Erprobung oder Entwicklung nachrichtendienstlicher Fähigkeiten.

231 Siehe in diesem Zusammenhang z. B. Abschnitt 5(h) der EO 14086, in dem klargestellt wird, dass die Schutzmaßnahmen der EO einen Rechtsanspruch begründen und von Einzelpersonen über den Rechtsbehelfsmechanismus durchgesetzt werden können.

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

ansonsten alle Empfehlungen des PCLOB berücksichtigen. Am 3. Juli 2023 veröffentlichte die US-Regierung diese aktualisierten Richtlinien und Verfahren[233] .

*3.2.1.2 Beschränkungen und Garantien bei der Erhebung personenbezogener Daten für Zwecke der nationalen Sicherheit*

(127) Die EO 14086 enthält eine Reihe weitreichender Anforderungen, die für alle nachrichtendienstlichen Tätigkeiten (Erhebung, Verwendung, Verbreitung usw. personenbezogener Daten) gelten.

(128) Erstens müssen solche Aktivitäten auf einem Gesetz oder einer Ermächtigung des Präsidenten beruhen und in Übereinstimmung mit dem US-Recht, einschließlich der Verfassung, durchgeführt werden[234] .

(129) Zweitens müssen geeignete Schutzvorkehrungen getroffen werden, um sicherzustellen, dass der Schutz der Privatsphäre und der bürgerlichen Freiheiten bei der Planung solcher Aktivitäten berücksichtigt wird[235] .

(130) Insbesondere dürfen nachrichtendienstliche Tätigkeiten nur durchgeführt werden, "wenn auf der Grundlage einer angemessenen Bewertung aller relevanten Faktoren festgestellt wurde, dass die Tätigkeiten erforderlich sind, um eine validierte nachrichtendienstliche Priorität voranzubringen" (zum Begriff der "validierten nachrichtendienstlichen Priorität" siehe Erwägungsgrund 135)[236] .

(131) Darüber hinaus dürfen solche Aktivitäten nur "in einem Umfang und in einer Weise durchgeführt werden, die in einem angemessenen Verhältnis zu der bestätigten nachrichtendienstlichen Priorität stehen, für die sie genehmigt wurden"[237] . Mit anderen Worten, es muss ein angemessenes Gleichgewicht "zwischen der Bedeutung der angestrebten nachrichtendienstlichen Priorität und den Auswirkungen auf die Privatsphäre und die bürgerlichen Freiheiten der betroffenen Personen, unabhängig von ihrer Staatsangehörigkeit oder ihrem Aufenthaltsort, hergestellt werden"[238] .

(132) Um sicherzustellen, dass diese allgemeinen Anforderungen - die die Grundsätze der Rechtmäßigkeit, Notwendigkeit und Verhältnismäßigkeit widerspiegeln - eingehalten werden, unterliegen die Tätigkeiten im Bereich der Signalnachrichtendienste der Aufsicht (siehe im Einzelnen Abschnitt 3.2.2)[239] .

(133) Diese übergreifenden Anforderungen werden in Bezug auf die Sammlung von Signalen durch eine Reihe von Bedingungen und Beschränkungen untermauert, die sicherstellen, dass der Eingriff in die Rechte des Einzelnen auf das zur Erreichung eines legitimen Ziels notwendige und verhältnismäßige Maß beschränkt ist.

(134) Erstens schränkt der EB die Gründe, aus denen Daten im Rahmen von nachrichtendienstlichen Tätigkeiten erhoben werden können, in zweierlei Hinsicht ein. Einerseits legt der EB die legitimen Ziele fest, die mit der Sammlung von Signalen verfolgt werden dürfen, z. B. um die Fähigkeiten, Absichten oder Aktivitäten ausländischer Organisationen, einschließlich internationaler terroristischer Organisationen, zu verstehen oder zu bewerten, die eine aktuelle oder potenzielle Bedrohung für die nationale Sicherheit der Vereinigten Staaten darstellen; um sich gegen ausländische militärische Fähigkeiten und Aktivitäten zu schützen; um transnationale Bedrohungen zu verstehen oder zu bewerten, die sich auf die globale Sicherheit auswirken, wie Klima- und andere ökologische Veränderungen, Risiken für die öffentliche Gesundheit und humanitäre Hilfe

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. Dies erfordert nicht immer, dass die nachrichtendienstliche Aufklärung das einzige Mittel ist, um Aspekte einer validierten nachrichtendienstlichen Priorität voranzubringen. So kann die Sammlung von Signalen beispielsweise dazu dienen, alternative Wege zur Validierung (z. B. zur Bestätigung von Informationen aus anderen nachrichtendienstlichen Quellen) oder zur Aufrechterhaltung eines zuverlässigen Zugangs zu denselben Informationen zu gewährleisten (Abschnitt 2 Buchstabe c) Ziffer i) Buchstabe 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.

Bedrohungen[240] . Andererseits listet der EO bestimmte Ziele auf, die auf keinen Fall mit nachrichtendienstlichen Aktivitäten verfolgt werden dürfen, z. B. zu dem Zweck, Kritik, Dissens oder die freie Äußerung von Ideen oder politischen Meinungen durch Einzelpersonen oder die Presse zu belasten; zu dem Zweck, Personen aufgrund ihrer ethnischen Zugehörigkeit, Rasse, ihres Geschlechts, ihrer Geschlechtsidentität, ihrer sexuellen Orientierung oder ihrer Religion zu benachteiligen; oder um US-Unternehmen einen Wettbewerbsvorteil zu verschaffen[241] .

(135) Darüber hinaus können sich die Nachrichtendienste nicht allein auf die in der EO 14086 festgelegten legitimen Ziele berufen, um die Sammlung von Signalen zu rechtfertigen, sondern müssen diese für operative Zwecke in konkretere Prioritäten umwandeln, für die Signals Intelligence gesammelt werden kann. Mit anderen Worten: Die tatsächliche Erfassung kann nur erfolgen, um eine spezifischere Priorität zu fördern. Diese Prioritäten werden in einem speziellen Verfahren festgelegt, das die Einhaltung der geltenden rechtlichen Anforderungen, einschließlich derjenigen in Bezug auf den Schutz der Privatsphäre und der bürgerlichen Freiheiten, gewährleisten soll. Konkret werden die nachrichtendienstlichen Prioritäten zunächst vom Direktor der Nationalen Nachrichtendienste (im Rahmen des so genannten National Intelligence Priorities Framework) entwickelt und dem Präsidenten zur Genehmigung vorgelegt[242] . Bevor der Direktor dem Präsidenten nachrichtendienstliche Prioritäten vorschlägt, muss er gemäß 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) weder dazu bestimmt ist noch voraussichtlich dazu führen wird, dass nachrichtendienstliche Signale für ein in der EO aufgeführtes verbotenes Ziel gesammelt werden, und (3) unter angemessener Berücksichtigung des Schutzes der Privatsphäre und der bürgerlichen Freiheiten aller Personen unabhängig von ihrer Staatsangehörigkeit oder ihrem Aufenthaltsort festgelegt wurde[243] . Falls der Direktor mit der Einschätzung des CLPO nicht einverstanden ist, müssen beide Ansichten dem Präsidenten vorgelegt werden[244] .

(136) Dieser Prozess stellt daher insbesondere sicher, dass Datenschutzaspekte bereits in der Anfangsphase, in der nachrichtendienstliche Prioritäten entwickelt werden, berücksichtigt werden.

(137) Zweitens wird, sobald eine nachrichtendienstliche Priorität festgelegt wurde, eine Reihe von Anforderungen an die Entscheidung gestellt, ob und in welchem Umfang nachrichtendienstliche Erkenntnisse gesammelt werden dürfen, um eine solche Priorität zu fördern. Mit diesen Anforderungen werden die übergreifenden Standards der Notwendigkeit und Verhältnismäßigkeit, die in Abschnitt 2 Buchstabe a des Erlasses festgelegt sind, umgesetzt.

(138) Insbesondere dürfen nachrichtendienstliche Erkenntnisse nur dann gesammelt werden, "wenn auf der Grundlage einer angemessenen Bewertung aller relevanten Faktoren festgestellt wurde, dass die Sammlung notwendig ist, um eine bestimmte nachrichtendienstliche Priorität voranzubringen"[245] . Bei der Entscheidung, ob eine bestimmte Erhebungsmaßnahme im Bereich der Signalaufklärung notwendig ist, um eine bestätigte nachrichtendienstliche Priorität zu fördern, müssen die US-Nachrichtendienste die Verfügbarkeit berücksichtigen,

---

240 Abschnitt 2(b)(i) EO 14086. Aufgrund der begrenzten Liste legitimer Ziele in der EO, die mögliche künftige Bedrohungen nicht umfasst, sieht die EO die Möglichkeit vor, dass der Präsident diese Liste aktualisieren kann, wenn neue nationale Sicherheitserfordernisse auftauchen, wie etwa neue Bedrohungen der nationalen Sicherheit. Solche Aktualisierungen müssen grundsätzlich veröffentlicht werden, es sei denn, der Präsident stellt fest, dass dies selbst ein Risiko für die nationale Sicherheit der Vereinigten Staaten darstellen würde (Abschnitt 2(b)(i)(B) EO 14086).

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 dem Leiter eines Teils der Intelligence Community festgelegt werden, die im Prinzip dieselben Kriterien anwenden müssen wie die in Abschnitt 2 Buchstabe b) Ziffer iii) Buchstabe A Nummern 1 bis 3 beschriebenen, siehe Abschnitt 4 Buchstabe n) EO 14086.

244 Abschnitt 2(b)(iii)(C) EO 14086.

245 Abschnitt 2(b) und (c)(i)(A) EO 14086.

Durchführbarkeit und Angemessenheit anderer, weniger eingreifender Quellen und Methoden, auch aus diplomatischen und öffentlichen Quellen[246] . Wenn verfügbar, müssen solche alternativen, weniger in die Privatsphäre eingreifenden Quellen und Methoden vorrangig genutzt werden[247] .

(139) Wenn bei der Anwendung dieser Kriterien die Sammlung von Signalen 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 zu finden - müssen alle relevanten Faktoren gebührend berücksichtigt werden, wie die Art des verfolgten Ziels, die Eingriffsintensität der Erhebungsmaßnahme, einschließlich ihrer Dauer, der wahrscheinliche Beitrag der Erhebung zum verfolgten Ziel, die vernünftigerweise vorhersehbaren Folgen für den Einzelnen sowie die Art und Sensibilität der zu erhebenden Daten[249] .

(140) Was die Art der Sammlung von Signalen betrifft, so muss die Sammlung von Daten innerhalb der Vereinigten Staaten, die für die vorliegende Angemessenheitsfeststellung am relevantesten ist, da sie Daten betrifft, die an Organisationen in den USA übermittelt wurden, immer gezielt erfolgen, wie in den Erwägungsgründen 142-153 näher erläutert.

(141) Die "Massenerhebung"[250] darf nur außerhalb der Vereinigten Staaten auf der Grundlage des EO 12333 durchgeführt werden. Auch in diesem Fall muss gemäß EO 14086 die gezielte Sammlung nach Prioritäten geordnet sein[251] . Umgekehrt sind Massenerhebungen nur dann zulässig, wenn die Informationen, die erforderlich sind, um eine bestätigte nachrichtendienstliche Priorität voranzubringen, nicht in angemessener Weise durch gezielte Erhebungen gewonnen werden können[252] . Wenn es notwendig ist, eine Massenerhebung von Daten außerhalb der Vereinigten Staaten durchzuführen, gelten besondere Schutzmaßnahmen gemäß EO 14086[253] . Erstens müssen Methoden und technische Maßnahmen angewandt werden, um die gesammelten Daten auf das zu beschränken, was notwendig ist, um eine validierte nachrichtendienstliche Priorität voranzutreiben, und gleichzeitig die Sammlung nicht relevanter Informationen zu minimieren[254] . Zweitens beschränkt der EO die Verwendung von Informationen

---

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.

250 D.h. die Sammlung großer Mengen von nachrichtendienstlichen Signalen, die aufgrund technischer oder operativer Erwägungen ohne die Verwendung von Unterscheidungsmerkmalen (z.B. ohne die Verwendung spezifischer Identifikatoren oder Auswahlbegriffe) erworben werden, siehe Abschnitt 4(b) EO 14086. Gemäß EO 14086 und wie in Erwägungsgrund 141 näher erläutert, findet eine Massenerhebung gemäß EO 12333 nur dann statt, wenn sie erforderlich ist, um bestimmte validierte nachrichtendienstliche Prioritäten voranzubringen, und sie unterliegt einer Reihe von Beschränkungen und Schutzmaßnahmen, die gewährleisten sollen, dass nicht wahllos auf Daten zugegriffen wird. Die Massenerhebung steht daher im Gegensatz zur allgemeinen und wahllosen Erhebung ("Massenüberwachung") ohne Einschränkungen und Schutzmaßnahmen.

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

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

253 Die besonderen Vorschriften der EO 14086 über die Massenerhebung gelten auch für eine gezielte Sammlung von Signalen, bei der vorübergehend Daten verwendet werden, die ohne Unterscheidungsmerkmale (z. B. spezifische Auswahlbegriffe oder Identifikatoren), d. h. in großen Mengen, erhoben wurden (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 Signalerfassung verwendet, nur für einen kurzen Zeitraum aufbewahrt 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 anfänglichen Sammlung ohne Unterscheidungsmerkmale darin, eine gezielte Sammlung von Informationen zu ermöglichen, indem eine bestimmte Kennung oder ein bestimmter Auswahlbegriff verwendet wird. In einem solchen Szenario werden nur Daten, die auf die Anwendung eines bestimmten Unterscheidungsmerkmals reagieren, in staatliche Datenbanken aufgenommen, während die übrigen Daten vernichtet werden. Eine solche gezielte Sammlung unterliegt daher weiterhin den allgemeinen Regeln, die für die Sammlung von Signalen gelten, einschließlich Abschnitt 2(a)-(b) und 2(c)(i) EO 14086.

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

(einschließlich der Abfrage) auf sechs spezifische Ziele zu beschränken, einschließlich des Schutzes vor Terrorismus, Geiselnahmen und der Gefangennahme von Personen durch oder im Namen einer ausländischen Regierung, Organisation oder Person, des Schutzes vor ausländischer Spionage, Sabotage oder Ermordung, des Schutzes vor Bedrohungen durch die Entwicklung, den Besitz oder die Verbreitung von Massenvernichtungswaffen oder damit zusammenhängenden Technologien und Bedrohungen usw.[255] Schließlich darf eine Abfrage von massenhaft gewonnenen nachrichtendienstlichen Erkenntnissen nur dann erfolgen, wenn dies zur Förderung einer validierten nachrichtendienstlichen Priorität erforderlich ist, und zwar in Verfolgung dieser sechs Ziele und im Einklang mit Strategien und Verfahren, die die Auswirkungen der Abfragen auf die Privatsphäre und die bürgerlichen Freiheiten aller Personen ungeachtet ihrer Staatsangehörigkeit oder ihres Aufenthaltsortes angemessen berücksichtigen[256] .

(142) Zusätzlich zu den Anforderungen von EO 14086 unterliegt die Sammlung von Daten, die an eine Organisation in den Vereinigten Staaten übermittelt wurden, spezifischen Beschränkungen und Schutzmaßnahmen, die in Abschnitt 702 FISA[257] geregelt sind. Abschnitt 702 FISA erlaubt die Sammlung von Informationen über ausländische Nachrichtendienste durch die gezielte Ansprache von Nicht-US-Personen, von denen man annimmt, dass sie sich außerhalb der Vereinigten Staaten befinden, und zwar mit der erzwungenen Unterstützung von US-Anbietern elektronischer Kommunikationsdienste[258] . Um Informationen über ausländische Nachrichtendienste gemäß Abschnitt 702 FISA zu sammeln, legen der Generalstaatsanwalt und der Direktor der Nationalen Nachrichtendienste dem Foreign Intelligence Surveillance Court (FISC) jährliche Bescheinigungen vor, in denen Kategorien von Informationen über ausländische Nachrichtendienste aufgeführt sind, die erworben werden sollen[259] . Den Bescheinigungen müssen Verfahren zur gezielten Erfassung, Minimierung und Abfrage beigefügt werden, die ebenfalls vom Gericht genehmigt werden und für die US-Geheimdienste rechtsverbindlich sind.

(143) Der FISC ist ein unabhängiges Gericht[260] , das durch ein Bundesgesetz geschaffen wurde und dessen Entscheidungen vor dem Foreign Intelligence Surveillance Court of Review (FISCR)[261] und schließlich vor dem Obersten Gerichtshof der Vereinigten Staaten[262] angefochten werden können. Der FISC (und FISCR) ist

---

255 Abschnitt 2(c)(ii)(B) EO 14086. Falls sich neue nationale Sicherheitsbedürfnisse ergeben, z. B. neue Bedrohungen der nationalen Sicherheit, kann der Präsident diese Liste aktualisieren. Solche Aktualisierungen müssen grundsätzlich veröffentlicht werden, es sei denn, der Präsident stellt fest, dass dies an sich eine Gefahr für die nationale Sicherheit der Vereinigten Staaten darstellen würde (Abschnitt 2(c)(ii)(C) EO 14086). Was die Abfrage von in großen Mengen erhobenen Daten betrifft, 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 der PCLOB feststellte, besteht die Überwachung nach Abschnitt 702 "ausschließlich darin, bestimmte [Nicht-US-]Personen ins Visier zu nehmen, über die eine individuelle Entscheidung getroffen wurde" (Privacy and Civil Liberties Oversight Board, Report on the Surveillance Program Operated Pursuant to Section 702 if the Foreign Intelligence Surveillance Act, 2. Juli 2014, Abschnitt 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.

259 50 U.S.C. § 1881a (g).

260 Der FISC setzt sich aus Richtern zusammen, die vom Obersten Richter der Vereinigten Staaten aus den Reihen der amtierenden
Richter des US-Bezirksgerichts, die zuvor vom Präsidenten ernannt und vom Senat bestätigt wurden. Die Richter, die eine lebenslange Amtszeit haben und nur aus wichtigem Grund abgesetzt werden können, sind für gestaffelte siebenjährige Amtszeiten im FISC tätig. Das FISA-Gesetz schreibt vor,

dass die Richter aus mindestens sieben verschiedenen Ländern stammen müssen.

U.S. Gerichtsbezirke. Siehe 50 U.S.C. § 1803 (a). Die Richter werden von erfahrenen Rechtsreferendaren unterstützt, die das juristische Personal des Gerichts bilden und rechtliche Analysen zu den Erhebungsanträgen erstellen. Siehe Brief des ehrenwerten Reggie B. Walton, Vorsitzender Richter am U.S. Foreign Intelligence Surveillance Court, an den ehrenwerten Patrick J. Leahy, Vorsitzender des Justizausschusses des US-Senats (29. Juli 2013) (Walton-Brief), S. 2, verfügbar unter https://fas.org/irp/news/2013/07/fisc-leahy.pdf.

261 Der FISCR setzt sich aus Richtern zusammen, die vom Obersten Richter der Vereinigten Staaten ernannt werden und aus folgenden Kreisen stammen

U.S. District Courts oder Courts of Appeals mit einer gestaffelten Amtszeit von sieben Jahren. 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).

unterstützt durch ein ständiges Gremium von fünf Rechtsanwälten und fünf technischen Experten, die über Fachwissen in Fragen der nationalen Sicherheit und der bürgerlichen Freiheiten verfügen[263] . Aus dieser Gruppe ernennt das Gericht eine Person, die als *"amicus curiae" bei* der Prüfung von Anträgen auf Erlass oder Überprüfung von Anordnungen mitwirkt, die nach Ansicht des Gerichts eine neue oder bedeutende Auslegung des Gesetzes darstellen, es sei denn, das Gericht hält eine solche Ernennung nicht für angemessen[264] . Auf diese Weise wird insbesondere sichergestellt, dass die Belange des Schutzes der Privatsphäre bei der Beurteilung durch das Gericht angemessen berücksichtigt werden. Das Gericht kann auch eine Einzelperson oder eine Organisation als amicus curiae ernennen, auch um technisches Fachwissen zur Verfügung zu stellen, wenn es dies für angemessen hält, oder auf Antrag einer Einzelperson oder einer Organisation die Erlaubnis erteilen, einen *amicus* curiae-Schriftsatz einzureichen[265] .

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

(145) Individuelle Zielfestlegungen werden von der National Security Agency (NSA), dem für die Zielfestlegung nach Abschnitt 702 FISA zuständigen Nachrichtendienst, gemäß den vom FISC genehmigten Zielfestlegungsverfahren getroffen, die von der NSA verlangen, auf der Grundlage der Gesamtheit der Umstände zu beurteilen, dass die Zielfestlegung auf eine bestimmte Person wahrscheinlich zur Erlangung einer in einer Bescheinigung angegebenen Kategorie von Informationen über ausländische Nachrichtendienste führt[268] . Diese Bewertung muss detailliert und faktenbasiert sein und sich auf das analytische Urteilsvermögen, die spezielle Ausbildung und Erfahrung des Analysten sowie die Art der zu beschaffenden nachrichtendienstlichen Informationen stützen[269] . Das Targeting erfolgt durch die Identifizierung so genannter Selektoren, die bestimmte Kommunikationseinrichtungen identifizieren, wie die E-Mail-Adresse oder Telefonnummer der Zielperson, aber niemals Schlüsselwörter oder Namen von Personen[270] .

---

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.. FISC Stellungnahme von 18 Oktober 2018, abrufbar unterhttps://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Op in_18Oct18.pdf , wie vom Foreign Intelligence Court of Review in seiner Stellungnahme vom 12. Juli 2019 bestätigt,
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, as amended, vom März 2018 (NSA targeting procedures), abrufbar unterhttps://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_NSA_Ta

r geting_27Mar18.pdf , S. 1-4, weiter erläutert im PCLOB-Bericht, S. 41-42.

[269] NSA-Zielverfahren, S. 4.

[270] Siehe PCLOB, Section 702 Report, S. 32-33, 45 mit weiteren Verweisen. Siehe auch Semiannual Assessment of Compliance with Procedures and Guidelines Issuant Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Submitted by the Attorney General and the Director of National Intelligence, Reporting Period: December 1, 2016 - May 31, 2017, S. 41 (Oktober 2018), verfügbar unter: https://www.dni.gov/files/icotr/18th_Joint_Assessment.pdf.

(146) Die NSA-Analysten ermitteln zunächst im Ausland ansässige Nicht-US-Personen, deren Überwachung nach Einschätzung der Analysten zu den in der Bescheinigung angegebenen relevanten ausländischen Erkenntnissen führen wird[271] . Wie in den Targeting-Verfahren der NSA dargelegt, kann die NSA nur dann eine Überwachung auf ein Ziel ausrichten, wenn sie bereits etwas über das Ziel erfahren hat[272] . Dies kann sich aus Informationen aus anderen Quellen ergeben, z. B. aus menschlichen Informationen. Durch 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 individualisierten Personen identifiziert wurden und ihr Targeting durch einen umfangreichen Überprüfungsmechanismus innerhalb der NSA[273] genehmigt wurde, werden Selektoren, die die von den Zielpersonen genutzten Kommunikationseinrichtungen (z. B. E-Mail-Adressen) identifizieren, "beauftragt" (d. h. entwickelt und angewendet)[274] .

(147) Die NSA muss die sachliche Grundlage für die Auswahl des Ziels dokumentieren[275] und in regelmäßigen Abständen nach der ersten Erfassung bestätigen, dass die Zielnorm weiterhin erfüllt ist[276] . Sobald die Zielvorgabe nicht mehr erfüllt ist, muss die Erfassung eingestellt werden[277] . Die Auswahl jedes Ziels durch die NSA und die Aufzeichnung jeder aufgezeichneten Zielbewertung und -begründung wird alle zwei Monate von Beamten der Geheimdienstaufsichtsbehörden des Justizministeriums auf die Einhaltung der Zielverfahren überprüft, die verpflichtet sind, dem FISC und dem Kongress jeden Verstoß zu melden[278] . Die schriftliche Dokumentation der NSA erleichtert dem FISC die Aufsicht darüber, ob bestimmte Personen gemäß Abschnitt 702 FISA im Einklang mit seinen in den Erwägungsgründen 173-174 beschriebenen Aufsichtsbefugnissen ordnungsgemäß erfasst werden[279] . Schließlich ist der Director of National Intelligence (DNI) auch verpflichtet, jedes Jahr die Gesamtzahl der Zielpersonen nach Abschnitt 702 FISA in öffentlichen jährlichen statistischen Transparenzberichten zu melden. Unternehmen, die FISA-Richtlinien nach Abschnitt 702 erhalten, können (über Transparenzberichte) aggregierte Daten über die bei ihnen eingehenden Anfragen veröffentlichen[280] .

---

271 PCLOB, Bericht über Abschnitt 702, S. 42-43.

272 NSA-Zielverfahren, S. 2.

273 PCLOB, Bericht über Abschnitt 702, S. 46. So muss die NSA beispielsweise überprüfen, ob eine Verbindung zwischen der Zielperson und dem Selektor besteht, sie muss dokumentieren, welche nachrichtendienstlichen Informationen aus dem Ausland voraussichtlich beschafft werden, diese Informationen müssen von zwei hochrangigen NSA-Analysten überprüft und genehmigt werden, und der gesamte Prozess wird für spätere Compliance-Prüfungen durch das ODNI und das Justizministerium nachverfolgt. Siehe NSA CLPO, NSA's Implementation of Foreign Intelligence Act Section 702, 16. April 2014.

274 50 U.S.C. § 1881a (h).

275 NSA-Zielverfahren, S. 8. Siehe auch PCLOB, Abschnitt 702-Bericht, S. 46. Das Versäumnis, eine schriftliche Begründung vorzulegen, stellt einen Verstoß gegen die Dokumentationspflicht dar, der dem FISC und dem Kongress gemeldet werden muss. Siehe Semiannual Assessment of Compliance with Procedures and Guidelines Issuant Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Submitted by the Attorney General and the Director of National Intelligence, Reporting Period: December 1, 2016 - May 31, 2017, S. 41 (Oktober 2018), DOJ/ODNI Compliance Report to FISC for Dec. 2016 - May 2017 at p. A-6, available at 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, at 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, at 2-3 (15. Juli 2015), wo es heißt, dass die Regierung "[i]f the Government later assesses that the continued tasking of a target's selector is not expected to result in the acquisition of foreign intelligence information, prompt detasking is required, and delay may result in a reportable compliance incident". Siehe auch die in Anhang VII enthaltenen Informationen.

278 PCLOB, Section 702 Report, S. 70-72; Regel 13(b) der Geschäftsordnung des United States Intelligence Überwachungsbehörde Gerichts, verfügbar unter 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 auf 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 unterschiedliche Beschränkungen und Garantien. Im Allgemeinen ist die Sammlung von Daten in großen Mengen gemäß Abschnitt 402 FISA (Pen-Register und Trap-and-Trace-Befugnis) und durch die Verwendung von NSL ausdrücklich verboten, und stattdessen ist die Verwendung spezifischer "Auswahlbedingungen" erforderlich[281] .

(149) Um eine herkömmliche individualisierte elektronische Überwachung (gemäß Abschnitt 105 FISA) durchführen zu können, müssen die Nachrichtendienste beim FISC einen Antrag mit einer Erklärung der Tatsachen und Umstände einreichen, auf die sie sich stützen, um die Annahme zu begründen, dass es einen wahrscheinlichen Grund gibt, dass die Einrichtung von einer ausländischen Macht oder einem Agenten einer ausländischen Macht genutzt wird oder genutzt werden soll[282] . Der FISC prüft unter anderem, ob auf der Grundlage der vorgelegten Fakten ein hinreichender Verdacht besteht, dass dies tatsächlich der Fall ist[283] .

(150) Zur Durchführung einer Durchsuchung von Räumlichkeiten oder Eigentum, die zu einer Inspektion, Beschlagnahme usw. von Informationen, Material oder Eigentum (z. B. eines Computergeräts) auf der Grundlage von Abschnitt 301 FISA führen soll, ist ein Antrag auf eine Anordnung durch das FISC erforderlich[284] . In einem solchen Antrag muss unter anderem dargelegt werden, dass ein hinreichender Verdacht besteht, dass es sich bei dem Ziel der Durchsuchung um eine ausländische Macht oder einen Agenten einer ausländischen Macht handelt, dass die zu durchsuchende Räumlichkeit oder das zu durchsuchende Eigentum Informationen über ausländische Nachrichtendienste enthält und dass sich die zu durchsuchende Räumlichkeit im Eigentum, in der Nutzung oder im Besitz einer ausländischen Macht (oder eines Agenten einer ausländischen Macht) befindet oder sich auf dem Weg zu oder von einer solchen befindet[285] .

(151) Ebenso erfordert die Installation von Pen-Registern oder Trap-and-Trace-Geräten (gemäß Abschnitt 402 FISA) einen Antrag auf Anordnung durch das FISC (oder einen US-Magistrate Judge) und die Verwendung eines spezifischen Auswahlbegriffs, d. h. eines Begriffs, der eine Person, ein Konto usw. spezifisch identifiziert und dazu dient, den Umfang der gesuchten Informationen so weit wie vernünftigerweise möglich einzuschränken[286] . Diese Befugnis betrifft nicht den Inhalt von Mitteilungen, sondern zielt vielmehr auf Informationen über den Kunden oder Teilnehmer, der einen Dienst nutzt (z. B. Name, Anschrift, Teilnehmernummer, Dauer/Art des empfangenen Dienstes, Quelle/Mechanismus der Zahlung).

(152) Abschnitt 501 FISA[287] , der die Erhebung von Geschäftsunterlagen eines gewöhnlichen Beförderungsunternehmens (d. h. einer Person oder Einrichtung, die gegen Entgelt Personen oder Sachen auf dem Land-, Schienen-, Wasser- oder Luftweg transportiert), einer öffentlichen Beherbergungseinrichtung (z. B. ein Hotel, Motel oder Gasthaus), einer Fahrzeugvermietungseinrichtung oder einer physischen Lagereinrichtung (d. h. die Raum für die Lagerung von Waren und Materialien zur Verfügung stellt oder Dienstleistungen im Zusammenhang damit erbringt)[288] gestattet, erfordert ebenfalls einen Antrag beim FISC oder einem Magistratsrichter. In diesem Antrag müssen die angeforderten Aufzeichnungen und die spezifischen und artikulierbaren Fakten angegeben werden, die Grund zu der Annahme geben, dass die Person, auf die sich die Aufzeichnungen beziehen, eine ausländische Macht oder ein Agent einer ausländischen Macht ist[289] .

281 50 U.S. Code § 1842(c)(3) und, in Bezug auf 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 Ein "Agent einer ausländischen Macht" kann auch Nicht-US-Personen umfassen, die sich am internationalen Terrorismus oder der internationalen Verbreitung von Massenvernichtungswaffen (einschließlich vorbereitender Handlungen) beteiligen (50 U.S.C. § 1801 (b)(1)).

283 50 U.S.C. § 1804. Siehe auch § 1841(4) in Bezug auf die Wahl der Auswahlbedingungen.

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 von Titel 18.

287 50 U.S.C. § 1862.

288 50 U.S.C. §§ 1861-1862.

289 50 U.S.C. § 1862(b).

(153) Schließlich sind NSL durch verschiedene Gesetze autorisiert und erlauben es den Ermittlungsbehörden, bestimmte Informationen (ohne den Inhalt der Kommunikation) von bestimmten Einrichtungen (z. B. Finanzinstituten, Kreditauskunfteien, Anbietern elektronischer Kommunikation) zu erhalten, die in Kreditauskünften, Finanzunterlagen und elektronischen Teilnehmer- und Transaktionsdaten enthalten sind[290] . Das NSL-Statut, das den Zugriff auf elektronische Kommunikation erlaubt, darf nur vom FBI verwendet werden und erfordert, dass die Anfragen einen Begriff verwenden, der eine Person, eine Einrichtung, eine Telefonnummer oder ein Konto spezifisch identifiziert und bestätigt, dass die Informationen für eine autorisierte nationale Sicherheitsuntersuchung zum Schutz vor internationalem Terrorismus oder geheimen nachrichtendienstlichen Aktivitäten relevant sind[291] . Die Empfänger einer NSL haben das Recht, diese vor Gericht anzufechten[292] .

*3.2.1.3 Weiterverwendung der gesammelten Informationen*

(154) Die Verarbeitung personenbezogener Daten, die von den US-Geheimdiensten im Rahmen der Signalaufklärung erhoben werden, unterliegt einer Reihe von Schutzmaßnahmen.

(155) Erstens muss jeder Nachrichtendienst eine angemessene Datensicherheit gewährleisten und verhindern, dass Unbefugte auf personenbezogene Daten zugreifen, die im Rahmen der Signalaufklärung erhoben wurden. Diesbezüglich sind in verschiedenen Instrumenten, einschließlich Gesetzen, Leitlinien und Normen, die Mindestanforderungen an die Informationssicherheit festgelegt (z. B. mehrstufige Authentifizierung, Verschlüsselung usw.)[293] . Der Zugang zu den gesammelten Daten muss auf autorisiertes, geschultes Personal beschränkt werden, das die Informationen zur Erfüllung seines Auftrags benötigt[294] . Generell müssen die Nachrichtendienste ihre Mitarbeiter angemessen schulen, auch in Bezug auf Verfahren zur Meldung und Behandlung von Gesetzesverstößen (einschließlich EO 14086)[295] .

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

(157) Drittens wird in der EO 14086 hinsichtlich der Datenspeicherung klargestellt, dass für personenbezogene Daten von Nicht-US-Personen dieselben Speicherfristen gelten wie für die Daten von

---

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).

293 Abschnitt 2(c)(iii)(B)(1) EO 14086. Siehe auch Titel VIII des National Security Act (mit detaillierten Anforderungen für den Zugang zu Verschlusssachen), E.O. 12333 Abschnitt 1.5 (verlangt von den Leitern der Agenturen der Intelligence Community, die Richtlinien 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" (weist den Ausschuss für nationale Sicherheitssysteme an, den Exekutivabteilungen und -agenturen Leitlinien für die Systemsicherheit nationaler 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 Endpunkt-Erkennungsdienste).

[294] Abschnitt 2(c)(iii)(B)(2) EO 14086. Darüber hinaus darf auf personenbezogene Daten, für die keine endgültige Entscheidung über die Aufbewahrung 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.

U.S. Personen[297] . Die Nachrichtendienste sind verpflichtet, spezifische Aufbewahrungsfristen und/oder die Faktoren festzulegen, die bei der Bestimmung der Länge der anwendbaren Aufbewahrungsfristen zu berücksichtigen sind (z. B. ob die Informationen Beweise für eine Straftat sind; ob die Informationen ausländische nachrichtendienstliche Informationen darstellen; ob die Informationen zum Schutz der Sicherheit von Personen oder Organisationen, einschließlich der Opfer oder Ziele des internationalen Terrorismus, erforderlich sind), die in verschiedenen Rechtsinstrumenten festgelegt sind[298] .

(158) Viertens gelten besondere Regeln für die Verbreitung personenbezogener Daten, die im Rahmen der Signalaufklärung erhoben wurden. Generell dürfen personenbezogene Daten über Nicht-US-Personen nur dann verbreitet werden, wenn es sich um dieselbe Art von Informationen handelt, die über US-Personen verbreitet werden können, z. B. Informationen, die zum Schutz der Sicherheit einer Person oder Organisation (wie Ziele, Opfer oder Geiseln internationaler terroristischer Organisationen) erforderlich sind[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 Weitergabe innerhalb der US-Regierung darf nur erfolgen, wenn eine befugte und geschulte Person die begründete Überzeugung 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 Weitergabe, die Art und der Umfang der weitergegebenen Daten sowie die möglichen schädlichen Auswirkungen auf die betroffene(n) Person(en) berücksichtigt werden[303] .

(159) Schließlich ist jeder Nachrichtendienst gemäß EO 14086 verpflichtet, eine angemessene Dokumentation über die Sammlung von nachrichtendienstlichen Signalen zu führen, auch um die Überwachung der Einhaltung der geltenden rechtlichen Anforderungen sowie wirksame Rechtsmittel zu erleichtern. Die Dokumentationsanforderungen umfassen Elemente wie die faktische Grundlage für die Einschätzung, dass eine bestimmte Erfassungsaktivität notwendig ist, um eine validierte nachrichtendienstliche Priorität voranzubringen[304] .

(160) Zusätzlich zu den oben erwähnten Schutzmaßnahmen der EO 14086 für die Verwendung von Informationen, die im Rahmen der Signalaufklärung gesammelt wurden, unterliegen alle US-Nachrichtendienste allgemeineren Anforderungen in Bezug auf Zweckbindung, Datenminimierung, Genauigkeit, Sicherheit, Aufbewahrung und Verbreitung, die sich insbesondere aus dem OMB-Rundschreiben Nr. A-130 ergeben,

---

297 Abschnitt 2(c)(iii)(A)(2)(a)-(c) EO 14086. Generell muss jede Agentur Strategien und Verfahren einführen, die darauf abzielen, die Verbreitung und Speicherung von personenbezogenen Daten, die durch Signalaufklärung gesammelt wurden, auf ein Minimum zu reduzieren (Abschnitt 2(c)(iii)(A) EO 14086).

298 Siehe z. B. Abschnitt 309 des Intelligence Authorization Act for Fiscal Year 2015; von einzelnen Nachrichtendiensten gemäß Abschnitt 702 FISA angenommene und vom FISC genehmigte Minimierungsverfahren; vom Generalstaatsanwalt und der FRA genehmigte Verfahren (die von US-Bundesbehörden, einschließlich nationaler Sicherheitsbehörden, verlangen, Aufbewahrungsfristen für ihre Unterlagen festzulegen, die von der National Archives and Record Administration genehmigt werden müssen).

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

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

301 So sieht beispielsweise das AGG-DOM vor, dass das FBI Informationen nur dann weitergeben darf,

wenn der Empfänger sie zur Erfüllung seines Auftrags oder zum Schutz der Öffentlichkeit benötigt.

302 Abschnitt 2(c)(iii)(A)(1)(c) EO 14086. Nachrichtendienste können beispielsweise Informationen verbreiten, die für strafrechtliche Ermittlungen relevant sind oder sich auf eine Straftat beziehen, z. B. durch die Verbreitung von Warnungen vor Morddrohungen, schweren Körperverletzungen oder Entführungen, die Verbreitung von Informationen über Cyberbedrohungen, Vorfälle oder Einbrüche sowie die Benachrichtigung von Opfern oder die Warnung potenzieller Opfer von Straftaten.

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

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

dem E-Government Act, dem Federal Records Act (siehe Erwägungsgründe 101-106) und den Leitlinien des Committee on National Security Systems (CNSS)[305] .

### *3.2.2 Beaufsichtigung*

(161) Die Tätigkeit der US-Geheimdienste unterliegt der Aufsicht verschiedener Gremien.

(162) Erstens verlangt die EO 14086, dass jeder Nachrichtendienst über hochrangige Beamte für Recht, Aufsicht und Einhaltung verfügt, um die Einhaltung des geltenden US-Rechts zu gewährleisten[306] . Sie müssen insbesondere eine regelmäßige Aufsicht über die Aktivitäten des Nachrichtendienstes im Bereich der Signaltechnik durchführen und dafür sorgen, dass alle Verstöße abgestellt werden. Die Nachrichtendienste müssen diesen Beamten Zugang zu allen relevanten Informationen gewähren, damit sie ihre Überwachungsaufgaben wahrnehmen können, und dürfen keine Maßnahmen ergreifen, die ihre Überwachungsaktivitäten behindern oder unzulässig beeinflussen[307] . Darüber hinaus muss jeder von einem Aufsichtsbeamten oder einem anderen Mitarbeiter festgestellte schwerwiegende Verstoß[308] unverzüglich dem Leiter des Nachrichtendienstes und dem Direktor des Nationalen Nachrichtendienstes gemeldet werden, der dafür sorgen muss, dass alle erforderlichen Maßnahmen ergriffen werden, um den schwerwiegenden Verstoß zu beheben und ein erneutes Auftreten zu verhindern[309] .

(163) Diese Aufsichtsfunktion wird von Beauftragten, die für die Einhaltung der Vorschriften zuständig sind, sowie von den Beauftragten für den Schutz der Privatsphäre und der bürgerlichen Freiheiten und den Generalinspektoren wahrgenommen[310] .

(164) Wie bei den Strafverfolgungsbehörden gibt es auch bei allen Nachrichtendiensten Datenschutz- und Bürgerrechtsbeauftragte[311] . Die Befugnisse dieser Beauftragten umfassen in der Regel die Überwachung von Verfahren, mit denen sichergestellt werden soll, dass die jeweilige Abteilung/Behörde die Belange des Schutzes der Privatsphäre und der bürgerlichen Freiheiten angemessen berücksichtigt und angemessene Verfahren zur Bearbeitung von Beschwerden von Personen eingerichtet hat, die der Ansicht sind, dass ihre Privatsphäre oder ihre bürgerlichen Freiheiten verletzt wurden (und in einigen Fällen, wie dem Office of the Director of National Intelligence (ODNI), können sie selbst befugt sein, Beschwerden zu untersuchen[312] ). Die Leiter der Nachrichtendienste müssen sicherstellen, dass die Beauftragten für den Schutz der Privatsphäre und die Wahrung der bürgerlichen Freiheiten über die zur Erfüllung ihres Auftrags erforderlichen Mittel verfügen, dass sie Zugang zu allen für die Erfüllung ihrer Aufgaben erforderlichen Materialien und Mitarbeitern erhalten und dass sie über vorgeschlagene Änderungen der Politik informiert und dazu konsultiert werden[313] . Die Beauftragten für den Schutz der Privatsphäre und der bürgerlichen Freiheiten erstatten dem Kongress und dem PCLOB regelmäßig Bericht, unter anderem über die Anzahl und Art der bei der Abteilung/Agentur eingegangenen Beschwerden mit einer

---

305 Siehe CNSS-Richtlinie Nr. 22, Cybersicherheits-Risikomanagementpolitik und CNSS-Anweisung 1253, die detaillierte Anleitungen für Sicherheitsmaßnahmen für nationale Sicherheitssysteme enthält.

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

307 Abschnitte 2(d)(i)(B)-(C) EO 14086.

308 D.h. ein systematischer oder vorsätzlicher Verstoß gegen geltendes US-Recht, der den Ruf oder die Integrität eines Teils der Intelligence Community angreifen oder die Angemessenheit einer Tätigkeit der Intelligence Community auf andere Weise in Frage stellen könnte, auch im Hinblick auf

erhebliche Auswirkungen auf die Privatsphäre und die bürgerlichen Freiheitsrechte der betroffenen Person(en), siehe Abschnitt 5 Buchstabe l) EO 14086.

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

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

311 Siehe 42 U.S.C. § 2000ee-1. Dazu gehören zum Beispiel das Außenministerium, das Justizministerium, das Heimatschutzministerium, das Verteidigungsministerium, die NSA, die Central Intelligence Agency (CIA), das FBI und das ODNI.

312 Siehe Abschnitt 3(c) EO 14086.

313 42 U.S.C. § 2000ee-1(d).

eine Zusammenfassung der Bearbeitung solcher Beschwerden, der durchgeführten Überprüfungen und Untersuchungen sowie der Auswirkungen der von dem Beauftragten durchgeführten Maßnahmen[314] .

(165) Zweitens verfügt jeder Nachrichtendienst über einen unabhängigen Generalinspektor, der u. a. für die Überwachung der Aktivitäten ausländischer Nachrichtendienste zuständig ist. Dazu gehört innerhalb des ODNI ein Office of the Inspector General of the Intelligence Community mit umfassender Zuständigkeit für die gesamte Intelligence Community, das befugt ist, Beschwerden oder Informationen über mutmaßlich rechtswidriges Verhalten oder Amtsmissbrauch im Zusammenhang mit Programmen und Tätigkeiten des ODNI und/oder der Intelligence Community zu untersuchen[315] . Wie bei den Strafverfolgungsbehörden (siehe Erwägungsgrund 109) sind diese Generalinspektoren gesetzlich unabhängig[316] und für die Durchführung von Prüfungen und Untersuchungen in Bezug auf die von der jeweiligen Stelle für Zwecke der nationalen Nachrichtendienste durchgeführten Programme und Operationen zuständig, auch im Hinblick auf Missbrauch oder Gesetzesverstöße[317] . Sie haben Zugang zu allen

---

314 Siehe 42 U.S.C. § 2000ee-1 (f)(1),(2). Aus dem Bericht des NSA-Büros für bürgerliche Freiheiten, Datenschutz und Transparenz für den Zeitraum Januar 2021 bis Juni 2021 geht beispielsweise hervor, dass es 591 Überprüfungen der Auswirkungen auf die bürgerlichen Freiheiten und den Datenschutz in verschiedenen Zusammenhängen durchgeführt hat, z. B. in Bezug auf Erhebungsaktivitäten, Vereinbarungen und Entscheidungen über die gemeinsame Nutzung von Informationen, Entscheidungen über die Vorratsdatenspeicherung usw., wobei verschiedene Faktoren berücksichtigt wurden, wie z. B. die Menge und die Art der mit der Aktivität verbundenen Informationen, die beteiligten Personen, der Zweck und die voraussichtliche Verwendung der Daten, die bestehenden Schutzmaßnahmen zur Minderung potenzieller Risiken für den Datenschutz usw. (https://media.defense.gov/2022/Apr/11/2002974486/-1/-1/1/REPORT%207_CLPT%20JANUARY%20-%20JUNE%202021%20_FINAL.PDF). Ähnlich verhält es sich mit der
Die Berichte des CIA-Büros für Datenschutz und bürgerliche Freiheiten für den Zeitraum Januar bis Juni 2019 enthalten Informationen über die Aufsichtstätigkeiten des Büros, z. B. eine Überprüfung der Einhaltung der Leitlinien des Generalstaatsanwalts gemäß EO 12333 in Bezug auf die Aufbewahrung und Verbreitung von Informationen, Leitlinien für die Umsetzung von PPD 28 und Anforderungen zur Ermittlung und Behandlung von Datenschutzverletzungen sowie Überprüfungen der Verwendung und Umgang von persönlichen Informationen (https://www.cia.gov/static/9d762fbef6669c7e6d7f17e227fad82c/2019-Q1-Q2-CIA-OPCL-Semi- Annual-Report.pdf).

315 Dieser Generalinspektor wird vom Präsidenten ernannt, muss vom Senat bestätigt werden und kann nur vom Präsidenten abgesetzt werden.

316 Die Generalinspektoren haben eine sichere Amtszeit und können nur vom Präsidenten abgesetzt werden, der dem Kongress die Gründe für eine solche Absetzung schriftlich mitteilen muss. Dies bedeutet nicht unbedingt, dass sie völlig frei von Weisungen sind. In einigen Fällen kann der Leiter des Ministeriums dem Generalinspektor verbieten, eine Prüfung oder Untersuchung einzuleiten, durchzuführen oder abzuschließen, wenn dies zur Wahrung wichtiger nationaler (Sicherheits-)Interessen für notwendig erachtet wird. Der Kongress muss jedoch über die Ausübung dieser Befugnis informiert werden und könnte auf dieser Grundlage den jeweiligen Direktor zur Verantwortung ziehen. Siehe z.B. Inspector General Act of 1978, § 8 (für das Verteidigungsministerium); § 8E (für das DOJ), § 8G (d)(2)(A),(B) (für die NSA); 50. U.S.C. § 403q (b) (für die CIA); Intelligence Authorization Act For Fiscal Year 2010, Sec 405(f) (für die Intelligence Community).

317 Inspector General Act von 1978, in der geänderten Fassung, Pub. L. 117-108 vom 8. April 2022. Wie in seinen Halbjahresberichten an den Kongress für den Zeitraum vom 1. April 2021 bis zum 31. März 2022 erläutert, hat der Generalinspekteur der NSA beispielsweise den Umgang mit Informationen über US-Personen, die im Rahmen von EO 12333 erhoben wurden, das Verfahren zur Bereinigung von Signals Intelligence-Daten, ein von der NSA verwendetes automatisches Targeting-Tool und die Einhaltung der Dokumentations- und Abfragebestimmungen in Bezug auf die Erhebung nach Abschnitt 702 FISA bewertet und in diesem Zusammenhang mehrere Empfehlungen abgegeben (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 Nachrichtendienste zur Informationssicherheit und zur unerlaubten Weitergabe von von Verschlusssachen nationalen Sicherheit Informationen (https://www.dni.gov/files/ICIG/Documents/Publications/Semiannual%20Report/2021/ICIG_Semiannual_Report_April_2021_to_September_2021.pdf, pp. 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).

Aufzeichnungen, Berichte, Prüfungen, Überprüfungen, Dokumente, Unterlagen, Empfehlungen oder sonstiges einschlägiges Material, erforderlichenfalls durch Vorladung, und können Zeugenaussagen machen[318] . Die Generalinspekteure verweisen Fälle mutmaßlicher strafrechtlicher Verstöße zur Verfolgung und geben Empfehlungen für Abhilfemaßnahmen an die Leiter der Behörden[319] . Ihre Empfehlungen sind zwar unverbindlich, aber ihre Berichte, auch über Folgemaßnahmen (oder das Fehlen solcher)[320] , werden in der Regel veröffentlicht und dem Kongress übermittelt, der auf dieser Grundlage seine eigene Aufsichtsfunktion ausüben kann (siehe Erwägungsgründe 168-169)[321] .

(166) Drittens überwacht das Intelligence Oversight Board (IOB), das im Rahmen des President's Intelligence Advisory Board (PIAB) eingerichtet wurde, die Einhaltung der Verfassung und aller geltenden Vorschriften durch die US-Nachrichtendienste[322] . Das PIAB ist ein beratendes Gremium innerhalb des Executive Office of the President, das sich aus 16 Mitgliedern zusammensetzt, die vom Präsidenten von außerhalb der US-Regierung ernannt werden. Die IOB besteht aus maximal fünf Mitgliedern, die vom Präsidenten aus den Reihen der PIAB-Mitglieder ernannt werden. Gemäß EO 12333[323] sind die Leiter aller Nachrichtendienste verpflichtet, dem IOB alle nachrichtendienstlichen Aktivitäten zu melden, bei denen Grund zu der Annahme besteht, dass sie möglicherweise rechtswidrig sind oder gegen eine Exekutivanordnung oder eine Direktive des Präsidenten verstoßen. Um sicherzustellen, dass das IOB Zugang zu den Informationen hat, die es zur Erfüllung seiner Aufgaben benötigt, weist die Executive Order 13462 den Director of National Intelligence 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] . Die IOB ist ihrerseits verpflichtet, den Präsidenten über nachrichtendienstliche Aktivitäten zu informieren, von denen sie annimmt, dass sie gegen US-Gesetze (einschließlich Executive Orders) verstoßen und die vom Generalstaatsanwalt, dem Direktor der Nationalen Nachrichtendienste oder dem Leiter eines Nachrichtendienstes nicht in angemessener Weise behandelt werden[325] . Darüber hinaus ist die IOB verpflichtet, den Generalstaatsanwalt über mögliche Verstöße gegen das Strafrecht zu informieren.

(167) Viertens: Die Nachrichtendienste unterliegen der Aufsicht durch den PCLOB. Gemäß seinem Gründungsstatut ist der PCLOB mit Aufgaben im Bereich der Terrorismusbekämpfung und deren Umsetzung betraut, um die Privatsphäre und die bürgerlichen Freiheiten zu schützen. Bei der Überprüfung der Maßnahmen der Nachrichtendienste hat er Zugang zu allen einschlägigen Aufzeichnungen, Berichten, Prüfungen, Dokumenten, Unterlagen und Empfehlungen der Nachrichtendienste,

---

318 Siehe Generalinspektionsgesetz von 1978, § 6.

319 Siehe *ebd*. §§ 4, 6-5.

320 Zu den Folgemaßnahmen zu den Berichten und Empfehlungen der Generalinspekteure, siehe z. B. die Reaktion auf einen Bericht des Generalinspekteurs des Justizministeriums, in dem festgestellt wurde, dass das FBI bei Anträgen von 2014 bis 2019 gegenüber der 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. ordnete der FBI-Direktor mehr als 40 Abhilfemaßnahmen an, darunter 12 speziell für das FISA-Verfahren in Bezug auf Dokumentation, Aufsicht, Aktenführung, Schulung und Audits) (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 beispielsweise auch die Prüfung des DoJ Inspector General of the FBI Office of the General Counsel's roles and responsibilities in overseeing compliance with applicable laws, policies, and procedures relating to the FBI's national security activities und Anhang 2, der ein Schreiben des FBI enthält, in dem alle Empfehlungen akzeptiert werden. Anhang 3 gibt einen Überblick über die Folgemaßnahmen und Informationen, die der

Generalinspekteur vom FBI benötigte, um seine Empfehlungen abschließen zu können (https://oig.justice.gov/sites/default/files/reports/22-116.pdf).

321 Siehe Inspector General Act von 1978, §§ 4(5), 5.

322 Siehe EO 13462.

323 Abschnitt 1.6(c) EO 12333.

324 Abschnitt 8(a) EO 13462.

325 Abschnitt 6(b) EO 13462.

einschließlich Verschlusssachen, Interviews führen und Zeugenaussagen hören[326] . Er erhält Berichte von den Beauftragten für bürgerliche Freiheiten und Datenschutz mehrerer Bundesministerien/Bundesbehörden[327] , kann Empfehlungen an die Regierung und die Nachrichtendienste aussprechen und erstattet den Kongressausschüssen und dem Präsidenten regelmäßig Bericht[328] . Die Berichte des Ausschusses, einschließlich der Berichte an den Kongress, müssen so weit wie möglich öffentlich zugänglich gemacht werden[329] . Das PCLOB hat mehrere Aufsichts- und Follow-up-Berichte veröffentlicht, darunter eine Analyse der auf der Grundlage von Abschnitt 702 FISA durchgeführten Programme und des Schutzes der Privatsphäre in diesem Zusammenhang, der Umsetzung von PPD 28 und EO 12333[330] . Das PCLOB ist auch mit der Wahrnehmung spezifischer Aufsichtsfunktionen in Bezug auf die Umsetzung von EO 14086 betraut, insbesondere mit der Überprüfung, ob die Verfahren der Agenturen mit dem EO in Einklang stehen (siehe Erwägungsgrund 126), und mit der Bewertung der Korrekturfunktion des Rechtsbehelfsmechanismus (siehe Erwägungsgrund 194).

(168) Fünftens: Zusätzlich zu den Aufsichtsmechanismen innerhalb der Exekutive sind spezielle Ausschüsse im US-Kongress (der Geheimdienst- und der Justizausschuss des Repräsentantenhauses und des Senats) für die Aufsicht über alle nachrichtendienstlichen Aktivitäten der USA im Ausland zuständig. Die Mitglieder dieser Ausschüsse haben Zugang zu Verschlusssachen sowie zu nachrichtendienstlichen Methoden und Programmen[331] . Die Ausschüsse üben ihre Aufsichtsfunktion auf unterschiedliche Weise aus, insbesondere durch Anhörungen, Untersuchungen, Überprüfungen und Berichte[332] .

(169) Die Kongressausschüsse erhalten regelmäßig Berichte über nachrichtendienstliche Tätigkeiten, u. a. vom Generalstaatsanwalt, dem Direktor der Nationalen Nachrichtendienste, den Nachrichtendiensten und anderen Aufsichtsgremien (z. B. den Generalinspekteuren), siehe Erwägungsgründe 164-165. Gemäß dem National Security Act stellt der Präsident insbesondere sicher, dass die Geheimdienstausschüsse des Kongresses umfassend und aktuell über die nachrichtendienstlichen Tätigkeiten der Vereinigten Staaten informiert werden, einschließlich aller wesentlichen

---

326 42 U.S.C. § 2000ee (g).

327 Siehe 42 U.S.C. § 2000ee-1 (f)(1)(A)(iii). Dazu gehören mindestens das Justizministerium, das Verteidigungsministerium, das Ministerium für Innere Sicherheit, der Direktor des Nationalen Nachrichtendienstes und der Zentrale Nachrichtendienst sowie jedes andere Ministerium, jede andere Behörde oder jedes andere Element der Exekutive, das von der PCLOB als geeignet für die Abdeckung bezeichnet wird.

328 42 U.S.C. §2000ee (e).

329 42 U.S.C. § 2000ee (f).

330 Verfügbar unter https://www.pclob.gov/Oversight.

331 50 U.S.C. § 3091.

332 So veranstalten die Ausschüsse beispielsweise thematische Anhörungen (siehe z . B. eine kürzlich durchgeführte Anhörung des Justizausschusses des Repräsentantenhauses Ausschusses zu "digitale dragnets", https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4983, und eine Anhörung des House Intelligence Ausschusses auf die Verwendung von AI durchdie Geheimdienste Gemeinschaft, https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=114263) regelmäßige Anhörungen zur Aufsicht, z.B. von der FBI und DoJ Nationale Sicherheit Abteilung, siehe https://www.judiciary.senate.gov/meetings/08/04/2022/oversight-of-the- f e d e r a l - b u r e a u - o f - Untersuchung; https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4966

und https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4899. Als Beispiel für eine Untersuchung siehe die Untersuchung des Geheimdienstausschusses des Senats zur russischen Einmischung in die Wahlen 2016 U.S.. Wahlen, siehe https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-russian-active-measures. Was die Berichterstattung betrifft, siehe z.B. den Überblick über die (Überwachungs-)Aktivitäten des Ausschusses im Bericht des Geheimdienstausschusses des Senats für den Zeitraum 4 Januar . 2019 - 3 Januar 2021 auf . den Senat, https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-covering-period-january-4.

voraussichtliche nachrichtendienstliche Tätigkeit, wie in diesem Unterkapitel gefordert"[333] . Darüber hinaus "stellt der Präsident sicher, dass jede illegale nachrichtendienstliche Tätigkeit unverzüglich den Nachrichtendienstausschüssen des Kongresses gemeldet wird, ebenso wie alle Korrekturmaßnahmen, die im Zusammenhang mit einer solchen illegalen Tätigkeit ergriffen wurden oder geplant sind"[334] .

(170) Darüber hinaus ergeben sich aus bestimmten Gesetzen zusätzliche Berichtspflichten. Insbesondere verpflichtet der FISA den Generalstaatsanwalt, die Geheimdienst- und Justizausschüsse des Senats und des Repräsentantenhauses über die Aktivitäten der Regierung im Rahmen bestimmter Abschnitte des FISA[335] "umfassend zu informieren". Außerdem muss die Regierung den Kongressausschüssen Kopien aller Entscheidungen, Anordnungen oder Stellungnahmen des FISC oder des FISCR zukommen lassen, die eine "wesentliche Auslegung oder Interpretation" der FISA-Bestimmungen beinhalten. Was die Überwachung gemäß Abschnitt 702 FISA betrifft, so wird die parlamentarische Kontrolle durch gesetzlich vorgeschriebene Berichte an die Geheimdienst- und Justizausschüsse sowie durch häufige Unterrichtungen und Anhörungen ausgeübt. Dazu gehören ein halbjährlicher Bericht des Generalstaatsanwalts, in dem die Anwendung von Abschnitt 702 FISA beschrieben wird, mit Belegdokumenten, einschließlich Berichten des Justizministeriums und des ODNI über die Einhaltung der Vorschriften und einer Beschreibung aller Vorfälle, in denen die Vorschriften nicht eingehalten wurden[336] , sowie eine separate halbjährliche Bewertung des Generalstaatsanwalts und des DNI, in der die Einhaltung der Verfahren zur gezielten Überwachung und Minimierung der Datenmenge dokumentiert wird[337] .

(171) Darüber hinaus verpflichtet das FISA-Gesetz die US-Regierung, dem Kongress (und der Öffentlichkeit) jedes Jahr die Anzahl der beantragten und erhaltenen FISA-Anordnungen sowie Schätzungen der Anzahl der von der Überwachung betroffenen US-Personen und Nicht-US-Personen offenzulegen, unter anderem[338] . Das Gesetz schreibt auch eine zusätzliche öffentliche Berichterstattung über die Anzahl der ausgestellten NSL vor, wiederum sowohl in Bezug auf US-Personen als auch auf Nicht-US-Personen (während es gleichzeitig den Empfängern von FISA-Anordnungen und -Bescheinigungen sowie NSL-Anträgen gestattet, unter bestimmten Bedingungen Transparenzberichte zu erstellen)[339] .

(172) Generell unternimmt die U.S. Intelligence Community verschiedene Anstrengungen, um Transparenz über ihre (ausländischen) nachrichtendienstlichen Aktivitäten herzustellen. So hat das ODNI im Jahr 2015 Grundsätze für die Transparenz der Nachrichtendienste und einen Transparenz-Implementierungsplan verabschiedet und jeden Nachrichtendienst angewiesen, einen Beauftragten für die Transparenz der Nachrichtendienste zu benennen, der die Transparenz fördert und Transparenzinitiativen leitet[340] . Im Rahmen dieser Bemühungen hat die Intelligence Community Teile von Strategien, Verfahren, Aufsichtsberichten, Berichten über Aktivitäten im Rahmen von Abschnitt 702 FISA und EO 12333, FISC-Entscheidungen und andere Dokumente freigegeben und tut dies auch weiterhin.

---

333 Siehe 50 U.S.C. § 3091(a)(1). Diese Bestimmung enthält die allgemeinen Anforderungen an die Aufsicht 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).

338 50 U.S.C. § 1873(b). Ferner heißt es in Abschnitt 402: "Der Direktor der Nationalen Nachrichtendienste führt in Absprache mit dem Generalstaatsanwalt eine Überprüfung der Freigabe

jeder Entscheidung, Anordnung oder Stellungnahme des Foreign Intelligence Surveillance Court oder des Foreign Intelligence Surveillance Court of Review (wie in Abschnitt 601(e) definiert) durch, die eine wesentliche Auslegung oder Interpretation einer Rechtsvorschrift enthält, einschließlich einer neuen oder wesentlichen Auslegung oder Interpretation des Begriffs "spezifischer Auswahlbegriff", und macht im Einklang mit dieser Überprüfung jede derartige Entscheidung, Anordnung oder Stellungnahme so weit wie möglich öffentlich zugänglich.

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.

Materialien zu veröffentlichen, u.a. auf einer speziellen Webseite "IC on the Record", die vom ODNI[341] verwaltet wird.

(173) Schließlich unterliegt die Erhebung personenbezogener Daten gemäß Abschnitt 702 FISA zusätzlich zu der in den Erwägungsgründen 162-168 erwähnten Überwachung durch die Aufsichtsgremien auch der Aufsicht durch den FISC[342] . Gemäß Regel 13 der FISC-Verfahrensregeln sind die Compliance-Beauftragten in den US-Geheimdiensten verpflichtet, dem DoJ und dem ODNI Verstöße gegen die FISA 702-Verfahren zur gezielten Erfassung, Minimierung und Abfrage von Daten zu melden, die diese wiederum dem FISC melden. Darüber hinaus legen das DoJ und das ODNI dem FISC halbjährliche gemeinsame Aufsichtsbewertungsberichte vor, in denen Trends bei der Einhaltung der Zielvorgaben aufgezeigt werden, statistische Daten bereitgestellt werden, Kategorien von Vorfällen bei der Einhaltung der Zielvorgaben beschrieben werden, die Gründe für das Auftreten bestimmter Vorfälle bei der Einhaltung der Zielvorgaben detailliert beschrieben werden und die Maßnahmen dargelegt werden, die die Nachrichtendienste ergriffen haben, um eine Wiederholung zu vermeiden[343] .

(174) Erforderlichenfalls (z. B. wenn Verstöße gegen die Verfahren zur gezielten Datenerhebung festgestellt werden) kann der Gerichtshof den betreffenden Nachrichtendienst anweisen, Abhilfemaßnahmen zu treffen[344] . Die betreffenden Abhilfemaßnahmen können von individuellen bis hin zu strukturellen Maßnahmen reichen, z. B. von der Beendigung der Datenerfassung und der Löschung unrechtmäßig erlangter Daten bis hin zu einer Änderung der Erhebungspraxis, auch in Form von Leitlinien und Schulungen für die Mitarbeiter[345] . Darüber hinaus prüft der FISC bei seiner jährlichen Überprüfung der Bescheinigungen nach Abschnitt 702, ob die vorgelegten Bescheinigungen den FISA-Anforderungen entsprechen. Stellt der FISC fest, dass die Bescheinigungen der Regierung nicht ausreichend waren, auch wegen bestimmter Vorfälle bei der Einhaltung der Vorschriften, kann er eine so genannte "deficiency order" erlassen, in der die Regierung aufgefordert wird, den Verstoß innerhalb von 30 Tagen zu beheben, oder in der die Regierung aufgefordert wird, die Umsetzung der Bescheinigung nach Abschnitt 702 einzustellen oder nicht zu beginnen. Schließlich bewertet die FISC Trends, die sie bei der Einhaltung von Vorschriften beobachtet, und

---

341 Siehe "IC on the Record", verfügbar unter https://icontherecord.tumblr.com/.

342 In der Vergangenheit kam der FISC zu dem Schluss, dass "es für das Gericht offensichtlich ist, dass die durchführenden Behörden sowie [das ODNI] und [die Abteilung für nationale Sicherheit des DOJ] beträchtliche Ressourcen für die Einhaltung der Vorschriften und die Aufsicht über die Einhaltung von Abschnitt 702 aufwenden. In der Regel werden Fälle der Nichteinhaltung umgehend festgestellt und geeignete Abhilfemaßnahmen ergriffen, zu denen auch die Löschung von Informationen gehört, die unrechtmäßig erlangt wurden oder nach den geltenden Verfahren anderweitig der Vernichtungspflicht unterliegen". FISA Court, Memorandum Opinion and Order [Überschrift unkenntlich gemacht] (2014), verfügbar

u

nter

https://www.dni.gov/files/documents/0928/FISC%20Memorandum%20Opinion%20and%20Order%20 26%20August%202014.pdf.

343 *Siehe z. B.* DOJ/ODNI FISA 702 Compliance Report to FISC for June 2018 - Nov. 2018 at 21-65.

344 50 U.S.C. § 1803(h). Siehe auch PCLOB, Section 702 Report, S. 76. Siehe auch die FISC Memorandum Opinion and Order vom 3. Oktober 2011 als Beispiel für eine Mängelanordnung, in der die Regierung angewiesen wurde zu zu korrigieren. die festgestellten Mängeln innerhalb von 30 Tagen. Verfügbar unterunter 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 FISC-Stellungnahme vom 18. Oktober 2018,

abrufbar unter https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opin._18Oct18.pdf, bestätigt durch das Foreign Intelligence Court of Review in seiner Stellungnahme vom 12. Juli 2019, verfügbar unter . https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISCR_Opinion_12Jul19.pdf, in der die FISC die Regierung unter anderem anordnete, bestimmte Melde-, Dokumentations- und Berichtspflichten gegenüber der 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 die FISC die Regierung anweist, bis zum 28. Februar 2020 einen schriftlichen Bericht über die Schritte vorzulegen, die die Regierung unternimmt, um die Verfahren zur Identifizierung und Entfernung von Berichten zu verbessern, die aus FISA-702-Informationen abgeleitet und aus Gründen der Einhaltung der Vorschriften zurückgerufen wurden, sowie über andere Angelegenheiten. Siehe auch Anhang VII.

können Änderungen der Verfahren oder zusätzliche Überwachung und Berichterstattung erforderlich sein, um Trends bei der Einhaltung der Vorschriften zu berücksichtigen[346] .

### *3.2.3 Abhilfe*

(175) Wie in diesem Abschnitt näher erläutert, gibt es in den Vereinigten Staaten eine Reihe von Möglichkeiten, die betroffenen Personen in der Union die Möglichkeit geben, vor einem unabhängigen und unparteiischen Gericht mit verbindlichen Befugnissen Klage zu erheben. Zusammengenommen ermöglichen sie es dem Einzelnen, Zugang zu seinen personenbezogenen Daten zu erhalten, die Rechtmäßigkeit des staatlichen Zugriffs auf seine Daten überprüfen zu lassen und im Falle eines Verstoßes die Beseitigung dieses Verstoßes zu erwirken, unter anderem durch Berichtigung oder Löschung seiner personenbezogenen Daten.

(176) Erstens wird im Rahmen des EO 14086 ein spezieller Rechtsbehelfsmechanismus eingerichtet, der durch die AG-Verordnung zur Einrichtung des Datenschutzüberprüfungsgerichts ergänzt wird, um Beschwerden von Einzelpersonen über US-Signalspionagetätigkeiten zu bearbeiten und beizulegen. Jede Person in der EU ist berechtigt, bei dem Rechtsbehelfsmechanismus eine Beschwerde über eine angebliche Verletzung von US-Gesetzen, die nachrichtendienstliche Tätigkeiten im Bereich der Signaltechnik regeln (z. B. EO 14086, Abschnitt 702 FISA, EO 12333), einzureichen, die ihre Interessen in Bezug auf Privatsphäre und bürgerliche Freiheiten beeinträchtigt[347] . Dieser Rechtsbehelfsmechanismus steht Personen aus Ländern oder Organisationen der regionalen Wirtschaftsintegration zur Verfügung, die vom Generalstaatsanwalt der USA als "qualifizierte Staaten" bezeichnet wurden[348] . Am 30. Juni 2023 werden die Europäische Union und die drei Länder der Europäischen Freihandelsassoziation, die zusammen den Europäischen Wirtschaftsraum bilden, vom Generalstaatsanwalt gemäß Abschnitt 3(f) EO 14086 als "qualifizierte Staaten" bezeichnet[349] . Diese Benennung erfolgt unbeschadet des Artikels 4 Absatz 2 des Vertrags über die Europäische Union.

(177) Eine betroffene Person in der Union, die eine solche Beschwerde einreichen möchte, muss diese bei einer Aufsichtsbehörde in einem EU-Mitgliedstaat einreichen, die für die Überwachung der Verarbeitung personenbezogener Daten durch öffentliche Stellen zuständig ist (eine Datenschutzbehörde)[350] . Dies gewährleistet einen einfachen 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 die in Erwägungsgrund 178 genannten Voraussetzungen für die Einreichung einer Beschwerde geprüft wurden, leitet die zuständige Datenschutzbehörde die Beschwerde über das Sekretariat des Europäischen Datenschutzausschusses an den Beschwerdemechanismus weiter.

(178) Die Anforderungen an die Zulässigkeit einer Beschwerde beim Beschwerdemechanismus sind gering, da die Betroffenen nicht nachweisen müssen, dass ihre Daten tatsächlich Gegenstand von US-Signalspionageaktivitäten waren[351] . Um dem Rechtsbehelfsmechanismus einen Ausgangspunkt für eine Überprüfung zu geben, müssen bestimmte grundlegende Informationen bereitgestellt werden, z . B. über die personenbezogenen Daten, von denen man annimmt, dass sie

---

346 Siehe Anhang VII.

347 Siehe Abschnitt 4(k)(iv) EO 14086, der vorsieht, dass eine Beschwerde beim Rechtsbehelfsverfahren von einem Beschwerdeführer eingereicht werden muss, der in seinem eigenen Namen handelt (d.h. nicht als Vertreter einer Regierung, Nichtregierungsorganisation oder zwischenstaatlichen Organisation). Der Begriff "nachteilig betroffen" setzt nicht voraus, dass der Beschwerdeführer eine bestimmte Schwelle erreicht, um Zugang zum Rechtsbehelfsverfahren zu erhalten (siehe hierzu

Erwägungsgrund 178). Vielmehr wird klargestellt, dass der CLPO des ODNI und der DPRC befugt sind, Verstöße gegen US-Rechtsvorschriften im Bereich der Funknachrichtendienste zu beheben, die sich nachteilig auf die Privatsphäre und die bürgerlichen Freiheiten eines Beschwerdeführers auswirken. Umgekehrt fallen Verstöße gegen Anforderungen des geltenden US-Rechts, die nicht dem Schutz des Einzelnen dienen (z. B. Haushaltsanforderungen), nicht in die Zuständigkeit des ODNI CLPO und des DPRC.

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.

die Identität der US-Regierungsstellen, von denen angenommen wird, dass sie an dem mutmaßlichen Verstoß beteiligt sind (falls bekannt); die Grundlage für die Behauptung, dass ein Verstoß gegen US-Recht vorliegt (obwohl auch hier nicht nachgewiesen werden muss, dass personenbezogene Daten tatsächlich von US-Geheimdiensten erhoben wurden) und die Art des beantragten Rechtsbehelfs.

(179) Die anfängliche Untersuchung von Beschwerden an diesen Rechtsbehelfsmechanismus wird vom ODNI CLPO durchgeführt, dessen bestehende gesetzliche Rolle und Befugnisse für die spezifischen Maßnahmen, die gemäß EO 14086[352] ergriffen werden, erweitert wurden. Innerhalb der Intelligence Community ist der CLPO unter anderem dafür verantwortlich, sicherzustellen, dass der Schutz der bürgerlichen Freiheiten und der Privatsphäre in angemessener Weise in die Strategien und Verfahren des ODNI und der Nachrichtendienste aufgenommen wird; er überwacht die Einhaltung der geltenden Anforderungen an die bürgerlichen Freiheiten und den Schutz der Privatsphäre durch das ODNI und führt Datenschutzfolgenabschätzungen durch[353] . Der CLPO des ODNI kann nur aus wichtigem Grund vom Director of National Intelligence entlassen werden, d.h. im Falle eines Fehlverhaltens, eines Vergehens, einer Sicherheitsverletzung, einer Pflichtverletzung oder einer Unfähigkeit[354] .

(180) Bei der Durchführung seiner Überprüfung hat der ODNI CLPO Zugang zu den Informationen für seine Bewertung und kann sich auf die obligatorische Unterstützung der Datenschutz- und Bürgerrechtsbeauftragten in den verschiedenen Nachrichtendiensten[355] verlassen. Den Nachrichtendiensten ist es untersagt, die Überprüfungen des ODNI CLPO zu behindern oder unangemessen zu beeinflussen. Dies gilt auch für den Direktor der nationalen Nachrichtendienste, der sich nicht in die Überprüfung einmischen darf[356] . Bei der Überprüfung einer Beschwerde muss der ODNI CLPO "das Gesetz unparteiisch anwenden", wobei er sowohl die nationalen Sicherheitsinteressen bei nachrichtendienstlichen Tätigkeiten als auch den Schutz der Privatsphäre berücksichtigen muss[357] .

(181) Im Rahmen seiner Überprüfung stellt das ODNI CLPO fest, ob ein Verstoß gegen geltende U.S.-Gesetzes stattgefunden hat, und entscheidet, wenn dies der Fall ist, über eine geeignete Abhilfemaßnahme[358] . Letzteres bezieht sich auf Maßnahmen, mit denen ein festgestellter Verstoß vollständig behoben wird, z. B. die Beendigung der unrechtmäßigen Datenerfassung, die Löschung unrechtmäßig erhobener Daten, die Löschung der Ergebnisse unzulässig durchgeführter Abfragen ansonsten rechtmäßig erhobener Daten, die Beschränkung des Zugriffs auf rechtmäßig erhobene Daten auf entsprechend geschultes Personal oder der Rückruf nachrichtendienstlicher Berichte, die unrechtmäßig erhobene oder unrechtmäßig verbreitete Daten enthalten[359] . Die Entscheidungen des ODNI CLPO zu einzelnen Beschwerden (einschließlich der Abhilfemaßnahmen) sind für die betroffenen Nachrichtendienste verbindlich[360] .

(182) Der ODNI CLPO muss seine Überprüfung dokumentieren und eine als Verschlusssache eingestufte Entscheidung vorlegen, in der er die Grundlage für seine faktischen Feststellungen, die Feststellung, ob ein erfasster Verstoß vorliegt, und die Festlegung der geeigneten Abhilfemaßnahmen erläutert[361] . Ergibt die Überprüfung des ODNI CLPO einen Verstoß gegen eine Behörde, die der Aufsicht des FISC unterliegt, muss der CLPO auch einen als Verschlusssache eingestuften Bericht an

---

352 Abschnitt 3(c)(iv) EO 14086. Siehe auch National Security Act 1947, 50 U.S.C. §403-3d, Abschnitt 103D über 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.

den stellvertretenden Generalstaatsanwalt für nationale Sicherheit, der seinerseits verpflichtet ist, den Verstoß dem FISC zu melden, der weitere Durchsetzungsmaßnahmen ergreifen kann (gemäß dem in den Erwägungsgründen 173-174 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 erfassten Verstöße festgestellt wurden oder der ODNI CLPO eine Entscheidung getroffen hat, die angemessene Abhilfemaßnahmen erfordert"[363] . Auf diese Weise kann die Vertraulichkeit von Tätigkeiten zum Schutz der nationalen Sicherheit gewahrt werden, während die Betroffenen eine Entscheidung erhalten, die bestätigt, dass ihre Beschwerde ordnungsgemäß untersucht und entschieden wurde. Diese Entscheidung kann außerdem von der betroffenen Person angefochten werden. Zu diesem Zweck wird er über die Möglichkeit informiert, beim DPRC Berufung einzulegen, um die Entscheidungen des CLPO überprüfen zu lassen (siehe Erwägungsgründe 184 und weitere), und darüber, dass für den Fall, dass das Gericht angerufen werden sollte, ein spezieller Anwalt ausgewählt wird, der die Interessen des Beschwerdeführers vertritt[364] .

(184) Jeder Beschwerdeführer sowie jeder Teil der Intelligence Community kann eine Überprüfung der Entscheidung des ODNI CLPO vor dem Data Protection Review Court (DPRC) beantragen. Solche Überprüfungsanträge müssen innerhalb von 60 Tagen nach Erhalt der Mitteilung des 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] . Betroffene Personen aus der Union können ihren Antrag erneut bei der zuständigen Datenschutzbehörde einreichen (siehe Erwägungsgrund 177).

(185) Der DPRC ist ein unabhängiges Gericht, das vom Generalstaatsanwalt auf der Grundlage von EO 14086[366] eingerichtet wurde. Es besteht aus mindestens sechs Richtern, die vom Generalstaatsanwalt in Absprache mit dem PCLOB, dem Handelsminister und dem Direktor der Nationalen Nachrichtendienste für eine verlängerbare Amtszeit von vier Jahren ernannt werden[367] . Die Ernennung der Richter durch den Generalstaatsanwalt richtet sich nach den Kriterien, die die Exekutive bei der Beurteilung von Bewerbern für die Bundesgerichtsbarkeit anwendet, wobei frühere richterliche Erfahrungen berücksichtigt werden[368] . Darüber hinaus müssen die Richter Juristen sein (d.h. aktive Mitglieder der Anwaltskammer und ordnungsgemäß zur Ausübung des Rechts zugelassen) und über angemessene Erfahrung im Bereich des Datenschutzes und der nationalen Sicherheit verfügen. Der Generalstaatsanwalt muss sich darum bemühen, dass mindestens die Hälfte der Richter zu jedem Zeitpunkt über richterliche Vorerfahrung verfügt, und alle Richter müssen über eine Sicherheitsüberprüfung verfügen, um Zugang zu Verschlusssachen der nationalen Sicherheit zu erhalten[369] .

(186) Nur Personen, die die in Erwägungsgrund 185 genannten Qualifikationen erfüllen und weder zum Zeitpunkt ihrer Ernennung noch in den vorangegangenen zwei Jahren Angestellte der Exekutive waren, können in den DPRC berufen werden. Ebenso können sie während ihrer Amtszeit bei der

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.
365 Abschnitte 201.6(a)-(b) AG-Verordnung.

366 Abschnitt 3(d)(i)) und die AG-Verordnung. Der Oberste Gerichtshof der Vereinigten Staaten hat dem Generalstaatsanwalt die Möglichkeit eingeräumt, unabhängige Gremien mit Entscheidungsbefugnis einzurichten, die auch über Einzelfälle 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 verschiedenen Anforderungen der EO 14086, z.B. die Kriterien und das Verfahren für die Ernennung und Entlassung von DPRC-Richtern, unterliegt insbesondere der Überwachung durch den Generalinspektor des Justizministeriums (siehe auch Erwägungsgrund 109 zu den gesetzlichen Befugnissen der Generalinspektoren).

367 Abschnitt 3(d)(i)(A) EO 14086 und Abschnitt 201.3(a) AG-Verordnung.

368 Abschnitt 201.3(b) AG-Verordnung.

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

DPRC dürfen die Richter keine offiziellen Aufgaben oder Anstellungen innerhalb der US-Regierung haben (außer als Richter am DPRC)[370] .

(187) Die Unabhängigkeit des Urteilsverfahrens wird durch eine Reihe von Garantien gewährleistet. Insbesondere ist es der Exekutive (dem Generalstaatsanwalt und den Nachrichtendiensten) untersagt, sich in die Überprüfung des DPRC einzumischen oder diese unangemessen zu beeinflussen[371] . Das DPRC selbst ist verpflichtet, Fälle unparteiisch zu beurteilen[372] und arbeitet nach seiner eigenen Geschäftsordnung (die mit Mehrheitsbeschluss angenommen wird). Darüber hinaus können die Richter der DPRC nur vom Generalstaatsanwalt und nur aus wichtigem Grund entlassen werden (d.h. wegen Fehlverhaltens, Fehlverhaltens, Verletzung der Sicherheit, Vernachlässigung der Pflichten oder Unfähigkeit), nachdem die für Bundesrichter geltenden Standards, die in den Regeln für das richterliche Verhalten und das Verfahren bei richterlicher Untauglichkeit festgelegt sind, gebührend berücksichtigt wurden[373] .

(188) Die Anträge an das DPRC werden von einem Gremium aus drei Richtern, einschließlich eines vorsitzenden Richters, geprüft, die im Einklang mit dem Verhaltenskodex für US-Richter[374] handeln müssen. Jedes Gremium wird von einem Sonderbeistand[375] unterstützt, der Zugang zu allen den Fall betreffenden Informationen hat, einschließlich Verschlusssachen[376] . Die Rolle des Sonderberaters besteht darin, sicherzustellen, dass die Interessen des Beschwerdeführers vertreten werden und dass das DPRC-Gremium über alle relevanten rechtlichen und faktischen Fragen gut informiert ist[377] . Um seinen Standpunkt zu einem Überprüfungsantrag einer Einzelperson an den DPRC zu untermauern, kann der Sonderberater den Beschwerdeführer durch schriftliche Fragen um Informationen bitten[378] .

---

370 Abschnitt 3(d)(i)(A) EO 14086 und Abschnitt 201.3(a) und (c) der AG-Verordnung. Personen, die in den DPRC berufen werden, dürfen außergerichtliche Tätigkeiten ausüben, einschließlich geschäftlicher, finanzieller, gemeinnütziger und treuhänderischer Tätigkeiten sowie der Ausübung des Rechtsanwaltsberufs, solange diese Tätigkeiten nicht die unparteiische Ausübung ihrer Pflichten oder die Wirksamkeit oder Unabhängigkeit des DPRC beeinträchtigen (Abschnitt 201.7(c) AG Regulation).

371 Abschnitt 3(d)(iii)-(iv) EO 14086 und Abschnitt 201.7(d) AG Regulation.

372 Abschnitt 3(d)(i)(D) EO 14086 und Abschnitt 201.9 AG-Verordnung.

373 Abschnitt 3(d)(iv) EO 14086 und Abschnitt 201.7(d) AG-Verordnung. Siehe auch Bumap vs. Vereinigte Staaten, 252

U.S. 512, 515 (1920), das den seit langem bestehenden Grundsatz im US-Recht bestätigte, dass die Befugnis zur Amtsenthebung mit der Ernennungsbefugnis einhergeht (wie auch vom Office of Legal Counsel des Justizministeriums in The Constitutional Separation of Powers Between the President and Congress, 20 Op. O.L.C. 124, 166 (1996), in Erinnerung gerufen).

374 Abschnitt 3(d)(i)(B) EO 14086 und Abschnitt 201.7(a)-(c) AG Regulation. Das Office of Privacy and Civil Liberties des Justizministeriums (OPCL), das für die administrative Unterstützung des DPRC und der Sonderbeauftragten zuständig ist (siehe Abschnitt 201.5 der AG-Verordnung), wählt nach dem Rotationsprinzip ein dreiköpfiges Gremium aus, wobei es darauf achtet, dass in jedem Gremium mindestens ein Richter mit früherer richterlicher Erfahrung vertreten ist (wenn keiner der Richter im Gremium über eine solche Erfahrung verfügt, übernimmt der zuerst vom OPCL ausgewählte Richter den Vorsitz).

375 Abschnitt 201.4 AG-Verordnung. Mindestens zwei Sonderberater werden vom Generalstaatsanwalt in Absprache mit dem Handelsminister, dem Direktor der nationalen Nachrichtendienste und dem PCLOB für zwei verlängerbare Amtszeiten ernannt. Die Sonderberater müssen über einschlägige Erfahrungen auf dem Gebiet des Datenschutzes und des Rechts der nationalen Sicherheit verfügen, erfahrene Anwälte sein, aktive Mitglieder der Anwaltskammer und ordnungsgemäß als Anwälte zugelassen sein. Darüber hinaus dürfen sie zum Zeitpunkt ihrer ersten Ernennung in den vorangegangenen zwei Jahren nicht bei der Exekutive beschäftigt gewesen sein. Für jede Prüfung eines Antrags wählt der vorsitzende Richter einen Sonderberater aus, der das Gremium unterstützt, siehe Abschnitt 201.8(a) AG-Verordnung.

376 Abschnitt 201.8(c) und 201.11 AG-Verordnung.

377 Abschnitt 3(d)(i)(C) EO 14086 und Abschnitt 201.8(e) AG-Verordnung. Der Sonderberater handelt

nicht als Bevollmächtigter des Beschwerdeführers und unterhält kein Mandatsverhältnis mit diesem.

378 Siehe Abschnitt 201.8(d)(e) AG-Verordnung. Solche Fragen werden zunächst vom OPCL in Absprache mit der zuständigen Stelle der Intelligence Community geprüft, um Verschlusssachen, vertrauliche oder geschützte Informationen zu ermitteln und auszuschließen, bevor sie an den Beschwerdeführer weitergeleitet werden. Zusätzliche Informationen, die der Sonderbeauftragte in Beantwortung solcher Fragen erhält, werden in die Eingaben des Sonderbeauftragten an den DPRC aufgenommen.

(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 angemessenen Abhilfemaßnahmen), wobei es sich zumindest auf die Aufzeichnungen der Untersuchung des ODNI CLPO stützt sowie auf Informationen und Vorlagen, die vom Beschwerdeführer, dem Sonderbeauftragten oder einem Nachrichtendienst[379] vorgelegt werden. Ein DPRC-Gremium hat Zugang zu allen Informationen, die für die Durchführung einer Überprüfung erforderlich sind und die es über das ODNI CLPO erhalten kann (das Gremium kann z. B. das CLPO auffordern, seine Aufzeichnungen durch zusätzliche Informationen oder Tatsachenfeststellungen zu ergänzen, wenn dies für die Durchführung der Überprüfung erforderlich ist)[380] .

(190) Beim Abschluss seiner Überprüfung kann das DPRC (1) entscheiden, dass es keine Beweise dafür gibt, dass nachrichtendienstliche Tätigkeiten im Zusammenhang mit personenbezogenen Daten des Beschwerdeführers stattgefunden haben, (2) entscheiden, dass die Feststellungen des ODNI CLPO rechtlich korrekt waren und durch stichhaltige Beweise gestützt wurden, oder (3) wenn das DPRC mit den Feststellungen des ODNI CLPO nicht einverstanden ist (ob ein Verstoß gegen geltendes US-Recht stattgefunden hat oder welche Abhilfemaßnahmen angemessen sind), seine eigenen Feststellungen treffen[381] .

(191) In allen Fällen trifft der DPRC eine schriftliche Entscheidung durch Mehrheitsbeschluss. Wird bei der Überprüfung ein Verstoß gegen die geltenden Vorschriften festgestellt, werden in der Entscheidung geeignete Abhilfemaßnahmen festgelegt, darunter die Löschung unrechtmäßig erhobener Daten, die Löschung der Ergebnisse unzulässig durchgeführter Abfragen, die Beschränkung des Zugriffs auf rechtmäßig erhobene Daten auf entsprechend geschultes Personal oder der Rückruf nachrichtendienstlicher Berichte, die ohne rechtmäßige Genehmigung 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 der Aufsicht des FISC unterliegende Befugnis festgestellt, muss das DPRC außerdem einen als Verschlusssache eingestuften Bericht an den stellvertretenden Generalstaatsanwalt für nationale Sicherheit übermitteln, der seinerseits verpflichtet ist, die Nichteinhaltung der Vorschriften dem FISC zu melden, das weitere Durchsetzungsmaßnahmen ergreifen kann (gemäß dem in den Erwägungsgründen 173-174 beschriebenen Verfahren)[384] .

(192) Jede Entscheidung eines DPRC-Gremiums wird an das ODNI CLPO[385] übermittelt. In Fällen, in denen die Überprüfung des DPRC durch einen Antrag des Beschwerdeführers ausgelöst wurde, wird der Beschwerdeführer über die nationale Behörde darüber informiert, dass das DPRC seine Überprüfung abgeschlossen hat und dass "bei der Überprüfung entweder keine erfassten Verstöße festgestellt wurden oder das DPRC eine Feststellung getroffen hat, die angemessene Abhilfemaßnahmen erfordert"[386] . Das Amt für Datenschutz

---

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

380 Abschnitt 3(d)(iii) EO 14086 und Abschnitt 201.9(b) AG-Verordnung.

381 Abschnitt 3(d)(i)(E) EO 14086 und Abschnitt 201.9(c)-(e) AG-Verordnung. Gemäß der Definition des Begriffs "angemessene Abhilfemaßnahmen" in Abschnitt 4(a) EO 14086 muss die DPRC bei der Entscheidung über eine Abhilfemaßnahme zur vollständigen Behebung eines Verstoßes "die Art und Weise berücksichtigen, wie ein Verstoß der festgestellten Art üblicherweise behoben wurde", d. h. die DPRC wird neben anderen Faktoren berücksichtigen, wie ähnliche Probleme in der Vergangenheit behoben wurden, um sicherzustellen, dass die Abhilfemaßnahme wirksam und angemessen ist.

382 Abschnitt 4(a) EO 14086.

383 Abschnitt 3(d)(ii) EO 14086 und Abschnitt 201.9(g) AG-Verordnung. Da die Entscheidung des DPRC

endgültig und verbindlich ist, kann keine andere Exekutiv- oder Verwaltungsinstitution/-körperschaft (einschließlich des Präsidenten der Vereinigten Staaten) die Entscheidung des DPRC aufheben. Dies wurde auch in der Rechtsprechung des Obersten Gerichtshofs bestätigt, der klarstellte, dass der Generalstaatsanwalt durch die Übertragung der einzigartigen Befugnis des Generalstaatsanwalts innerhalb der Exekutive, verbindliche Entscheidungen zu erlassen, an ein unabhängiges Gremium, sich selbst die Möglichkeit nimmt, die Entscheidung dieses Gremiums in irgendeiner Weise zu diktieren (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) AG-Verordnung.

385 Abschnitt 201.9(h) AG-Verordnung.

386 Abschnitt 3(d)(i)(H) EO 14086 und Abschnitt 201.9(h) AG-Verordnung. Hinsichtlich der Art der Anmeldung siehe Abschnitt 201.9 (h)(3) AG-VO.

and Civil Liberties of the DoJ führt ein Verzeichnis aller vom DPRC geprüften Informationen und aller ergangenen Entscheidungen, das künftigen DPRC-Gremien als nicht verbindlicher Präzedenzfall zur Verfügung gestellt wird[387] .

(193) Das DoC ist außerdem verpflichtet, für jeden Beschwerdeführer, der eine Beschwerde eingereicht hat, ein Verzeichnis zu führen[388] . Um die Transparenz zu erhöhen, muss das DoC mindestens alle fünf Jahre mit den einschlägigen Nachrichtendiensten Kontakt aufnehmen, um zu überprüfen, ob die Informationen, die eine Überprüfung durch das DPRC betreffen, freigegeben wurden[389] . Ist dies der Fall, wird die betreffende Person darauf hingewiesen, dass diese Informationen nach geltendem Recht verfügbar sein können (d. h., dass sie nach dem Gesetz über die Informationsfreiheit Zugang zu diesen Informationen beantragen kann, siehe Erwägungsgrund 199).

(194) Schließlich wird das ordnungsgemäße Funktionieren dieses Rechtsbehelfsmechanismus einer regelmäßigen und unabhängigen Bewertung unterzogen. Genauer gesagt unterliegt das Funktionieren des Rechtsbehelfsmechanismus gemäß EO 14086 einer jährlichen Überprüfung durch das PCLOB, einer unabhängigen Einrichtung (siehe Erwägungsgrund 110)[390] . Im Rahmen dieser Überprüfung wird der PCLOB unter anderem beurteilen, ob der ODNI CLPO und das DPRC Beschwerden fristgerecht bearbeitet haben, ob sie uneingeschränkten Zugang zu den erforderlichen Informationen erhalten haben, ob die materiellen Garantien der EO 14086 im Überprüfungsprozess ordnungsgemäß berücksichtigt wurden und ob die Intelligence Community den Feststellungen des ODNI CLPO und des DPRC in vollem Umfang nachgekommen ist. Der PCLOB wird dem Präsidenten, dem Generalstaatsanwalt, dem Direktor der Nationalen Nachrichtendienste, den Leitern der Nachrichtendienste, dem ODNI CLPO und den Nachrichtendienstausschüssen des Kongresses einen Bericht über das Ergebnis seiner Überprüfung vorlegen, der auch in einer nicht klassifizierten Fassung veröffentlicht wird und der wiederum in die regelmäßige Überprüfung der Funktionsweise des vorliegenden Beschlusses durch die Kommission einfließen wird. Der Generalstaatsanwalt, der Direktor der Nationalen Nachrichtendienste, der CLPO des ODNI und die Leiter der Nachrichtendienste sind verpflichtet, alle in diesen Berichten enthaltenen Empfehlungen umzusetzen oder anderweitig zu berücksichtigen. Darüber hinaus wird der PCLOB jährlich öffentlich bescheinigen, ob der Abhilfemechanismus Beschwerden im Einklang mit den Anforderungen der EO 14086 bearbeitet.

(195) Neben dem spezifischen Rechtsbehelfsverfahren, das im Rahmen von EO 14086 eingerichtet wurde, stehen allen Personen (unabhängig von ihrer Staatsangehörigkeit oder ihrem Wohnsitz) Rechtsbehelfe vor den ordentlichen Gerichten der USA zur Verfügung[391] .

(196) Insbesondere bieten das FISA und ein damit zusammenhängendes Gesetz Einzelpersonen die Möglichkeit, eine Zivilklage auf Schadenersatz gegen die Vereinigten Staaten zu erheben, wenn Informationen über sie unrechtmäßig und vorsätzlich verwendet oder weitergegeben wurden[392] ; die U S A zu verklagen.

---

387 Abschnitt 201.9(j) Ag-Verordnung.

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.

391 Voraussetzung für den Zugang zu diesen Rechtsmitteln ist der Nachweis der Klagebefugnis. Dieser

Standard, der für jede Person unabhängig von ihrer Staatsangehörigkeit gilt, ergibt sich aus dem Erfordernis des "Falles oder der Kontroverse" in Artikel III der US-Verfassung. Nach Ansicht des Obersten Gerichtshofs setzt dies voraus, dass (1) der Einzelne eine "tatsächliche Verletzung" erlitten hat (d. h. eine Verletzung eines rechtlich geschützten Interesses, die konkret und spezifiziert ist und tatsächlich vorliegt oder unmittelbar bevorsteht), (2) ein Kausalzusammenhang zwischen der Verletzung und dem vor Gericht angefochtenen Verhalten besteht und (3) es wahrscheinlich und nicht spekulativ ist, dass eine positive Entscheidung des Gerichts die Verletzung beseitigen wird (siehe *Lujan v. Defenders of Wildlife*, 504 U.S. 555 (1992)).

392 18 U.S.C. § 2712.

Regierungsbeamte, die in ihrer persönlichen Eigenschaft handeln, auf Schadensersatz zu verklagen[393] ; und die Rechtmäßigkeit der Überwachung anzufechten (und die Unterdrückung der Informationen anzustreben), falls die US-Regierung beabsichtigt, Informationen, die aus der elektronischen Überwachung gewonnen oder abgeleitet wurden, gegen die Person in Gerichts- oder Verwaltungsverfahren in den USA zu verwenden oder offenzulegen[394] . Allgemeiner ausgedrückt: Wenn die Regierung beabsichtigt, Informationen, die sie bei nachrichtendienstlichen Operationen erhalten hat, gegen einen Verdächtigen in einem Strafverfahren zu verwenden, sind sie aufgrund verfassungsrechtlicher und gesetzlicher Bestimmungen[395] verpflichtet, bestimmte Informationen offenzulegen, damit der Angeklagte die Rechtmäßigkeit der Erhebung und Verwendung der Beweismittel durch die Regierung anfechten kann.

(197) Darüber hinaus gibt es mehrere spezifische Möglichkeiten, Rechtsmittel gegen Regierungsbeamte einzulegen, wenn diese unrechtmäßig auf personenbezogene Daten zugreifen oder diese nutzen, auch zu angeblichen Zwecken der nationalen Sicherheit (z. B. Computer Fraud and Abuse Act[396] ; Electronic Communications Privacy Act[397] ; Right to Financial Privacy Act[398] ). Alle diese Klagen beziehen sich auf bestimmte Daten, Ziele und/oder Arten des Zugriffs (z. B. Fernzugriff auf einen Computer über das Internet) und sind unter bestimmten Bedingungen möglich (z. B. vorsätzliches/vorsätzliches Verhalten, Verhalten außerhalb der amtlichen Funktion, erlittener Schaden).

(198) Eine allgemeinere Rechtsbehelfsmöglichkeit bietet das APA[399] , demzufolge "jede Person, die aufgrund von Maßnahmen der Behörde ein rechtliches Unrecht erleidet oder von Maßnahmen der Behörde nachteilig betroffen oder geschädigt wird", berechtigt ist, eine gerichtliche Überprüfung zu beantragen[400] . Dies schließt die Möglichkeit ein, das Gericht aufzufordern, "Maßnahmen, Feststellungen und Schlussfolgerungen der Behörde für rechtswidrig zu erklären und aufzuheben, die [...] willkürlich, willkürlich, ermessensmissbräuchlich oder anderweitig nicht im Einklang mit dem Gesetz sind"[401] . So entschied beispielsweise ein Bundesberufungsgericht im Jahr 2015 über eine APA-Klage, dass die Massenerfassung von Telefonie-Metadaten durch die US-Regierung nicht durch Abschnitt 501 FISA[402] genehmigt wurde.

(199) Schließlich hat jede Person zusätzlich zu den in den Erwägungsgründen 176-198 genannten Rechtsbehelfen das Recht, auf der Grundlage des FOIA Zugang zu bestehenden Unterlagen von Bundesbehörden zu erhalten, auch wenn diese personenbezogene Daten der Person enthalten[403] . Ein solcher Zugang kann auch die Einleitung von Verfahren vor ordentlichen Gerichten erleichtern, auch um die Klagebefugnis nachzuweisen. Die Behörden können Informationen zurückhalten, die unter bestimmte aufgezählte Ausnahmen fallen, einschließlich des Zugangs zu als Verschlusssache eingestuften Informationen über die nationale Sicherheit und zu Informationen über Ermittlungen der Strafverfolgungsbehörden[404] , aber Beschwerdeführer, die

---

393 50 U.S.C. § 1810.

394 50 U.S.C. § 1806.

395 *Siehe Brady v. Maryland,* 373 U.S. 83 (1963) und den 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 der Behörde - und nicht "vorläufige, verfahrenstechnische oder Zwischenmaßnahmen" der Behörde - der gerichtlichen Überprüfung. 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 Sammlung von Massentelefonaten wurde 2015 durch den USA FREEDOM Act beendet.

403 5 U.S.C. § 552. Ähnliche Gesetze gibt es auf bundesstaatlicher Ebene.

404 Ist dies der Fall, erhält die Person in der Regel nur eine Standardantwort, in der die Behörde es ablehnt, die Existenz von Aufzeichnungen zu bestätigen oder zu leugnen. Siehe *ACLU* gegen *CIA*, 710 F.3d 422 (D.C. Cir. 2014). Die Kriterien für die Einstufung und die Dauer der Einstufung sind in der Executive Order 13526 festgelegt, die als allgemeine Regel vorsieht, dass ein bestimmtes Datum oder Ereignis für die Aufhebung der Einstufung auf der Grundlage der Dauer der nationalen Sicherheitsempfindlichkeit der Informationen festgelegt werden muss, zu dem die Informationen automatisch freigegeben werden müssen (siehe Abschnitt 1.5 der EO 13526).

mit der Antwort unzufrieden sind, haben die Möglichkeit, diese anzufechten, indem sie eine verwaltungsrechtliche und anschließend eine gerichtliche Überprüfung (vor Bundesgerichten) beantragen[405] .

(200) Daraus folgt, dass der Zugriff der US-Strafverfolgungsbehörden und der nationalen Sicherheitsbehörden auf personenbezogene Daten, die in den Anwendungsbereich dieses Beschlusses fallen, einem Rechtsrahmen unterliegt, der die Bedingungen für den Zugriff festlegt und sicherstellt, dass der Zugriff auf die Daten und ihre Weiterverwendung auf das notwendige Maß beschränkt ist und in einem angemessenen Verhältnis zu dem verfolgten Ziel des öffentlichen Interesses steht. Diese Garantien können von Personen, die über wirksame Rechtsbehelfe verfügen, geltend gemacht werden.

## 4. SCHLUSSFOLGERUNG

(201) Die Kommission ist der Ansicht, dass die Vereinigten Staaten - durch die vom US-Handelsministerium herausgegebenen Grundsätze - ein Schutzniveau für personenbezogene Daten gewährleisten, die von der Union an zertifizierte Organisationen in den Vereinigten Staaten gemäß dem EU-US-Datenschutzrahmen übermittelt werden, das im Wesentlichen dem durch die Verordnung (EU) 2016/679 garantierten Schutzniveau entspricht.

(202) Darüber hinaus ist die Kommission der Ansicht, dass die wirksame Anwendung der Grundsätze durch Transparenzverpflichtungen und die Verwaltung der DPF durch das DoC gewährleistet ist. Darüber hinaus ermöglichen es die Kontrollmechanismen und Rechtsbehelfe im US-Recht insgesamt, Verstöße gegen die Datenschutzvorschriften in der Praxis festzustellen und zu ahnden, und bieten den betroffenen Personen Rechtsbehelfe, um Zugang zu den sie betreffenden personenbezogenen Daten und schließlich deren Berichtigung oder Löschung zu erhalten.

(203) Schließlich ist die Kommission auf der Grundlage der verfügbaren Informationen über die US-Rechtsordnung, einschließlich der in den Anhängen VI und VII enthaltenen Informationen, der Auffassung, dass Eingriffe in die Grundrechte der Personen, deren personenbezogene Daten nach dem EU-US-Datenschutzrahmen von der Union in die Vereinigten Staaten übermittelt werden, durch US-Behörden im öffentlichen Interesse, insbesondere zu Zwecken der Strafverfolgung und der nationalen Sicherheit, auf das zur Erreichung des betreffenden rechtmäßigen Ziels unbedingt erforderliche Maß beschränkt werden und dass ein wirksamer Rechtsschutz gegen solche Eingriffe besteht. In Anbetracht der vorstehenden Feststellungen sollte daher entschieden 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 nach dem EU-US-Datenschutzrahmen zertifizierte Organisationen übermittelt werden.

(204) Da die durch EO 14086 festgelegten Beschränkungen, Schutzmaßnahmen und Rechtsbehelfsmechanismen wesentliche Elemente des US-Rechtsrahmens sind, auf die sich die Bewertung der Kommission stützt, beruht der Erlass dieses Beschlusses insbesondere auf der Annahme aktualisierter Strategien und Verfahren zur Umsetzung von EO 14086 durch alle US-Geheimdienste und der Benennung der Union als qualifizierte Organisation für die Zwecke des Rechtsbehelfsmechanismus, die am 3. Juli 2023 (siehe Erwägungsgrund 126) bzw. am 30. Juni 2023 (siehe Erwägungsgrund 176) erfolgt sind.

## 5. AUSWIRKUNGEN DIESES BESCHLUSSES UND MASSNAHMEN DER DATENSCHUTZBEHÖRDEN

405 Das Gericht entscheidet nach dem "de novo"-Prinzip, ob Unterlagen rechtmäßig zurückgehalten werden, und kann die Regierung zwingen, Zugang zu den Unterlagen zu gewähren (5 U.S.C. § 552(a)(4)(B)).

(205) Die Mitgliedstaaten und ihre Organe sind verpflichtet, die erforderlichen Maßnahmen zu ergreifen, um den Rechtsakten der Unionsorgane nachzukommen, da diese als rechtmäßig gelten und dementsprechend Rechtswirkungen entfalten, solange sie nicht zurückgenommen, im Rahmen einer Nichtigkeitsklage aufgehoben oder aufgrund eines Vorabentscheidungsersuchens oder einer Einrede der Rechtswidrigkeit für nichtig erklärt werden.

(206) Folglich ist ein Angemessenheitsbeschluss der Kommission, der gemäß Artikel 45 Absatz 3 der Verordnung (EU) 2016/679 angenommen wurde, für alle Organe der Mitgliedstaaten, an die er gerichtet ist, einschließlich ihrer unabhängigen Aufsichtsbehörden, verbindlich. Insbesondere können Übermittlungen von einem für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter in der Union an zertifizierte Organisationen in den Vereinigten Staaten erfolgen, ohne dass eine weitere Genehmigung eingeholt werden muss.

(207) Es sei daran erinnert, dass gemäß Artikel 58 Absatz 5 der Verordnung (EU) 2016/679 und wie der Gerichtshof in seinem Urteil in der Rechtssache *Schrems (*[406] ) erläutert hat, das nationale Recht einer nationalen Datenschutzbehörde, die die Vereinbarkeit eines Angemessenheitsbeschlusses der Kommission mit den Grundrechten des Einzelnen auf Schutz der Privatsphäre und Datenschutz in Frage stellt, einen Rechtsbehelf zur Verfügung stellen muss, um diese Einwände vor einem nationalen Gericht vorzubringen, das gegebenenfalls ein Vorabentscheidungsersuchen an den Gerichtshof richten muss[407] .

## 6. ÜBERWACHUNG UND ÜBERPRÜFUNG DIESER ENTSCHEIDUNG

(208) Nach der Rechtsprechung des Gerichtshofs[408] und wie in Artikel 45 Absatz 4 der Verordnung (EU) 2016/679 anerkannt, sollte die Kommission nach dem Erlass eines Angemessenheitsbeschlusses die einschlägigen Entwicklungen in dem Drittland kontinuierlich überwachen, um zu beurteilen, ob das Drittland weiterhin ein im Wesentlichen gleichwertiges Schutzniveau gewährleistet. Eine solche Überprüfung ist in jedem Fall erforderlich, wenn die Kommission Informationen erhält, die Anlass zu berechtigten Zweifeln in dieser Hinsicht geben.

(209) Daher sollte die Kommission die Situation in den Vereinigten Staaten in Bezug auf den rechtlichen Rahmen und die tatsächliche Praxis der Verarbeitung personenbezogener Daten, wie sie in dieser Entscheidung bewertet wird, laufend überwachen. Um diesen Prozess zu erleichtern, sollten die US-Behörden die Kommission unverzüglich über wesentliche Entwicklungen in der US-Rechtsordnung, die sich auf den Rechtsrahmen auswirkt, der Gegenstand dieses Beschlusses ist, sowie jegliche Entwicklung der Praktiken im Zusammenhang mit der Verarbeitung der in diesem Beschluss bewerteten personenbezogenen Daten, und zwar sowohl in Bezug auf die Verarbeitung personenbezogener Daten durch zertifizierte Organisationen in den Vereinigten Staaten als auch in Bezug auf die Beschränkungen und Garantien, die für den Zugang zu personenbezogenen Daten durch öffentliche Stellen gelten.

(210) Damit die Kommission ihre Überwachungsfunktion wirksam wahrnehmen kann, sollten die Mitgliedstaaten die Kommission außerdem über alle einschlägigen Maßnahmen der nationalen Datenschutzbehörden unterrichten, insbesondere über Anfragen oder Beschwerden betroffener Personen in der Union über die Übermittlung personenbezogener Daten aus der Union an zertifizierte Organisationen in den Vereinigten Staaten. Die Kommission sollte auch über alle Hinweise darauf unterrichtet werden, dass die Maßnahmen von US-Behörden, die für die Verhütung, Ermittlung, Feststellung oder Verfolgung von Straftaten oder für

406 *Schrems*, Ziffer 65.

407 *Schrems*, Rdnr. 65: "Es obliegt dem nationalen Gesetzgeber, Rechtsbehelfe vorzusehen, die es der betroffenen nationalen Aufsichtsbehörde ermöglichen, die von ihr für begründet gehaltenen Einwände vor den nationalen Gerichten geltend zu machen, damit diese, wenn sie ihre Zweifel an der Gültigkeit der Entscheidung der Kommission teilen, ein Vorabentscheidungsersuchen zur Prüfung der Gültigkeit der Entscheidung stellen können."

408 *Schrems*, Ziffer 76.

nationale Sicherheit, einschließlich etwaiger Aufsichtsorgane, nicht das erforderliche Schutzniveau gewährleisten.

(211) Gemäß 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 im Rahmen der DPF EU-USA gewährleisteten Schutzniveaus noch sachlich und rechtlich begründet sind. Da insbesondere die EO 14086 und die AG-Verordnung die Schaffung neuer Mechanismen und die Umsetzung neuer Schutzmaßnahmen erfordern, sollte dieser Beschluss innerhalb eines Jahres nach seinem Inkrafttreten einer ersten Überprüfung unterzogen werden, um festzustellen, ob alle relevanten Elemente vollständig umgesetzt wurden und in der Praxis wirksam funktionieren. Im Anschluss an diese erste Überprüfung und je nach deren Ergebnis wird die Kommission in enger Abstimmung mit dem gemäß Artikel 93 Absatz 1 der Verordnung (EU) 2016/679 eingesetzten Ausschuss und dem Europäischen Datenschutzausschuss über die Periodizität künftiger Überprüfungen entscheiden[410] .

(212) Zur Durchführung der Überprüfungen sollte die Kommission mit dem DoC, der FTC und dem DoT zusammentreffen, gegebenenfalls in Begleitung anderer Dienststellen und Agenturen, die an der Umsetzung der EU-US-DSGVO beteiligt sind, sowie - bei Angelegenheiten, die den Zugang der Regierung zu Daten betreffen - mit Vertretern des DoJ, des ODNI (einschließlich des CLPO), anderer Elemente der Intelligence Community, des DPRC sowie der Sonderanwälte. Die Teilnahme an dieser Sitzung sollte den Vertretern der Mitglieder des Europäischen Datenschutzausschusses offen stehen.

(213) Die Überprüfungen sollten sich auf alle Aspekte des Funktionierens dieses Beschlusses in Bezug auf die Verarbeitung personenbezogener Daten in den Vereinigten Staaten erstrecken, insbesondere auf die Anwendung und Umsetzung der Grundsätze unter besonderer Berücksichtigung des Schutzes bei Weiterübermittlungen, auf die Entwicklung der einschlägigen Rechtsprechung, auf die Wirksamkeit der Ausübung der Rechte des Einzelnen, auf die Überwachung und Durchsetzung der Einhaltung der Grundsätze; sowie die Beschränkungen und Schutzvorkehrungen in Bezug auf den Zugang der Regierung, insbesondere die Umsetzung und Anwendung der mit EO 14086 eingeführten Schutzvorkehrungen, einschließlich der von den Nachrichtendiensten entwickelten Strategien und Verfahren; das Zusammenspiel zwischen EO 14086 und Abschnitt 702 FISA und EO 12333; und die Wirksamkeit der Aufsichtsmechanismen und Rechtsbehelfe (einschließlich der Funktionsweise des mit EO 14086 eingeführten neuen Rechtsbehelfsmechanismus). Im Zusammenhang mit diesen Überprüfungen wird auch der Zusammenarbeit zwischen den Datenschutzbehörden und den zuständigen Behörden der Vereinigten Staaten Aufmerksamkeit gewidmet, einschließlich der Entwicklung von Leitlinien und anderen Auslegungsinstrumenten für die Anwendung der Grundsätze sowie für andere Aspekte der Funktionsweise des Rechtsrahmens.

(214) Auf der Grundlage dieser 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) Geht aus verfügbaren Informationen, insbesondere aus Informationen, die sich aus der Überwachung dieses Beschlusses ergeben oder von den Behörden der USA oder der Mitgliedstaaten zur Verfügung gestellt werden, hervor, dass das Schutzniveau für die gemäß diesem Beschluss übermittelten Daten nicht mehr gewährleistet werden kann

409 Gemäß Artikel 45 Absatz 3 der Verordnung (EU) 2016/679 "sieht der Durchführungsrechtsakt einen Mechanismus für eine regelmäßige Überprüfung vor, [...] bei der alle relevanten Entwicklungen in dem Drittland oder der internationalen Organisation berücksichtigt werden."

410 Artikel 45 Absatz 3 der Verordnung (EU) 2016/679 sieht vor, dass eine regelmäßige Überprüfung "mindestens alle vier Jahre" stattfinden muss. Siehe auch Europäischer Datenschutzausschuss, Referent für Angemessenheit, WP 254 rev. 01.

angemessen ist, sollte die Kommission die zuständigen US-Behörden unverzüglich davon in Kenntnis setzen und sie auffordern, innerhalb eines bestimmten, angemessenen Zeitrahmens geeignete Maßnahmen zu ergreifen.

(216) Sollten die zuständigen US-Behörden nach Ablauf dieses Zeitrahmens diese Maßnahmen nicht ergreifen oder auf andere Weise zufriedenstellend nachweisen, 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 mit dem Ziel einleiten, die Entscheidung zu ändern, insbesondere indem sie die Datenübermittlung an zusätzliche Bedingungen knüpft oder den Geltungsbereich der Angemessenheitsfeststellung auf Datenübermittlungen beschränkt, für die weiterhin ein angemessenes Schutzniveau gewährleistet ist.

(218) Insbesondere sollte die Kommission das Verfahren zur Aussetzung oder Aufhebung in folgenden Fällen einleiten

(a) Hinweise darauf, dass Organisationen, die im Rahmen dieses Beschlusses personenbezogene Daten von der Union erhalten haben, die Grundsätze nicht einhalten und dass die zuständigen Aufsichts- und Durchsetzungsstellen nicht wirksam gegen diese Nichteinhaltung vorgehen;

(b) Hinweise darauf, dass die US-Behörden die geltenden Bedingungen und Beschränkungen für den Zugang von US-Behörden zu personenbezogenen Daten, die im Rahmen der EU-US-DSGVO übermittelt werden, zu Zwecken der Strafverfolgung und der nationalen Sicherheit nicht einhalten; oder

(c) das Versäumnis, Beschwerden betroffener Personen aus der Union wirksam zu bearbeiten, auch durch den CLPO des ODNI und/oder das DPRC.

(219) Die Kommission sollte auch in Erwägung ziehen, das Verfahren zur Änderung, Aussetzung oder Aufhebung dieses Beschlusses einzuleiten, wenn die zuständigen US-Behörden die Informationen oder Klarstellungen, die für die Bewertung des Schutzniveaus der aus der Union in die Vereinigten Staaten übermittelten personenbezogenen Daten oder für die Einhaltung dieses Beschlusses erforderlich sind, nicht vorlegen. In diesem Zusammenhang sollte die Kommission berücksichtigen, inwieweit die einschlägigen Informationen aus anderen Quellen beschafft werden können.

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

## 8. ABSCHLIESSENDE ÜBERLEGUNGEN

(221) Der Europäische Datenschutzausschuss veröffentlichte seine Stellungnahme[411] , die bei der Ausarbeitung dieses Beschlusses berücksichtigt wurde.

411 Stellungnahme 5/2023 zum Entwurf eines Durchführungsbeschlusses der Europäischen Kommission über die Angemessenheit des Schutzes personenbezogener Daten gemäß dem EU-US-Datenschutzrahmen vom 28. Februar 2023.

(222) Das Europäische Parlament nahm eine Entschließung zur Angemessenheit des durch den EU-US-Datenschutzrahmen gewährten Schutzes an[412] .

(223) Die in diesem Beschluss vorgesehenen Maßnahmen stehen im Einklang mit der Stellungnahme des gemäß Artikel 93 Absatz 1 der Verordnung (EU) 2016/679 eingesetzten Ausschusses.

HAT DIESEN BESCHLUSS ANGENOMMEN:

*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 US-Handelsministerium geführten und öffentlich zugänglichen "Data Privacy Framework List" gemäß Anhang I Abschnitt I.3 aufgeführt sind.

*Artikel 2*

Machen die zuständigen Behörden in den Mitgliedstaaten zum Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten von ihren Befugnissen gemäß Artikel 58 der Verordnung (EU) 2016/679 in Bezug auf die in Artikel 1 dieses Beschlusses genannten Datenübermittlungen Gebrauch, so unterrichtet der betreffende Mitgliedstaat unverzüglich die Kommission.

*Artikel 3*

1. Die Kommission überwacht fortlaufend die Anwendung des Rechtsrahmens, der Gegenstand dieses Beschlusses ist, einschließlich der Bedingungen, unter denen die Weiterübermittlung erfolgt, die Rechte des Einzelnen ausgeübt werden und die US-Behörden Zugang zu den auf der Grundlage dieses Beschlusses übermittelten Daten haben, um zu beurteilen, ob die Vereinigten Staaten weiterhin ein angemessenes Schutzniveau im Sinne von Artikel 1 gewährleisten.

2. Die Mitgliedstaaten und die Kommission unterrichten einander über Fälle, in denen sich herausstellt, dass die Stellen in den Vereinigten Staaten, die gesetzlich befugt sind, die Einhaltung der in Anhang I aufgeführten Grundsätze durchzusetzen, keine wirksamen Aufdeckungs- und Überwachungsmechanismen bereitstellen, die es ermöglichen, Verstöße gegen die in Anhang I aufgeführten Grundsätze in der Praxis zu erkennen und zu ahnden.

3. Die Mitgliedstaaten und die Kommission unterrichten einander über alle Hinweise darauf, dass die Eingriffe der für die Verfolgung der nationalen Sicherheit, der Strafverfolgung oder anderer öffentlicher Interessen zuständigen US-Behörden in das Recht natürlicher Personen auf Schutz ihrer personenbezogenen Daten über das erforderliche und verhältnismäßige Maß hinausgehen und/oder dass es keinen wirksamen Rechtsschutz gegen solche Eingriffe gibt.

4. Ein Jahr nach dem Datum der Bekanntgabe dieses Beschlusses an die Mitgliedstaaten und anschließend in einem Rhythmus, der in enger Abstimmung mit dem gemäß Artikel 93 Absatz 1 der Verordnung (EU) 2016/679 eingesetzten Ausschuss und dem Europäischen Datenschutzausschuss festgelegt wird, bewertet die Kommission die in Artikel 1 Absatz 1 genannte Feststellung auf der Grundlage aller verfügbaren Informationen, einschließlich Informationen

412 Entschließung des Europäischen Parlaments vom 11. Mai 2023 zur Angemessenheit des durch den EU-US-Datenschutzrahmen gewährten Schutzes (2023/2501(RSP)).

die sich aus der gemeinsam mit den zuständigen Behörden der Vereinigten Staaten durchgeführten Überprüfung ergeben haben.

5. Hat die Kommission Hinweise darauf, dass ein angemessenes Schutzniveau nicht mehr gewährleistet ist, unterrichtet sie die zuständigen US-Behörden. Erforderlichenfalls beschließt sie gemäß Artikel 45 Absatz 5 der Verordnung (EU) 2016/679 die Aussetzung, Änderung oder Aufhebung dieses Beschlusses oder die Einschränkung seines Anwendungsbereichs. Die Kommission kann einen solchen Beschluss auch fassen, wenn die mangelnde Kooperationsbereitschaft der US-Regierung die Kommission daran hindert, festzustellen, ob die Vereinigten Staaten weiterhin ein angemessenes Schutzniveau gewährleisten.

*Artikel 4*

Diese Entscheidung ist an die Mitgliedstaaten

gerichtet. Geschehen zu Brüssel am 10.7.2023

*Für die Kommission Didier REYNDERS Mitglied der Kommission*

CERTIFIED COPY
For the Secretary-General

Martine DEPREZ
Director
Decision-making & Collegiality
EUROPEAN COMMISSION

EUROPÄISCHE
KOMMISSION

Brüssel, 10.7.2023
K(2023) 4745 endgültig

ANHÄNGE 1 bis 7

**ANHÄNGE**

***zum***

**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 EU-US-Datenschutzrahmen**

**ANHANG I**

**VOM US-AMERIKANISCHEN HANDELSMINISTERIUM HERAUSGEGEBENE DATENSCHUTZ-RAHMENPRINZIPIEN DER EU UND DER USA**

## 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 ihre jeweiligen Bürger, Volkswirtschaften und Gesellschaften anerkennen, verfolgen die Vereinigten Staaten beim Schutz der Privatsphäre einen anderen Ansatz als die EU. Die Vereinigten Staaten verfolgen einen sektoralen Ansatz, der sich auf eine Mischung aus Gesetzgebung, Regulierung und Selbstregulierung stützt. Das US-Handelsministerium ("das Ministerium") gibt die Datenschutz-Rahmengrundsätze EU-USA einschließlich der ergänzenden Grundsätze (zusammen "die Grundsätze") und Anhang I der Grundsätze ("Anhang I") im Rahmen seiner gesetzlichen Befugnis zur Förderung und Entwicklung des internationalen Handels (15 U.S.C. § 1512) heraus. Die Grundsätze wurden in Absprache mit der Europäischen Kommission ("die Kommission"), der Industrie und anderen Interessengruppen entwickelt, um den Handel zwischen den Vereinigten Staaten und der EU zu erleichtern. Die Grundsätze sind ein wesentlicher Bestandteil der EU-U.S. Data Privacy Framework ("EU-U.S. DPF") bieten Organisationen in den Vereinigten Staaten einen zuverlässigen Mechanismus für die Übermittlung personenbezogener Daten aus der EU in die Vereinigten Staaten und stellen gleichzeitig sicher, dass die betroffenen Personen in der EU bei der Verarbeitung ihrer personenbezogenen Daten in Nicht-EU-Ländern weiterhin von wirksamen Garantien und Schutzmaßnahmen profitieren, wie sie in den europäischen Rechtsvorschriften vorgesehen sind. Die Grundsätze sind ausschließlich für berechtigte Organisationen in den Vereinigten Staaten bestimmt, die personenbezogene Daten aus der EU erhalten, um sich für die EU-US-DSGVO zu qualifizieren und somit von der Angemessenheitsentscheidung der Kommission zu profitieren.[1] Die Grundsätze berühren nicht die Anwendung der Verordnung (EU) 2016/679 ("Allgemeine Datenschutzverordnung" oder "DSGVO")[2] , die für die Verarbeitung personenbezogener Daten in den EU-Mitgliedstaaten gilt. Die Grundsätze schränken auch nicht die Datenschutzpflichten ein, die ansonsten nach US-Recht gelten.

2. Um sich bei der Übermittlung personenbezogener Daten aus der EU auf die EU-US-DSGVO berufen zu können, muss eine Organisation ihre Einhaltung der Grundsätze gegenüber dem Ministerium (oder dessen Beauftragten) selbst bescheinigen. Während die Entscheidung von Organisationen, der EU-US-DSGVO beizutreten, völlig freiwillig ist, ist die tatsächliche Einhaltung der Grundsätze obligatorisch: Organisationen, die sich gegenüber dem Ministerium selbst zertifizieren und öffentlich erklären, dass sie sich zur Einhaltung der Grundsätze verpflichten, müssen die Grundsätze vollständig einhalten. Um dem DPF EU-USA beizutreten, muss eine Organisation (a) den Ermittlungs- und Durchsetzungsbefugnissen der Federal Trade Commission (FTC), des US-Verkehrsministeriums (DOT) oder einer anderen gesetzlichen Einrichtung unterliegen, die die Einhaltung der Grundsätze wirksam gewährleistet *(andere von der EU anerkannte gesetzliche Einrichtungen der USA können in Zukunft als Anhang aufgenommen werden)*;
(b) sich öffentlich zur Einhaltung der Grundsätze zu verpflichten; (c) seine

Datenschutzpolitik im Einklang mit diesen Grundsätzen öffentlich bekannt zu geben; und (d) die Grundsätze vollständig umzusetzen

---

[1] Unter der Voraussetzung, dass die Entscheidung der Kommission über die Angemessenheit des Schutzes, den die DPF EU-USA bietet, auch für Island, Liechtenstein und Norwegen gilt, wird die DPF EU-USA sowohl die EU als auch diese drei Länder abdecken
Länder. Folglich sind Verweise auf die EU und ihre Mitgliedstaaten so zu verstehen, dass sie Island, Liechtenstein und Norwegen einschließen.

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

sie[3] . Die Nichteinhaltung der Vorschriften durch eine Organisation kann von der FTC gemäß Abschnitt 5 des Federal Trade Commission (FTC)-Gesetzes zum Verbot unlauterer oder irreführender Handlungen im oder mit Bezug auf den Handel (15 U.S.C. § 45) und vom Verkehrsministerium gemäß 49
U.S.C. § 41712, der es einem Luftfahrtunternehmen oder einem Flugscheinvermittler verbietet, sich an unlauteren oder irreführenden Praktiken im Luftverkehr oder beim Verkauf von Luftverkehrsleistungen zu beteiligen, oder nach anderen Gesetzen oder Vorschriften, die solche Handlungen verbieten.

3. Das Ministerium wird eine maßgebliche Liste von US-Organisationen führen und der Öffentlichkeit zugänglich machen, die sich gegenüber dem Ministerium selbst zertifiziert und sich zur Einhaltung der Grundsätze verpflichtet haben (die "Data Privacy Framework List"). EU-
Die Vorteile der US-DSGVO sind ab dem Datum gewährleistet, an dem das Ministerium die Organisation auf die Datenschutz-Rahmenliste setzt. Das Ministerium wird diejenigen Organisationen von der Datenschutz-Rahmenliste streichen, die sich freiwillig aus der EU-US-DSGVO zurückziehen oder ihre jährliche Neuzertifizierung gegenüber dem Ministerium versäumen; diese Organisationen müssen entweder weiterhin die Grundsätze auf die personenbezogenen Daten anwenden, die sie im Rahmen der EU-US-DSGVO erhalten haben, und dem Ministerium jährlich ihre Verpflichtung dazu bestätigen (d. *h.*, (d.h. solange sie diese Informationen aufbewahren), einen "angemessenen" Schutz für die Informationen durch ein anderes zulässiges Mittel zu gewährleisten (z.B. durch einen Vertrag, der die Anforderungen der von der Kommission angenommenen einschlägigen Standardvertragsklauseln vollständig widerspiegelt), oder die Informationen zurückzugeben oder zu löschen. Das Ministerium wird auch diejenigen Organisationen von der Datenschutz-Rahmenliste streichen, die die Grundsätze dauerhaft nicht eingehalten haben; diese Organisationen müssen die personenbezogenen Daten, die sie im Rahmen der EU-US-Datenschutzrahmenvereinbarung erhalten haben, zurückgeben oder löschen. Die Streichung einer Organisation von der Datenschutz-Rahmenliste bedeutet, dass sie nicht mehr berechtigt ist, von der Angemessenheitsentscheidung der Kommission zum Erhalt personenbezogener Daten aus der EU zu profitieren.

4. Das Ministerium wird auch ein verbindliches Verzeichnis der US-Organisationen führen und der Öffentlichkeit zugänglich machen, die sich zuvor gegenüber dem Ministerium selbst zertifiziert hatten, aber von der Datenschutz-Rahmenliste gestrichen wurden. Das Ministerium wird deutlich darauf hinweisen, dass diese Organisationen nicht an der EU-US-DSGVO teilnehmen; dass die Streichung von der Datenschutz-Rahmenliste bedeutet, dass diese Organisationen nicht behaupten können, die EU-US-DSGVO einzuhalten, und dass sie alle Erklärungen oder irreführenden Praktiken vermeiden müssen, die eine Teilnahme an der EU-US-DSGVO implizieren; und dass diese Organisationen nicht mehr berechtigt sind, von der Angemessenheitsentscheidung der Kommission zu profitieren und personenbezogene Daten aus der EU zu erhalten. Eine Organisation, die weiterhin behauptet, an der EU-US-DSGVO teilzunehmen, oder die andere falsche Darstellungen im Zusammenhang mit der EU-US-DSGVO macht, nachdem sie von der Datenschutz-Rahmenliste gestrichen wurde, kann Gegenstand von Durchsetzungsmaßnahmen der FTC, des US-Verkehrsministeriums oder anderer Durchsetzungsbehörden sein.

5. Die Einhaltung dieser Grundsätze kann eingeschränkt werden: (a) soweit dies erforderlich ist, um einer gerichtlichen Anordnung nachzukommen oder um Anforderungen des öffentlichen Interesses, der Strafverfolgung oder der nationalen Sicherheit zu erfüllen, einschließlich der Fälle, in denen Gesetze oder staatliche Vorschriften entgegenstehende Verpflichtungen begründen; (b) durch

Gesetze, Gerichtsbeschlüsse oder staatliche Vorschriften, die ausdrückliche Ermächtigungen schaffen, sofern eine Organisation bei der Ausübung einer solchen Ermächtigung nachweisen kann, dass die Nichteinhaltung der Grundsätze auf das Maß beschränkt ist, das zur Wahrung der durch diese Ermächtigung geförderten überwiegenden berechtigten Interessen erforderlich ist; oder (c) wenn die Datenschutz-Grundverordnung Ausnahmen oder Abweichungen zulässt, unter den darin festgelegten Bedingungen, sofern diese Ausnahmen oder Abweichungen in vergleichbaren Kontexten angewendet werden. In diesem Zusammenhang sind die Schutzmaßnahmen im US-Recht zum Schutz

[3] Die Rahmenprinzipien des EU-US-Datenschutzschildes wurden in die "Rahmenprinzipien des EU-US-Datenschutzes" geändert. (*Siehe* Ergänzungsgrundsatz zur Selbstzertifizierung).

Die Grundsätze zum Schutz der Privatsphäre und der bürgerlichen Freiheiten umfassen die in der Executive Order 14086[4] geforderten Maßnahmen unter den dort genannten Bedingungen (einschließlich der Anforderungen an die Notwendigkeit und Verhältnismäßigkeit). Im Einklang mit dem Ziel, den Schutz der Privatsphäre zu verbessern, sollten sich die Organisationen um eine vollständige und transparente Umsetzung dieser Grundsätze bemühen, auch indem sie sich bemühen, in ihren Datenschutzrichtlinien anzugeben, wo Ausnahmen von den Grundsätzen gemäß Buchstabe b) zulässig sind. Aus demselben Grund wird von den Organisationen erwartet, dass sie sich für den höheren Schutz entscheiden, wenn dies nach den Grundsätzen und/oder dem US-Recht möglich ist.

6. Organisationen sind verpflichtet, die Grundsätze auf alle personenbezogenen Daten anzuwenden, die unter Berufung auf die EU-US-DSGVO übermittelt werden, nachdem sie in die EU-US-DSGVO aufgenommen wurden. Eine Organisation, die sich dafür entscheidet, die Vorteile der EU-US-DSGVO auf personenbezogene Personaldaten auszudehnen, die aus der EU zur Verwendung im Rahmen eines Beschäftigungsverhältnisses übermittelt werden, muss dies bei ihrer Selbstzertifizierung gegenüber dem Ministerium angeben und die im ergänzenden Grundsatz zur Selbstzertifizierung festgelegten Anforderungen erfüllen.

7. Für Fragen der Auslegung und der Einhaltung der Grundsätze und der einschlägigen Datenschutzrichtlinien durch die an der EU teilnehmenden Organisationen gilt amerikanisches Recht.
U.S. DPF, es sei denn, diese Organisationen haben sich zur Zusammenarbeit mit den EU-Datenschutzbehörden verpflichtet. Sofern nicht anders angegeben, gelten alle Bestimmungen der Grundsätze dort, wo sie relevant sind.

8. Definitionen:

   a. "Personenbezogene Daten" und "personenbezogene Informationen" sind Daten über eine identifizierte oder identifizierbare Person, die in den Anwendungsbereich der DSGVO fallen, von einer Organisation in den Vereinigten Staaten aus der EU erhalten und in irgendeiner Form aufgezeichnet wurden.

   b. "Verarbeitung" personenbezogener Daten ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte 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 Verbreitung sowie das Löschen oder Vernichten.

   c. "Für die Verarbeitung Verantwortlicher" ist eine Person oder Organisation, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet.

9. Das Datum des Inkrafttretens der Grundsätze und des Anhangs I der Grundsätze ist das Datum des Inkrafttretens der Angemessenheitsentscheidung der Europäischen Kommission.

## II. PRINZIPIEN

[4] Executive Order vom 7. Oktober 2022, "Enhancing Safeguards for United States Signals Intelligence Activities".

## 1. HINWEIS

a. Eine Organisation muss Einzelpersonen darüber informieren:

i. seine Teilnahme an der EU-US-DSGVO mitzuteilen und einen Link oder die Webadresse für die Datenschutzrahmenliste anzugeben,

ii. die Art der erhobenen personenbezogenen Daten und ggf. die US-Einheiten oder US-Tochtergesellschaften der Organisation, die sich ebenfalls an die Grundsätze halten,

[4] Executive Order vom 7. Oktober 2022, "Enhancing Safeguards for United States Signals Intelligence Activities".

iii. ihre Verpflichtung, alle personenbezogenen Daten, die sie aus der EU unter Berufung auf die EU-US-DSGVO erhalten, den Grundsätzen zu unterwerfen,

iv. die Zwecke, für die sie personenbezogene Daten über sie sammelt und verwendet,

v. wie man sich mit Anfragen oder Beschwerden an die Organisation wenden kann, einschließlich der zuständigen Niederlassung in der EU, die auf solche Anfragen oder Beschwerden reagieren kann,

vi. die Art oder Identität der Dritten, an die sie personenbezogene Daten weitergibt, und die Zwecke, für die sie dies tut,

vii. das Recht des Einzelnen auf Zugang zu seinen personenbezogenen Daten,

viii. die Wahlmöglichkeiten und Mittel, die die Organisation dem Einzelnen zur Verfügung stellt, um die Nutzung und Weitergabe seiner personenbezogenen Daten einzuschränken,

ix. die unabhängige Streitbeilegungsstelle, die für die Bearbeitung von Beschwerden und die Bereitstellung geeigneter, für den Einzelnen kostenloser Rechtsbehelfe zuständig ist, und ob es sich dabei um (1) das von den Datenschutzbehörden eingerichtete Gremium, (2) einen alternativen Streitbeilegungsanbieter mit Sitz in der EU oder (3) einen alternativen Streitbeilegungsanbieter mit Sitz in den Vereinigten Staaten handelt,

x. den Ermittlungs- und Durchsetzungsbefugnissen der FTC, des US-Verkehrsministeriums oder anderer in den USA zugelassener gesetzlicher Stellen unterliegt,

xi. die Möglichkeit für den Einzelnen, unter bestimmten Bedingungen ein verbindliches Schiedsverfahren in Anspruch zu nehmen,[5]

xii. das Erfordernis, personenbezogene Daten auf rechtmäßige Anfragen von Behörden hin offenzulegen, auch um Anforderungen der nationalen Sicherheit oder der Strafverfolgung zu erfüllen, und

xiii. seine Haftung im Falle der Weitergabe an Dritte.

b. Dieser Hinweis muss in klarer und auffälliger Sprache erfolgen, wenn Personen zum ersten Mal aufgefordert werden, der Organisation personenbezogene Daten zur Verfügung zu stellen, oder so bald wie möglich danach, auf jeden Fall aber bevor die Organisation diese Daten für einen anderen Zweck verwendet als den, für den sie ursprünglich von der übermittelnden Organisation erhoben oder verarbeitet wurden, oder sie zum ersten Mal an einen Dritten weitergibt.

## 2. CHOICE

a. Eine Organisation muss Einzelpersonen die Möglichkeit bieten, zu wählen (d. *h.* zu widersprechen), ob ihre persönlichen Daten (i) an Dritte

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

weitergegeben oder (ii) für einen Zweck verwendet werden sollen, der sich wesentlich von dem/den Zweck(en) unterscheidet, für den/die sie ursprünglich erhoben oder später genehmigt wurden.

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

durch den Einzelnen. Der Einzelne muss über klare, auffällige und leicht zugängliche Mechanismen verfügen, um seine Wahlfreiheit auszuüben.

b. Abweichend vom vorstehenden Absatz ist es nicht erforderlich, eine Wahlmöglichkeit vorzusehen, wenn die Weitergabe an einen Dritten erfolgt, der als Beauftragter Aufgaben im Namen und auf Anweisung der Organisation wahrnimmt. Eine Organisation muss jedoch immer einen Vertrag mit dem Beauftragten abschließen.

c. Für sensible Daten (*d. h.* personenbezogene Daten, die Auskunft über den Gesundheitszustand, die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, die Mitgliedschaft in einer Gewerkschaft oder Informationen über das Sexualleben einer Person geben) müssen Organisationen die ausdrückliche Zustimmung (*d. h.* Opt-in) der betroffenen Personen einholen, wenn diese Daten (i) an Dritte weitergegeben oder (ii) für einen anderen Zweck als denjenigen verwendet werden sollen, für den sie ursprünglich erhoben wurden oder für den die betroffenen Personen nachträglich ihre Zustimmung erteilt haben, indem sie ihre Opt-in-Wahl getroffen haben. Darüber hinaus sollte eine Organisation alle personenbezogenen Daten, die sie von einem Dritten erhält, als sensibel behandeln, wenn der Dritte sie als sensibel identifiziert und behandelt.

## 3. VERANTWORTLICHKEIT FÜR DIE WEITERÜBERMITTLUNG

a. Bei der Übermittlung personenbezogener Daten an einen Dritten, der als für die Verarbeitung Verantwortlicher fungiert, müssen die Organisationen die Grundsätze der Benachrichtigung und der Wahlmöglichkeit einhalten. Die Organisationen müssen außerdem einen Vertrag mit dem für die Verarbeitung Verantwortlichen abschließen, der vorsieht, dass diese Daten nur für begrenzte und festgelegte Zwecke verarbeitet werden dürfen, die mit der von der Person erteilten Einwilligung übereinstimmen, und dass der Empfänger das gleiche Schutzniveau wie die Grundsätze gewährleistet und die Organisation benachrichtigt, wenn er feststellt, dass er diese Verpflichtung nicht mehr erfüllen kann. Der Vertrag muss vorsehen, dass der für die Verarbeitung Verantwortliche im Falle einer solchen Feststellung die Verarbeitung einstellt oder andere angemessene und geeignete Schritte unternimmt, um Abhilfe zu schaffen.

b. Bei der Übermittlung personenbezogener Daten an einen Dritten, der als Beauftragter handelt, müssen Organisationen: (i) solche Daten nur für begrenzte und genau festgelegte Zwecke übermitteln; (ii) sich vergewissern, dass der Beauftragte verpflichtet ist, mindestens das gleiche Maß an Datenschutz zu gewährleisten, wie es in den Grundsätzen gefordert wird; (iii) angemessene und geeignete Maßnahmen ergreifen, um sicherzustellen, dass der Beauftragte die übermittelten personenbezogenen Daten tatsächlich in einer Weise verarbeitet, die mit den Verpflichtungen der Organisation nach den Grundsätzen vereinbar ist; (iv) von dem Beauftragten zu verlangen, dass er die Organisation benachrichtigt, wenn er feststellt, dass er seiner Verpflichtung, das in den Grundsätzen geforderte Schutzniveau zu gewährleisten, nicht mehr nachkommen kann; (v) nach einer Benachrichtigung, auch gemäß (iv), angemessene und geeignete Schritte zu unternehmen, um die unbefugte Verarbeitung zu beenden und Abhilfe zu schaffen; und (vi) dem Ministerium auf Anfrage eine Zusammenfassung oder ein repräsentatives Exemplar der einschlägigen Datenschutzbestimmungen seines Vertrags

mit dem Beauftragten zu übermitteln.

## 4. SICHERHEIT

a. Organisationen, die personenbezogene Daten erstellen, verwalten, nutzen oder verbreiten, müssen angemessene und geeignete Maßnahmen ergreifen, um sie vor Verlust, Missbrauch und unbefugtem Zugriff, Offenlegung, Änderung und Zerstörung zu schützen, wobei die mit der Verarbeitung verbundenen Risiken und die Art der personenbezogenen Daten gebührend zu berücksichtigen sind.

## 5. DATENINTEGRITÄT UND ZWECKBINDUNG

a. Im Einklang mit den Grundsätzen müssen personenbezogene Daten auf die Informationen beschränkt werden, die für die Zwecke der Verarbeitung relevant sind.[6] Eine Organisation darf personenbezogene Daten nicht in einer Weise verarbeiten, die mit den Zwecken unvereinbar ist, für die sie erhoben oder später von der betroffenen Person genehmigt wurden. Soweit es für diese Zwecke erforderlich ist, muss eine Organisation angemessene Maßnahmen ergreifen, um sicherzustellen, dass personenbezogene Daten für den beabsichtigten Zweck zuverlässig, richtig, vollständig und aktuell sind. Eine Organisation muss die Grundsätze so lange einhalten, wie sie solche Daten aufbewahrt.

b. Informationen dürfen nur so lange in einer Form aufbewahrt werden, die die betreffende Person identifiziert oder identifizierbar macht[7] , wie sie einem Verarbeitungszweck im Sinne von 5(a) dienen. Diese Verpflichtung hindert Organisationen nicht daran, personenbezogene Daten für längere Zeiträume zu verarbeiten, solange und soweit diese Verarbeitung vernünftigerweise den Zwecken der Archivierung im öffentlichen Interesse, des Journalismus, der Literatur und Kunst, der wissenschaftlichen oder historischen Forschung und der statistischen Analyse dient. In diesen Fällen unterliegt die Verarbeitung den anderen Grundsätzen und Bestimmungen der Datenschutzrichtlinie EU-USA. Organisationen sollten angemessene und geeignete Maßnahmen ergreifen, um diese Bestimmung zu befolgen.

## 6. ACCESS

a. Der Einzelne muss Zugang zu den personenbezogenen Daten haben, die eine Organisation über ihn besitzt, und er muss die Möglichkeit haben, diese Daten zu berichtigen, zu ergänzen oder zu löschen, wenn sie unrichtig sind oder unter Verletzung der Grundsätze verarbeitet wurden, es sei denn, der Aufwand oder die Kosten für die Gewährung des Zugangs stünden in keinem Verhältnis zu den Risiken für die Privatsphäre des Einzelnen in dem betreffenden Fall oder die Rechte anderer Personen als des Einzelnen würden verletzt.

## 7. RÜCKGRIFF, DURCHSETZUNG UND HAFTUNG

a. Zu einem wirksamen Schutz der Privatsphäre gehören solide Mechanismen, die die Einhaltung der Grundsätze gewährleisten, Rechtsmittel für Personen, die von der Nichteinhaltung der Grundsätze betroffen sind, und Konsequenzen für die Organisation, wenn die Grundsätze nicht befolgt werden. Solche Mechanismen müssen mindestens Folgendes umfassen:

   i. leicht zugängliche, unabhängige Rechtsbehelfsmechanismen, mit denen die Beschwerden und Streitigkeiten jedes Einzelnen kostenlos und unter Bezugnahme auf die Grundsätze untersucht und zügig beigelegt werden, sowie die Gewährung von Schadenersatz, wenn das geltende Recht oder privatwirtschaftliche Initiativen dies vorsehen;

   ii. Follow-up-Verfahren, um zu überprüfen, ob die Bescheinigungen und Behauptungen der Organisationen über ihre Datenschutzpraktiken der Wahrheit entsprechen

[6] Je nach den Umständen können Beispiele für vereinbare Verarbeitungszwecke solche sein, die vernünftigerweise den Kundenbeziehungen, der Einhaltung von Vorschriften und rechtlichen Erwägungen, der Rechnungsprüfung,

der Sicherheit und der Betrugsprävention, der Wahrung oder Verteidigung der gesetzlichen Rechte der Organisation oder anderen Zwecken dienen, die mit den Erwartungen einer vernünftigen Person angesichts des Kontextes der Sammlung übereinstimmen.

[7] In diesem Zusammenhang ist eine Person "identifizierbar", wenn sie angesichts der Mittel zur Identifizierung, die nach vernünftigem Ermessen verwendet werden können (unter anderem unter Berücksichtigung der Kosten und des Zeitaufwands für die Identifizierung und der zum Zeitpunkt der Verarbeitung verfügbaren Technologie), und der Form, in der die Daten aufbewahrt werden, nach vernünftigem Ermessen von der Organisation oder einem Dritten identifiziert werden könnte, wenn dieser Zugang zu den Daten hätte.

und dass die Praktiken zum Schutz der Privatsphäre wie vorgelegt umgesetzt wurden, insbesondere im Hinblick auf Fälle der Nichteinhaltung; und

iii. Verpflichtungen zur Behebung von Problemen, die sich aus der Nichteinhaltung der Grundsätze durch Organisationen ergeben, die die Einhaltung der Grundsätze ankündigen, sowie Konsequenzen für solche Organisationen. Die Sanktionen müssen streng genug sein, um die Einhaltung der Grundsätze durch die Organisationen sicherzustellen.

b. Die Organisationen und die von ihnen gewählten unabhängigen Beschwerdemechanismen müssen unverzüglich auf Anfragen und Ersuchen des Ministeriums um Informationen über die DPF EU-USA reagieren. Alle Organisationen müssen zügig auf Beschwerden über die Einhaltung der Grundsätze reagieren, die von den Behörden der EU-Mitgliedstaaten über das Ministerium eingereicht werden. Organisationen, die sich für eine Zusammenarbeit mit den Datenschutzbehörden entschieden haben, einschließlich Organisationen, die Personaldaten verarbeiten, müssen in Bezug auf die Untersuchung und Beilegung von Beschwerden direkt mit diesen Behörden zusammenarbeiten.

c. Die Organisationen sind zur Schlichtung von Ansprüchen und zur Einhaltung der in Anhang I festgelegten Bedingungen verpflichtet, sofern eine Einzelperson ein verbindliches Schiedsverfahren beantragt hat, indem sie die betreffende Organisation benachrichtigt und die in Anhang I festgelegten Verfahren und Bedingungen einhält.

d. Im Zusammenhang mit einer Weitergabe trägt eine teilnehmende Organisation die Verantwortung für die Verarbeitung personenbezogener Daten, die sie im Rahmen der EU-US-DSGVO erhält und anschließend an einen Dritten weitergibt, der als Beauftragter in ihrem Namen handelt. Die teilnehmende Organisation bleibt nach den Grundsätzen haftbar, wenn ihr Beauftragter solche personenbezogenen Daten in einer Weise verarbeitet, die nicht mit den Grundsätzen vereinbar ist, es sei denn, die Organisation weist nach, dass sie für das Ereignis, das den Schaden verursacht hat, nicht verantwortlich ist.

e. Wenn eine Organisation einer gerichtlichen Anordnung unterliegt, die auf der Nichteinhaltung von Vorschriften beruht, oder einer Anordnung einer US-Behörde (z. B. FTC oder DOT), die in den Grundsätzen oder in einem künftigen Anhang zu den Grundsätzen aufgeführt ist und auf der Nichteinhaltung von Vorschriften beruht, muss die Organisation alle relevanten Abschnitte eines dem Gericht oder der US-Behörde vorgelegten Berichts über die Einhaltung von Vorschriften oder Bewertungen veröffentlichen, soweit dies mit den Vertraulichkeitsanforderungen vereinbar ist. Das Ministerium hat eine spezielle Anlaufstelle für DPAs eingerichtet, die bei Problemen mit der Einhaltung der Vorschriften durch die teilnehmenden Organisationen helfen soll. Die FTC und das US-Verkehrsministerium werden Hinweise des Ministeriums und der Behörden der EU-Mitgliedstaaten auf die Nichteinhaltung der Grundsätze vorrangig prüfen und vorbehaltlich bestehender Vertraulichkeitsbeschränkungen zeitnah Informationen über die Hinweise mit den Behörden des verweisenden Staates austauschen.

## III. ERGÄNZENDE GRUNDSÄTZE

### 1. Sensible Daten

a. Eine Organisation muss in Bezug auf sensible Daten keine ausdrückliche Zustimmung (d. *h.* Opt-in) einholen, wenn es sich um eine Verarbeitung handelt:

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

ii. die zur Geltendmachung von Rechtsansprüchen oder zur Verteidigung erforderlich sind;

iii. die für die medizinische Versorgung oder Diagnose erforderlich sind;

iv. im Rahmen der rechtmäßigen Tätigkeiten einer Stiftung, eines Vereins oder einer sonstigen Einrichtung ohne Erwerbszweck mit politischer, weltanschaulicher, religiöser oder gewerkschaftlicher Zielsetzung und unter der Bedingung, dass sich die Verarbeitung ausschließlich auf die Mitglieder der Einrichtung oder auf Personen bezieht, die im Zusammenhang mit den Zwecken der Einrichtung regelmäßig mit ihr in Kontakt stehen, und dass die Daten nicht ohne Einwilligung der betroffenen Personen an Dritte weitergegeben werden;

v. notwendig sind, um die Verpflichtungen der Organisation im Bereich des Arbeitsrechts zu erfüllen; oder

vi. die sich auf Daten beziehen, die von der betreffenden Person offenkundig öffentlich gemacht wurden.

### 2. Journalistische Ausnahmen

a. In Anbetracht des verfassungsrechtlichen Schutzes der Pressefreiheit in den USA muss der Erste Verfassungszusatz die Abwägung zwischen den Rechten einer freien Presse, die im Ersten Verfassungszusatz der US-Verfassung verankert sind, und den Interessen des Schutzes der Privatsphäre regeln, wenn es um die Aktivitäten von US-Personen oder Organisationen geht.

b. Personenbezogene Daten, die für die Veröffentlichung, Ausstrahlung oder andere Formen der öffentlichen Kommunikation von journalistischem Material gesammelt werden, unabhängig davon, ob sie verwendet werden oder nicht, sowie Informationen, die in bereits veröffentlichtem Material aus Medienarchiven enthalten sind, unterliegen nicht den Anforderungen der Grundsätze.

### 3. Sekundäre Haftung

a. Internet Service Provider ("ISPs"), Telekommunikationsanbieter und andere Organisationen sind nach den Grundsätzen nicht haftbar, wenn sie im Namen einer anderen Organisation lediglich Informationen übertragen, weiterleiten, vermitteln oder zwischenspeichern. Die EU-US-DSGVO begründet keine Sekundärhaftung. Soweit eine Organisation lediglich als Kanal für die von Dritten übermittelten Daten fungiert und nicht über die Zwecke und Mittel der Verarbeitung dieser personenbezogenen Daten entscheidet, wäre sie nicht haftbar.

### 4. Durchführung von Due-Diligence-Prüfungen und Audits

a. Die Tätigkeit von Wirtschaftsprüfern und Investmentbankern kann die Verarbeitung personenbezogener Daten ohne die Zustimmung oder das Wissen der betroffenen Person beinhalten. Dies ist nach den Grundsätzen der Benachrichtigung, der Wahlmöglichkeit und des Zugangs unter den unten beschriebenen Umständen zulässig.

b. Aktiengesellschaften und Unternehmen, die sich in engem Besitz befinden, einschließlich der teilnehmenden Organisationen, sind regelmäßig Gegenstand von Prüfungen. Solche Prüfungen,

insbesondere solche, die potenzielles Fehlverhalten untersuchen, können gefährdet werden, wenn sie zu früh offengelegt werden. In ähnlicher Weise wird eine beteiligte Organisation, die an einer potenziellen Fusion oder Übernahme beteiligt ist, eine "Due-Diligence"-Prüfung durchführen müssen oder Gegenstand einer solchen sein. Dies erfordert häufig die Erhebung und Verarbeitung personenbezogener Daten, z. B. Informationen über leitende Angestellte und andere wichtige Mitarbeiter. Eine vorzeitige Offenlegung könnte die Transaktion behindern oder sogar gegen geltende Wertpapiervorschriften verstoßen. Investmentbanker und Anwälte, die eine Due-Diligence-Prüfung durchführen, oder Wirtschaftsprüfer, die eine Prüfung vornehmen, dürfen Informationen ohne Wissen der betroffenen Person nur in dem Umfang und für den Zeitraum verarbeiten, der erforderlich ist, um gesetzliche oder im öffentlichen Interesse liegende Anforderungen zu erfüllen, sowie unter anderen Umständen, in denen die Anwendung dieser Grundsätze die legitimen Interessen der Organisation beeinträchtigen würde. Zu diesen berechtigten Interessen gehören die Überwachung der Einhaltung der gesetzlichen Verpflichtungen von Organisationen und legitime Buchhaltungstätigkeiten sowie das Erfordernis der Vertraulichkeit im Zusammenhang mit möglichen Übernahmen, Fusionen, Joint Ventures oder anderen ähnlichen Transaktionen, die von Investmentbankern oder Wirtschaftsprüfern durchgeführt werden.

## 5. Die Rolle der Datenschutzbehörden

a. Die Organisationen werden ihre Verpflichtung zur Zusammenarbeit mit den Datenschutzbehörden wie unten beschrieben umsetzen. Im Rahmen der EU-US-DSGVO müssen sich US-Organisationen, die personenbezogene Daten aus der EU erhalten, verpflichten, wirksame Mechanismen einzusetzen, um die Einhaltung der Grundsätze zu gewährleisten. Wie im Grundsatz "Rückgriff, Durchsetzung und Haftung" dargelegt, müssen die teilnehmenden Organisationen insbesondere Folgendes gewährleisten (a)(i) Rechtsbehelfe für Personen, auf die sich die Daten beziehen; (a)(ii) Folgeverfahren zur Überprüfung, ob die Bescheinigungen und Behauptungen, die sie über ihre Datenschutzpraktiken abgegeben haben, der Wahrheit entsprechen; und (a)(iii) Verpflichtungen zur Behebung von Problemen, die sich aus der Nichteinhaltung der Grundsätze ergeben, sowie Konsequenzen für diese Organisationen. Eine Organisation kann die Punkte (a)(i) und (a)(iii) des Grundsatzes des Rückgriffs, der Durchsetzung und der Haftung erfüllen, wenn sie die hier dargelegten Anforderungen an die Zusammenarbeit mit den Datenschutzbehörden einhält.

b. Eine Organisation verpflichtet sich, mit den Datenschutzbehörden zusammenzuarbeiten, indem sie in ihrer Selbstzertifizierung für die EU-US-DSGK gegenüber dem Ministerium erklärt, dass die Organisation:

   i. sich dafür entscheidet, die Anforderung unter Buchstabe a) Ziffer i) und Ziffer iii) des Grundsatzes des Rückgriffs, der Durchsetzung und der Haftung zu erfüllen, indem er sich zur Zusammenarbeit mit den Datenschutzbehörden verpflichtet;

   ii. mit den Datenschutzbehörden bei der Untersuchung und Beilegung von Beschwerden, die im Rahmen der Grundsätze vorgebracht werden, zusammenarbeiten; und

   iii. befolgt alle Ratschläge der Datenschutzbehörden, wenn diese der Ansicht sind, dass die Organisation spezifische Maßnahmen ergreifen muss, um die Grundsätze einzuhalten, einschließlich

Abhilfe- oder Ausgleichsmaßnahmen zugunsten von Personen, die von einer Nichteinhaltung der Grundsätze betroffen sind, und bestätigt den Datenschutzbehörden schriftlich, dass solche Maßnahmen ergriffen wurden.

c. Funktionsweise der DPA-Panels

i. Die Zusammenarbeit mit den Datenschutzbehörden erfolgt in Form von Information und Beratung auf folgende Weise:

1. Die Beratung durch die Datenschutzbehörden erfolgt über ein informelles Gremium von Datenschutzbehörden, das auf EU-Ebene eingerichtet wird und *unter anderem* dazu beitragen soll, ein harmonisiertes und kohärentes Vorgehen zu gewährleisten.

2. Das Gremium wird die betroffenen US-Organisationen bei ungelösten Beschwerden von Einzelpersonen über den Umgang mit personenbezogenen Daten, die im Rahmen der EU-US-DSGVO aus der EU übermittelt wurden, beraten. Mit dieser Beratung soll sichergestellt werden, dass die Grundsätze korrekt angewandt werden, und sie wird alle Abhilfemaßnahmen für die betroffene(n) Person(en) umfassen, die die Datenschutzbehörden für angemessen halten.

3. Das Gremium berät auf Empfehlung der betreffenden Organisationen und/oder bei Beschwerden, die direkt von Einzelpersonen gegen Organisationen eingehen, die sich zur Zusammenarbeit mit den Datenschutzbehörden für die Zwecke der EU-US-DSGVO verpflichtet haben, und ermutigt die betreffenden Personen, zunächst die von der Organisation angebotenen internen Regelungen zur Bearbeitung von Beschwerden zu nutzen, und hilft ihnen gegebenenfalls dabei.

4. Ein Gutachten wird erst dann erstellt, wenn beide Streitparteien ausreichend Gelegenheit hatten, sich zu äußern und alle gewünschten Beweise vorzulegen. Das Gremium wird sich bemühen, so schnell wie möglich eine Stellungnahme abzugeben, um ein ordnungsgemäßes Verfahren zu gewährleisten. In der Regel ist das Gremium bestrebt, innerhalb von 60 Tagen nach Eingang einer Beschwerde oder Verweisung einen Rat zu erteilen, wenn möglich auch schneller.

5. Das Gremium veröffentlicht die Ergebnisse seiner Prüfung der ihm vorgelegten Beschwerden, wenn es dies für angebracht hält.

6. Die Erteilung von Ratschlägen durch das Gremium führt nicht zu einer Haftung des Gremiums oder der einzelnen Datenschutzbehörden.

ii. Wie bereits erwähnt, müssen sich Organisationen, die sich für diese Option der Streitbeilegung entscheiden, verpflichten, den Ratschlägen der DPAs Folge zu leisten. Kommt eine Organisation der Empfehlung nicht innerhalb von 25 Tagen nach und hat sie keine zufriedenstellende Erklärung für die Verzögerung abgegeben, teilt das Gremium seine Absicht mit, entweder die Angelegenheit an die FTC, das DOT oder eine andere US-Bundes- oder einzelstaatliche Behörde zu verweisen, die gesetzlich befugt ist, in Fällen von Täuschung oder Falschdarstellung Durchsetzungsmaßnahmen zu ergreifen, oder zu dem Schluss zu kommen, dass die Kooperationsvereinbarung ernsthaft verletzt wurde und daher als null und nichtig zu betrachten ist. Im letzteren Fall informiert das Gremium das Ministerium, damit die Datenschutz-Rahmenliste ordnungsgemäß geändert werden kann. Die Nichteinhaltung der Verpflichtung zur

Zusammenarbeit mit den Datenschutzbehörden sowie die Nichteinhaltung der Grundsätze können als irreführende Praktiken gemäß Abschnitt 5 des FTC Act (15 U.S.C. § 45), 49 U.S.C. § 41712 oder einem ähnlichen Gesetz verfolgt werden.

d. Ein Unternehmen, das möchte, dass seine EU-US-DSGVO-Vorteile auch für Personaldaten gelten, die im Rahmen des Beschäftigungsverhältnisses aus der EU übermittelt werden, muss sich verpflichten, in Bezug auf diese Daten mit den Datenschutzbehörden zusammenzuarbeiten (*siehe* ergänzender Grundsatz zu Personaldaten).

e. Organisationen, die sich für diese Option entscheiden, müssen eine jährliche Gebühr entrichten, die die Betriebskosten des Gremiums decken soll. Darüber hinaus können sie aufgefordert werden, alle notwendigen Übersetzungskosten zu übernehmen, die sich aus der Prüfung von Befassungen oder Beschwerden gegen sie durch das Gremium ergeben. Die Höhe der Gebühr wird vom Ministerium nach Rücksprache mit 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 bei der Festlegung geeigneter Verfahren für die Verteilung der durch die Gebühr eingenommenen Gelder sowie bei anderen verfahrenstechnischen und administrativen Aspekten des Panels eng mit der Kommission und den Datenschutzbehörden zusammenarbeiten. Das Ministerium und die Kommission können vereinbaren, die Häufigkeit der Erhebung der Gebühr zu ändern.

**6. Selbstzertifizierung**

a. Die Vorteile der EU-US-DSGVO sind ab dem Datum gewährleistet, an dem das Ministerium die Organisation auf die Datenschutz-Rahmenliste setzt. Das Ministerium wird eine Organisation erst dann auf die Datenschutz-Rahmenliste setzen, wenn es festgestellt hat, dass die ursprüngliche Selbstzertifizierung der Organisation vollständig ist, und es wird die Organisation von dieser Liste streichen, wenn sie sich freiwillig zurückzieht, ihre jährliche Neuzertifizierung nicht abschließt oder die Grundsätze dauerhaft nicht einhält (*siehe* Zusatzgrundsatz zur Streitbeilegung und Durchsetzung).

b. Für eine erstmalige Selbstzertifizierung oder eine spätere Neuzertifizierung für die EU-U.S. DPF muss eine Organisation dem Ministerium jedes Mal eine Einreichung durch einen leitenden Angestellten im Namen der Organisation vorlegen, die ihre Einhaltung der Grundsätze ([8] ) selbstzertifiziert oder rezertifiziert (je nach Fall):

i. den Namen der selbstzertifizierenden oder rezertifizierenden US-Organisation sowie den Namen aller ihrer US-Einheiten oder US-Tochtergesellschaften, die sich ebenfalls an die Grundsätze halten, die die Organisation abdecken möchte;

ii. eine Beschreibung der Tätigkeiten der Organisation in Bezug auf personenbezogene Daten, die im Rahmen der EU-US-DSGVO aus der EU erhalten würden;

iii. eine Beschreibung der einschlägigen Datenschutzpolitik(en) der Organisation für solche personenbezogenen Daten, einschließlich:

1. falls die Organisation über eine öffentliche Website verfügt, die entsprechende Webadresse, unter der die Datenschutzbestimmungen abrufbar sind, oder falls die Organisation keine öffentliche Website hat, die Adresse, unter der die Datenschutzbestimmungen öffentlich einsehbar sind; und
2. das Datum des Inkrafttretens;

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

iv. eine Kontaktstelle innerhalb der Organisation für die Bearbeitung von Beschwerden, Zugangsanträgen und anderen Fragen, die sich aus den Grundsätzen ergeben[9] :

1. Name(n), Berufsbezeichnung(en) (soweit zutreffend), E-Mail-Adresse(n) und Telefonnummer(n) der zuständigen Person(en) oder der zuständigen Kontaktstelle(n) innerhalb der Organisation; und
2. die entsprechende US-Postanschrift der Organisation;

v. die spezielle gesetzliche Stelle, die für Klagen gegen die Organisation wegen möglicher unlauterer oder betrügerischer Praktiken und Verstöße gegen Gesetze oder Vorschriften zum Schutz der Privatsphäre zuständig ist (und die in den Grundsätzen oder einem künftigen Anhang zu den Grundsätzen aufgeführt ist);

vi. den Namen eines Datenschutzprogramms, an dem die Organisation beteiligt ist;

vii. die Überprüfungsmethode (d. *h.* Selbsteinschätzung oder externe Überprüfung der Einhaltung der Vorschriften, einschließlich der dritten Partei, die diese Überprüfung durchführt);[10] und

viii. den/die entsprechenden unabhängigen Mechanismus/e, der/die für die Untersuchung ungelöster Beschwerden im Zusammenhang mit den Grundsätzen zur Verfügung steht/stehen.[11]

c. Wenn die Organisation wünscht, dass ihre EU-US-DSGVO-Leistungen auch für Personaldaten gelten, die aus der EU zur Verwendung im Rahmen des Beschäftigungsverhältnisses übermittelt werden, kann sie dies tun, wenn eine in den Grundsätzen oder einem künftigen Anhang zu den Grundsätzen aufgeführte Behörde für Klagen gegen die Organisation im Zusammenhang mit der Verarbeitung von Personaldaten zuständig ist. Darüber hinaus muss die Organisation dies in ihrer ersten Selbstzertifizierungserklärung sowie in jeder Neuzertifizierungserklärung angeben und erklären, dass sie mit der/den betreffenden EU-Behörde(n) in Übereinstimmung mit den Ergänzenden Grundsätzen zu Personaldaten und der Rolle der Datenschutzbehörden (soweit zutreffend) zusammenarbeiten und die Ratschläge dieser Behörden befolgen wird. Die Organisation muss dem Ministerium auch ein Exemplar ihrer Datenschutzpolitik für das Personalwesen zur Verfügung stellen und angeben, wo die Datenschutzpolitik für die betroffenen Mitarbeiter einsehbar ist.

d. Das Ministerium wird die Datenschutz-Rahmenliste der Organisationen, die eine vollständige Erstzertifizierung eingereicht haben, führen und öffentlich zugänglich machen und diese Liste auf der Grundlage der jährlich eingereichten Neuzertifizierungen sowie der gemäß dem ergänzenden Grundsatz zur Streitbeilegung und Durchsetzung eingegangenen Meldungen aktualisieren. Eine solche Neuzertifizierung muss mindestens einmal jährlich erfolgen, andernfalls wird die Organisation von der Datenschutz-Rahmenliste gestrichen und die Vorteile der EU-US-Datenschutzgrundverordnung sind nicht mehr gewährleistet. Alle Organisationen, die vom Ministerium auf die Datenschutz-Rahmenliste gesetzt werden, müssen über einschlägige Datenschutzrichtlinien verfügen, die dem Grundsatz der Benachrichtigung entsprechen und in diesen Datenschutzrichtlinien angeben, dass sie

[9] Der primäre "Organisationskontakt" oder der "Unternehmensbeauftragte" darf nicht außerhalb der Organisation stehen (z. *B.* ein externer Rechtsberater oder ein externer Berater).
[10] *Siehe* Zusätzlicher Grundsatz zur Verifizierung.
[11] *Siehe den* ergänzenden Grundsatz zur Streitbeilegung und Vollstreckung.

sich an die Grundsätze halten.[12] Falls online verfügbar, muss die Datenschutzrichtlinie einer Organisation einen Hyperlink zur Website des Datenschutzrahmens des Ministeriums und einen Hyperlink zur Website oder zum Beschwerdeformular des unabhängigen Rechtsbehelfsmechanismus enthalten, der zur Verfügung steht, um ungelöste, mit den Grundsätzen zusammenhängende Beschwerden kostenlos für den Einzelnen zu untersuchen.

e. Die Grundsätze gelten unmittelbar nach der Selbstzertifizierung. Teilnehmende Organisationen, die sich zuvor nach den Rahmenprinzipien des EU-US-Datenschutzschilds selbst zertifiziert haben, müssen ihre Datenschutzrichtlinien aktualisieren und stattdessen auf die "Rahmenprinzipien des EU-US-Datenschutzschilds" verweisen. Diese Organisationen müssen diesen Verweis so bald wie möglich, spätestens jedoch drei Monate nach Inkrafttreten der EU-U.S. Datenschutz-Rahmenprinzipien aufnehmen.

f. Eine Organisation muss alle personenbezogenen Daten, die sie aus der EU im Rahmen des EU-US-DSGVO erhält, den Grundsätzen unterwerfen. Die Verpflichtung zur Einhaltung der Grundsätze ist in Bezug auf personenbezogene Daten, die während des Zeitraums, in dem die Organisation die Vorteile der EU-US-DSGVO genießt, erhalten wurden, nicht zeitlich befristet.
Ihre Verpflichtung bedeutet, dass sie die Grundsätze so lange auf diese Daten anwenden wird, wie die Organisation sie speichert, nutzt oder weitergibt, auch wenn sie die EU-US-DSGVO aus irgendeinem Grund verlässt. Eine Organisation, die aus der EU-US-DSGVO austreten möchte, muss dies dem Ministerium im Voraus mitteilen. In dieser Mitteilung muss auch angegeben werden, was die Organisation mit den personenbezogenen Daten tun wird, die sie im Rahmen der EU-US-DSGVO erhalten hat (d. *h. die* Daten aufbewahren, zurückgeben oder löschen, und falls sie die Daten aufbewahren wird, die genehmigten Mittel, mit denen sie den Schutz der Daten gewährleisten wird). Eine Organisation, die sich aus der EU-US-DSGVO zurückzieht, aber solche Daten behalten möchte, muss entweder dem Ministerium jährlich ihre Verpflichtung bestätigen, die Grundsätze weiterhin auf die Daten anzuwenden, oder einen "angemessenen" Schutz für die Daten durch ein anderes zulässiges Mittel gewährleisten (z. B. durch einen Vertrag, der die Anforderungen der von der Kommission angenommenen einschlägigen Standardvertragsklauseln vollständig widerspiegelt); andernfalls muss die Organisation die Informationen zurückgeben oder löschen.[13] Eine Organisation, die aus der EU-US-DSGVO ausscheidet, muss aus allen relevanten Datenschutzrichtlinien alle Verweise auf die EU-US-DSGVO entfernen, die implizieren, dass die Organisation weiterhin an der EU-US-DSGVO teilnimmt und Anspruch auf deren Vorteile hat.

g. Eine Organisation, die aufgrund einer Änderung des Unternehmensstatus (z. B. durch Fusion, Übernahme, Konkurs oder Auflösung) als eigenständige juristische Person aufhört zu existieren, muss dies dem Ministerium im Voraus mitteilen. In der Mitteilung sollte auch angegeben werden, ob die aus der Änderung hervorgehende Organisation

[12] Eine Organisation, die sich zum ersten Mal selbst zertifiziert, darf die Teilnahme an der EU-US-DSGVO erst dann in ihrer endgültigen Datenschutzpolitik geltend machen, wenn das Ministerium der Organisation mitteilt, dass sie dies tun darf. Die Organisation muss dem Ministerium bei der ersten Selbstzertifizierung einen Entwurf ihrer Datenschutzpolitik vorlegen, der mit den Grundsätzen übereinstimmt. Sobald das Ministerium festgestellt hat, dass die ursprüngliche Selbstzertifizierung der Organisation vollständig ist, wird das Ministerium die

Organisation benachrichtigen, dass sie ihre EU-US-DSGVO-konformen Datenschutzrichtlinien fertig stellen (*z. B.* gegebenenfalls veröffentlichen) soll. Die Organisation muss das Ministerium unverzüglich benachrichtigen, sobald die entsprechenden Datenschutzrichtlinien fertiggestellt sind; zu diesem Zeitpunkt wird das Ministerium die Organisation in die Data Privacy Framework List aufnehmen.

[13] Wenn sich eine Organisation zum Zeitpunkt ihres Rücktritts dafür entscheidet, die personenbezogenen Daten, die sie unter Berufung auf die EU-US-DSGVO erhalten hat, aufzubewahren und dem Ministerium jährlich zu bestätigen, dass sie die Grundsätze weiterhin auf diese Daten anwendet, muss die Organisation dem Ministerium einmal jährlich nach ihrem Rücktritt (d. *h.* bis zum Ende des
Organisation einen "angemessenen" Schutz für diese Daten durch ein anderes zulässiges Mittel bietet oder alle diese Daten zurückgibt oder löscht und das Ministerium über diese Maßnahme informiert), was sie mit diesen personenbezogenen Daten gemacht hat, was sie mit allen personenbezogenen Daten, die sie weiterhin aufbewahrt, machen wird und wer als ständiger Ansprechpartner für Fragen im Zusammenhang mit den Grundsätzen dienen wird.

Änderung des Unternehmensstatus (i) weiterhin an der EU-US-DSGF durch eine bestehende Selbstzertifizierung teilnehmen; (ii) sich als neuer Teilnehmer an der EU-US-DSGF selbst zertifizieren (z. *B*. wenn die neue oder überlebende Einheit nicht bereits über eine bestehende Selbstzertifizierung verfügt, durch die sie an der EU-US-DSGF teilnehmen könnte); oder (iii) andere Sicherheitsvorkehrungen treffen, wie z. B. eine schriftliche Vereinbarung, die die weitere Anwendung der Grundsätze auf alle personenbezogenen Daten gewährleistet, die die Organisation im Rahmen der EU-US-DSGF erhalten hat.
US-DSGVO und werden aufbewahrt. Wenn weder (i), (ii) noch (iii) zutrifft, müssen alle personenbezogenen Daten, die im Rahmen der EU-US-DSGVO erhalten wurden, unverzüglich zurückgegeben oder gelöscht werden.

h. Wenn eine Organisation die DPF EU-USA aus irgendeinem Grund verlässt, muss sie alle Erklärungen entfernen, die darauf hindeuten, dass die Organisation weiterhin an der DPF EU-USA teilnimmt oder Anspruch auf die Vorteile der DPF EU-USA hat. Das EU-U.S. DPF-Zertifizierungszeichen, falls verwendet, muss ebenfalls entfernt werden. Jede Falschdarstellung gegenüber der Öffentlichkeit in Bezug auf die Einhaltung der Grundsätze durch eine Organisation kann von der FTC, dem US-Verkehrsministerium oder einer anderen zuständigen Regierungsbehörde verfolgt werden. Falsche Angaben gegenüber dem Ministerium können nach dem False Statements Act (18 U.S.C. § 1001) strafbar sein.

## 7. Überprüfung

a. Die Organisationen müssen Verfahren zur Nachverfolgung vorsehen, um zu überprüfen, ob die Bescheinigungen und Behauptungen, die sie über ihre Datenschutzpraktiken zwischen der EU und den USA abgeben, der Wahrheit entsprechen und ob diese Datenschutzpraktiken wie dargestellt und in Übereinstimmung mit den Grundsätzen umgesetzt wurden.

b. Um die Überprüfungsanforderungen des Grundsatzes des Rückgriffs, der Durchsetzung und der Haftung zu erfüllen, muss eine Organisation solche Bescheinigungen und Behauptungen entweder durch eine Selbstbewertung oder durch externe Überprüfungen der Einhaltung der Vorschriften verifizieren.

c. Hat sich die Organisation für eine Selbstbewertung entschieden, so muss sie nachweisen, dass ihre Datenschutzpolitik in Bezug auf personenbezogene Daten, die sie aus der EU erhalten hat, korrekt, umfassend und leicht zugänglich ist, den Grundsätzen entspricht und vollständig umgesetzt wird (d*. h., dass sie diese* einhält). Es muss auch angeben, dass Einzelpersonen über alle internen Vorkehrungen für die Bearbeitung von Beschwerden und über den/die unabhängigen Beschwerdemechanismus/-mechanismen informiert werden, durch den/die sie Beschwerden vorbringen können; dass es über Verfahren für die Schulung von Mitarbeitern in der Umsetzung der Grundsätze und für die Ahndung von Verstößen gegen die Grundsätze verfügt; und dass es über interne Verfahren für die regelmäßige Durchführung objektiver Überprüfungen der Einhaltung der oben genannten Bestimmungen verfügt. Eine Erklärung, die bestätigt, dass die Selbstbewertung abgeschlossen wurde, muss mindestens einmal jährlich von einem leitenden Angestellten oder einem anderen bevollmächtigten Vertreter der Organisation unterzeichnet und auf Anfrage von Einzelpersonen oder im Zusammenhang mit einer Untersuchung oder einer Beschwerde wegen

Nichteinhaltung der Vorschriften zur Verfügung gestellt werden.

d. Hat sich die Organisation für eine externe Überprüfung der Einhaltung der Vorschriften entschieden, so muss diese nachweisen, dass ihre Datenschutzpolitik in Bezug auf personenbezogene Daten aus der EU korrekt, umfassend und leicht zugänglich ist, den Grundsätzen entspricht und vollständig umgesetzt wird (d*. h., dass* sie eingehalten wird). Es muss auch angeben, dass Einzelpersonen über die Mechanismen informiert werden, über die sie Beschwerden einreichen können. Zu den Überprüfungsmethoden können u. a. Audits, stichprobenartige Überprüfungen, der Einsatz von "Lockvögeln" oder gegebenenfalls der Einsatz technologischer Hilfsmittel gehören. Eine Erklärung, die bestätigt, dass eine externe Überprüfung der Einhaltung der Vorschriften erfolgreich durchgeführt wurde

Der ausgefüllte Fragebogen muss mindestens einmal jährlich entweder vom Prüfer oder von einem leitenden Angestellten oder einem anderen bevollmächtigten Vertreter der Organisation unterzeichnet und auf Anfrage von Einzelpersonen oder im Rahmen einer Untersuchung oder einer Beschwerde über die Einhaltung der Vorschriften zur Verfügung gestellt werden.

e. Organisationen müssen ihre Aufzeichnungen über die Umsetzung ihrer EU-Vorschriften aufbewahren.
U.S. DPF-Datenschutzpraktiken und stellen sie auf Anfrage im Rahmen einer Untersuchung oder einer Beschwerde über die Nichteinhaltung der Grundsätze der unabhängigen Streitbeilegungsstelle, die für die Untersuchung von Beschwerden zuständig ist, oder der Behörde, die für unlautere und irreführende Praktiken zuständig ist, zur Verfügung. Die Organisationen müssen auch unverzüglich auf Anfragen und andere Informationsersuchen des Ministeriums bezüglich der Einhaltung der Grundsätze durch die Organisation reagieren.

## 8. Zugang

a. Das Zugangsprinzip in der Praxis

i. Nach den Grundsätzen ist das Auskunftsrecht von grundlegender Bedeutung für den Schutz der Privatsphäre. Insbesondere ermöglicht es dem Einzelnen, die Richtigkeit der über ihn gespeicherten Informationen zu überprüfen. Der Grundsatz des Zugangs bedeutet, dass der Einzelne das Recht hat:

1. von einer Organisation eine Bestätigung darüber zu erhalten, ob die Organisation sie betreffende personenbezogene Daten verarbeitet oder nicht;[14]

2. ihnen diese Daten mitgeteilt haben, damit sie deren Richtigkeit und die Rechtmäßigkeit der Verarbeitung überprüfen können, und

3. die Daten berichtigen, ändern oder löschen zu lassen, wenn sie unrichtig sind oder unter Verstoß gegen die Grundsätze verarbeitet wurden.

ii. Einzelpersonen müssen Anträge auf Zugang zu ihren personenbezogenen Daten nicht begründen. Bei der Beantwortung von Anträgen auf Zugang zu personenbezogenen Daten sollten sich die Organisationen zunächst von den Anliegen leiten lassen, die zu den Anträgen geführt haben. Wenn beispielsweise ein Antrag auf Zugang zu personenbezogenen Daten vage oder weit gefasst ist, kann eine Organisation mit der betroffenen Person in einen Dialog treten, um die Gründe für den Antrag besser zu verstehen und die entsprechenden Informationen zu finden. Die Organisation könnte sich danach erkundigen, mit welchen Bereichen der Organisation die Person interagiert hat oder welche Art von Informationen oder deren Verwendung Gegenstand der Anfrage ist.

iii. Im Einklang mit der grundlegenden Natur des Zugangs sollten Organisationen sich stets nach Treu und Glauben bemühen, Zugang zu gewähren. Wenn beispielsweise bestimmte Informationen geschützt werden müssen und ohne weiteres von anderen personenbezogenen Informationen, die Gegenstand eines

Zugangsantrags sind, getrennt werden können, sollte die Organisation die geschützten Informationen unkenntlich machen und die anderen Informationen zugänglich machen. Stellt eine Organisation fest, dass der Zugang in einem bestimmten Fall eingeschränkt werden sollte, sollte sie der antragstellenden Person Folgendes mitteilen

[14] Die Organisation sollte Anfragen einer Person zu den Zwecken der Verarbeitung, den betroffenen Kategorien personenbezogener Daten und den Empfängern oder Kategorien von Empfängern, an die die personenbezogenen Daten weitergegeben werden, beantworten.

Zugang mit einer Erklärung, warum sie diese Entscheidung getroffen hat, und einer Kontaktstelle für weitere Fragen.

b. Aufwand oder Kosten für die Bereitstellung des Zugangs

i. Das Recht auf Zugang zu personenbezogenen Daten kann unter außergewöhnlichen Umständen eingeschränkt werden, wenn die legitimen Rechte anderer Personen als der betroffenen Person verletzt würden oder wenn der Aufwand oder die Kosten für die Gewährung des Zugangs in dem betreffenden Fall in keinem Verhältnis zu den Risiken für die Privatsphäre der Person stehen würden. Kosten und Aufwand sind wichtige Faktoren, die berücksichtigt werden sollten, aber sie sind nicht ausschlaggebend für die Frage, ob die Gewährung des Zugangs angemessen ist.

ii. Wenn die personenbezogenen Daten beispielsweise für Entscheidungen verwendet werden, die sich erheblich auf die Person auswirken (z. *B. die* Verweigerung oder Gewährung wichtiger Leistungen wie Versicherungen, Hypotheken oder Arbeitsstellen), dann müsste die Organisation diese Informationen in Übereinstimmung mit den anderen Bestimmungen dieser ergänzenden Grundsätze offenlegen, auch wenn es relativ schwierig oder teuer ist, sie bereitzustellen. Wenn die angeforderten persönlichen Informationen nicht sensibel sind oder nicht für Entscheidungen verwendet werden, die den Einzelnen erheblich beeinträchtigen, aber leicht verfügbar und kostengünstig zu beschaffen sind, müsste eine Organisation Zugang zu diesen Informationen gewähren.

c. Vertrauliche Geschäftsinformationen

i. Vertrauliche Geschäftsinformationen sind Informationen, die eine Organisation vor der Offenlegung geschützt hat, wenn die Offenlegung einem Wettbewerber auf dem Markt helfen würde. Organisationen können den Zugang verweigern oder einschränken, wenn die Gewährung des vollständigen Zugangs ihre eigenen vertraulichen Geschäftsinformationen offenlegen würde, wie z. B. von der Organisation erstellte Marketing-Rückschlüsse oder Klassifizierungen, oder die vertraulichen Geschäftsinformationen einer anderen Person, die einer vertraglichen Verpflichtung zur Vertraulichkeit unterliegt.

ii. Wenn vertrauliche Geschäftsinformationen ohne weiteres von anderen personenbezogenen Informationen, die Gegenstand eines Zugangsantrags sind, getrennt werden können, sollte die Organisation die vertraulichen Geschäftsinformationen unkenntlich machen und die nicht vertraulichen Informationen zur Verfügung stellen.

d. Organisation von Datenbanken

i. Der Zugang kann in Form einer Offenlegung der relevanten persönlichen Informationen durch eine Organisation an den Einzelnen erfolgen und erfordert nicht, dass der Einzelne Zugang zur Datenbank einer Organisation erhält.

ii. Der Zugang muss nur in dem Umfang gewährt werden, in dem eine Organisation die personenbezogenen Daten speichert. Der Grundsatz des Zugangs selbst begründet keine Verpflichtung,

Dateien mit personenbezogenen Daten aufzubewahren, zu pflegen, zu reorganisieren oder umzustrukturieren.

e. Wann kann der Zugang eingeschränkt werden?

i. Da Organisationen sich stets nach Treu und Glauben bemühen müssen, Einzelpersonen Zugang zu ihren personenbezogenen Daten zu gewähren, sind die Umstände, unter denen Organisationen diesen Zugang einschränken können, begrenzt, und alle Gründe für die Einschränkung des Zugangs müssen spezifisch sein. Wie bei der DSGVO,

Eine Organisation kann den Zugang zu Informationen einschränken, wenn die Offenlegung die Wahrung wichtiger, entgegenstehender öffentlicher Interessen wie die nationale Sicherheit, die Verteidigung oder die öffentliche Sicherheit beeinträchtigen könnte. Darüber hinaus kann der Zugang verweigert werden, wenn personenbezogene Daten ausschließlich zu Forschungs- oder Statistikzwecken verarbeitet werden. Weitere Gründe für die Verweigerung oder Einschränkung des Zugangs sind:

1. Eingriffe in die Vollstreckung oder Durchsetzung des Rechts oder in private Rechtsstreitigkeiten, einschließlich der Verhütung, Ermittlung oder Feststellung von Straftaten oder des Rechts auf ein faires Verfahren;

2. Offenlegung, wenn die legitimen Rechte oder wichtigen Interessen anderer verletzt würden;

3. die Verletzung eines gesetzlichen oder sonstigen beruflichen Privilegs oder einer Verpflichtung;

4. Beeinträchtigung von Sicherheitsuntersuchungen oder Beschwerdeverfahren von Mitarbeitern oder im Zusammenhang mit der Nachfolgeplanung von Mitarbeitern und Unternehmensumstrukturierungen; oder

5. Beeinträchtigung der Vertraulichkeit, die bei Überwachungs-, Inspektions- oder Regulierungsfunktionen im Zusammenhang mit einer ordnungsgemäßen Verwaltung oder bei künftigen oder laufenden Verhandlungen mit der Organisation erforderlich ist.

ii. Eine Organisation, die eine Ausnahmeregelung in Anspruch nimmt, muss deren Notwendigkeit nachweisen, und Einzelpersonen sollten die Gründe für die Zugangsbeschränkung sowie eine Kontaktstelle für Rückfragen genannt werden.

f. <u>Recht auf Bestätigung und Erhebung einer Gebühr zur Deckung der Kosten für die Gewährung des Zugangs</u>

i. Eine Person hat das Recht, eine Bestätigung darüber zu erhalten, ob diese Organisation über sie betreffende personenbezogene Daten verfügt oder nicht. Eine Person hat auch das Recht, dass ihr die sie betreffenden personenbezogenen Daten mitgeteilt werden. Eine Organisation kann eine Gebühr erheben, die nicht übermäßig hoch ist.

ii. Die Erhebung einer Gebühr kann z. B. gerechtfertigt sein, wenn die Anträge auf Zugang offensichtlich überhöht sind, insbesondere aufgrund ihres Wiederholungscharakters.

iii. Der Zugang darf nicht aus Kostengründen verweigert werden, wenn die Person anbietet, die Kosten zu übernehmen.

g. <u>Wiederholte oder langwierige Anträge auf Zugang</u>

i. Eine Organisation kann die Anzahl der Zugriffe auf die Daten einer bestimmten Person innerhalb eines bestimmten Zeitraums angemessen begrenzen. Bei der Festlegung solcher Beschränkungen sollte eine Organisation Faktoren wie die

Häufigkeit, mit der Informationen aktualisiert werden, den Zweck, für den die Daten verwendet werden, und die Art der Informationen berücksichtigen.

h. Betrügerische Anträge auf Zugang

i. Eine Organisation ist nicht verpflichtet, Zugang zu gewähren, wenn sie nicht über ausreichende Informationen verfügt, um die Identität der antragstellenden Person zu bestätigen.

i. Zeitrahmen für Antworten

i. Organisationen sollten Auskunftsersuchen innerhalb eines angemessenen Zeitraums, in angemessener Weise und in einer für die betroffene Person leicht verständlichen Form beantworten. Eine Organisation, die betroffenen Personen in regelmäßigen Abständen Informationen zur Verfügung stellt, kann einem individuellen Auskunftsersuchen mit ihrer regelmäßigen Offenlegung nachkommen, wenn dies keine übermäßige Verzögerung darstellt.

## 9. Daten der Personalabteilung

a. Abdeckung durch die DPF EU-USA

i. Wenn eine Organisation in der EU personenbezogene Daten über ihre (ehemaligen oder gegenwärtigen) Mitarbeiter, die im Rahmen des Beschäftigungsverhältnisses erhoben wurden, an eine Muttergesellschaft, eine Tochtergesellschaft oder einen nicht angeschlossenen Dienstleister in den Vereinigten Staaten, die an der EU-US-DSGVO teilnehmen, weitergibt, kommt die Weitergabe in den Genuss der Vorteile der EU-US-DSGVO. In solchen Fällen unterliegt die Erhebung der Daten und ihre Verarbeitung vor der Übermittlung den nationalen Gesetzen des EU-Mitgliedstaats, in dem sie erhoben wurden, und alle Bedingungen oder Einschränkungen für ihre Übermittlung gemäß diesen Gesetzen müssen beachtet werden.

ii. Die Grundsätze sind nur dann relevant, wenn individuell identifizierte oder identifizierbare Datensätze übermittelt oder abgerufen werden. Statistische Berichte, die sich auf aggregierte Beschäftigungsdaten stützen und keine personenbezogenen Daten enthalten, oder die Verwendung anonymisierter Daten werfen keine Datenschutzbedenken auf.

b. Anwendung der Grundsätze der Bekanntmachung und der Wahlmöglichkeit

i. Eine US-Organisation, die im Rahmen der EU-US-DSGVO Arbeitnehmerdaten aus der EU erhalten hat, darf diese nur in Übereinstimmung mit den Grundsätzen der Benachrichtigung und Wahlmöglichkeit an Dritte weitergeben oder für andere Zwecke verwenden. Beabsichtigt eine Organisation beispielsweise, personenbezogene Daten, die im Rahmen des Beschäftigungsverhältnisses erhoben wurden, für nichtbeschäftigungsbezogene Zwecke zu verwenden, wie z. B. für Marketingkommunikation, muss die US-Organisation den betroffenen Personen zuvor die erforderliche Wahlmöglichkeit einräumen, es sei denn, sie haben die Verwendung der Daten für solche Zwecke bereits genehmigt. Eine solche Verwendung darf nicht mit den Zwecken unvereinbar sein, für die die personenbezogenen Daten erhoben oder von der betroffenen Person nachträglich genehmigt wurden. Darüber hinaus dürfen solche Entscheidungen nicht dazu verwendet werden, Beschäftigungsmöglichkeiten einzuschränken oder Strafmaßnahmen gegen die betreffenden Mitarbeiter zu ergreifen.

ii. Es ist zu beachten, dass bestimmte allgemein gültige Bedingungen für die Übermittlung aus einigen EU-Mitgliedstaaten eine andere Verwendung solcher Informationen auch nach der Übermittlung außerhalb der EU ausschließen können und dass diese Bedingungen eingehalten werden müssen.

iii. Darüber hinaus sollten die Arbeitgeber angemessene Anstrengungen unternehmen, um den Wünschen der Arbeitnehmer in Bezug auf den Schutz der Privatsphäre Rechnung zu tragen. Dies könnte Folgendes beinhalten,

zum Beispiel den Zugang zu den personenbezogenen Daten einschränken, bestimmte Daten anonymisieren oder Codes oder Pseudonyme vergeben, wenn die tatsächlichen Namen für den jeweiligen Verwaltungszweck nicht erforderlich sind.

iv. In dem Umfang und für den Zeitraum, der erforderlich ist, um die Fähigkeit der Organisation, Beförderungen, Ernennungen oder andere ähnliche Beschäftigungsentscheidungen zu treffen, nicht zu beeinträchtigen, muss eine Organisation keine Ankündigung und Wahlmöglichkeit anbieten.

c. Anwendung des Grundsatzes des Zugangs

i. Der ergänzende Grundsatz über den Zugang zu Daten enthält Hinweise auf Gründe, die eine Verweigerung oder Einschränkung des Zugangs auf Anfrage im Zusammenhang mit der Personalverwaltung rechtfertigen können. Natürlich müssen Arbeitgeber in der EU die lokalen Vorschriften einhalten und sicherstellen, dass EU-Beschäftigte unabhängig vom Ort der Datenverarbeitung und -speicherung Zugang zu den Informationen haben, die in ihrem Heimatland gesetzlich vorgeschrieben sind. Die EU-US-DSGVO verlangt, dass eine Organisation, die solche Daten in den Vereinigten Staaten verarbeitet, bei der Gewährung dieses Zugangs entweder direkt oder über den EU-Arbeitgeber kooperiert.

d. Vollstreckung

i. Sofern personenbezogene Daten nur im Rahmen des Beschäftigungsverhältnisses verwendet werden, bleibt die Hauptverantwortung für die Daten gegenüber dem Arbeitnehmer bei der Organisation in der EU. Daraus folgt, dass europäische Arbeitnehmer, die sich über die Verletzung ihrer Datenschutzrechte beschweren und mit den Ergebnissen interner Überprüfungs-, Beschwerde- und Einspruchsverfahren (oder etwaiger Beschwerdeverfahren im Rahmen eines Vertrags mit einer Gewerkschaft) nicht zufrieden sind, sich an die staatliche oder nationale Datenschutz- oder Arbeitsbehörde in dem Land wenden sollten, in dem die Arbeitnehmer arbeiten. Dies gilt auch für Fälle, in denen die US-Organisation, die die Informationen vom Arbeitgeber erhalten hat, für den mutmaßlich falschen Umgang mit ihren personenbezogenen Daten verantwortlich ist und somit ein mutmaßlicher Verstoß gegen die Grundsätze vorliegt. Dies ist der effizienteste Weg, um die sich häufig überschneidenden Rechte und Pflichten zu regeln, die sich aus dem lokalen Arbeitsrecht und den Arbeitsverträgen sowie aus dem Datenschutzrecht ergeben.

ii. Eine an der EU-US-DSGVO teilnehmende US-Organisation, die im Rahmen des Beschäftigungsverhältnisses aus der EU übermittelte EU-Personaldaten verwendet und möchte, dass solche Übermittlungen von der EU-US-DSGVO erfasst werden, muss sich daher verpflichten, bei Untersuchungen der zuständigen EU-Behörden mitzuwirken und deren Ratschläge in solchen Fällen zu befolgen.

e. Anwendung des Grundsatzes der Rechenschaftspflicht bei Weitergabe

i. Für gelegentliche beschäftigungsbezogene betriebliche Erfordernisse der teilnehmenden Organisation in Bezug auf

personenbezogene Daten, die im Rahmen der EU-US-DSGVO übermittelt werden, wie z. B. die Buchung eines Flugs, eines Hotelzimmers oder eines Versicherungsschutzes, können Übermittlungen personenbezogener Daten einer kleinen Anzahl von Mitarbeitern an für die Verarbeitung Verantwortliche erfolgen, ohne dass der Grundsatz des Zugangs oder der Abschluss eines Vertrags mit dem dritten für die Verarbeitung Verantwortlichen zur Anwendung kommt, wie es sonst nach dem Grundsatz der Rechenschaftspflicht bei der Weiterübermittlung erforderlich wäre, vorausgesetzt, die teilnehmende Organisation hat die Grundsätze der Benachrichtigung und der Wahlmöglichkeit beachtet.

## 10. Obligatorische Verträge für die Weitergabe

a. Verträge zur Datenverarbeitung

i. Wenn personenbezogene Daten aus der EU in die Vereinigten Staaten nur zum Zwecke der Verarbeitung übermittelt werden, ist ein Vertrag erforderlich, unabhängig von der Teilnahme des Auftragsverarbeiters an der EU-US-DSGVO.

ii. Für die Verarbeitung Verantwortliche in der EU müssen immer einen Vertrag abschließen, wenn eine Übermittlung zur reinen Verarbeitung erfolgt, unabhängig davon, ob die Verarbeitung innerhalb oder außerhalb der EU stattfindet und ob der Auftragsverarbeiter an der EU-US-DSGVO beteiligt ist oder nicht. Zweck des Vertrags ist es, sicherzustellen, dass der Auftragsverarbeiter:

1. handelt nur auf Anweisung des Controllers;

2. geeignete technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten vor zufälliger oder unrechtmäßiger Zerstörung oder zufälligem Verlust, Änderung, unberechtigter Weitergabe oder unberechtigtem Zugriff vorsieht und weiß, ob eine Weitergabe zulässig ist; und

3. unter Berücksichtigung der Art der Verarbeitung den für die Verarbeitung Verantwortlichen dabei unterstützt, Personen, die ihre Rechte gemäß den Grundsätzen ausüben, zu antworten.

iii. Da ein angemessener Schutz durch die teilnehmenden Organisationen gewährleistet ist, ist für Verträge mit diesen Organisationen über die reine Verarbeitung keine vorherige Genehmigung erforderlich.

b. Übertragungen innerhalb einer kontrollierten Gruppe von Unternehmen oder Körperschaften

i. Wenn personenbezogene Daten zwischen zwei für die Verarbeitung Verantwortlichen innerhalb einer kontrollierten Gruppe von Unternehmen oder Einrichtungen übermittelt werden, ist nach dem Grundsatz der Rechenschaftspflicht bei der Weiterübermittlung nicht immer ein Vertrag erforderlich. Für die Verarbeitung Verantwortliche innerhalb einer kontrollierten Gruppe von Unternehmen oder Einrichtungen können sich bei solchen Übermittlungen auf andere Instrumente stützen, z. B. auf verbindliche EU-Unternehmensregeln oder andere konzerninterne Instrumente (z. *B*. Programme zur Einhaltung von Vorschriften und zur Kontrolle), die die Kontinuität des Schutzes personenbezogener Daten gemäß den Grundsätzen gewährleisten. Im Falle solcher Übermittlungen bleibt die beteiligte Organisation für die Einhaltung der Grundsätze verantwortlich.

c. Übertragungen zwischen Controllern

i. Bei Übermittlungen zwischen für die Verarbeitung Verantwortlichen muss der empfangende für die Verarbeitung Verantwortliche weder eine teilnehmende Organisation sein noch über einen unabhängigen Rückgriffsmechanismus verfügen. Die teilnehmende Organisation muss einen Vertrag mit dem dritten für

die Verarbeitung Verantwortlichen im Empfängerland abschließen, der dasselbe Schutzniveau bietet wie die EU-US-DSGVO, mit Ausnahme der Anforderung, dass der dritte für die Verarbeitung Verantwortliche eine teilnehmende Organisation sein oder über einen unabhängigen Rückgriffsmechanismus verfügen muss, sofern er einen gleichwertigen Mechanismus zur Verfügung stellt.

## 11. Streitbeilegung und Vollstreckung

a. Das Prinzip des Rückgriffs, der Durchsetzung und der Haftung legt die Anforderungen für die Durchsetzung derEU-U.S. DPFfest. Wieman die

Die Anforderungen von Buchstabe a Ziffer ii des Grundsatzes sind in dem ergänzenden Grundsatz zur Verifizierung festgelegt. Dieser ergänzende Grundsatz befasst sich mit den Punkten (a)(i) und (a)(iii), die beide unabhängige Rückgriffsmechanismen erfordern. Diese Mechanismen können unterschiedliche Formen annehmen, müssen aber den Anforderungen des Grundsatzes für Rückgriff, Durchsetzung und Haftung entsprechen. Organisationen erfüllen die Anforderungen wie folgt: (i) Einhaltung privatwirtschaftlich entwickelter Datenschutzprogramme, die die Grundsätze in ihre Regeln aufnehmen und wirksame Durchsetzungsmechanismen der im Grundsatz des Rückgriffs, der Durchsetzung und der Haftung beschriebenen Art umfassen; (ii) Einhaltung gesetzlicher oder behördlicher Aufsichtsbehörden, die die Bearbeitung individueller Beschwerden und die Beilegung von Streitigkeiten vorsehen; oder (iii) Verpflichtung zur Zusammenarbeit mit den Datenschutzbehörden in der EU oder ihren bevollmächtigten Vertretern.

b. Diese Liste dient der Veranschaulichung und ist nicht einschränkend. Der Privatsektor kann zusätzliche Durchsetzungsmechanismen entwickeln, sofern sie die Anforderungen des Grundsatzes des Rückgriffs, der Durchsetzung und der Haftung sowie der ergänzenden Grundsätze erfüllen. Bitte beachten Sie, dass die Anforderungen des Regress-, Durchsetzungs- und Haftungsprinzips zusätzlich zu der Anforderung gelten, dass Selbstregulierungsbemühungen gemäß Abschnitt 5 des FTC Act (15 U.S.C. § 45), der unlautere oder irreführende Handlungen verbietet, durchsetzbar sein müssen. 49
U.S.C. § 41712, der es einem Luftfahrtunternehmen oder einem Flugscheinvermittler verbietet, sich an unlauteren oder irreführenden Praktiken im Luftverkehr oder beim Verkauf von Luftverkehrsleistungen zu beteiligen, oder ein anderes Gesetz oder eine andere Verordnung, die solche Handlungen verbietet.

c. Um die Einhaltung ihrer Verpflichtungen im Rahmen der EU-US-DSGVO zu gewährleisten und die Verwaltung des Programms zu unterstützen, müssen die Organisationen sowie ihre unabhängigen Regressmechanismen auf Anfrage des Ministeriums Informationen über die EU-US-DSGVO zur Verfügung stellen. Darüber hinaus müssen die Organisationen zügig auf Beschwerden bezüglich der Einhaltung der Grundsätze reagieren, die von den Datenschutzbehörden über das Ministerium eingereicht werden. In der Antwort sollte darauf eingegangen werden, ob die Beschwerde begründet ist und, falls ja, wie die Organisation das Problem beheben wird. Das Ministerium wird die Vertraulichkeit der Informationen, die es erhält, in Übereinstimmung mit dem US-Recht schützen.

d. <u>Rückgriffsmechanismen</u>

i. Einzelpersonen sollten ermutigt werden, ihre Beschwerden bei der zuständigen Organisation vorzubringen, bevor sie sich an unabhängige Rechtsmittel wenden. Die Organisationen müssen einer Person innerhalb von 45 Tagen nach Eingang einer Beschwerde antworten. Ob ein Regressmechanismus unabhängig ist, ist eine Tatsachenfrage, die insbesondere durch Unparteilichkeit, transparente Zusammensetzung und Finanzierung sowie eine nachgewiesene Erfolgsbilanz nachgewiesen werden kann. Wie im Grundsatz zu Rechtsbehelfen, Durchsetzung und Haftung gefordert, müssen die Rechtsbehelfe, die Einzelpersonen zur Verfügung stehen, leicht zugänglich und

für Einzelpersonen kostenlos sein. Unabhängige Streitbeilegungsstellen sollten jede Beschwerde von Einzelpersonen prüfen, es sei denn, sie ist offensichtlich unbegründet oder unseriös. Dies schließt nicht aus, dass die unabhängige Streitbeilegungsstelle, die den Rechtsbehelfsmechanismus betreibt, Anforderungen an die Eignung aufstellt, doch sollten solche Anforderungen transparent und gerechtfertigt sein (z. B. um Beschwerden auszuschließen, die nicht in den Anwendungsbereich des Programms fallen oder in einem anderen Forum zu behandeln sind), und sie sollten nicht dazu führen, dass die Verpflichtung, berechtigte Beschwerden zu prüfen, untergraben wird. Darüber hinaus sollten die Beschwerdemechanismen dem Einzelnen folgende Möglichkeiten bieten

vollständige und leicht zugängliche Informationen darüber, wie das Streitbeilegungsverfahren funktioniert, wenn sie eine Beschwerde einreichen. Diese Informationen sollten einen Hinweis auf die Datenschutzpraktiken des Verfahrens im Einklang mit den Grundsätzen enthalten. Sie sollten auch bei der Entwicklung von Instrumenten wie z. B. Standard-Beschwerdeformularen zusammenarbeiten, um das Beschwerdeverfahren zu erleichtern.

ii. Unabhängige Rückgriffsmechanismen müssen auf ihren öffentlichen Websites Informationen über die Grundsätze und die Dienstleistungen, die sie im Rahmen der EU-US-DSGVO erbringen, bereitstellen. Diese Informationen müssen Folgendes umfassen: (1) Informationen über oder einen Link zu den Anforderungen der Grundsätze an unabhängige Rechtsbehelfsmechanismen; (2) einen Link zur Website des Ministeriums für den Datenschutz; (3) eine Erklärung, dass ihre Streitbeilegungsdienste im Rahmen der EU-US-DSGVO für Einzelpersonen kostenlos sind; (4) eine Beschreibung, wie eine Beschwerde im Zusammenhang mit den Grundsätzen eingereicht werden kann; (5) den Zeitrahmen, in dem Beschwerden im Zusammenhang mit den Grundsätzen bearbeitet werden; und (6) eine Beschreibung des Spektrums an möglichen Rechtsbehelfen.

iii. Unabhängige Streitbeilegungsmechanismen müssen einen Jahresbericht mit aggregierten Statistiken über ihre Streitbeilegungsdienste veröffentlichen. Der Jahresbericht muss Folgendes enthalten: (1) die Gesamtzahl der im Berichtsjahr eingegangenen Beschwerden im Zusammenhang mit den Grundsätzen;
(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 Anhang I dargelegt, steht einer Einzelperson die Möglichkeit eines Schiedsverfahrens zur Verfügung, um bei verbleibenden Ansprüchen festzustellen, ob eine teilnehmende Organisation ihre Verpflichtungen aus den Grundsätzen in Bezug auf diese Person verletzt hat und ob eine solche Verletzung ganz oder teilweise nicht behoben wurde. Diese Option ist nur für diese Zwecke verfügbar. Diese Option steht beispielsweise nicht in Bezug auf die Ausnahmen von den Grundsätzen[15] oder in Bezug auf eine Behauptung über die Angemessenheit der DPF EU-USA zur Verfügung. Im Rahmen dieser Schlichtungsoption ist das "EU-U.S. Data Privacy Framework Panel" (bestehend aus einem oder drei Schiedsrichtern, je nach Vereinbarung der Parteien) befugt, personenbezogene, nicht monetäre Billigkeitsmaßnahmen (wie Zugang, Berichtigung, Löschung oder Rückgabe der betreffenden personenbezogenen Daten) zu verhängen, die erforderlich sind, um die Verletzung der Grundsätze nur in Bezug auf die betreffende Person zu beheben. Einzelpersonen und teilnehmende Organisationen können die gerichtliche Überprüfung und Vollstreckung der Schiedsentscheidungen nach US-Recht gemäß dem Federal Arbitration Act beantragen.

e. <u>Rechtsbehelfe und Sanktionen</u>

i. Die von der unabhängigen Streitbeilegungsstelle getroffenen Abhilfemaßnahmen sollten dazu führen, dass die Auswirkungen der Nichteinhaltung von der Organisation rückgängig gemacht oder korrigiert werden, soweit dies möglich ist, und dass die künftige Verarbeitung durch die Organisation im Einklang mit den Grundsätzen erfolgt und gegebenenfalls die Verarbeitung der personenbezogenen Daten der Person, die die Beschwerde eingereicht hat, eingestellt wird

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

aufhören. Die Sanktionen müssen streng genug sein, um die Einhaltung der Grundsätze durch die Organisation zu gewährleisten. Eine Reihe von unterschiedlich strengen Sanktionen ermöglicht es den Streitbeilegungsstellen, auf unterschiedliche Grade der Nichteinhaltung angemessen zu reagieren. Zu den Sanktionen sollten sowohl die öffentliche Bekanntmachung von Verstößen als auch die Verpflichtung gehören, unter bestimmten Umständen Daten zu löschen.[16] Weitere Sanktionen könnten die Aussetzung und der Entzug eines Siegels, die Entschädigung von Einzelpersonen für Verluste infolge der Nichteinhaltung und Unterlassungsurteile sein. Unabhängige Streitbeilegungsstellen des Privatsektors und Selbstregulierungsgremien müssen der zuständigen Regierungsstelle bzw. den Gerichten und dem Ministerium mitteilen, wenn die teilnehmenden Organisationen ihren Entscheidungen nicht nachkommen.

f. FTC-Aktion

i. Die FTC hat sich verpflichtet, vorrangig Verweise auf die Nichteinhaltung der Grundsätze zu prüfen, die von (i) Selbstregulierungsgremien für den Datenschutz und anderen unabhängigen Streitbeilegungsgremien, (ii) EU-Mitgliedstaaten und (iii) dem Ministerium eingehen, um festzustellen, ob Abschnitt 5 des FTC-Gesetzes, der unlautere oder irreführende Handlungen oder Praktiken im Handel verbietet, verletzt wurde. Kommt die FTC zu dem Schluss, dass sie Grund zu der Annahme hat, dass gegen Abschnitt 5 verstoßen wurde, kann sie die Angelegenheit durch eine verwaltungsrechtliche Unterlassungsverfügung, die die beanstandeten Praktiken verbietet, oder durch Einreichung einer Klage bei einem Bundesbezirksgericht klären, die im Erfolgsfall zu einer entsprechenden bundesgerichtlichen Verfügung führen kann. Dies gilt auch für falsche Behauptungen über die Einhaltung der Grundsätze oder die Teilnahme an der EU-US-DSGVO durch Organisationen, die entweder nicht mehr auf der Datenschutz-Rahmenliste stehen oder sich gegenüber dem Ministerium nie selbst zertifiziert haben. Die FTC kann zivilrechtliche Strafen für Verstöße gegen eine verwaltungsrechtliche Unterlassungsanordnung erwirken und kann zivil- oder strafrechtliche Verachtung für Verstöße gegen eine bundesgerichtliche Anordnung geltend machen. Die FTC wird das Ministerium von allen derartigen Maßnahmen unterrichten, die sie ergreift. Das Department ermutigt andere Regierungsstellen, es über die endgültige Entscheidung solcher Verweisungen oder anderer Entscheidungen über die Einhaltung der Grundsätze zu informieren.

g. Anhaltende Nichteinhaltung der Vorschriften

i. Wenn eine Organisation die Grundsätze dauerhaft nicht einhält, ist sie nicht mehr berechtigt, die EU-US-DSGVO in Anspruch zu nehmen. Organisationen, die die Grundsätze dauerhaft nicht einhalten, werden vom Ministerium von der Datenschutzrahmenliste gestrichen und müssen die personenbezogenen Daten, die sie im Rahmen der EU-US-DSGVO erhalten haben, zurückgeben oder löschen.

ii. Eine dauerhafte Nichteinhaltung liegt vor, wenn eine Organisation, die sich gegenüber dem Ministerium selbst zertifiziert hat, sich weigert, einer endgültigen Entscheidung einer Selbstregulierungsstelle, einer unabhängigen Streitbeilegungsstelle oder einer Regierungsstelle Folge zu leisten, oder wenn eine solche Stelle, einschließlich des Ministeriums, feststellt, dass eine Organisation häufig gegen

[16] Es liegt im Ermessen der unabhängigen Schlichtungsstellen, unter welchen Umständen sie diese Sanktionen anwenden. Die Sensibilität der betreffenden Daten ist ein Faktor, der bei der Entscheidung, ob die Löschung von Daten verlangt werden sollte, zu berücksichtigen ist, ebenso wie die Frage, ob eine Organisation Informationen unter eklatantem Verstoß gegen die Grundsätze gesammelt, verwendet oder weitergegeben hat.

die Grundsätze so weit einhalten, dass ihre Behauptung, die Grundsätze einzuhalten, nicht mehr glaubwürdig ist. In Fällen, in denen eine solche Feststellung von einer anderen Stelle als dem Ministerium getroffen wird, muss die Organisation das Ministerium unverzüglich über diesen Sachverhalt informieren. Die Unterlassung dieser Mitteilung kann nach dem False Statements Act (18 U.S.C. § 1001) strafbar sein. Der Rückzug einer Organisation aus einem Selbstregulierungsprogramm des Privatsektors zum Schutz der Privatsphäre oder einem unabhängigen Streitbeilegungsmechanismus entbindet sie nicht von ihrer Verpflichtung zur Einhaltung der Grundsätze und würde eine anhaltende Nichteinhaltung darstellen.

iii. Das Ministerium wird eine Organisation von der Datenschutz-Rahmenliste streichen, wenn sie die Vorschriften dauerhaft nicht einhält, auch als Reaktion auf eine Mitteilung, die es von der Organisation selbst, einer Selbstregulierungsorganisation für den Datenschutz oder einer anderen unabhängigen Stelle zur Beilegung von Streitigkeiten oder einer Regierungsstelle erhält, jedoch erst, nachdem es die Organisation zuvor 30 Tage lang benachrichtigt und ihr Gelegenheit zur Stellungnahme gegeben hat[17] . Dementsprechend wird aus der vom Ministerium geführten Datenschutz-Rahmenliste deutlich hervorgehen, welchen Organisationen die Vorteile der EU-US-DSGVO zugesichert werden und welchen Organisationen sie nicht mehr zugesichert werden.

iv. Eine Organisation, die die Teilnahme an einem Selbstregulierungsgremium zum Zwecke der erneuten Zulassung zur EPF EU-USA beantragt, muss diesem Gremium vollständige Informationen über ihre frühere Teilnahme an der EPF EU-USA übermitteln.
U.S. DPF.

**12. Wahlmöglichkeit - Zeitpunkt des Ausstiegs**

a. Im Allgemeinen soll der Grundsatz der Wahlfreiheit sicherstellen, dass personenbezogene Daten in einer Weise verwendet und offengelegt werden, die mit den Erwartungen und Entscheidungen des Einzelnen übereinstimmt. Dementsprechend sollte eine Person die Möglichkeit haben, die Verwendung personenbezogener Daten für Direktmarketing jederzeit abzulehnen, wobei die Organisation angemessene Grenzen setzen muss, wie z. B. eine Frist, um die Ablehnung wirksam werden zu lassen. Eine Organisation kann auch ausreichende Informationen verlangen, um die Identität der Person zu bestätigen, die das "Opt-out" beantragt. In den Vereinigten Staaten können Einzelpersonen diese Option durch ein zentrales "Opt-out"-Programm ausüben. In jedem Fall sollte der Einzelne einen leicht zugänglichen und erschwinglichen Mechanismus haben, um diese Option auszuüben.

b. Ebenso kann eine Organisation Informationen für bestimmte Direktmarketingzwecke verwenden, wenn es nicht möglich ist, der Person die Möglichkeit zu geben, sich vor der Verwendung der Informationen dagegen zu entscheiden, wenn die Organisation der Person gleichzeitig (und auf Anfrage jederzeit) die Möglichkeit gibt, den Erhalt weiterer Direktmarketingmitteilungen (ohne Kosten für die Person) abzulehnen, und die Organisation den Wünschen der Person nachkommt.

## 13. Reise-Informationen

a. Reservierungsdaten von Fluggästen und andere Reisedaten, wie z. B. Vielflieger- oder Hotelbuchungsdaten und Informationen über besondere Bedürfnisse, wie z. B. Mahlzeiten, die religiösen Anforderungen entsprechen, oder körperliche Unterstützung, können an Organisationen außerhalb der EU auf verschiedene Weise übermittelt werden

[17] Das Ministerium gibt in der Mitteilung die Frist an, die der Organisation für die Beantwortung der Mitteilung zur Verfügung steht und die in der Regel weniger als 30 Tage beträgt.

Umstände. 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 wenn 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 der EU-US-DSGVO angeschlossen haben, bieten einen angemessenen Schutz für personenbezogene Daten und können daher auf der Grundlage von Artikel 45 DSGVO Datenübermittlungen aus der EU entgegennehmen, ohne dass sie ein Übermittlungsinstrument gemäß Artikel 46 DSGVO einrichten oder die Bedingungen von Artikel 49 DSGVO erfüllen müssen. Da die EU-US-DSGVO besondere Vorschriften für sensible Informationen enthält, können solche Informationen (die beispielsweise im Zusammenhang mit dem Bedarf der Kunden an körperlicher Unterstützung erhoben werden müssen) in die Übermittlungen an die teilnehmenden Organisationen einbezogen werden. In allen Fällen muss die Organisation, die die Informationen übermittelt, jedoch die Gesetze des EU-Mitgliedstaates einhalten, in dem sie tätig ist, die *u. a.* besondere Bedingungen für den Umgang mit sensiblen Daten vorsehen können.

## 14. Pharmazeutische und medizinische Produkte

a. Anwendung der Gesetze der EU/Mitgliedstaaten oder der Grundsätze

i. Das Recht der EU/Mitgliedstaaten gilt für die Erhebung der personenbezogenen Daten und für jede Verarbeitung, die vor der Übermittlung in die Vereinigten Staaten stattfindet. Die Grundsätze gelten für die Daten, sobald sie in die Vereinigten Staaten übermittelt worden sind. Daten, die für die pharmazeutische Forschung und andere Zwecke verwendet werden, sollten gegebenenfalls anonymisiert werden.

b. Künftige wissenschaftliche Forschung

i. Personenbezogene Daten, die im Rahmen spezifischer medizinischer oder pharmazeutischer Forschungsstudien gewonnen wurden, spielen oft eine wertvolle Rolle für die künftige wissenschaftliche Forschung. Wenn personenbezogene Daten, die für eine Forschungsstudie erhoben wurden, an eine US-Organisation im Rahmen der EU-US-DSGVO weitergeleitet werden, kann die Organisation die Daten für eine neue wissenschaftliche Forschungsaktivität verwenden, wenn eine angemessene Benachrichtigung und Wahlmöglichkeit in der ersten Instanz gegeben wurde. Eine solche Mitteilung sollte Informationen über künftige spezifische Verwendungszwecke der Daten enthalten, z. B. regelmäßige Nachuntersuchungen, verwandte Studien oder Marketing.

ii. Es versteht sich, dass nicht alle künftigen Verwendungszwecke der Daten angegeben werden können, da sich ein neuer Forschungszweck aus neuen Erkenntnissen über die ursprünglichen Daten, neuen medizinischen Entdeckungen und Fortschritten sowie Entwicklungen im Bereich der öffentlichen Gesundheit und der Rechtsvorschriften ergeben könnte. Gegebenenfalls sollte die Mitteilung daher eine Erklärung enthalten, dass personenbezogene Daten in zukünftigen medizinischen und pharmazeutischen Forschungsaktivitäten verwendet werden können, die nicht vorhergesehen wurden. Steht

die Verwendung nicht im Einklang mit dem/den allgemeinen Forschungszweck(en), für den/die die personenbezogenen Daten ursprünglich erhoben wurden oder in den/die die betroffene Person nachträglich eingewilligt hat, muss eine neue Einwilligung eingeholt werden.

c. Rücktritt von einer klinischen Prüfung

i. Die Teilnehmer können jederzeit beschließen oder aufgefordert werden, aus einer klinischen Prüfung auszusteigen. Alle personenbezogenen Daten, die vor dem Rücktritt erhoben wurden, können weiterhin zusammen mit anderen erhobenen Daten verarbeitet werden

als Teil der klinischen Prüfung, wenn dies dem Teilnehmer bei seiner Zustimmung zur Teilnahme in der Mitteilung deutlich gemacht wurde.

d. Übertragungen für Regulierungs- und Aufsichtszwecke

i. Unternehmen der Pharma- und Medizintechnikbranche dürfen personenbezogene Daten aus klinischen Prüfungen, die in der EU durchgeführt werden, an Aufsichtsbehörden in den Vereinigten Staaten zum Zwecke der Regulierung und Überwachung übermitteln. Ähnliche Übermittlungen sind im Einklang mit den Grundsätzen der Benachrichtigung und der Wahlmöglichkeit auch an andere Parteien als die Aufsichtsbehörden erlaubt, z. B. an Unternehmensstandorte und andere Forscher.

e. "Verblendete" Studien

i. Um die Objektivität vieler klinischer Studien zu gewährleisten, dürfen die Teilnehmer und häufig auch die Prüfer keinen Zugang zu Informationen darüber erhalten, welche Behandlung die einzelnen Teilnehmer erhalten. Dies würde die Gültigkeit der Forschungsstudie und der Ergebnisse gefährden. Teilnehmer an solchen klinischen Prüfungen (so genannte "verblindete" Studien) müssen keinen Zugang zu den Daten über ihre Behandlung während der Prüfung erhalten, wenn diese Einschränkung bei der Aufnahme des Teilnehmers in die Prüfung erklärt wurde und die Offenlegung solcher Informationen die Integrität der Forschungsbemühungen gefährden würde.

ii. Die Zustimmung zur Teilnahme an der Prüfung unter diesen Bedingungen ist ein angemessener Verzicht auf das Recht auf Auskunft. Nach Abschluss der Prüfung und Auswertung der Ergebnisse sollten die Teilnehmer auf Wunsch Zugang zu ihren Daten erhalten. Sie sollten sich in erster Linie an den Arzt oder einen anderen Leistungserbringer des Gesundheitswesens wenden, von dem sie im Rahmen der klinischen Prüfung behandelt wurden, oder in zweiter Linie an die Sponsororganisation.

f. Überwachung der Produktsicherheit und -wirksamkeit

i. Ein Pharma- oder Medizinprodukteunternehmen muss die Grundsätze in Bezug auf die Grundsätze "Mitteilung", "Wahlmöglichkeit", "Rechenschaftspflicht bei Weitergabe" und "Zugang" bei seinen Aktivitäten zur Überwachung der Produktsicherheit und -wirksamkeit, einschließlich der Meldung von unerwünschten Ereignissen und der Nachverfolgung von Patienten/Probanden, die bestimmte Arzneimittel oder Medizinprodukte verwenden, nicht anwenden, soweit die Einhaltung der Grundsätze mit der Einhaltung gesetzlicher Vorschriften kollidiert. Dies gilt sowohl für Berichte von Gesundheitsdienstleistern an Pharma- und Medizinprodukteunternehmen als auch für Berichte von Pharma- und Medizinprodukteunternehmen an Regierungsbehörden wie die Food and Drug Administration.

g. Schlüsselcodierte Daten

i. In der Regel werden die Forschungsdaten bei ihrer Entstehung vom Hauptforscher mit einem eindeutigen Schlüssel versehen, um die Identität der einzelnen Probanden nicht preiszugeben. Pharmazeutische Unternehmen, die diese Forschung sponsern,

erhalten den Schlüssel nicht. Der eindeutige Schlüsselcode befindet sich nur im Besitz des Forschers, so dass er die Versuchsperson unter besonderen Umständen identifizieren kann (z. *B.* wenn eine weitere medizinische Behandlung erforderlich ist). Eine Übermittlung derart kodierter Daten aus der EU in die Vereinigten Staaten, die nach EU-Recht personenbezogene Daten sind, würde unter die Grundsätze fallen.

## 15. Öffentliche Aufzeichnungen und öffentlich zugängliche Informationen

a. Eine Organisation muss die Grundsätze der Sicherheit, der Datenintegrität und Zweckbindung sowie des Rückgriffs, der Durchsetzung und der Haftung auf personenbezogene Daten aus öffentlich zugänglichen Quellen anwenden. Diese Grundsätze gelten auch für personenbezogene Daten, die aus öffentlichen Aufzeichnungen erhoben werden (*d. h.* Aufzeichnungen, die von staatlichen Behörden oder Einrichtungen auf jeder Ebene geführt werden und die von der Öffentlichkeit eingesehen werden können).

b. Es ist nicht erforderlich, die Grundsätze der Benachrichtigung, Auswahl oder Rechenschaftspflicht bei der Weitergabe auf öffentlich zugängliche Informationen anzuwenden, solange diese nicht mit nicht öffentlich zugänglichen Informationen kombiniert werden und alle von der jeweiligen Rechtsordnung festgelegten Bedingungen für die Konsultation eingehalten werden. Auch ist es in der Regel nicht erforderlich, die Grundsätze der Benachrichtigung, Auswahl oder Rechenschaftspflicht bei der Weitergabe auf öffentlich zugängliche Informationen anzuwenden, es sei denn, der europäische Übermittler gibt an, dass diese Informationen Beschränkungen unterliegen, die die Anwendung dieser Grundsätze durch die Organisation für die von ihr beabsichtigten Verwendungszwecke erfordern. Die Organisationen haften nicht dafür, wie solche Informationen von denjenigen verwendet werden, die diese Informationen aus veröffentlichten Materialien erhalten.

c. Stellt sich heraus, dass eine Organisation personenbezogene Daten absichtlich unter Verstoß gegen die Grundsätze veröffentlicht hat, damit sie oder andere von diesen Ausnahmen profitieren können, kann sie die Vorteile der EU-US-DSGVO nicht mehr in Anspruch nehmen.

d. Es ist nicht notwendig, den Grundsatz des Zugangs auf Informationen aus öffentlichen Aufzeichnungen anzuwenden, solange diese nicht mit anderen personenbezogenen Informationen kombiniert werden (abgesehen von geringen Mengen, die zur Indexierung oder Organisation der Informationen aus öffentlichen Aufzeichnungen verwendet werden); allerdings sind alle von der jeweiligen Rechtsprechung festgelegten Bedingungen für die Einsichtnahme zu beachten. Werden dagegen Informationen aus öffentlichen Aufzeichnungen mit anderen nicht öffentlichen Informationen kombiniert (mit Ausnahme der oben genannten), muss eine Organisation Zugang zu all diesen Informationen gewähren, sofern sie nicht anderen zulässigen Ausnahmen unterliegen.

e. Wie bei Informationen aus öffentlichen Aufzeichnungen ist es nicht erforderlich, Zugang zu Informationen zu gewähren, die der breiten Öffentlichkeit bereits zugänglich sind, solange sie nicht mit nicht öffentlich zugänglichen Informationen kombiniert werden. Organisationen, die öffentlich zugängliche Informationen verkaufen, können für die Beantwortung von Anträgen auf Zugang zu diesen Informationen die übliche Gebühr erheben. Alternativ können Einzelpersonen den Zugang zu ihren Informationen bei der Organisation beantragen, die die Daten ursprünglich zusammengestellt hat.

## 16. Zugangsanträge von Behörden

a. Um Transparenz in Bezug auf rechtmäßige Anträge von Behörden auf Zugang zu personenbezogenen Daten zu schaffen, können die teilnehmenden Organisationen freiwillig regelmäßige Transparenzberichte über die Anzahl der Anträge auf Zugang zu

personenbezogenen Daten herausgeben, die sie von Behörden aus Gründen der Strafverfolgung oder der nationalen Sicherheit erhalten, soweit eine solche Offenlegung nach geltendem Recht zulässig ist.

b. Die von den teilnehmenden Organisationen in diesen Berichten zur Verfügung gestellten Informationen können zusammen mit den von den Nachrichtendiensten freigegebenen Informationen und anderen Informationen zur Information der Öffentlichkeit genutzt werden.

regelmäßige gemeinsame Überprüfung der Funktionsweise der EU-US-DPF im Einklang mit den Grundsätzen.

c. Das Fehlen einer Benachrichtigung gemäß Buchstabe a) Ziffer xii) des Benachrichtigungsgrundsatzes darf eine Organisation nicht daran hindern oder ihre Fähigkeit beeinträchtigen, auf rechtmäßige Anfragen zu reagieren.

## ANHANG I: ARBITRALES MODELL

Dieser Anhang I enthält die Bedingungen, unter denen die an der EU-US-DSGVO teilnehmenden Organisationen gemäß dem Rückgriffs-, Durchsetzungs- und Haftungsgrundsatz zur Schlichtung von Ansprüchen verpflichtet sind. Die nachstehend beschriebene Option der verbindlichen Schlichtung gilt für bestimmte "Restansprüche" in Bezug auf Daten, die unter die EU-US-DSGVO fallen. Der Zweck dieser Option besteht darin, einen raschen, unabhängigen und fairen Mechanismus zu schaffen, der den Betroffenen die Möglichkeit bietet, behauptete Verstöße gegen die Grundsätze zu klären, die nicht durch einen der anderen Mechanismen der EU-US-DSGVO gelöst werden können.

### A. Umfang

Diese Schlichtungsmöglichkeit steht einer Einzelperson zur Verfügung, um bei verbleibenden Ansprüchen festzustellen, ob eine teilnehmende Organisation ihre Verpflichtungen aus den Grundsätzen gegenüber dieser Person verletzt hat und ob eine solche Verletzung ganz oder teilweise nicht behoben wurde. Diese Option ist nur für diese Zwecke verfügbar. Diese Möglichkeit besteht zum Beispiel nicht in Bezug auf die Ausnahmen von den Grundsätzen[18] oder in Bezug auf eine Behauptung über die Angemessenheit der EU-US-DSGVO.

### B. Verfügbare Abhilfemaßnahmen

Bei dieser Schlichtungsoption ist das "EU-U.S. Data Privacy Framework Panel" (das Schiedsgericht, das je nach Vereinbarung der Parteien aus einem oder drei Schiedsrichtern besteht) befugt, personenbezogene, nicht monetäre Abhilfemaßnahmen (wie Zugang, Berichtigung, Löschung oder Rückgabe der betreffenden personenbezogenen Daten) zu verhängen, die erforderlich sind, um die Verletzung der Grundsätze nur in Bezug auf die betreffende Person zu beheben. Dies sind die einzigen Befugnisse des EU-US-Datenschutzgremiums in Bezug auf Rechtsbehelfe. Bei der Erwägung von Abhilfemaßnahmen ist das EU-US-Datenschutzgremium verpflichtet, andere Abhilfemaßnahmen zu berücksichtigen, die bereits durch andere Mechanismen im Rahmen der EU-US-Datenschutz-Grundverordnung auferlegt wurden. Schadenersatz, Kosten, Gebühren oder andere Abhilfemaßnahmen sind nicht vorgesehen.
verfügbar. Jede Partei trägt ihre eigenen Anwaltskosten.

### C. Anforderungen vor der Schlichtung

Eine Person, die sich für die Inanspruchnahme dieser Schlichtungsmöglichkeit entscheidet, muss folgende Schritte unternehmen, bevor sie ein Schiedsverfahren einleitet: (1) den behaupteten Verstoß direkt bei der Organisation zur Sprache bringen und der Organisation Gelegenheit geben, die Angelegenheit innerhalb des in Abschnitt (d)(i) des Ergänzenden Grundsatzes zur Streitbeilegung und Durchsetzung festgelegten Zeitrahmens zu klären; (2) den unabhängigen Rechtsbehelfsmechanismus gemäß den Grundsätzen in Anspruch nehmen, ohne dass der Einzelperson Kosten entstehen; (3) die Angelegenheit über das DPA der betreffenden Person an das Ministerium herantragen und dem Ministerium Gelegenheit geben, sich nach besten Kräften zu bemühen, die Angelegenheit innerhalb des im Schreiben der Internationalen Handelsbehörde des Ministeriums genannten Zeitrahmens zu lösen, ohne dass der betreffenden Person Kosten entstehen.

Diese Schlichtungsmöglichkeit kann nicht in Anspruch genommen werden, wenn derselbe von der betroffenen Person behauptete Verstoß gegen die Grundsätze (1) zuvor Gegenstand eines verbindlichen Schiedsverfahrens war, (2) Gegenstand eines rechtskräftigen Urteils in einem Gerichtsverfahren war, an dem die betroffene Person beteiligt war, oder (3) zuvor von den Parteien beigelegt wurde. Darüber hinaus kann diese Option nicht in Anspruch genommen

werden, wenn eine Datenschutzbehörde (1) gemäß dem ergänzenden Grundsatz zur Rolle der Datenschutzbehörden oder dem ergänzenden Grundsatz zu Personaldaten befugt ist oder (2) befugt ist, den behaupteten Verstoß direkt mit der Organisation zu klären. Die Befugnis einer Datenschutzbehörde, dieselbe Forderung gegenüber einem für die Verarbeitung Verantwortlichen in der EU zu klären, schließt die Inanspruchnahme dieser Schlichtungsmöglichkeit gegenüber einer anderen juristischen Person, die nicht an die Befugnis der Datenschutzbehörde gebunden ist, nicht aus.

[18] Die Grundsätze, Überblick, Absatz. 5.

## D. Verbindlichkeit der Beschlüsse

Die Inanspruchnahme dieser verbindlichen Schlichtungsmöglichkeit ist völlig freiwillig. Die Entscheidungen des Schiedsgerichts sind für alle Parteien verbindlich. Nach Inanspruchnahme des Schiedsverfahrens verzichtet die Person auf die Möglichkeit, in einem anderen Forum Abhilfe für denselben behaupteten Verstoß zu suchen, es sei denn, dass
Wenn die geltend gemachte Rechtsverletzung nicht vollständig beseitigt werden kann, schließt die Anrufung eines Schiedsgerichts einen Schadensersatzanspruch, der ansonsten vor Gericht geltend gemacht werden kann, nicht aus.

## E. Überprüfung und Durchsetzung

Einzelpersonen und teilnehmende Organisationen können die gerichtliche Überprüfung und Vollstreckung der Schiedsentscheidungen nach US-Recht gemäß dem Federal Arbitration Act beantragen.[19] Solche Fälle müssen bei dem Bundesbezirksgericht eingereicht werden, in dessen Zuständigkeitsbereich sich der Hauptgeschäftssitz der teilnehmenden Organisation befindet.

Diese Schlichtungsmöglichkeit dient der Beilegung individueller Streitigkeiten, und die Entscheidungen des Schiedsgerichts sind nicht dazu bestimmt, als überzeugender oder bindender Präzedenzfall in Angelegenheiten zu fungieren, an denen andere Parteien beteiligt sind, auch nicht in künftigen Schlichtungsverfahren oder vor Gerichten der EU oder der USA oder in Verfahren der FTC.

## F. Die Schiedsinstanz

Die Parteien werden die Schiedsrichter für das EU-US-Datenschutz-Gremium aus der nachstehend aufgeführten Liste der Schiedsrichter auswählen.

Im Einklang mit dem geltenden Recht erstellen das Ministerium und die Kommission eine Liste von mindestens zehn Schiedsrichtern, die auf der Grundlage von Unabhängigkeit, Integrität und Fachwissen ausgewählt werden. Im Zusammenhang mit diesem Verfahren gelten die folgenden Bestimmungen:

Schlichter:

---

[19] Kapitel 2 des Federal Arbitration Act ("FAA") sieht vor, dass "eine Schiedsvereinbarung oder ein Schiedsspruch aus einem Rechtsverhältnis, ob vertraglich oder nicht, das als kommerziell angesehen wird, einschließlich einer in [Abschnitt 2 des FAA] beschriebenen Transaktion, eines Vertrags oder einer Vereinbarung, unter das Übereinkommen [über die Anerkennung und Vollstreckung ausländischer Schiedssprüche vom 10. Juni 1958, 21 U.S.T. 2519, T.I.A.S. Nr. 6997 ("New Yorker Übereinkommen")] fällt". 9 U.S.C. § 202. Das FAA sieht ferner vor, dass "eine Vereinbarung oder ein Schiedsspruch, die sich aus einer solchen Beziehung ergeben, die ausschließlich zwischen Bürgern der Vereinigten Staaten besteht, als nicht unter das [New Yorker] Übereinkommen fallend angesehen wird, es sei denn, diese Beziehung betrifft im Ausland belegenes Vermögen, sieht eine Erfüllung oder Vollstreckung im Ausland vor oder hat eine andere angemessene Beziehung zu einem oder mehreren ausländischen Staaten." *Id.* Nach Kapitel 2 "kann jede am Schiedsverfahren beteiligte Partei bei jedem nach diesem Kapitel zuständigen Gericht einen Beschluss zur Bestätigung des Schiedsspruchs gegenüber jeder anderen am Schiedsverfahren beteiligten Partei beantragen. Das Gericht bestätigt den Schiedsspruch, es sei denn, es stellt einen der Gründe für die Versagung oder den Aufschub der Anerkennung oder Vollstreckung des Schiedsspruchs fest, die in dem genannten [New Yorker] Übereinkommen aufgeführt sind." *Id.* § 207. Kapitel 2 sieht ferner vor, dass "[d]ie Bezirksgerichte der Vereinigten Staaten . . die ursprüngliche Zuständigkeit für ... eine Klage oder ein Verfahren [nach dem New Yorker Übereinkommen] haben, unabhängig von der Höhe des Streitwerts". *Id.* § 203.

Kapitel 2 sieht außerdem vor, dass "Kapitel 1 auf Klagen und Verfahren nach diesem Kapitel Anwendung findet, soweit dieses Kapitel nicht im Widerspruch zu diesem Kapitel oder dem von den Vereinigten Staaten ratifizierten [New Yorker] Übereinkommen steht". *Id.* §
208. Kapitel 1 sieht wiederum vor, dass "[eine] schriftliche Bestimmung in ... einem Vertrag über ein Handelsgeschäft, wonach eine Streitigkeit, die sich später aus einem solchen Vertrag oder Geschäft ergibt, oder die

Weigerung, diesen Vertrag oder dieses Geschäft ganz oder teilweise zu erfüllen, oder eine schriftliche Vereinbarung, eine bestehende Streitigkeit, die sich aus einem solchen Vertrag, Geschäft oder einer Weigerung ergibt, einem Schiedsverfahren zu unterwerfen, gültig, unwiderruflich und vollstreckbar ist, es sei denn, es liegen gesetzliche oder billigkeitsrechtliche Gründe für die Aufhebung eines Vertrags vor". *Id.* § 2. Kapitel 1 sieht ferner vor, dass "jede an dem Schiedsverfahren beteiligte Partei bei dem so bezeichneten Gericht eine Anordnung zur Bestätigung des Schiedsspruchs beantragen kann, woraufhin das Gericht einer solchen Anordnung zustimmen muss, sofern der Schiedsspruch nicht gemäß den Abschnitten 10 und 11 [des FAA] aufgehoben, geändert oder berichtigt wird". *Id.* § 9.

(1) verbleiben für einen Zeitraum von drei Jahren auf der Liste, es sei denn, es liegen außergewöhnliche Umstände oder eine Streichung aus wichtigem Grund vor, die vom Ministerium nach vorheriger Mitteilung an die Kommission um weitere drei Jahre verlängert werden kann;
(2) unterliegt keinen Weisungen einer der Parteien, einer teilnehmenden Organisation, der USA, der EU, eines EU-Mitgliedstaates oder einer anderen Regierungs-, Behörden- oder Vollzugsbehörde und ist auch nicht mit einer solchen verbunden; und
(3) müssen in den Vereinigten Staaten als Anwälte zugelassen sein und Experten für das US-Datenschutzrecht sein, die auch über Fachwissen im EU-Datenschutzrecht verfügen.

## G. Schiedsgerichtsverfahren

Das Ministerium und die Kommission haben sich im Einklang mit dem geltenden Recht auf die Annahme von Schiedsregeln geeinigt, die die Verfahren vor dem EU-US-Datenschutzgremium regeln.[20] Für den Fall, dass die für das Verfahren geltenden Regeln geändert werden müssen, werden das Ministerium und die Kommission vereinbaren, diese Regeln zu ändern oder eine andere Reihe bestehender, gut etablierter US-Schiedsverfahren anzunehmen, vorbehaltlich der folgenden Erwägungen:

1. Eine Einzelperson kann ein verbindliches Schiedsverfahren einleiten, indem sie der Organisation eine "Mitteilung" zukommen lässt, die den oben genannten Voraussetzungen für ein Schiedsverfahren entspricht. Die Mitteilung enthält eine Zusammenfassung der gemäß Absatz C unternommenen Schritte zur Klärung des Anspruchs, eine Beschreibung des mutmaßlichen Verstoßes und, nach Wahl der Person, alle unterstützenden Dokumente und Materialien und/oder eine Erörterung des Rechts im Zusammenhang mit dem mutmaßlichen Anspruch.
2. Es werden Verfahren entwickelt, die sicherstellen, dass eine Person, die denselben Verstoß geltend macht, keine doppelten Abhilfemaßnahmen oder Verfahren erhält.
3. Die FTC kann parallel zum Schiedsverfahren tätig werden.
4. Kein Vertreter der USA, der EU oder eines EU-Mitgliedstaates oder einer anderen Regierungsbehörde, öffentlichen Stelle oder Vollstreckungsbehörde darf an diesen Schiedsverfahren teilnehmen, vorausgesetzt, dass die Datenschutzbehörden auf Ersuchen einer EU-Person lediglich bei der Erstellung der Bekanntmachung behilflich sein können, jedoch keinen Zugang zur Offenlegung oder zu anderen Materialien im Zusammenhang mit diesen Schiedsverfahren haben.
5. Das Schiedsverfahren findet in den Vereinigten Staaten statt, und der Betroffene kann entweder per Video oder per Telefon teilnehmen, was für ihn kostenlos ist. Eine persönliche Teilnahme ist nicht erforderlich.

[20] Das Internationale Zentrum für Streitbeilegung ("IZRS"), die internationale Abteilung der American Arbitration Association ("AAA") (zusammen "IZRS-AAA"), wurde vom Ministerium ausgewählt, um Schiedsverfahren gemäß Anhang I der Grundsätze zu verwalten und den dort genannten Schiedsfonds zu führen. Am 15. September 2017 einigten sich das Ministerium und die Kommission auf die Annahme einer Schiedsgerichtsordnung zur Regelung der in Anhang I der Grundsätze beschriebenen verbindlichen Schiedsverfahren 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 kamen überein, die Schiedsgerichtsordnung und den Verhaltenskodex an die Aktualisierungen im Rahmen der EU-Schiedsgerichtsbarkeit anzupassen.
U.S. DPF, und das Ministerium wird mit der ICDR-AAA zusammenarbeiten, um diese Aktualisierungen vorzunehmen.

6. Die Sprache des Schiedsverfahrens ist Englisch, sofern die Parteien nichts anderes vereinbaren. Auf begründeten Antrag und unter Berücksichtigung der Tatsache, ob die betreffende Person durch einen Anwalt vertreten ist, werden ein Dolmetscher für die schiedsrichterliche Anhörung sowie eine Übersetzung der schiedsrichterlichen Unterlagen kostenlos zur Verfügung gestellt, es sei denn, das EU-US-Datenschutzgremium stellt fest, dass dies unter den Umständen des jeweiligen Schiedsverfahrens zu ungerechtfertigten oder unverhältnismäßigen Kosten führen würde.
7. Die den Schiedsrichtern vorgelegten Unterlagen werden vertraulich behandelt und nur im Zusammenhang mit dem Schiedsverfahren verwendet.
8. Falls erforderlich, kann eine individualisierte Offenlegung gestattet werden, die von den Parteien vertraulich behandelt und nur im Zusammenhang mit dem Schiedsverfahren verwendet wird.
9. Schlichtungen sollten innerhalb von 90 Tagen nach Zustellung der Mitteilung an die betreffende Organisation abgeschlossen werden, sofern die Parteien nichts anderes vereinbaren.

## H. Kosten

Die Schiedsrichter sollten angemessene Maßnahmen ergreifen, um die Kosten oder Gebühren für das Schiedsverfahren so gering wie möglich zu halten.

Das Ministerium wird im Einklang mit dem geltenden Recht die Aufrechterhaltung eines Fonds erleichtern, zu dem die teilnehmenden Organisationen Beiträge leisten müssen, die zum Teil von der Größe der Organisation abhängen und die die Kosten für das Schiedsverfahren, einschließlich der Gebühren für den Schiedsrichter, bis zu einem Höchstbetrag ("Obergrenzen") decken. Der Fonds wird von einer dritten Partei verwaltet, die dem Ministerium regelmäßig über die Tätigkeit des Fonds Bericht erstatten wird. Das Ministerium wird mit der dritten Partei zusammenarbeiten, um die Funktionsweise des Fonds regelmäßig zu überprüfen, einschließlich der Notwendigkeit, die Höhe der Beiträge oder die Obergrenzen für die Schiedsgerichtskosten anzupassen, und unter anderem die Anzahl der Schiedsverfahren sowie die Kosten und den Zeitplan der Schiedsverfahren berücksichtigen, wobei sichergestellt wird, dass den teilnehmenden Organisationen keine übermäßige finanzielle Belastung auferlegt wird. Das Ministerium unterrichtet die Kommission über das Ergebnis dieser Überprüfungen mit der dritten Partei und teilt der Kommission im Voraus etwaige Anpassungen der Beitragshöhe mit. Anwaltshonorare sind nicht durch diese Bestimmung oder einen Fonds im Rahmen dieser Bestimmung abgedeckt.

**ANHANG II**

**HANDELSMINISTERIUM DER VEREINIGTEN STAATEN**
**Handelsminister**
Washington, D.C. 20230

6. Juli 2023

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

Sehr geehrter Herr Kommissar Reynders:

Im Namen der Vereinigten Staaten freue ich mich, Ihnen hiermit ein Paket von Unterlagen zum Datenschutzrahmen zwischen der EU und den USA zu übermitteln, das in Verbindung mit der Durchführungsverordnung 14086 "Verbesserung der Garantien für die Aktivitäten der Vereinigten Staaten im Bereich der Signalnachrichtendienste" und 28 CFR Teil 201 zur Änderung der Vorschriften des Justizministeriums zur Einrichtung des "Datenschutzüberprüfungsgerichts" wichtige und detaillierte Verhandlungen zur Stärkung des Schutzes der Privatsphäre und der bürgerlichen Freiheiten widerspiegelt. Diese Verhandlungen haben zu neuen Schutzmaßnahmen geführt, die sicherstellen sollen, dass die Aktivitäten der US-Nachrichtendienste für die Verfolgung bestimmter nationaler Sicherheitsziele notwendig und verhältnismäßig sind, sowie zu einem neuen Mechanismus, mit dem Einzelpersonen in der Europäischen Union (EU) Rechtsmittel einlegen können, wenn sie glauben, dass sie unrechtmäßig Zielscheibe von Aktivitäten der Nachrichtendienste sind, was zusammen den Schutz personenbezogener Daten in der EU gewährleisten wird. Der EU-US-Datenschutzrahmen wird eine integrative und wettbewerbsfähige digitale Wirtschaft unterstützen. Wir sollten beide stolz auf die Verbesserungen sein, die sich in diesem Rahmen widerspiegeln und die den Schutz der Privatsphäre auf der ganzen Welt verbessern werden. Dieses Paket bildet zusammen mit der Durchführungsverordnung, den Verordnungen und anderen öffentlich zugänglichen Materialien eine sehr solide Grundlage für eine neue Angemessenheitsfeststellung durch die Europäische Kommission.[1]

Die folgenden Materialien sind beigefügt:

- Die EU-US-Rahmengrundsätze für den Datenschutz, einschließlich der ergänzenden Grundsätze (zusammen "die Grundsätze") und Anhang I der Grundsätze (d. *h.* ein Anhang, in dem die Bedingungen festgelegt sind, unter denen die Datenschutz-Rahmenorganisationen verpflichtet sind, bestimmte Restansprüche in Bezug auf personenbezogene Daten, die unter die Grundsätze fallen, zu schlichten);

[1] Unter der Voraussetzung, dass die Entscheidung der Kommission über die Angemessenheit des Schutzes, den der EU-US-Datenschutzrahmen bietet, auch für Island, Liechtenstein und Norwegen gilt, wird das EU-US-Datenschutzrahmenpaket sowohl die Europäische Union als auch diese drei Länder abdecken.

- Ein Schreiben der Internationalen Handelsbehörde des Ministeriums, die das Datenschutzrahmenprogramm verwaltet, in dem die Verpflichtungen beschrieben werden, die unser Ministerium eingegangen ist, um sicherzustellen, dass der EU-US-Datenschutzrahmen effektiv funktioniert;
- Ein Schreiben der Federal Trade Commission, in dem sie die Durchsetzung der Grundsätze beschreibt;
- Ein Schreiben des Verkehrsministeriums, in dem die Durchsetzung der Grundsätze beschrieben wird;
- ein vom Office of the Director of National Intelligence verfasstes Schreiben über die für die nationalen Sicherheitsbehörden der USA geltenden Schutzmaßnahmen und Beschränkungen; und
- Ein Schreiben des Justizministeriums über Schutzmaßnahmen und Beschränkungen für Zugang der US-Regierung für Zwecke der Strafverfolgung und des öffentlichen Interesses.

Das vollständige EU-US-Datenschutz-Rahmenpaket wird auf der Datenschutz-Website des Ministeriums veröffentlicht, und die Grundsätze und Anhang I der Grundsätze werden am Tag des Inkrafttretens der Angemessenheitsentscheidung der Europäischen Kommission wirksam.

Sie können sicher sein, dass die Vereinigten Staaten diese Verpflichtungen ernst nehmen. Wir freuen uns darauf, bei der Umsetzung des EU-US-Datenschutzrahmens mit Ihnen zusammenzuarbeiten und die nächste Phase dieses Prozesses gemeinsam in Angriff zu nehmen.

Mit freundlichen Grüßen,

Gina M. Raimondo

**ANHANG III**

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

12. Dezember 2022

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

Sehr geehrter Herr Kommissar Reynders:

Im Namen der International Trade Administration ("ITA") freue ich mich, die Verpflichtungen zu beschreiben, die das Handelsministerium ("das Ministerium") eingegangen ist, um den Schutz personenbezogener Daten durch seine Verwaltung und Überwachung des Data Privacy Framework-Programms zu gewährleisten. Der Abschluss des EU-U.S. Data Privacy Framework ("EU-U.S. DPF") ist eine große Errungenschaft für den Schutz der Privatsphäre und für die Unternehmen auf beiden Seiten des Atlantiks, da es den Bürgern der EU die Gewissheit gibt, dass ihre Daten geschützt werden und dass sie Rechtsmittel haben, um Bedenken im Zusammenhang mit ihren Daten auszuräumen, und es Tausenden von Unternehmen ermöglichen wird
weiterhin investieren und sich anderweitig in Handel und Gewerbe über den Atlantik hinweg engagieren, zum Nutzen unserer jeweiligen Volkswirtschaften und Bürger. Das DPF EU-USA ist das Ergebnis jahrelanger harter Arbeit und Zusammenarbeit mit Ihnen und Ihren Kollegen in der Europäischen Kommission ("die Kommission").
Wir freuen uns darauf, weiterhin mit der Kommission zusammenzuarbeiten, um sicherzustellen, dass diese gemeinsame Anstrengung effektiv funktioniert.

Die EU-US-DSGVO wird sowohl für Einzelpersonen als auch für Unternehmen erhebliche Vorteile bringen. Erstens bietet sie eine Reihe wichtiger Datenschutzmaßnahmen für die Daten von EU-Bürgern, die in die Vereinigten Staaten übermittelt werden. Es verlangt von den teilnehmenden US-Organisationen, eine konforme Datenschutzpolitik zu entwickeln und sich öffentlich zur Einhaltung der "EU-U.S. Data Privacy Framework Principles", einschließlich der ergänzenden Grundsätze (zusammen "die
Grundsätze") und Anhang I der Grundsätze (d. *h.* ein Anhang mit den Bedingungen, unter denen EU-DPF-Organisationen in den USA sind verpflichtet, bestimmte verbleibende Ansprüche in Bezug auf personenbezogene Daten, die unter die Grundsätze fallen, schiedsrichterlich zu regeln, so dass die Verpflichtung nach US-Recht durchsetzbar wird[1] ; sie müssen ihre Einhaltung jährlich gegenüber dem Ministerium neu zertifizieren; sie müssen kostenlose, unabhängige Streitbeilegungsverfahren anbieten

[1] Organisationen, die sich selbst zur Einhaltung der EU-U.S. Privacy Shield Framework Principles verpflichtet haben und die Vorteile der Teilnahme am EU-U.S. DPF nutzen möchten, müssen die "EU-U.S. Data Privacy Framework Principles" einhalten. Diese Verpflichtung zur Einhaltung der "EU-U.S. Data Privacy Framework Grundsätze" müssen sich so bald wie möglich, spätestens jedoch drei Monate nach Inkrafttreten der "EU-U.S. Data Privacy Framework Principles" in den Datenschutzrichtlinien dieser teilnehmenden Organisationen widerspiegeln. (*Siehe* Abschnitt (e) des ergänzenden Grundsatzes zur Selbstzertifizierung).

Auflösung für EU-Personen; und unterliegt den Ermittlungs- und Durchsetzungsbefugnissen einer eine in den Grundsätzen aufgeführte US-Gesetzesbehörde (z. *B.* die Federal Trade Commission (FTC) und das Verkehrsministerium (DOT)) oder eine in einem künftigen Anhang zu den Grundsätzen aufgeführte US-Gesetzesbehörde. Während die Entscheidung einer Organisation, sich selbst zu zertifizieren, freiwillig ist, kann eine Organisation, die sich öffentlich zu den EU-U.S. DPF verpflichtet, ihre Verpflichtung nach US-Recht durch die FTC, das DOT oder eine andere US-Behörde durchsetzen, je nachdem, welche Behörde für die teilnehmende Organisation zuständig ist. Zweitens wird die EU-U.S. DPF es Unternehmen in den Vereinigten Staaten, einschließlich Tochtergesellschaften europäischer Unternehmen in den Vereinigten Staaten, ermöglichen, personenbezogene Daten aus der Europäischen Union zu erhalten, um den Datenfluss zu erleichtern, der den transatlantischen Handel unterstützt. Der Datenverkehr zwischen den Vereinigten Staaten und der Europäischen Union ist der größte der Welt und untermauert die 7,1 Billionen Dollar schweren Wirtschaftsbeziehungen zwischen den USA und der EU, die Millionen von Arbeitsplätzen auf beiden Seiten des Atlantiks sichern. Unternehmen, die auf transatlantische Datenströme angewiesen sind, kommen aus allen Branchen und umfassen große Fortune-500-Firmen sowie viele kleine und mittlere Unternehmen. Transatlantische Datenströme ermöglichen es US-Organisationen, Daten zu verarbeiten, die erforderlich sind, um europäischen Bürgern Waren, Dienstleistungen und Beschäftigungsmöglichkeiten anzubieten.

Das Ministerium ist bestrebt, eng und produktiv mit unseren EU-Kollegen zusammenzuarbeiten, um das Datenschutzrahmenprogramm effektiv zu verwalten und zu überwachen. Dieses Engagement spiegelt sich in der Entwicklung und kontinuierlichen Verfeinerung einer Vielzahl von Ressourcen durch das Ministerium wider, um Organisationen bei der Selbstzertifizierung zu unterstützen, in der Einrichtung einer Website, die gezielte Informationen für Interessengruppen bereitstellt, in der Zusammenarbeit mit der Kommission und den europäischen Datenschutzbehörden zur Entwicklung von Leitlinien, die wichtige Elemente des EU-US-DSGVO klären, in der Öffentlichkeitsarbeit zur Förderung eines besseren Verständnisses der Datenschutzverpflichtungen von Organisationen sowie in der Aufsicht und Überwachung der Einhaltung der Anforderungen des Programms durch die Organisationen.

Unsere laufende Zusammenarbeit mit geschätzten EU-Kollegen wird es dem Ministerium ermöglichen, sicherzustellen, dass die EU-US-DSGVO effektiv 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 die EU-US-DSGVO, die ein Beispiel für diese Zusammenarbeit ist, es der Kommission ermöglichen wird, einen neuen Angemessenheitsbeschluss zu erlassen, der es Organisationen erlaubt, die EU-US-DSGVO zu nutzen, um personenbezogene Daten aus der Europäischen Union in die Vereinigten Staaten im Einklang mit dem EU-Recht zu übertragen.

**Verwaltung und Beaufsichtigung des Datenschutz-Rahmenprogramms durch das Handelsministerium**

Das Ministerium ist fest entschlossen, das Rahmenprogramm für den Datenschutz wirksam zu verwalten und zu überwachen, und wird entsprechende Anstrengungen unternehmen und angemessene Ressourcen bereitstellen, um dieses Ergebnis zu gewährleisten. Das Ministerium wird eine maßgebliche Liste von US-Organisationen führen und der Öffentlichkeit zugänglich machen, die sich gegenüber dem Ministerium selbst zertifiziert und sich zur Einhaltung der Grundsätze verpflichtet haben (die "Datenschutz-Rahmenliste"), und diese Liste auf der Grundlage der von den teilnehmenden Organisationen eingereichten

jährlichen Neuzertifizierungen und durch Streichung von Organisationen aktualisieren, wenn diese sich freiwillig zurückziehen, die jährliche Neuzertifizierung nicht in Übereinstimmung mit den Verfahren des Ministeriums durchführen oder sich als dauerhaft nicht konform erweisen. Das Ministerium wird auch ein maßgebliches Verzeichnis der US-Organisationen, die von der Datenschutz-Rahmenliste gestrichen wurden, führen und der Öffentlichkeit zugänglich machen und den Grund für die Streichung jeder Organisation angeben. Die vorgenannte maßgebliche Liste und das Verzeichnis werden der Öffentlichkeit auf der Website des Ministeriums zugänglich gemacht.

Website des Ministeriums zum Datenschutzrahmen. Auf der Website des Datenschutzrahmens wird an prominenter Stelle erklärt, dass jede Organisation, die von der Liste des Datenschutzrahmens gestrichen wird, nicht mehr behaupten darf, dass sie an der EU-US-DSGVO teilnimmt oder diese einhält und dass sie möglicherweise personenbezogene Daten im Rahmen der EU-US-DSGVO erhält. Eine solche Organisation muss jedoch weiterhin die Grundsätze auf die personenbezogenen Daten anwenden, die sie während ihrer Teilnahme an der EU-US-DSGVO erhalten hat, solange sie diese Daten aufbewahrt. Das Ministerium verpflichtet sich im Rahmen seines übergreifenden, fortlaufenden Engagements für die wirksame Verwaltung und Überwachung des Data Privacy Framework-Programms insbesondere zu folgenden Maßnahmen:

Überprüfung der Selbstzertifizierungsanforderungen

- Bevor das Ministerium die erste Selbstzertifizierung oder die jährliche Neuzertifizierung einer Organisation (zusammenfassend als "Selbstzertifizierung" bezeichnet) abschließt und eine Organisation auf die Datenschutz-Rahmenliste setzt oder dort belässt, prüft es, ob die Organisation zumindest die einschlägigen Anforderungen des ergänzenden Grundsatzes zur Selbstzertifizierung in Bezug auf die Informationen erfüllt hat, die eine Organisation in ihrer Selbstzertifizierung dem Ministerium vorlegen muss, und ob sie zu gegebener Zeit eine einschlägige Datenschutzrichtlinie vorgelegt hat, die Einzelpersonen über alle 13 aufgezählten Elemente des Grundsatzes der Mitteilung informiert. Das Ministerium wird überprüfen, ob die Organisation dies getan hat:
    - die Organisation, die ihre Selbstzertifizierung einreicht, sowie alle US-Einheiten oder US-Tochtergesellschaften der selbstzertifizierenden Organisation, die sich ebenfalls an die Grundsätze halten, die die Organisation durch ihre Selbstzertifizierung abdecken möchte;
    - die erforderlichen Kontaktinformationen der Organisation (z. *B.* Kontaktinformationen für bestimmte Personen und/oder Stellen innerhalb der selbstzertifizierenden Organisation, die für die Bearbeitung von Beschwerden, Zugangsanträgen und anderen Fragen im Zusammenhang mit der EU-US-DSGVO zuständig sind);
    - den Zweck bzw. die Zwecke, für den bzw. die die Organisation die von der Europäischen Union erhaltenen personenbezogenen Daten erheben und verwenden wird;
    - angegeben, welche personenbezogenen Daten aus der Europäischen Union im Rahmen der EU-US-DSGVO übermittelt werden und somit unter die Selbstzertifizierung fallen;
    - wenn die Organisation eine öffentliche Website hat, die Webadresse, unter der die entsprechenden Datenschutzrichtlinien auf dieser Website leicht zugänglich sind, oder, wenn die Organisation keine öffentliche Website hat, eine Kopie der entsprechenden Datenschutzrichtlinien und den Ort, an dem diese Datenschutzrichtlinien von den betroffenen Personen eingesehen werden können (d. *h.* von den betroffenen Mitarbeitern, wenn es sich bei den entsprechenden Datenschutzrichtlinien um Datenschutzrichtlinien der Personalabteilung handelt, oder von der Öffentlichkeit, wenn es sich bei den entsprechenden Datenschutzrichtlinien nicht um Datenschutzrichtlinien der Personalabteilung handelt);
    - zu gegebener Zeit (d. *h.* zunächst nur in einem Entwurf der Datenschutzrichtlinien, der zusammen mit dem Antrag eingereicht wird, wenn es sich um eine erste Selbstzertifizierung handelt; andernfalls in einer endgültigen und gegebenenfalls veröffentlichten Datenschutzrichtlinie) eine Erklärung, dass es die Grundsätze einhält, sowie einen Hyperlink oder die Webadresse für die Datenschutz-Rahmenprogramm-Website des Ministeriums (z. *B.* die Homepage oder die Datenschutz-Rahmenprogramm-Webseite) in seine einschlägigen Datenschutzrichtlinien aufzunehmen;

- zu gegebener Zeit alle 12 anderen im Informationsgrundsatz aufgezählten Elemente (z. *B*. die Möglichkeit für die betroffene EU-Person, unter bestimmten Bedingungen ein verbindliches Schiedsverfahren in Anspruch zu nehmen, die Verpflichtung zur Offenlegung personenbezogener Daten auf rechtmäßige Anfragen von Behörden, einschließlich der Erfüllung von Anforderungen der nationalen Sicherheit oder der Strafverfolgung, und die Haftung im Falle der Weitergabe an Dritte) in ihre jeweilige Datenschutzpolitik aufgenommen hat;
- die spezifische gesetzliche Stelle, die für Klagen gegen die Organisation wegen möglicher unlauterer oder irreführender Praktiken und Verstöße gegen folgende Bestimmungen zuständig ist

Gesetze oder Vorschriften zum Schutz der Privatsphäre (und die in den Grundsätzen oder einem künftigen Anhang zu den Grundsätzen aufgeführt sind);
    - alle Datenschutzprogramme, an denen die Organisation beteiligt ist;
    - hat angegeben, ob es sich bei der relevanten Methode (d. *h.* bei den Folgeverfahren, die es bereitstellen muss) zur Überprüfung der Einhaltung der Grundsätze um eine "Selbstbewertung" (*d. h*. interne Überprüfung) oder um eine "externe Überprüfung" (*d. h.* Überprüfung durch Dritte) handelt, und wenn es sich bei der relevanten Methode um eine externe Überprüfung handelt, hat es auch angegeben, welche dritte Partei diese Überprüfung durchgeführt hat;
    - den geeigneten unabhängigen Rechtsbehelfsmechanismus zu ermitteln, der für die Bearbeitung von Beschwerden im Rahmen der Grundsätze zur Verfügung steht, und dem Betroffenen kostenlos einen angemessenen Rechtsbehelf zu gewähren.
        - Hat sich die Organisation für einen unabhängigen Regressmechanismus entschieden, der von einer alternativen Streitbeilegungsstelle des Privatsektors angeboten wird, so hat sie in ihrer einschlägigen Datenschutzrichtlinie einen Hyperlink zu oder die Webadresse für die entsprechende Website oder das Beschwerdeformular des Mechanismus aufgenommen, der für die Untersuchung ungelöster Beschwerden gemäß den Grundsätzen zur Verfügung steht.
        - Wenn die Organisation entweder verpflichtet ist (d. *h. in Bezug auf* Personaldaten, die im Rahmen des Beschäftigungsverhältnisses aus der Europäischen Union übermittelt werden) oder sich dafür entschieden hat, bei der Untersuchung und Beilegung von Beschwerden, die im Rahmen der Grundsätze vorgebracht werden, mit den zuständigen Datenschutzbehörden zusammenzuarbeiten, hat sie sich zu einer solchen Zusammenarbeit mit den Datenschutzbehörden und zur Befolgung ihrer diesbezüglichen Ratschläge verpflichtet, spezifische Maßnahmen zur Einhaltung der Grundsätze zu ergreifen.
- Das Ministerium wird auch überprüfen, ob die von der Organisation vorgelegte Selbstzertifizierung mit ihrer/ihren einschlägigen Datenschutzpolitik(en) übereinstimmt. Möchte eine selbstzertifizierende Organisation ihre US-Einheiten oder US-Tochtergesellschaften einbeziehen, die über separate, einschlägige Datenschutzrichtlinien verfügen, wird das Ministerium auch die einschlägigen Datenschutzrichtlinien dieser erfassten Einheiten oder Tochtergesellschaften überprüfen, um sicherzustellen, dass sie alle erforderlichen Elemente des Grundsatzes der Mitteilung enthalten.
- Das Ministerium wird mit den gesetzlichen Stellen (z. *B.* FTC und DOT) zusammenarbeiten, um zu überprüfen, ob die Organisationen der Zuständigkeit der jeweiligen gesetzlichen Stelle unterliegen, die in ihren Selbstzertifizierungsunterlagen angegeben ist, wenn das Ministerium Grund hat, daran zu zweifeln, dass sie dieser Zuständigkeit unterliegen.
- Das Ministerium wird mit privatwirtschaftlichen alternativen Streitbeilegungsstellen zusammenarbeiten, um zu überprüfen, ob die Organisationen aktiv für den in ihrer Selbstzertifizierung angegebenen unabhängigen Rechtsbehelfsmechanismus registriert sind, und mit diesen Stellen zusammenarbeiten, um zu überprüfen, ob die Organisationen aktiv für die in ihrer Selbstzertifizierung angegebene externe Überprüfung der Einhaltung der Vorschriften registriert sind, wenn diese Stellen beide Arten von Dienstleistungen anbieten können.
- Das Ministerium wird mit der vom Ministerium ausgewählten dritten Partei zusammenarbeiten, die als Verwahrer der durch die DPA-Panel-Gebühr (d.*h.* die jährliche Gebühr zur Deckung der Betriebskosten des DPA-Panels) eingenommenen Gelder fungiert, um zu überprüfen, ob die Organisationen diese Gebühr für das betreffende Jahr gezahlt haben, sofern die Organisationen die DPAs als den relevanten unabhängigen Regressmechanismus identifiziert haben.
- Das Ministerium wird mit der dritten Partei zusammenarbeiten, die vom Ministerium für die Verwaltung von Schiedsverfahren gemäß dem in Anhang I der Grundsätze genannten Schiedsfonds ausgewählt wurde, um zu überprüfen, ob die Organisationen zu diesem

Schiedsfonds beigetragen haben.

- Stellt das Ministerium bei der Überprüfung der von den Organisationen eingereichten Selbstzertifizierungsunterlagen Probleme fest, so teilt es ihnen mit, dass sie alle diese Probleme innerhalb des vom Ministerium festgelegten Zeitrahmens lösen müssen.[2] Das Ministerium wird die Organisationen auch darüber informieren, dass, wenn sie nicht innerhalb des vom Ministerium festgelegten Zeitrahmens reagieren oder ihre Selbstzertifizierung nicht gemäß den Verfahren des Ministeriums vervollständigen, diese Selbstzertifizierungsanträge als aufgegeben betrachtet werden, und dass alle

[2] Was z. *B.* die Neuzertifizierung betrifft, so wird erwartet, dass die Organisationen alle derartigen Fragen innerhalb von 45 Tagen klären, vorbehaltlich der Festlegung eines anderen, angemessenen Zeitrahmens durch das Ministerium.

Falsche Angaben über die Teilnahme einer Organisation an der DPF EU-USA oder deren Einhaltung können von der FTC, dem US-Verkehrsministerium oder einer anderen zuständigen Regierungsbehörde verfolgt werden. Das Ministerium wird die Organisationen über die Kontaktmöglichkeiten informieren, die die Organisationen dem Ministerium mitgeteilt haben.

Erleichterung der Zusammenarbeit mit alternativen Streitbeilegungsstellen, die prinzipienbezogene Dienstleistungen erbringen

- Das Ministerium wird mit alternativen Streitbeilegungsstellen des Privatsektors zusammenarbeiten, die unabhängige Regressmechanismen anbieten, die zur Verfügung stehen, um ungelöste Beschwerden, die im Rahmen der Grundsätze vorgebracht werden, zu untersuchen, um zu überprüfen, ob sie mindestens die Anforderungen des ergänzenden Grundsatzes zur Streitbeilegung und Durchsetzung erfüllen. Das Ministerium wird überprüfen, ob sie:
    - auf ihren öffentlichen Websites Informationen über die Grundsätze und die von ihnen im Rahmen der EU-US-DSGVO erbrachten Dienstleistungen bereitstellen, die Folgendes umfassen müssen: (1) Informationen über oder einen Hyperlink zu den Anforderungen der Grundsätze an unabhängige Rechtsbehelfsmechanismen; (2) einen Hyperlink zur Website des Ministeriums zum Datenschutzrahmen; (3) eine Erklärung, dass ihre Streitbeilegungsdienste im Rahmen der EU-US-DSGVO für Einzelpersonen kostenlos sind; (4) eine Beschreibung, wie eine Beschwerde im Zusammenhang mit den Grundsätzen eingereicht werden kann; (5) den Zeitrahmen, in dem Beschwerden im Zusammenhang mit den Grundsätzen bearbeitet werden; und (6) eine Beschreibung des Spektrums möglicher Rechtsmittel. Das Ministerium wird die Stellen rechtzeitig über wesentliche Änderungen bei der Überwachung und Verwaltung des Datenschutzrahmenprogramms durch das Ministerium informieren, sofern solche Änderungen bevorstehen oder bereits vorgenommen wurden und für die Rolle, die die Stellen im Rahmen der EU-US-DSGVO spielen, relevant sind;
    - einen Jahresbericht mit aggregierten Statistiken über ihre Streitbeilegungsdienste zu veröffentlichen, der Folgendes enthalten muss: (1) die Gesamtzahl der im Berichtsjahr eingegangenen Beschwerden im Zusammenhang mit den Grundsätzen; (2) die Arten der eingegangenen Beschwerden; (3) Qualitätsmaßstäbe für die Streitbeilegung, z. B. die Dauer der Bearbeitung von Beschwerden; und (4) die Ergebnisse der eingegangenen Beschwerden, insbesondere die Anzahl und Art der verhängten Abhilfemaßnahmen oder Sanktionen. Das Ministerium wird den Stellen spezifische, ergänzende Leitlinien dazu zur Verfügung stellen, welche Informationen sie in diesen Jahresberichten bereitstellen sollten, die diese Anforderungen näher ausführen (z. *B.* Auflistung der spezifischen Kriterien, die eine Beschwerde erfüllen muss, damit sie für die Zwecke des Jahresberichts als eine auf die Grundsätze bezogene Beschwerde angesehen wird), sowie andere Arten von Informationen, die sie bereitstellen sollten (z. *B.*, wenn die Stelle auch einen auf die Grundsätze bezogenen Überprüfungsdienst anbietet, eine Beschreibung, wie die Stelle tatsächliche oder potenzielle Interessenkonflikte in Situationen vermeidet, in denen sie einer Organisation sowohl Überprüfungsdienste als auch Streitbeilegungsdienste bereitstellt). In den zusätzlichen Leitlinien des Ministeriums wird auch das Datum genannt, bis zu dem die Jahresberichte der Stellen für den jeweiligen Berichtszeitraum veröffentlicht werden sollten.

Nachfassen bei Organisationen, die von der Datenschutz-Rahmenliste gestrichen werden möchten oder wurden

- Wenn eine Organisation sich aus der EU-US-DSGVO zurückziehen möchte, wird das Ministerium verlangen, dass die Organisation alle Verweise auf die EU-US-DSGVO, die

implizieren, dass sie weiterhin an der EU-US-DSGVO teilnimmt und dass sie personenbezogene Daten gemäß der EU-US-DSGVO erhalten kann, aus allen relevanten Datenschutzrichtlinien entfernt (*siehe* Beschreibung der Verpflichtung des Ministeriums, nach falschen Angaben über die Teilnahme zu suchen). Das Ministerium wird außerdem verlangen, dass die Organisation einen entsprechenden Fragebogen ausfüllt und an das Ministerium übermittelt, um dies zu überprüfen:

- seinen Wunsch, sich zurückzuziehen;
- welche der folgenden Maßnahmen sie mit den personenbezogenen Daten ergreifen wird, die sie unter Berufung auf die EU-US-DSGVO erhalten hat, während sie an der EU-US-DSGVO teilgenommen hat: (a) Aufbewahrung dieser Daten, weitere Anwendung der Grundsätze auf diese Daten und jährliche Bestätigung gegenüber dem Ministerium, dass sie sich verpflichtet, die Grundsätze auf diese Daten anzuwenden; (b) Aufbewahrung dieser Daten und Gewährleistung eines "angemessenen" Schutzes für diese Daten durch ein anderes zugelassenes Mittel; oder (c) Rückgabe oder Löschung aller dieser Daten bis zu einem bestimmten Datum; und
- der innerhalb der Organisation als ständiger Ansprechpartner für Fragen im Zusammenhang mit den Grundsätzen dienen wird.

- Wenn eine Organisation (a), wie oben beschrieben, gewählt hat, wird das Ministerium auch verlangen, dass sie jedes Jahr nach ihrem Austritt (*d.h. bis zum ersten Jahrestag ihres Austritts) folgende Daten* ausfüllt und dem Ministerium übermittelt (d.h. bis zum ersten Jahrestag ihres Rücktritts sowie bis zu jedem weiteren Jahrestag, es sei denn, die Organisation sorgt entweder für einen "angemessenen" Schutz dieser Daten durch ein anderes zulässiges Mittel oder sie gibt alle diese Daten zurück oder löscht sie und benachrichtigt das Ministerium von dieser Maßnahme) einen geeigneten Fragebogen ausfüllen und dem Ministerium vorlegen, um zu überprüfen, was sie mit diesen personenbezogenen Daten getan hat, was sie mit allen personenbezogenen Daten, die sie weiterhin aufbewahrt, tun wird und wer innerhalb der Organisation als ständiger Ansprechpartner für Fragen im Zusammenhang mit den Grundsätzen dienen wird.
- Wenn eine Organisation ihre Selbstzertifizierung hat auslaufen lassen (*d.h*. weder die jährliche Neuzertifizierung ihrer Einhaltung der Grundsätze abgeschlossen hat noch aus einem anderen Grund, wie z.B. einem Rücktritt, von der Datenschutz-Rahmenliste gestrichen wurde), wird das Ministerium sie anweisen, einen entsprechenden Fragebogen auszufüllen und dem Ministerium vorzulegen, um zu überprüfen, ob sie die Zertifizierung zurückziehen oder erneut zertifizieren möchte:
  - und, falls sie sich zurückziehen möchte, weiter überprüfen, was sie mit den personenbezogenen Daten tun wird, die sie im Vertrauen auf die EU-US-DSGVO erhalten hat, während sie an der EU-US-DSGVO teilgenommen hat (*siehe* vorherige Beschreibung, was eine Organisation überprüfen muss, wenn sie sich zurückziehen möchte);
  - und, falls sie eine erneute Zertifizierung anstrebt, weiter zu überprüfen, ob sie während des Ablaufs ihres Zertifizierungsstatus die Grundsätze auf personenbezogene Daten angewandt hat, die sie im Rahmen der EU-US-DSGVO erhalten hat, und zu erläutern, welche Schritte sie unternehmen wird, um die offenen Fragen zu klären, die ihre erneute Zertifizierung verzögert haben.
- Wenn eine Organisation aus einem der folgenden Gründe von der Data Privacy Framework List gestrichen wird: (a) Rückzug aus der EU-U.S. DPF, (b) Versäumnis, die jährliche Neuzertifizierung ihrer Einhaltung der Grundsätze abzuschließen (d*.h.*, (d.h. entweder begonnen, aber nicht rechtzeitig abgeschlossen oder gar nicht erst begonnen) oder (c) "anhaltende Nichteinhaltung": Das Ministerium sendet eine Benachrichtigung an die Kontaktperson(en), die in der Selbstzertifizierung der Organisation genannt wurde(n), in der der Grund für die Streichung angegeben ist und in der erklärt wird, dass die Organisation nicht mehr ausdrücklich oder stillschweigend behaupten darf, dass sie an der EU-US-DSGVO teilnimmt oder diese einhält und dass sie gemäß der EU-US-DSGVO personenbezogene Daten erhalten darf. In der Benachrichtigung, die auch andere, auf den Grund der Streichung zugeschnittene Inhalte enthalten kann, wird darauf hingewiesen, dass Organisationen, die ihre Teilnahme an der EU-US-DSGVO oder die Einhaltung der EU-US-DSGVO falsch darstellen, einschließlich der Fälle, in denen sie darstellen, dass sie an der EU-US-DSGVO teilnehmen, nachdem sie von der Datenschutz-Rahmenliste gestrichen wurden, Gegenstand von Durchsetzungsmaßnahmen der FTC, des US-Verkehrsministeriums oder einer anderen zuständigen Regierungsstelle sein können.

Suche nach und Umgang mit falschen Teilnahmeanträgen

- Wenn eine Organisation: (a) sich von der Teilnahme an der DPF EU-USA zurückzieht, (b) die jährliche Re-Zertifizierung ihrer Einhaltung der Grundsätze nicht abschließt (d*.h.*, (d.h., sie hat entweder mit der jährlichen Neuzertifizierung begonnen, sie aber nicht rechtzeitig abgeschlossen oder sie hat die jährliche Neuzertifizierung gar nicht erst begonnen), (c) sie wird als Teilnehmerin der DPF EU-USA insbesondere wegen "anhaltender Nichterfüllung" gestrichen, oder (d) sie schließt die erste Selbstzertifizierung ihrer Einhaltung der Grundsätze nicht ab (d*.h.*, sie hat die Selbstzertifizierung begonnen, sie aber nicht abgeschlossen).

Das Ministerium wird von *Amts* wegen prüfen, ob die von der Organisation veröffentlichten Datenschutzrichtlinien Verweise auf die EU-US-DSGVO enthalten, die implizieren, dass die Organisation an der EU-US-DSGVO teilnimmt und dass sie personenbezogene Daten gemäß der EU-US-DSGVO erhalten kann. 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, wenn die Organisation ihre Teilnahme an der EU-DSGVO weiterhin falsch darstellt.
U.S. DPF. Das Ministerium wird die Organisation über die dem Ministerium mitgeteilten Kontaktmöglichkeiten oder erforderlichenfalls über andere geeignete Mittel informieren. Wenn die Organisation weder die Verweise entfernt noch selbst bescheinigt, dass sie die EU-US-DPF in Übereinstimmung mit den Verfahren des Ministeriums, wird das Ministerium die Angelegenheit *von Amts wegen* an die FTC, das DOT oder eine andere geeignete Durchsetzungsbehörde weiterleiten oder andere geeignete Maßnahmen ergreifen, um die ordnungsgemäße Verwendung des EU-US-DPF-Zertifizierungszeichens sicherzustellen;

- Das Ministerium wird weitere Anstrengungen unternehmen, um falsche Behauptungen über die Teilnahme an der EU-U.S. DPF und die missbräuchliche Verwendung des EU-U.S. DPF-Zertifizierungszeichens aufzudecken, auch durch Organisationen, die im Gegensatz zu den oben beschriebenen Organisationen noch nicht einmal mit dem Selbstzertifizierungsprozess begonnen haben (z. *B.* Durchführung geeigneter Internetrecherchen, um Verweise auf die EU-U.S. DPF in den Datenschutzrichtlinien der Organisationen zu finden). Wenn das Ministerium im Rahmen dieser Bemühungen falsche Behauptungen über die Teilnahme an der EU-US-DSGVO und die missbräuchliche Verwendung des EU-US-DSGVO-Zertifizierungszeichens feststellt, wird das Ministerium die Organisation davon in Kenntnis setzen, dass das Ministerium die Angelegenheit gegebenenfalls an die zuständige Behörde weiterleiten wird, um mögliche Durchsetzungsmaßnahmen einzuleiten, wenn die Organisation ihre Teilnahme an der EU-US-DSGVO weiterhin falsch darstellt.
  U.S. DPF. Das Ministerium informiert die Organisation über die Kontaktmöglichkeiten, die die Organisation dem Ministerium gegebenenfalls zur Verfügung gestellt hat, oder gegebenenfalls über andere geeignete Mittel. Wenn die Organisation weder die Verweise entfernt noch ihre Konformität mit der DPF EU-USA gemäß den Verfahren des Ministeriums selbst bescheinigt, wird das Ministerium die Angelegenheit *von Amts wegen* an die FTC, das DOT oder eine andere geeignete Durchsetzungsbehörde weiterleiten oder andere geeignete Maßnahmen ergreifen, um die ordnungsgemäße Verwendung des DPF EU-USA-Zertifizierungszeichens sicherzustellen;
- Das Ministerium prüft und bearbeitet umgehend konkrete, nicht unbegründete Beschwerden über falsche Behauptungen über eine Beteiligung der EU-US-DSGVO, die beim Ministerium eingehen (z. *B.* Beschwerden von den Datenschutzbehörden, unabhängigen Rechtsbehelfsmechanismen, die von alternativen Streitbeilegungsstellen des Privatsektors angeboten werden, von betroffenen Personen, Unternehmen aus der EU und den USA sowie von anderen Dritten); und
- Das Ministerium kann weitere geeignete Abhilfemaßnahmen ergreifen. Falsche Angaben gegenüber dem Ministerium können nach dem False Statements Act (18 U.S.C. § 1001) strafbar sein.

Regelmäßige Überprüfung der Einhaltung der Vorschriften und Bewertung des Rahmenprogramms für den Datenschutz von *Amts wegen*

- Das Ministerium wird fortlaufend Anstrengungen unternehmen, um die tatsächliche Einhaltung der Vorschriften durch die DPF-Organisationen der EU und der USA zu überwachen und Probleme zu ermitteln, die Folgemaßnahmen rechtfertigen könnten. Insbesondere wird das Ministerium *von Amts wegen* routinemäßige Stichprobenkontrollen bei zufällig ausgewählten DPF-Organisationen in der EU und in den USA sowie Ad-hoc-Stichprobenkontrollen bei bestimmten DPF-Organisationen in der EU und in den USA durchführen, wenn potenzielle Mängel bei der Einhaltung der Vorschriften festgestellt werden (z. *B*,

(a) dass die Kontaktstelle(n), die für die Bearbeitung von Beschwerden, Auskunftsersuchen und anderen Fragen im Zusammenhang mit der EU-US-Datenschutz-Grundverordnung zuständig ist/sind, verfügbar ist/sind; (b) dass die öffentlich zugängliche Datenschutzrichtlinie der Organisation sowohl auf der öffentlichen Website als auch über einen Hyperlink auf der Liste der Datenschutz-Grundverordnung leicht einsehbar ist; (c) dass die Organisation, falls zutreffend, ihre Datenschutzrichtlinien öffentlich zugänglich macht. a) dass die Kontaktstelle(n), die für die Bearbeitung von Beschwerden, Auskunftsersuchen und anderen Fragen im Zusammenhang mit der EU-US-Datenschutz-Grundverordnung zuständig ist/sind, erreichbar ist/sind; b) dass die öffentlich zugänglichen Datenschutzrichtlinien der Organisation sowohl auf der öffentlichen Website der Organisation als auch über einen Hyperlink auf der Datenschutz-Rahmenliste für die Öffentlichkeit leicht zugänglich sind; c) dass die Datenschutzrichtlinien der Organisation weiterhin die in den Grundsätzen beschriebenen Anforderungen an die Selbstzertifizierung erfüllen; und d) dass der von der Organisation angegebene unabhängige Rechtsbehelfsmechanismus für Beschwerden im Rahmen der EU-US-Datenschutz-Grundverordnung verfügbar ist.

die DPF EU-USA. Das Ministerium wird auch aktiv die Nachrichten auf Berichte hin überwachen, die glaubwürdige Beweise für die Nichteinhaltung der Vorschriften durch DPF-Organisationen aus der EU und den USA liefern;

- Im Rahmen der Überprüfung der Einhaltung der Grundsätze wird das Ministerium verlangen, dass eine DPF-Organisation aus der EU und den USA einen detaillierten Fragebogen ausfüllt und dem Ministerium vorlegt, wenn: (a) das Ministerium konkrete, nicht unbegründete Beschwerden über die Einhaltung der Grundsätze durch die Organisation erhalten hat, (b) die Organisation nicht zufriedenstellend auf Anfragen des Ministeriums nach Informationen über die EPF EU-USA antwortet oder (c) es glaubwürdige Beweise dafür gibt, dass die Organisation ihre Verpflichtungen im Rahmen der EU-US DPF nicht einhält.
  U.S. DPF. Hat das Ministerium einen solchen detaillierten Fragebogen an eine Organisation gesandt und erhält diese keine zufriedenstellende Antwort auf den Fragebogen, informiert das Ministerium die Organisation darüber, dass das Ministerium die Angelegenheit gegebenenfalls an die zuständige Behörde weiterleiten wird, um mögliche Durchsetzungsmaßnahmen zu ergreifen, wenn das Ministerium keine rechtzeitige und zufriedenstellende Antwort von der Organisation erhält. Das Ministerium informiert die Organisation über die Kontaktmöglichkeiten, die die Organisation dem Ministerium mitgeteilt hat, oder gegebenenfalls über andere geeignete Mittel. Wenn die Organisation nicht rechtzeitig und zufriedenstellend antwortet, wird das Ministerium die Angelegenheit *von Amts wegen* an die FTC, das DOT oder eine andere geeignete Durchsetzungsbehörde weiterleiten oder andere geeignete Maßnahmen ergreifen, um die Einhaltung der Vorschriften sicherzustellen. Das Ministerium konsultiert gegebenenfalls die zuständigen Datenschutzbehörden zu solchen Überprüfungen der Einhaltung der Vorschriften; und
- Das Ministerium wird in regelmäßigen Abständen die Verwaltung und Überwachung des Datenschutzrahmenprogramms bewerten, um sicherzustellen, dass seine Überwachungsbemühungen, einschließlich der Bemühungen, die durch die Verwendung von Suchwerkzeugen unternommen werden (z. *B.* um nach defekten Links zu den Datenschutzrichtlinien von EU-US-Organisationen zu suchen), angemessen sind, um bestehende und neu auftretende Probleme anzugehen.

Anpassen der Datenschutzrahmen-Website an die Zielgruppen

Das Ministerium wird die Website zum Datenschutzrahmen auf die folgenden Zielgruppen zuschneiden: Einzelpersonen aus der EU, Unternehmen aus der EU, Unternehmen aus den USA und Datenschutzbehörden. Die Aufnahme von Material, das sich direkt an EU-Personen und EU-Unternehmen richtet, wird die Transparenz in mehrfacher Hinsicht erleichtern. Im Hinblick auf EU-Personen wird die Website Folgendes klar erläutern: (1) die Rechte, die die DSGVO den EU-Personen einräumt; (2) die Rechtsmittel, die EU-Personen zur Verfügung stehen, wenn sie der Meinung sind, dass eine Organisation gegen ihre Verpflichtung zur Einhaltung der Grundsätze verstoßen hat; und (3) wie man Informationen über die Selbstzertifizierung einer Organisation im Rahmen der DSGVO findet. Im Hinblick auf EU-Unternehmen wird es die Überprüfung erleichtern, ob: (1) ob ein Unternehmen an der EU-US-DSGVO teilnimmt; (2) welche Art von Informationen von der EU-US-DSGVO-Selbstzertifizierung eines Unternehmens abgedeckt wird; (3) welche Datenschutzrichtlinien für die abgedeckten Informationen gelten; und (4) welche Methode das Unternehmen verwendet, um seine Einhaltung der Grundsätze zu überprüfen. Im Hinblick auf US-Unternehmen wird klar erläutert: (1) die Vorteile der Teilnahme an der EU-US-DSGVO; (2) wie man der EU-US-DSGVO beitreten kann und wie man sich erneut zertifizieren lassen oder aus der EU-US-DSGVO austreten kann; und (3) wie die Vereinigten Staaten die EU-US-DSGVO verwalten und durchsetzen. Die Aufnahme von Material, das sich direkt an die Datenschutzbehörden richtet (z. *B.* Informationen über die spezielle Kontaktstelle des Ministeriums für Datenschutzbehörden und ein Hyperlink zu prinzipienbezogenen Inhalten auf der FTC-Website), wird sowohl die

Zusammenarbeit als auch die Transparenz erleichtern. Das Ministerium wird auch auf Ad-hoc-Basis mit der Kommission und dem Europäischen Datenschutzausschuss (EDPB) zusammenarbeiten, um zusätzliches, aktuelles Material (z. *B.* Antworten auf häufig gestellte Fragen) für die Verwendung auf der Datenschutzrahmen-Website zu entwickeln, wenn solche Informationen die effiziente Verwaltung und Überwachung des Datenschutzrahmenprogramms erleichtern würden.

Erleichterung der Zusammenarbeit mit den Datenschutzbehörden

Um die Möglichkeiten der Zusammenarbeit mit den Datenschutzbehörden zu verbessern, wird das Ministerium eine spezielle Kontaktstelle im Ministerium einrichten, die als Verbindungsstelle zu den Datenschutzbehörden fungiert. In Fällen, in denen eine Datenschutzbehörde der Ansicht ist, dass eine EU-US-DSGVO die Grundsätze nicht einhält, einschließlich einer Beschwerde einer EU-Person, kann sich die Datenschutzbehörde an die spezielle Kontaktstelle des Ministeriums wenden, um die Organisation zur weiteren Prüfung zu verweisen. Das Ministerium wird sich nach besten Kräften bemühen, die Lösung der Beschwerde mit der EU-US-DPF-Organisation zu erleichtern. Innerhalb von 90 Tagen nach Eingang der Beschwerde wird das Ministerium die Datenschutzbehörde über den aktuellen Stand informieren. Die spezielle Kontaktstelle wird auch Hinweise auf Organisationen entgegennehmen, die fälschlicherweise behaupten, an der DPF EU-USA teilzunehmen. Die spezielle Kontaktstelle wird alle beim Ministerium eingegangenen Verweise der Datenschutzbehörden verfolgen, und das Ministerium wird im Rahmen der unten beschriebenen gemeinsamen Überprüfung einen Bericht vorlegen, in dem die jährlich bei ihm eingehenden Beschwerden zusammengefasst werden. Die spezielle Kontaktstelle wird den Datenschutzbehörden bei der Suche nach Informationen über die Selbstzertifizierung einer bestimmten Organisation oder die frühere Teilnahme an der EU-US-Dopingkontrollstelle behilflich sein, und die spezielle Kontaktstelle wird Anfragen der Datenschutzbehörden bezüglich der Umsetzung bestimmter EU-US-Dopingkontrollanforderungen beantworten. Das Ministerium wird auch mit der Kommission und dem EDPB bei verfahrenstechnischen und administrativen Aspekten des DPA-Panels zusammenarbeiten, einschließlich der Festlegung geeigneter Verfahren für die Verteilung der durch die DPA-Panelgebühr eingenommenen Mittel. Wir gehen davon aus, dass die Kommission mit dem Ministerium zusammenarbeiten wird, um die Lösung aller Probleme zu erleichtern, die im Zusammenhang mit diesen Verfahren auftreten könnten. Darüber hinaus wird das Ministerium den Datenschutzbehörden Material über die EU-US-DSGVO zur Verfügung stellen, das sie auf ihren eigenen Websites veröffentlichen können, um die Transparenz für EU-Bürger und EU-Unternehmen zu erhöhen. Eine stärkere Sensibilisierung für die EU-US-DSGVO und die sich daraus ergebenden Rechte und Pflichten dürfte es erleichtern, auftretende Probleme zu erkennen, so dass diese angemessen gelöst werden können.

Erfüllung der in Anhang I der Grundsätze eingegangenen Verpflichtungen

Das Ministerium wird seinen Verpflichtungen gemäß Anhang I der Grundsätze nachkommen und u. a. eine Liste von Schiedsrichtern führen, die gemeinsam mit der Kommission auf der Grundlage von Unabhängigkeit, Integrität und Sachkenntnis ausgewählt werden, und gegebenenfalls die vom Ministerium ausgewählte dritte Partei bei der Verwaltung von Schiedsverfahren gemäß Anhang I der Grundsätze und der Verwaltung des dort genannten Schiedsfonds unterstützen.[3] Das Ministerium wird mit der Drittpartei zusammenarbeiten, um unter anderem zu überprüfen, ob die Drittpartei eine Website mit Anleitungen zum Schiedsverfahren unterhält, einschließlich: (1) der Einleitung von Verfahren und der Einreichung von Dokumenten; (2) der vom Ministerium geführten Liste von Schiedsrichtern und der Auswahl von Schiedsrichtern aus dieser Liste; (3) der vom Ministerium und der Kommission angenommenen Schiedsverfahren und Verhaltenskodizes für Schiedsrichter;[4] und (4) der Erhebung und Zahlung von Schiedsrichtergebühren. Darüber hinaus wird das Ministerium mit der dritten Partei zusammenarbeiten, um die Funktionsweise des Schiedsfonds regelmäßig zu überprüfen, einschließlich der Notwendigkeit, die Höhe der Beiträge oder die Obergrenzen (d.*h.* die Höchstbeträge) für die Schiedskosten anzupassen, und unter anderem die Anzahl der Schiedsverfahren sowie die Kosten und den Zeitplan der Schiedsverfahren zu

berücksichtigen, wobei eine übermäßige finanzielle Belastung vermieden werden soll.

---

[3] Das Internationale Zentrum für Streitbeilegung ("IZRS"), die internationale Abteilung der American Arbitration Association ("AAA") (zusammen "IZRS-AAA"), wurde vom Ministerium ausgewählt, um Schiedsverfahren gemäß Anhang I der Grundsätze zu verwalten und den dort genannten Schiedsfonds zu führen.

[4] Am 15. September 2017 einigten sich das Ministerium und die Kommission auf die Annahme einer Reihe von Schiedsregeln zur Regelung verbindlicher Schiedsverfahren, die in Anhang I der Grundsätze beschrieben sind, 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 sind übereingekommen, die Schiedsgerichtsordnung und den Verhaltenskodex an die Aktualisierungen im Rahmen der DPF EU-USA anzupassen, und das Ministerium wird mit der ICDR-AAA zusammenarbeiten, um diese Aktualisierungen vorzunehmen.

die den DPF-Organisationen der EU und der USA auferlegt werden. Das Ministerium wird die Kommission über das Ergebnis solcher Überprüfungen mit dem Dritten unterrichten und die Kommission vorab über etwaige Anpassungen der Höhe der Beiträge informieren.

Durchführung gemeinsamer Überprüfungen der Funktionsweise der DPF zwischen der EU und den USA

Das Ministerium und andere Agenturen werden in regelmäßigen Abständen Treffen mit der Kommission, interessierten Datenschutzbehörden und geeigneten Vertretern des EDPB abhalten, bei denen das Ministerium über den aktuellen Stand der EU-US-DSGVO informieren wird. Bei den Treffen werden aktuelle Fragen im Zusammenhang mit der Funktionsweise, Umsetzung, Überwachung und Durchsetzung des Datenschutzrahmenprogramms erörtert. Bei den Treffen können gegebenenfalls auch verwandte Themen erörtert werden, wie z. B. andere Datenübertragungsmechanismen, die von den Garantien der EU-US-DSGVO profitieren.

Aktualisierung von Gesetzen

Das Ministerium wird sich in angemessener Weise bemühen, die Kommission über wesentliche Entwicklungen in der Gesetzgebung der Vereinigten Staaten zu informieren, soweit sie für die DPF EU-USA im Bereich des Datenschutzes und der Beschränkungen und Garantien für den Zugang zu personenbezogenen Daten durch US-Behörden und deren anschließende Verwendung von Bedeutung sind.

Zugang der US-Regierung zu persönlichen Daten

Die Vereinigten Staaten haben die Executive Order 14086 "Enhancing Safeguards for United States Signals Intelligence Activities" und 28 CFR part 201 zur Änderung der Vorschriften des Justizministeriums erlassen, um das Datenschutz-Überprüfungsgericht (Data Protection Review Court - DPRC) einzurichten, die einen starken Schutz für personenbezogene Daten im Hinblick auf den Zugriff der Regierung auf Daten für Zwecke der nationalen Sicherheit bieten. Der Schutz umfasst die Stärkung des Schutzes der Privatsphäre und der bürgerlichen Freiheiten, um zu gewährleisten, dass die Aktivitäten der US-Signalerfassung für die Verfolgung definierter nationaler Sicherheitsziele notwendig und verhältnismäßig sind, die Einrichtung eines neuen Rechtsbehelfsmechanismus mit unabhängiger und verbindlicher Autorität und die Verbesserung der bestehenden strengen und vielschichtigen Aufsicht über die Aktivitäten der US-Signalerfassung. Durch diese Schutzmaßnahmen können EU-Personen einen neuen mehrstufigen Rechtsbehelfsmechanismus in Anspruch nehmen, der einen unabhängigen DPRC umfasst, der sich aus Personen zusammensetzt, die nicht der US-Regierung angehören und die uneingeschränkte Befugnis haben, über Ansprüche zu entscheiden und bei Bedarf Abhilfemaßnahmen anzuordnen. Das Ministerium wird ein Verzeichnis der EU-Personen führen, die eine qualifizierte Beschwerde gemäß der Executive Order 14086 und 28 CFR Teil 201 einreichen. Fünf Jahre nach dem Datum dieses Schreibens und danach alle fünf Jahre wird sich das Ministerium mit den zuständigen Stellen in Verbindung setzen, um zu erfahren, ob die Informationen über die Überprüfung von qualifizierten Beschwerden oder die Überprüfung von Anträgen auf Überprüfung, die beim DPRC eingereicht wurden, freigegeben wurden. Wenn derartige Informationen freigegeben wurden, 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 behandelt werden, die den rechtlichen Anforderungen der EU in Bezug auf den Zugang der Behörden zu den Daten entspricht.

Auf der Grundlage der Grundsätze, der Executive Order 14086, 28 CFR part 201 und der begleitenden Schreiben und Materialien, einschließlich der Verpflichtungen des Ministeriums hinsichtlich der Verwaltung und Überwachung des Data Privacy Framework-Programms, gehen wir davon aus, dass die Kommission feststellen wird, dass das EU-U.S. DPF einen angemessenen Schutz für die

Für die Zwecke des EU-Rechts und der Datenübermittlung aus der Europäischen Union an Organisationen, die an der EU-US-DSGVO teilnehmen, wird dies auch weiterhin der Fall sein. Wir gehen auch davon aus, dass Übermittlungen an US-Organisationen, die auf der Grundlage von EU-Standardvertragsklauseln oder verbindlichen EU-Unternehmensregeln erfolgen, durch die Bedingungen dieser Vereinbarungen weiter erleichtert werden.

Mit freundlichen Grüßen,

Marisa Lago

Marisa Lago

**ANHANG IV**

VEREINIGTE STAATEN VON AMERIKA

Bundeshandelskommission

WASHINGTON, D.C. 20580

Büro des Vorsitzenden

9. Juni 2023

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

Sehr geehrter Herr Kommissar Reynders:

Die Federal Trade Commission der Vereinigten Staaten ("FTC") weiß es zu schätzen, dass sie Gelegenheit hat, ihre Rolle bei der Durchsetzung der Grundsätze des EU-U.S. Data Privacy Framework ("EU- U.S. DPF") zu erläutern. Die FTC setzt sich seit langem für den Schutz der Verbraucher und der Privatsphäre über die Grenzen hinweg ein, und wir engagieren uns für die Durchsetzung der handelsrechtlichen Aspekte dieses Rahmens. Die FTC nimmt diese Aufgabe seit dem Jahr 2000 wahr, und zwar im Zusammenhang mit dem Safe Harbor und zuletzt seit 2016 im Zusammenhang mit dem EU-U.S. Privacy Shield Framework.[1] Am 16. Juli 2020 erklärte der Gerichtshof der Europäischen Union ("EuGH") die Angemessenheitsentscheidung der Europäischen Kommission, die dem EU-US-Datenschutzschild zugrunde liegt, für ungültig, und zwar auf der Grundlage anderer Aspekte als der von der FTC durchgesetzten Handelsgrundsätze. Die USA und die Europäische Kommission haben seitdem den EU-US-Datenschutzrahmen ausgehandelt, um dem Urteil des EuGH Rechnung zu tragen.

Mit diesem Schreiben bekräftige ich das Engagement der FTC für eine konsequente Durchsetzung der EU-US-Datenschutzgrundsätze. Insbesondere bekräftigen wir unser Engagement in drei Schlüsselbereichen: (1) Verweisungspriorisierung und Ermittlungen; (2) Einholung und Überwachung von Anordnungen; und (3) Durchsetzungszusammenarbeit mit EU-Datenschutzbehörden ("DPAs").

## I. Einführung

### a. FTC Durchsetzung des Datenschutzes und politische Arbeit

Die FTC verfügt über umfassende zivilrechtliche Durchsetzungsbefugnisse zur Förderung des Verbraucherschutzes und des Wettbewerbs im gewerblichen Bereich. Im Rahmen ihres Verbraucherschutzmandats setzt die FTC eine Vielzahl von Gesetzen zum Schutz der Privatsphäre und der Sicherheit der Verbraucher und ihrer Daten durch.

[1] Letter from Chairwoman Edith Ramirez to Věra Jourová, Commissioner for Justice, Consumers and Gender Equality of the European Commission, Describing Federal Trade Commission Enforcement of the New EU-U.S. Privacy Shield Framework (29. Februar 2016), *verfügbar 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 auch schon früher verpflichtet, das Safe-Harbor-Programm 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. Dieses Schreiben ersetzt diese früheren Verpflichtungen.

Das wichtigste von der FTC durchgesetzte Gesetz, der FTC Act, verbietet "unfaire" oder "betrügerische" Handlungen oder Praktiken im oder mit Bezug auf den Handel.[2] Die FTC setzt auch gezielte Gesetze zum Schutz von Gesundheits-, Kredit- und anderen Finanzdaten sowie von Online-Daten von Kindern durch und hat zu jedem dieser Gesetze Durchführungsbestimmungen erlassen.[3]

Die FTC hat in letzter Zeit auch zahlreiche Initiativen ergriffen, um ihre Arbeit zum Schutz der Privatsphäre zu verstärken.

Im August 2022 kündigte die FTC an, dass sie Regeln zur Bekämpfung von schädlicher kommerzieller Überwachung und laxer Datensicherheit erwägt.[4] Ziel des Projekts ist es, eine solide öffentliche Dokumentation zu erstellen, die Aufschluss darüber gibt, ob die FTC Regeln zur Bekämpfung der kommerziellen Überwachung und der Datensicherheitspraktiken erlassen sollte und wie diese Regeln möglicherweise aussehen sollten. Wir freuen uns über Kommentare von EU-Stakeholdern zu dieser und anderen Initiativen.

Auf unseren "PrivacyCon"-Konferenzen kommen weiterhin führende Forscher zusammen, um die neuesten Forschungsergebnisse und Trends im Zusammenhang mit dem Schutz der Privatsphäre der Verbraucher und der Datensicherheit zu diskutieren. Wir haben auch die Fähigkeit unserer Behörde 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 Kollegen bei der Europäischen Kommission angekündigt, der sich mit datenschutzrelevanten Themen wie dunklen Mustern und Geschäftsmodellen befasst, die durch eine allgegenwärtige Datenerfassung gekennzeichnet sind.[5] Außerdem haben wir vor kurzem einen Bericht an den Kongress herausgegeben, in dem wir vor den Schäden warnen, die mit dem Einsatz von künstlicher Intelligenz ("AI") verbunden sind, um die vom Kongress festgestellten Online-Schäden zu beseitigen. In diesem Bericht wurden Bedenken hinsichtlich Ungenauigkeit, Voreingenommenheit, Diskriminierung und schleichender kommerzieller Überwachung geäußert.[6]

### b. U.S.-Rechtsschutz zugunsten der EU-Verbraucher

Die EU-US-DSGVO steht im Kontext der größeren US-Datenschutzlandschaft, die auch die EU-Verbraucher in mehrfacher Hinsicht schützt. Das im FTC Act verankerte Verbot unlauterer oder irreführender Handlungen oder Praktiken beschränkt sich nicht auf den Schutz von US-Verbrauchern vor US-Unternehmen, da es auch Praktiken einschließt, die (1) eine vernünftigerweise vorhersehbare Schädigung in den USA verursachen oder wahrscheinlich verursachen werden.

die Vereinigten Staaten, oder (2) ein wesentliches Verhalten in den Vereinigten Staaten beinhalten. Außerdem kann die FTC zum Schutz ausländischer Verbraucher alle Rechtsmittel einsetzen, die zum Schutz inländischer Verbraucher zur Verfügung stehen.[7]

---

[2] 15 U.S.C. § 45(a). Die FTC ist nicht zuständig für die Strafverfolgung oder Fragen der nationalen Sicherheit. Ebenso wenig kann die FTC in die meisten anderen staatlichen Maßnahmen eingreifen. Darüber hinaus gibt es Ausnahmen von der Zuständigkeit der FTC für gewerbliche Tätigkeiten, u. a. für Banken, Fluggesellschaften, das Versicherungswesen und die Tätigkeit von Telekommunikationsdienstleistern als "common carrier". Die FTC ist auch nicht für die meisten gemeinnützigen Organisationen zuständig, wohl aber für Schein-Wohltätigkeitsorganisationen oder andere gemeinnützige Organisationen, die in Wirklichkeit gewinnorientiert arbeiten. Die FTC ist auch für Non-Profit-Organisationen zuständig, die zum Nutzen ihrer gewinnorientierten Mitglieder tätig sind, indem sie diesen Mitgliedern z. B. erhebliche wirtschaftliche Vorteile verschaffen. In einigen Fällen deckt sich die Zuständigkeit der FTC mit der anderer Strafverfolgungsbehörden. Wir haben enge Arbeitsbeziehungen zu Bundes- und Landesbehörden aufgebaut und arbeiten eng mit ihnen zusammen, um Untersuchungen zu koordinieren oder gegebenenfalls Überweisungen vorzunehmen.

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

[4] *Siehe* Pressemitteilung, Fed. Trade Comm'n, FTC Explores Rules Cracking Down on Commercial Surveillance and Lax Data Security Practices (Aug. 11, 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, Fed. Trade Comm'n, FTC Report Warns About Using Artificial Intelligence to Combat Online Problems (Juni 16, 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 ausländischen Handel betreffen, die (i) eine vernünftigerweise vorhersehbare Schädigung in den Vereinigten Staaten verursachen oder wahrscheinlich verursachen werden; oder (ii) ein wesentliches Verhalten innerhalb der Vereinigten Staaten beinhalten. 15 U.S.C. § 45(a)(4)(A).

Die FTC setzt auch andere gezielte Gesetze durch, deren Schutz sich auch auf Nicht-US-Verbraucher erstreckt, wie z. B. den Children's Online Privacy Protection Act (COPPA"). COPPA schreibt unter anderem vor, dass Betreiber von Websites und Online-Diensten, die sich an Kinder richten, oder von Websites für ein allgemeines Publikum, die wissentlich personenbezogene Daten von Kindern unter 13 Jahren erheben, die Eltern darüber informieren und die überprüfbare Zustimmung der Eltern einholen müssen. In den USA ansässige Websites und Dienste, die dem COPPA unterliegen und personenbezogene Daten von ausländischen Kindern erfassen, müssen das COPPA einhalten. Auch Websites und Online-Dienste mit Sitz im Ausland müssen COPPA einhalten, wenn sie sich an Kinder in den Vereinigten Staaten richten oder wissentlich personenbezogene Daten von Kindern in den Vereinigten Staaten erheben. Zusätzlich zu den US-Bundesgesetzen, die von der FTC durchgesetzt werden, können auch andere Bundes- und Landesgesetze zum Verbraucherschutz, zu Datenschutzverletzungen und zum Schutz der Privatsphäre den EU-Verbrauchern zusätzliche Vorteile bieten.

### c. FTC-Durchsetzungsaktivitäten

Die FTC hat sowohl im Rahmen von Safe Harbor als auch von EU-U.S. Privacy Shield Verfahren angestrengt und das EU-U.S. Privacy Shield auch dann noch durchgesetzt, als der EuGH die Angemessenheitsentscheidung, die dem EU-U.S. Privacy Shield zugrunde liegt, für ungültig erklärte.[8] Mehrere der jüngsten Beschwerden der FTC enthielten Vorwürfe, dass Unternehmen gegen die EU-
U.S. Privacy Shield-Bestimmungen, unter anderem in Verfahren gegen Twitter,[9] CafePress,[10] und Flo.[11] In der Vollstreckungsklage gegen Twitter hat die FTC 150 Millionen Dollar von Twitter erhalten, weil das Unternehmen mit seinen Praktiken, die mehr als 140 Millionen Kunden betreffen, gegen eine frühere FTC-Anordnung verstoßen hat, darunter auch gegen den Grundsatz 5 des EU-US-Datenschutzschildes (Datenintegrität und Zweckbindung). Darüber hinaus verlangt die Anordnung der Behörde, dass Twitter seinen Nutzern die Verwendung sicherer Multi-Faktor-Authentifizierungsmethoden ermöglicht, bei denen die Nutzer ihre Telefonnummern nicht angeben müssen.

Im Fall von *CafePress warf* die FTC dem Unternehmen vor, die sensiblen Daten von Verbrauchern nicht zu schützen, einen größeren Datenschutzverstoß zu vertuschen und gegen die Grundsätze 2 (Wahlmöglichkeit), 4 (Sicherheit) und 6 (Zugang) des EU-US-Datenschutzschilds zu verstoßen. Die Anordnung der FTC verlangt von dem Unternehmen, die unzureichenden Authentifizierungsmaßnahmen durch eine Multifaktor-Authentifizierung zu ersetzen, die Menge der gesammelten und gespeicherten Daten erheblich einzuschränken, die Sozialversicherungsnummern zu verschlüsseln und die Informationssicherheitsprogramme durch einen Dritten bewerten zu lassen und der FTC eine Kopie zu übermitteln, die veröffentlicht werden kann.

In *Flo* behauptete die FTC, dass die App zur Nachverfolgung der Fruchtbarkeit Gesundheitsinformationen der Nutzer an Drittanbieter von Datenanalysen weitergegeben hat, obwohl sie sich verpflichtet hatte, diese Informationen geheim zu halten. Die
Die FTC-Beschwerde verweist insbesondere auf die Interaktionen des Unternehmens mit EU-Verbrauchern und darauf, dass Flo gegen die Grundsätze des EU-US-Datenschutzschilds 1 (Benachrichtigung), 2 (Wahlmöglichkeit), 3 (Verantwortlichkeit für die Weitergabe) und 5 (Datenintegrität und Zweckbindung) verstoßen hat. Die Anordnung der Behörde verlangt von Flo unter anderem, die betroffenen Nutzer über die Offenlegung ihrer personenbezogenen Daten zu informieren und alle Dritten, die Gesundheitsdaten der Nutzer erhalten haben, anzuweisen, diese Daten zu vernichten.
Wichtig ist, dass die Anordnungen der FTC alle Verbraucher weltweit schützen, die mit einem US-Unternehmen zu tun haben, und nicht nur die Verbraucher, die eine Beschwerde eingereicht haben.

Viele frühere Fälle der Durchsetzung von Safe Harbor und des EU-US-Datenschutzschilds betrafen Organisationen, die eine erste Selbstzertifizierung durch das

Department of

[8] Anhang A enthält eine Liste der Safe Harbor- und Privacy Shield-Angelegenheiten der FTC.
[9] *Siehe* Pressemitteilung, Fed. Trade Comm'n, 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, Fed. Trade Comm'n, FTC Takes Action Against CafePress for Data Breach Cover Up (März 15, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/03/ftc-takes-action-against-cafepress-data- breach-cover.
[11] *See* Press Release, Fed. Trade Comm'n, 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.

Commerce, versäumten es aber, ihre jährliche Selbstzertifizierung aufrechtzuerhalten, während sie sich weiterhin als aktuelle Teilnehmer ausgaben. Andere Fälle betrafen falsche Behauptungen über die Teilnahme von Organisationen, die nie eine erste Selbstzertifizierung durch das Handelsministerium vorgenommen hatten. Wir gehen davon aus, dass wir unsere proaktiven Durchsetzungsbemühungen in Zukunft auf die Arten von Verstößen gegen die DPF-Prinzipien zwischen der EU und den USA konzentrieren werden, die in Fällen wie Twitter, CafePress und Flo vorgebracht wurden. In der Zwischenzeit wird das Handelsministerium den Selbstzertifizierungsprozess verwalten und überwachen, die maßgebliche Liste der EU-U.S. DPF-Teilnehmer führen und andere Fragen zur Teilnahme am Programm klären.[12] Wichtig ist, dass Organisationen, die eine Teilnahme am EU-U.S. DPF-Programm beanspruchen, der materiellen Durchsetzung der EU-U.S. DPF-Prinzipien unterliegen können, auch wenn sie ihre Selbstzertifizierung nicht durch das Handelsministerium vornehmen oder aufrechterhalten.

## II. Verweisungspriorisierung und Ermittlungen

Wie bereits im Rahmen des US-EU Safe Harbor Framework und des EU-U.S. Privacy Shield Framework verpflichtet sich die FTC, Verweise des Handelsministeriums und der EU-Mitgliedstaaten auf die EU-U.S. DPF Principles vorrangig zu prüfen. Wir werden auch vorrangig Verweise von Selbstregulierungsorganisationen für den Datenschutz und anderen unabhängigen Streitbeilegungsstellen wegen Nichteinhaltung der EU-U.S. DPF-Prinzipien berücksichtigen.

Zur Erleichterung von Verweisungen im Rahmen der DPF EU-USA aus den EU-Mitgliedstaaten hat die FTC ein standardisiertes Verweisungsverfahren eingeführt und den EU-Mitgliedstaaten Leitlinien für die Art von Informationen an die Hand gegeben, die der FTC bei ihrer Untersuchung einer Verweisung am besten helfen. Im Rahmen dieser Bemühungen hat die FTC eine Kontaktstelle für Verweisungen aus den EU-Mitgliedstaaten benannt. Sie ist dann am nützlichsten, wenn die verweisende Behörde eine Voruntersuchung des mutmaßlichen Verstoßes durchgeführt hat und mit der FTC bei einer Untersuchung zusammenarbeiten kann.

Nach Erhalt einer solchen Verweisung durch das Handelsministerium, einen EU-Mitgliedstaat, eine Selbstregulierungsorganisation oder eine andere unabhängige Streitbeilegungsstelle kann die FTC eine Reihe von Maßnahmen ergreifen, um die aufgeworfenen Probleme zu lösen. So können wir beispielsweise die Datenschutzrichtlinien der Organisation überprüfen, weitere Informationen direkt von der Organisation oder von Dritten einholen, mit der verweisenden Stelle Kontakt aufnehmen, beurteilen, ob es ein Muster von Verstößen oder eine erhebliche Anzahl von betroffenen Verbrauchern gibt, feststellen, ob die Verweisung Fragen betrifft, die in den Zuständigkeitsbereich des Handelsministeriums fallen, beurteilen, ob zusätzliche Anstrengungen zur Unterrichtung der Marktteilnehmer hilfreich wären, und gegebenenfalls ein Durchsetzungsverfahren einleiten.

Neben der vorrangigen Behandlung von Verweisen des Handelsministeriums, der EU-Mitgliedstaaten und von Selbstregulierungsorganisationen für den Datenschutz oder anderen unabhängigen Streitbeilegungsgremien[13] wird die FTC auch weiterhin auf eigene Initiative erhebliche Verstöße gegen die EU-U.S.-Grundsätze 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 untersucht, ob die fragliche Einrichtung EU- und US-Datenschutzbestimmungen einhält.
Zusicherungen des US-Datenschutzschilds. Wenn das Unternehmen solche Zusicherungen gemacht hat und die Untersuchung offensichtliche Verstöße gegen die Grundsätze des EU-US-Datenschutzschildes ergeben hat, hat die FTC die Vorwürfe von Verstößen gegen das EU-US-Datenschutzschild in ihre Durchsetzungsmaßnahmen aufgenommen. Wir werden diesen proaktiven Ansatz fortsetzen, jetzt auch in Bezug auf die EU-US-Datenschutzschild-Grundsätze.

[12] Schreiben von Marisa Lago, Unterstaatssekretärin für internationalen Handel, an den ehrenwerten Didier

Reynders, Kommissar für Justiz, Europäische Kommission (12. Dezember 2022).
[13] Obwohl die FTC einzelne Verbraucherbeschwerden nicht löst oder vermittelt, versichert sie, dass sie Verweisungen von EU-DPAs auf die EU-U.S. DPF-Prinzipien vorrangig behandeln wird. Darüber hinaus nutzt die FTC die Beschwerden in ihrer Consumer-Sentinel-Datenbank, auf die auch viele andere Strafverfolgungsbehörden zugreifen können, um Trends zu erkennen, Durchsetzungsprioritäten festzulegen und potenzielle Ermittlungsziele zu identifizieren. EU-Bürger können das gleiche Beschwerdesystem nutzen, das auch US-Verbrauchern zur Verfügung steht, um eine Beschwerde bei der FTC einzureichen: https://reportfraud.ftc.gov/. Für individuelle Beschwerden über die DPF-Prinzipien zwischen der EU und den USA ist es für EU-Bürger jedoch möglicherweise am sinnvollsten, Beschwerden bei der Datenschutzbehörde ihres Mitgliedstaats oder einer unabhängigen Streitbeilegungsstelle einzureichen.

## III. Beantragung und Überwachung von Aufträgen

Die FTC bekräftigt auch ihre Verpflichtung, Vollstreckungsanordnungen zu erwirken und zu überwachen, um die Einhaltung der EU-U.S. DPF-Prinzipien sicherzustellen. Wir werden die Einhaltung der EU-U.S. DPF-Prinzipien durch eine Reihe geeigneter Unterlassungsbestimmungen in künftigen Anordnungen der FTC zu den EU-U.S. DPF-Prinzipien verlangen. Verstöße gegen die Verwaltungsanordnungen der FTC können zivilrechtliche Strafen von bis zu 50.120 Dollar pro Verstoß bzw. 50.120 Dollar pro Tag bei fortgesetztem Verstoß nach sich ziehen,[14] die sich im Falle von Praktiken, die viele Verbraucher betreffen, auf Millionen von Dollar belaufen können. Jede Zustimmungsanordnung enthält auch Bestimmungen zur Berichterstattung und Einhaltung der Vorschriften. Die beauftragten Unternehmen müssen Dokumente, die ihre Einhaltung der Vorschriften belegen, für eine bestimmte Anzahl von Jahren aufbewahren. Die Anordnungen müssen auch an die Mitarbeiter weitergegeben werden, die für die Einhaltung der Anordnung verantwortlich sind.

Wie bei allen ihren Anordnungen überwacht die FTC systematisch die Einhaltung der bestehenden Anordnungen zum EU-US-Datenschutzschild und ergreift bei Bedarf Maßnahmen zu deren Durchsetzung.[15] Wichtig ist, dass die Anordnungen der FTC weiterhin alle Verbraucher weltweit schützen, die mit einem Unternehmen interagieren, und nicht nur die Verbraucher, die eine Beschwerde eingereicht haben. Schließlich wird die FTC eine Online-Liste der Unternehmen führen, die von Anordnungen betroffen sind, die im Zusammenhang mit der Durchsetzung der EU-U.S. DPF-Prinzipien ergangen sind.[16]

## IV. Durchsetzungszusammenarbeit mit EU-DPAs

Die FTC erkennt die wichtige Rolle an, die die EU-Datenschutzbehörden bei der Einhaltung der EU-US-DSGVO spielen können, und befürwortet eine verstärkte Konsultation und 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 vorbehaltlich der Vertraulichkeitsgesetze und -beschränkungen Informationen über Verweisungen mit den verweisenden Durchsetzungsbehörden austauschen, einschließlich des Status von Verweisungen. Soweit dies angesichts der Anzahl und Art der eingegangenen Verweisungen möglich ist, werden die übermittelten Informationen eine Bewertung der vermittelten Angelegenheiten enthalten, einschließlich einer Beschreibung der wesentlichen aufgeworfenen Fragen und der Maßnahmen, die zur Behebung von Rechtsverstößen im Zuständigkeitsbereich der FTC ergriffen wurden. Die FTC wird der verweisenden Behörde auch Rückmeldung über die Art der erhaltenen Verweisungen geben, um die Wirksamkeit der Bemühungen zur Bekämpfung rechtswidrigen Verhaltens zu erhöhen. Ersucht eine verweisende Behörde um Informationen über den Status einer bestimmten Verweisung, um ihr eigenes Vollstreckungsverfahren fortzusetzen, wird die FTC unter Berücksichtigung der Anzahl der in Frage kommenden Verweisungen und vorbehaltlich der Vertraulichkeit und anderer rechtlicher Anforderungen antworten.

Die FTC wird auch eng mit den Datenschutzbehörden der EU zusammenarbeiten, um Unterstützung bei der Durchsetzung zu leisten. In geeigneten Fällen könnte dies den Austausch von Informationen und die Unterstützung bei Ermittlungen gemäß dem U.S. SAFE WEB Act umfassen, der die FTC zur Unterstützung ausländischer Strafverfolgungsbehörden ermächtigt, wenn die ausländische Behörde Gesetze durchsetzt, die Praktiken verbieten, die im Wesentlichen denjenigen ähneln, die durch die von der FTC durchgesetzten Gesetze verboten sind.[17] Im Rahmen dieser Unterstützung kann die FTC Informationen weitergeben, die sie im Zusammenhang mit einer FTC-Untersuchung erhalten hat, und Zwangsmaßnahmen gegen

---

[14] 15 U.S.C. § 45(m); 16 C.F.R. § 1.98. Dieser Betrag wird in regelmäßigen Abständen an die Inflation angepasst.
[15] Letztes Jahr hat die FTC beschlossen, das Verfahren zur Untersuchung von Wiederholungstätern zu

straffen. *Siehe* Pressemitteilung, Fed. Trade Comm'n, FTC Authorizes Investigations into Key Enforcement Priorities (Jul. 1, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/07/ftc-authorizes-investigations-key-enforcement- priorities.

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

[17] Bei der Entscheidung, ob sie von ihrer Befugnis nach dem U.S. SAFE WEB Act Gebrauch machen soll, berücksichtigt die FTC *unter anderem*: "(A) ob die ersuchende Behörde sich bereit erklärt hat, der Kommission gegenseitige Unterstützung zu gewähren oder gewähren wird; (B) ob die Befolgung des Ersuchens dem öffentlichen Interesse der Vereinigten Staaten schaden würde; und (C) ob die Untersuchung oder das Durchsetzungsverfahren der ersuchenden Behörde Handlungen oder Praktiken betrifft, die einer erheblichen Anzahl von Personen Schaden zufügen oder zufügen können. 15 U.S.C. § 46(j)(3). Diese Befugnis gilt nicht für die Durchsetzung von Wettbewerbsgesetzen.

Die FTC ist befugt, im Namen der EU-Behörde, die ihre eigenen Ermittlungen durchführt, mündliche Aussagen von Zeugen oder Angeklagten im Zusammenhang mit dem Durchsetzungsverfahren der Behörde einzuholen, vorbehaltlich der Anforderungen des US-amerikanischen SAFE WEB Act. Die FTC macht von dieser Befugnis regelmäßig Gebrauch, um andere Behörden in der ganzen Welt in Fällen von Datenschutz und Verbraucherschutz zu unterstützen.

Zusätzlich zu den Konsultationen mit den verweisenden EU-Datenschutzbehörden zu fallspezifischen Fragen wird die FTC an regelmäßigen Treffen mit benannten Vertretern des Europäischen Datenschutzausschusses ("EDPB") teilnehmen, um allgemein zu erörtern, wie die Zusammenarbeit bei der Durchsetzung verbessert werden kann. Die FTC wird außerdem zusammen mit dem Handelsministerium, der Europäischen Kommission und Vertretern des EDPB an der regelmäßigen Überprüfung der EU-US-DSGVO teilnehmen, um deren Umsetzung zu diskutieren. Die FTC unterstützt auch die Entwicklung von Instrumenten, die die Zusammenarbeit mit den Datenschutzbehörden in der EU sowie mit anderen Datenschutzbehörden auf der ganzen Welt verbessern werden. Die FTC freut sich, ihr Engagement für die Durchsetzung der Aspekte des gewerblichen Sektors der EU-US-DSGVO zu bekräftigen. Wir sehen unsere Partnerschaft mit den EU-Kollegen als einen wichtigen Teil des Datenschutzes für unsere und Ihre Bürger an.

Mit freundlichen Grüßen,

Lina M. Khan
Vorsitz, Federal Trade Commission

# Anhang A

## Durchsetzung von Datenschutzschild und Safe Harbor

| | Docket/FTC File No. | Fall | Link |
|---|---|---|---|
| | | | |
| 1 | FTC-Akte Nr. 2023062<br>Fall Nr. 3:22-cv-03070<br>(N.D. Cal.) | US vs. **Twitter, Inc.** | Twitter |
| 2 | FTC-Akte Nr. 192 3209 | In Sachen Residual Pumpkin Entity, LLC, vormals d/b/a **CafePress**, und PlanetArt, LLC, d/b/a **CafePress** | CafePress |
| 3 | FTC-Akte Nr. 192 3133<br>Aktenzeichen C-4747 | In der Angelegenheit **Flo Health, Inc.** | Flo Gesundheit |
| 4 | FTC-Akte Nr. 192 3050<br>Aktenzeichen C-4723 | In der Angelegenheit **Ortho-Clinical Diagnostics, Inc.** | Ortho-Klinik |
| 5 | FTC-Akte Nr. 192 3092<br>Aktenzeichen C-4709 | In der Angelegenheit **T&M Protection, LLC** | T&M Schutz |
| 6 | FTC-Akte Nr. 192 3084<br>Aktenzeichen C-4704 | In der Angelegenheit **TDARX, Inc.** | TDARX |
| 7 | FTC-Akte Nr. 192 3093<br>Aktenzeichen C-4706 | In der Angelegenheit **Global Data Vault, LLC** | Globale Daten |
| 8 | FTC-Akte Nr. 192 3078<br>Aktenzeichen C-4703 | In der Angelegenheit **Incentive Services, Inc.** | Incentive -Dienste |
| 9 | FTC-Akte Nr. 192 3090<br>Aktenzeichen C-4705 | In der Angelegenheit **Click Labs, Inc.** | Klick-Labore |
| 10 | FTC-Akte Nr. 182 3192<br>Aktenzeichen C-4697 | In der Angelegenheit **Medable, Inc.** | Abrufbar unter |
| 11 | FTC-Akte Nr. 182 3189<br>Dossier Nr. 9386 | In der Angelegenheit NTT Global Data Centers Americas, Inc. als Rechtsnachfolgerin von **RagingWire Data Centers, Inc.** | RagingWire |
| 12 | FTC-Akte Nr. 182 3196<br>Aktenzeichen C-4702 | In der Angelegenheit **Thru, Inc.** | Über |
| 13 | FTC-Akte Nr. 182 3188<br>Aktenzeichen C-4698 | In der Angelegenheit **DCR Workforce, Inc.** | DCR Belegschaft |
| 14 | FTC-Akte Nr. 182 3194<br>Dossier Nr. C-4700 | In der Angelegenheit **LotaData, Inc.** | LotaData |
| 15 | FTC-Akte Nr. 182 3195<br>Aktenzeichen C-4701 | In der Angelegenheit **EmpiriStat, Inc.** | EmpiriStat |
| 16 | FTC-Akte Nr. 182 3193<br>Aktenzeichen C-4699 | In Sachen 214 Technologies, Inc., auch d/b/a **Trueface.ai** | Trueface.ai |
| 17 | FTC-Akte Nr. 182 3107<br>Dossier Nr. 9383 | In der Angelegenheit **Cambridge Analytica, LLC** | Cambridge Analytica |
| 18 | FTC-Akte Nr. 182 3152<br>Aktenzeichen C-4685 | In der Angelegenheit **SecureTest, Inc.** | SecurTest |
| 19 | FTC-Akte Nr. 182 3144<br>Aktenzeichen C-4664 | In der Angelegenheit **VenPath, Inc.** | VenPath |

| | | | |
|---|---|---|---|
| 20 | FTC-Akte Nr. 182 3154<br>Aktenzeichen C-4666 | In der Angelegenheit **SmartStart Employment Screening, Inc.** | SmartStart |
| 21 | FTC-Akte Nr. 182 3143<br>Aktenzeichen C-4663 | In der Angelegenheit **mResourceLLC,** d/b/a Loop Works LLC | mResource |
| 22 | FTC-Akte Nr. 182 3150<br>Aktenzeichen C-4665 | In der Angelegenheit **Idmission LLC** | IDmission |
| 23 | FTC-Akte Nr. 182 3100<br>Aktenzeichen C-4659 | In der Angelegenheit **ReadyTech Corporation** | ReadyTech |
| 24 | FTC-Akte Nr. 172 3173<br>Aktenzeichen C-4630 | In der Angelegenheit **Decusoft, LLC** | Decusoft |
| 25 | FTC-Akte Nr. 172 3171<br>Aktenzeichen C-4628 | In der Angelegenheit **Tru Communication, Inc.** | Tru |
| 26 | FTC-Akte Nr. 172 3172<br>Aktenzeichen C-4629 | In der Angelegenheit **Md7, LLC** | Md7 |
| 30 | FTC-Akte Nr. 152 3198<br>Aktenzeichen C-4543 | In der Angelegenheit **Jhayrmaine Daniels (d/b/a California Skate-Line)** | Jhayrmaine Daniels |
| 31 | FTC-Akte Nr. 152 3190<br>Aktenzeichen C-4545 | In der Angelegenheit **Dale Jarrett Racing Adventure, Inc.** | Dale Jarrett |
| 32 | FTC-Akte Nr. 152 3141<br>Aktenzeichen C-4540 | In der Angelegenheit **Golf Connect, LLC** | Golf verbinden |
| 33 | FTC-Akte Nr. 152 3202<br>Aktenzeichen C-4546 | In der Angelegenheit **Inbox Group, LLC** | Posteingang Gruppe |
| 34 | Aktenzeichen 152 3187<br>Aktenzeichen C-4542 | In der Angelegenheit **IOActive, Inc.** | IOAktiv |
| 35 | FTC-Akte Nr. 152 3140<br>Aktenzeichen C-4549 | In der Angelegenheit **Jubilant Clinsys, Inc.** | Jubel |
| 36 | FTC-Akte Nr. 152 3199<br>Aktenzeichen C-4547 | In der Angelegenheit **Just Bagels Manufacturing, Inc.** | Nur Bagels |
| 37 | FTC-Akte Nr. 152 3138<br>Aktenzeichen C-4548 | In der Angelegenheit **NAICS Association, LLC** | NAICS |
| 38 | FTC-Akte Nr. 152 3201<br>Aktenzeichen C-4544 | In der Angelegenheit **One Industries Corp.** | Eine Industrie |
| 39 | FTC-Akte Nr. 152 3137<br>Aktenzeichen C-4550 | In der Angelegenheit **Pinger, Inc.** | Pinger |
| 40 | FTC-Akte Nr. 152 3193<br>Aktenzeichen C-4552 | In der Angelegenheit **SteriMed Medical Waste Solutions** | SteriMed |
| 41 | FTC-Akte Nr. 152 3184<br>Aktenzeichen C-4541 | In der Angelegenheit **Contract Logix, LLC** | Vertrag Logix |
| 42 | FTC-Akte Nr. 152 3185<br>Aktenzeichen C-4551 | In der Angelegenheit **Forensics Consulting Solutions, LLC** | Forensische Beratung |
| 43 | FTC-Akte Nr. 152 3051<br>Aktenzeichen C-4526 | In der Angelegenheit **American Int'l Mailing, Inc.** | AIM |
| 44 | FTC-Akte Nr. 152 3015<br>Aktenzeichen C-4525 | In der Angelegenheit **TES Franchising, LLC** | TES |
| 45 | FTC-Akte Nr. 142 3036<br>Aktenzeichen C-4459 | In der Angelegenheit **American Apparel, Inc.** | American Apparel |

| | | | |
|---|---|---|---|
| 46 | FTC-Akte Nr. 142 3026<br>Aktenzeichen C-4469 | In der Angelegenheit **Fantage.com, Inc.** | Fantage |
| 47 | FTC-Akte Nr. 142 3017<br>Aktenzeichen C-4461 | In der Angelegenheit **Apperian, Inc.** | Apperian |
| 48 | FTC-Akte Nr. 142 3018<br>Aktenzeichen C-4462 | In der Angelegenheit **Atlanta Falcons Football Club, LLC** | Atlanta-Falken |
| 49 | FTC-Akte Nr. 142 3019<br>Aktenzeichen C-4463 | In der Angelegenheit **Baker Tilly Virchow Krause, LLP** | Baker Tilly |
| 50 | FTC-Akte Nr. 142 3020<br>Aktenzeichen C-4464 | In der Angelegenheit **BitTorrent, Inc.** | BitTorrent |
| 51 | FTC-Akte Nr. 142 3022<br>Aktenzeichen C-4465 | In der Angelegenheit **Charles River Laboratories, Int'l** | Charles River |
| 52 | FTC-Akte Nr. 142 3023<br>Aktenzeichen C-4466 | In der Angelegenheit **DataMotion, Inc.** | DataMotion |
| 53 | FTC-Akte Nr. 142 3024<br>Aktenzeichen C-4467 | In der Angelegenheit **DDC Laboratories, Inc.** d/b/a DNA Diagnostics Center | DDC |
| 54 | FTC-Akte Nr. 142 3028<br>Aktenzeichen C-4470 | In der Angelegenheit **Level 3 Communications, LLC** | Stufe 3 |
| 55 | FTC-Akte Nr. 142 3025<br>Aktenzeichen C-4468 | In der Angelegenheit **PDB Sports, Ltd.** d/b/a Denver Broncos Football Club, LLP | Broncos |
| 56 | FTC-Akte Nr. 142 3030<br>Aktenzeichen C-4471 | In der Angelegenheit **Reynolds Consumer Products, Inc.** | Reynolds |
| 57 | FTC-Akte Nr. 142 3031<br>Aktenzeichen C-4472 | In der Angelegenheit **Receivable Management Services Corporation** | Debitoren manageme nt |
| 58 | FTC-Akte Nr. 142 3032<br>Aktenzeichen C-4473 | In der Angelegenheit **Tennessee Football, Inc.** | Tennessee Fußball |
| 59 | FTC-Akte Nr. 102 3058<br>Aktenzeichen C-4369 | In Sachen **Myspace LLC** | Myspace |
| 60 | FTC-Akte Nr. 092 3184<br>Aktenzeichen C-4365 | In der Angelegenheit **Facebook, Inc.** | Facebook |
| 61 | FTC-Akte Nr. 092 3081<br>Zivilklage Nr. 09-CV-5276 (C.D. Cal.) | FTC gegen Javian Karnani, und **Balls of Kryptonite, LLC**, d/b/a Bite Size Deals, LLC, und Best Priced Brands, LLC | Kugeln aus Kryptonit |
| 62 | FTC-Akte Nr. 102 3136<br>Aktenzeichen C-4336 | In der Angelegenheit **Google, Inc.** | Google |
| 63 | FTC-Akte Nr. 092 3137<br>Aktenzeichen C-4282 | In der Angelegenheit **World Innovators, Inc.** | Welt-Innovatore n |
| 64 | FTC-Akte Nr. 092 3141<br>Aktenzeichen C-4271 | In der Angelegenheit **Progressive Gaitways LLC** | Progressive Gehwege |
| 65 | FTC-Akte Nr. 092 3139<br>Aktenzeichen C-4270 | In der Angelegenheit **Onyx Graphics, Inc.** | Onyx-Grafiken |
| 66 | FTC-Akte Nr. 092 3138<br>Aktenzeichen C-4269 | In der Angelegenheit von **ExpatEdge Partners, LLC** | ExpatEdge |
| 67 | FTC-Akte Nr. 092 3140<br>Aktenzeichen C-4281 | In der Angelegenheit **Directors Desk LLC** | Direktorenpult |
| 68 | FTC-Akte Nr. 092 3142<br>Aktenzeichen C-4272 | In der Angelegenheit **Collectify LLC** | Sammeln Sie |

**ANHANG V**

THE SECRETARY OF TRANSPORTATION
WASHINGTON, DC 20590

6. Juli 2023

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

Sehr geehrter Herr Kommissar Reynders:

Das Verkehrsministerium der Vereinigten Staaten ("Department" oder "DOT") ist dankbar für die Gelegenheit, seine Rolle bei der Durchsetzung der Grundsätze des EU-U.S. Data Privacy Framework ("EU-U.S. DPF") zu beschreiben. Der EU-US-Datenschutzrahmen wird eine entscheidende Rolle beim Schutz personenbezogener Daten spielen, die bei kommerziellen Transaktionen in einer zunehmend vernetzten Welt übermittelt werden. Sie wird es den Unternehmen ermöglichen, wichtige Geschäfte in der globalen Wirtschaft zu tätigen, und gleichzeitig sicherstellen, dass die Verbraucher in der EU weiterhin einen wichtigen Schutz ihrer Privatsphäre genießen.

Das US-Verkehrsministerium hat sein Engagement für die Durchsetzung des Safe-Harbor-Rahmens zwischen den USA und der EU erstmals vor mehr als 22 Jahren in einem Schreiben an die Europäische Kommission öffentlich zum Ausdruck gebracht; dieses Engagement wurde 2016 in einem Schreiben zum EU-U.S. Privacy Shield Framework wiederholt und erweitert. Das US-Verkehrsministerium verpflichtete sich in diesen Schreiben, die Datenschutzgrundsätze des Safe Harbor-Rahmens zwischen den USA und der EU und anschließend die Grundsätze des EU-U.S.-Datenschutzschilds energisch durchzusetzen. Das US-Verkehrsministerium weitet diese Verpflichtung auf die Grundsätze des EU-US-Datenschutzschildes aus, und dieses Schreiben erinnert an diese Verpflichtung.

Insbesondere bekräftigt das US-Verkehrsministerium sein Engagement in den folgenden Schlüsselbereichen: (1) vorrangige Untersuchung mutmaßlicher Verstöße gegen die EU-US-DSGVO; (2) angemessene Durchsetzungsmaßnahmen gegen Einrichtungen, die falsche oder irreführende Behauptungen über die Teilnahme an der EU-US-DSGVO aufstellen; und (3) Überwachung und Veröffentlichung von Durchsetzungsanordnungen in Bezug auf Verstöße gegen die EU-US-DSGVO. Wir stellen Informationen über jede dieser Verpflichtungen und, für den notwendigen Kontext, relevante Hintergrundinformationen über die Rolle des US-Verkehrsministeriums beim Schutz der Privatsphäre der Verbraucher und der Durchsetzung der EU-US-DSGVO-Grundsätze zur Verfügung.

## 1. Hintergrund

A. Die Datenschutzbehörde des US-Verkehrsministeriums

Das Ministerium setzt sich nachdrücklich für den Schutz der Informationen ein, die Verbraucher den Fluggesellschaften und Flugscheinvermittlern zur Verfügung stellen. Die Befugnis des US-Verkehrsministeriums, in diesem Bereich Maßnahmen zu ergreifen, findet sich in 49 U.S.C. 41712, der es einem Luftfahrtunternehmen oder einem Flugscheinvermittler verbietet, sich an "unlauteren oder irreführenden Praktiken" im Luftverkehr oder beim Verkauf von

Luftverkehrsleistungen zu beteiligen. Abschnitt 41712 ist an Abschnitt 5 des Federal Trade Commission (FTC) Act (15 U.S.C. 45) angelehnt. Kürzlich hat das US-Verkehrsministerium (DOT) Vorschriften zur Definition unlauterer und irreführender Praktiken erlassen, die sowohl mit der Rechtsprechung des DOT als auch der FTC übereinstimmen (14 CFR § 399.79). Eine Praxis ist insbesondere dann "unlauter", wenn sie einen erheblichen Schaden verursacht oder wahrscheinlich verursacht, der nicht vernünftigerweise vermeidbar ist, und der Schaden nicht durch Vorteile für die Verbraucher oder den Wettbewerb aufgewogen wird. Eine Praxis ist für die Verbraucher "irreführend", wenn sie wahrscheinlich Folgendes bewirkt

einen unter den gegebenen Umständen vernünftig handelnden Verbraucher in Bezug auf eine wesentliche Angelegenheit irreführen. Ein Sachverhalt ist wesentlich, wenn er wahrscheinlich das Verhalten oder die Entscheidung des Verbrauchers in Bezug auf ein Produkt oder eine Dienstleistung beeinflusst hat. Abgesehen von diesen allgemeinen Grundsätzen legt das US-Verkehrsministerium Abschnitt 41712 so aus, dass er Beförderern und Flugscheinvermittlern Folgendes untersagt: (1) Verstöße gegen die Bestimmungen ihrer Datenschutzpolitik; (2) Verstöße gegen Vorschriften des Ministeriums, in denen bestimmte Datenschutzpraktiken als unlauter oder irreführend bezeichnet werden; oder (3) Verstöße gegen den Children's Online Privacy Protection Act (COPPA) oder die FTC-Vorschriften zur Umsetzung des COPPA; oder (4) die Nichteinhaltung der EU-U.S. DPF-Prinzipien als Teilnehmer der DPF.[1]

Wie bereits erwähnt, ist das US-Verkehrsministerium nach Bundesrecht ausschließlich für die Regulierung der Datenschutzpraktiken von Fluggesellschaften zuständig und teilt sich die Zuständigkeit mit der FTC in Bezug auf die Datenschutzpraktiken von Flugscheinvermittlern beim Verkauf von Flugreisen.

Sobald sich ein Luftfahrtunternehmen oder ein Verkäufer von Luftverkehrsleistungen öffentlich zu den EU-U.S. DPF-Prinzipien bekennt, kann das Ministerium die gesetzlichen Befugnisse von Section 41712 nutzen, um die Einhaltung dieser Prinzipien sicherzustellen. Sobald ein Fluggast einem Luftfahrtunternehmen oder Flugscheinvermittler, der sich zur Einhaltung der EU-U.S. DPF-Prinzipien verpflichtet hat, Informationen zur Verfügung stellt, wäre daher jede Unterlassung seitens des Luftfahrtunternehmens oder des Flugscheinvermittlers ein Verstoß gegen Section 41712.

B. Praktiken der Durchsetzung

Das Amt für Verbraucherschutz in der Luftfahrt (Office of Aviation Consumer Protection, "OACP")[2] untersucht und verfolgt Fälle gemäß 49 U.S.C. 41712. Es setzt das gesetzliche Verbot in Abschnitt 41712 gegen unlautere und betrügerische Praktiken durch, und zwar in erster Linie durch Verhandlungen, die Ausarbeitung von Unterlassungsanordnungen und die Ausarbeitung von Anordnungen zur Festsetzung von Zivilstrafen. Das Amt erfährt von möglichen Verstößen hauptsächlich durch Beschwerden, die es von Einzelpersonen, Reisebüros, Fluggesellschaften sowie US-amerikanischen und ausländischen Regierungsbehörden erhält. Verbraucher können über die Website des US-Verkehrsministeriums Datenschutzbeschwerden gegen Fluggesellschaften und Reisebüros einreichen.[3]

Kommt es in einem Fall nicht zu einer vernünftigen und angemessenen Einigung, ist das OACP befugt, ein Vollstreckungsverfahren einzuleiten, das eine Beweisanhörung vor einem Verwaltungsrichter des US-Verkehrsministeriums umfasst (ALJ). Der ALJ ist befugt, Unterlassungsanordnungen und zivilrechtliche Sanktionen zu erlassen. Verstöße gegen Abschnitt 41712 können zur Ausstellung von Unterlassungserklärungen führen. Anordnungen und die Verhängung zivilrechtlicher Strafen von bis zu 37.377 $ für jeden Verstoß gegen Abschnitt 41712.

Das Ministerium ist nicht befugt, einzelnen Beschwerdeführern Schadenersatz zuzusprechen oder sie finanziell zu entschädigen. Das Ministerium ist jedoch befugt, Vergleiche zu genehmigen, die sich aus den Ermittlungen des OACP ergeben und die den Verbrauchern direkt zugute kommen (z. B. in Form von Bargeld oder Gutscheinen) und mit den ansonsten an die US-Regierung zu zahlenden Geldstrafen verrechnet werden. Dies ist in der Vergangenheit geschehen und kann auch im Zusammenhang mit dem EU-US-Abkommen geschehen. DPF-Prinzipien, wenn die Umstände dies rechtfertigen. Wiederholte Verstöße gegen Abschnitt 41712 durch eine
Dies könnte in gravierenden Fällen dazu führen, dass eine Fluggesellschaft als nicht mehr betriebsfähig eingestuft wird und somit ihre wirtschaftliche Betriebsgenehmigung verliert.

Bislang sind beim Verkehrsministerium relativ wenige Beschwerden über angebliche Verstöße gegen den Datenschutz durch Flugscheinverkaufsstellen oder Fluggesellschaften eingegangen. Wenn sie auftreten, werden sie nach den oben dargelegten Grundsätzen untersucht.

---

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

[2] Ehemals bekannt als Office of Aviation Enforcement and Proceedings.

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

C. DOT-Rechtsschutz zum Vorteil der EU-Verbraucher

Gemäß Abschnitt 41712 gilt das Verbot unlauterer oder irreführender Praktiken bei der Beförderung im Luftverkehr oder beim Verkauf von Luftverkehrsleistungen für US-amerikanische und ausländische Luftfahrtunternehmen sowie für Flugscheinvermittler. Das US-Verkehrsministerium geht häufig gegen US-amerikanische und ausländische Fluggesellschaften wegen Praktiken vor, die sich sowohl auf ausländische als auch auf US-amerikanische Verbraucher auswirken, und zwar auf der Grundlage, dass die Praktiken der Fluggesellschaft im Rahmen der Beförderung in die oder aus den Vereinigten Staaten stattgefunden haben. Das US-Verkehrsministerium wird auch in Zukunft alle zur Verfügung stehenden Rechtsmittel nutzen, um sowohl ausländische als auch US-amerikanische Verbraucher vor unlauteren oder irreführenden Praktiken im Luftverkehr durch regulierte Unternehmen zu schützen.

Das US-Verkehrsministerium setzt in Bezug auf Fluggesellschaften auch andere gezielte Gesetze durch, deren Schutz sich auch auf Nicht-US-Verbraucher erstreckt, wie z. B. den Children's Online Privacy Act ("COPPA"). COPPA schreibt unter anderem vor, dass Betreiber von Websites und Online-Diensten, die sich an Kinder richten, oder von Websites für ein allgemeines Publikum, die wissentlich personenbezogene Daten von Kindern unter 13 Jahren erheben, die Eltern darüber informieren und die überprüfbare Zustimmung der Eltern einholen müssen. In den USA ansässige Websites und Dienste, die dem COPPA unterliegen und personenbezogene Daten von ausländischen Kindern erfassen, müssen das COPPA einhalten. Auch Websites und Online-Dienste mit Sitz im Ausland müssen COPPA einhalten, wenn sie sich an Kinder in den Vereinigten Staaten richten oder wissentlich personenbezogene Daten von Kindern in den Vereinigten Staaten erheben. Sofern US-amerikanische oder ausländische Fluggesellschaften, die in den Vereinigten Staaten tätig sind, gegen COPPA verstoßen, wäre das US-Verkehrsministerium für die Einleitung von Durchsetzungsmaßnahmen zuständig.

## II. Durchsetzung der EU-U.S. DPF-Prinzipien

Entscheidet sich eine Fluggesellschaft oder ein Flugscheinvermittler für die Teilnahme an der EU-U.S. DPF und erhält das Ministerium eine Beschwerde, dass eine solche Fluggesellschaft oder ein solcher Flugscheinvermittler angeblich gegen die EU-U.S. DPF-Prinzipien verstoßen hat, würde das Ministerium die folgenden Schritte unternehmen, um die EU-U.S. DPF-Prinzipien energisch durchzusetzen.

A. Prioritäten bei der Untersuchung mutmaßlicher Verstöße

Das OACP des Ministeriums wird jede Beschwerde untersuchen, in der Verstöße gegen die Grundsätze der EU-US-DSGVO behauptet werden, einschließlich Beschwerden von EU-Datenschutzbehörden ("DPAs"), und Durchsetzungsmaßnahmen ergreifen, wenn es Beweise für einen Verstoß gibt. Darüber hinaus wird das OACP mit der FTC und dem Handelsministerium zusammenarbeiten und sich vorrangig mit Behauptungen befassen, dass die beaufsichtigten Unternehmen die im Rahmen der EU-US-DSGVO eingegangenen Datenschutzverpflichtungen nicht einhalten.

Nach Erhalt einer Anschuldigung wegen eines Verstoßes gegen die Grundsätze der EU-US-DSGVO kann das OACP im Rahmen seiner Untersuchung eine Reihe von Maßnahmen ergreifen. Zum Beispiel kann es die Fahrscheinstelle überprüfen oder
Sie würde die Datenschutzrichtlinien der Fluggesellschaft prüfen, weitere Informationen von der Flugscheinagentur oder der Fluggesellschaft oder von Dritten einholen, mit der verweisenden Stelle Kontakt aufnehmen und beurteilen, ob es ein Muster von Verstößen oder eine erhebliche Anzahl von betroffenen Verbrauchern gibt. Darüber hinaus würde sie feststellen, ob die Angelegenheit in den Zuständigkeitsbereich des Handelsministeriums oder der FTC fällt, prüfen, ob Verbraucher- und Unternehmensaufklärung hilfreich wäre, und gegebenenfalls ein Durchsetzungsverfahren einleiten.

Wenn das Ministerium Kenntnis von möglichen Verstößen gegen die EU-U.S. DPF-Prinzipien durch Fahrkartenverkäufer erhält, wird es sich mit der FTC in dieser Angelegenheit abstimmen. Wir werden die FTC und das Handelsministerium auch über das Ergebnis jeder Durchsetzungsmaßnahme der EU-U.S. DPF-Prinzipien informieren.

B. Umgang mit falschen oder irreführenden Teilnahmebehauptungen

Das Ministerium ist weiterhin entschlossen, Verstöße gegen die DPF-Prinzipien der EU und der USA zu untersuchen, einschließlich falscher oder irreführender Behauptungen über die Teilnahme an der DPF der EU und der USA. Wir werden vorrangig Empfehlungen des Handelsministeriums in Bezug auf Organisationen berücksichtigen, die sich in unzulässiger Weise als Teilnehmer der DPF EU-USA ausgeben oder die EU-U.S. DPF-Zertifizierungszeichen ohne Genehmigung.

Darüber hinaus weisen wir darauf hin, dass eine Organisation, die in ihren Datenschutzrichtlinien die Einhaltung der EU-US-DSGVO-Prinzipien zusagt, durch das Versäumnis, eine Selbstzertifizierung durch das Handelsministerium vorzunehmen oder aufrechtzuerhalten, wahrscheinlich nicht von der Durchsetzung dieser Verpflichtungen durch das US-Handelsministerium befreit wird.

C. Überwachung und Veröffentlichung von Vollstreckungsbescheiden bei Verstößen gegen die EU-US-DSGVO

Das OACP des Ministeriums wird auch weiterhin Vollstreckungsanordnungen überwachen, um die Einhaltung der EU-U.S. DPF-Prinzipien zu gewährleisten. Wenn das Amt eine Anordnung erlässt, die eine Fluggesellschaft oder einen Flugscheinvermittler anweist, künftige Verstöße gegen die EU-U.S. DPF-Prinzipien und Section 41712 zu unterlassen, wird es insbesondere die Einhaltung der Unterlassungsbestimmung in der Anordnung durch das Unternehmen überwachen. Darüber hinaus wird die Behörde sicherstellen, dass Anordnungen, die sich aus Fällen von EU-U.S. DPF-Prinzipien ergeben, auf ihrer Website verfügbar sind.

Wir freuen uns auf die weitere Zusammenarbeit mit unseren Partnern auf Bundesebene und den EU-Stakeholdern bei der EU-U.S. DPF-Angelegenheiten.

Ich hoffe, dass diese Informationen hilfreich sind. Wenn Sie Fragen haben oder weitere Informationen benötigen, können Sie mich gerne kontaktieren.

Mit freundlichen Grüßen,

Pete Buttigieg

**ANHANG VI**

U.S. Justizministerium, Abteilung

für Strafsachen

Büro des stellvertretenden GeneralstaatsanwaltsWashington , D.C. 20530

23. Juni 2023

Frau Ana Gallego Torres
Generaldirektor 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, die verwendet werden, um kommerzielle Daten und andere Informationen von Unternehmen in den Vereinigten Staaten für die Strafverfolgung oder für Zwecke des öffentlichen Interesses (zivil- und aufsichtsrechtlich) zu erhalten, einschließlich der in diesen Behörden festgelegten Zugangsbeschränkungen.[1] Alle in diesem Schreiben beschriebenen rechtlichen Verfahren sind insofern nicht diskriminierend, als sie dazu dienen, Informationen von Unternehmen in den Vereinigten Staaten zu erhalten, auch von Unternehmen, die sich im Rahmen des EU-US-Datenschutzrahmens selbst zertifizieren, und zwar ohne Rücksicht auf die Staatsangehörigkeit oder den Wohnsitz der betroffenen Person. Darüber hinaus können Unternehmen, die in den Vereinigten Staaten ein gerichtliches Verfahren erhalten, dieses vor Gericht anfechten (siehe unten).[2]

Von besonderer Bedeutung im Hinblick auf die Beschlagnahme von Daten durch Behörden ist der vierte Zusatzartikel zur Verfassung der Vereinigten Staaten, in dem es heißt: "Das Recht des Volkes, in seinen Personen, Häusern, Papieren und Sachen vor unangemessenen Durchsuchungen und Beschlagnahmen sicher zu sein, darf nicht verletzt werden, und es dürfen keine Durchsuchungsbefehle ausgestellt werden, es sei denn, es liegt ein wahrscheinlicher Grund vor, der durch einen Eid oder eine eidesstattliche Erklärung bestätigt wird und in dem der zu durchsuchende Ort und die zu beschlagnahmenden Personen oder Sachen genau beschrieben sind." U.S. Const. Amend. IV. Wie der Oberste Gerichtshof der Vereinigten Staaten

[1] Dieser Überblick beschreibt nicht die Ermittlungsinstrumente der nationalen Sicherheit, die von den Strafverfolgungsbehörden bei Ermittlungen zum Terrorismus und zu anderen Fragen der nationalen Sicherheit eingesetzt werden, einschließlich der National Security Letters (NSLs) für bestimmte Datensätze in Kreditauskünften, Finanzunterlagen und elektronischen Teilnehmer- und Transaktionsdatensätzen, 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 für elektronische Überwachung, Durchsuchungsbefehle, Geschäftsunterlagen und andere Informationserhebungen gemäß dem Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801 et seq.

[2] Dieses Schreiben befasst sich mit den Strafverfolgungs- und Regulierungsbehörden des Bundes. Verstöße gegen einzelstaatliches Recht werden von den einzelstaatlichen Strafverfolgungsbehörden untersucht und vor einzelstaatlichen Gerichten verhandelt. Die staatlichen Strafverfolgungsbehörden verwenden Haftbefehle und Vorladungen, die nach staatlichem Recht ausgestellt wurden, im Wesentlichen auf die gleiche Weise wie hier beschrieben, jedoch mit der Möglichkeit, dass staatliche Rechtsverfahren zusätzlichen Schutz durch staatliche Verfassungen oder Gesetze genießen, die über die der US-Verfassung hinausgehen. Der Schutz durch das Recht des Bundesstaates muss mindestens gleichwertig sein mit dem Schutz durch die

US-Verfassung, einschließlich, aber nicht beschränkt auf den Vierten Verfassungszusatz.

In der Entscheidung Berger gegen den Staat New York wurde festgestellt, dass "der grundlegende Zweck dieses Verfassungszusatzes, wie er in zahllosen Entscheidungen dieses Gerichts anerkannt wurde, darin besteht, die Privatsphäre und die Sicherheit des Einzelnen vor willkürlichen Eingriffen von Regierungsbeamten zu schützen". 388 U.S. 41, 53 (1967) (unter Berufung auf Camara
v. Mun. Court of San Francisco, 387 U.S. 523, 528 (1967)). Bei strafrechtlichen Ermittlungen im Inland verlangt der Vierte Verfassungszusatz im Allgemeinen, dass Strafverfolgungsbeamte vor der Durchführung einer Durchsuchung eine gerichtliche Anordnung einholen. Siehe Katz v. United States, 389 U.S. 347, 357 (1967). Standards für die Ausstellung eines Durchsuchungsbefehls, wie z. B. die Erfordernisse des hinreichenden Verdachts und der Spezifizität, gelten sowohl für Durchsuchungs- und Beschlagnahmebefehle als auch für Durchsuchungsbefehle für den gespeicherten Inhalt elektronischer Kommunikation, die gemäß dem Stored Communications Act (siehe unten) ausgestellt werden. Wenn das Erfordernis eines Durchsuchungsbefehls nicht gilt, unterliegt die Tätigkeit der Regierung immer noch einer "Angemessenheitsprüfung" gemäß dem Vierten Verfassungszusatz. Die Verfassung selbst stellt daher sicher, dass die US-Regierung keine unbegrenzte oder willkürliche Befugnis zur Beschlagnahme privater Informationen hat.[3]

Strafverfolgungsbehörden:

Bundesstaatsanwälte, die Beamte des Justizministeriums (DOJ) sind, und Bundesermittlungsbeamte, einschließlich Agenten des Federal Bureau of Investigation (FBI), einer Strafverfolgungsbehörde innerhalb des DOJ, sind in der Lage, die Vorlage von Dokumenten und anderen Aufzeichnungen von Unternehmen in den Vereinigten Staaten für strafrechtliche Ermittlungszwecke durch verschiedene Arten von Zwangsverfahren zu erzwingen, darunter Vorladungen der Grand Jury, administrative Vorladungen und Durchsuchungsbefehle, und können andere Kommunikationen gemäß den Bundesbehörden für strafrechtliche Abhörmaßnahmen und Pen-Register erwerben.

Vorladungen vor der Grand Jury oder vor Gericht: Strafrechtliche Vorladungen werden zur Unterstützung gezielter Ermittlungen der Strafverfolgungsbehörden eingesetzt. Eine Grand Jury Subpoena ist ein offizielles Ersuchen, das von einer Grand Jury (in der Regel auf Antrag eines Bundesstaatsanwalts) ausgestellt wird, um eine Grand Jury-Untersuchung zu einem bestimmten vermuteten Verstoß gegen das Strafrecht zu unterstützen. Grand Jurys sind ein Ermittlungsziel des Gerichts und werden von einem Richter oder Staatsanwalt eingesetzt. Mit einer Vorladung kann jemand aufgefordert werden, in einem Verfahren auszusagen oder Geschäftsunterlagen, elektronisch gespeicherte Informationen oder andere materielle Gegenstände vorzulegen oder zur Verfügung zu stellen. Die Informationen müssen für die Untersuchung relevant sein, und die Vorladung darf nicht unangemessen sein, weil sie zu weit gefasst ist, oder weil sie repressiv oder belastend ist. Ein Empfänger kann einen Antrag stellen, um eine Vorladung aus diesen Gründen anzufechten.
Siehe Fed. R. Crim. P. 17. Unter bestimmten Umständen können Vorladungen zur Vorlage von Dokumenten verwendet werden, nachdem der Fall von der Grand Jury angeklagt wurde.

Administrative Vorladungsbefugnis: Behördliche Vorladungsbefugnisse können in straf- oder zivilrechtlichen Ermittlungen ausgeübt werden. Im Rahmen der Strafverfolgung erlauben mehrere Bundesgesetze die Verwendung von Verwaltungsvorladungen zur Vorlage oder Bereitstellung von Geschäftsunterlagen, elektronisch gespeicherten Informationen oder anderen greifbaren Gegenständen, die für Ermittlungen im Zusammenhang mit Betrug im Gesundheitswesen, Kindesmissbrauch, Geheimdienstschutz, Fällen von Betäubungsmitteln und Ermittlungen der Generalinspektion, an denen Regierungsbehörden beteiligt sind, relevant sind. Wenn die Regierung versucht, eine behördliche Vorladung vor Gericht durchzusetzen, kann der Empfänger der behördlichen Vorladung, wie auch der Empfänger einer Vorladung der Grand Jury, argumentieren, dass die Vorladung unangemessen ist, weil sie zu weit gefasst ist oder weil sie repressiv oder beschwerlich ist.

[3] In Bezug auf die oben erörterten Grundsätze des Vierten Verfassungszusatzes zum Schutz der Privatsphäre und der Sicherheitsinteressen wenden die US-Gerichte diese Grundsätze regelmäßig auf neue Arten von Ermittlungsinstrumenten der Strafverfolgung an, die durch technologische Entwicklungen ermöglicht werden. Im Jahr 2018 entschied der Oberste Gerichtshof beispielsweise, dass die Beschaffung von historischen Standortdaten eines Mobilfunkunternehmens durch die Regierung im Rahmen einer Strafverfolgungsuntersuchung über einen längeren Zeitraum eine "Durchsuchung" darstellt, für die eine richterliche Anordnung nach dem Vierten Verfassungszusatz erforderlich ist. Carpenter v. United States, 138 S. Ct. 2206 (2018).

Gerichtsbeschlüsse für Pen Register und Trap and Traces: Im Rahmen der strafrechtlichen Pen-Register- und Trap-and-Trace-Bestimmungen können die Strafverfolgungsbehörden eine gerichtliche Anordnung zum Erwerb von Echtzeitdaten einholen, nicht-inhaltliche Wähl-, Leitweg-, Adressierungs- und Signalisierungsinformationen über eine Telefonnummer oder E-Mail, wenn bestätigt wird, dass die bereitgestellten Informationen für eine laufende strafrechtliche Untersuchung relevant sind. Siehe 18 U.S.C. §§ 3121-3127. Die Verwendung oder Installation eines solchen Geräts außerhalb des Gesetzes stellt ein Bundesverbrechen dar.

Gesetz zum Schutz der Privatsphäre in der elektronischen Kommunikation (ECPA): Zusätzliche Vorschriften regeln den Zugang der Regierung zu Teilnehmerinformationen, Verkehrsdaten und gespeicherten Kommunikationsinhalten, die sich im Besitz von Internet-Diensteanbietern (auch bekannt als "ISPs"), Telefongesellschaften und anderen Drittanbietern befinden, gemäß Titel II des ECPA, auch Stored Communications Act (SCA) genannt, 18 U.S.C. §§ 2701-2712. Der SCA legt ein System gesetzlicher Datenschutzrechte fest, die den Zugang der Strafverfolgungsbehörden zu Daten über das hinaus einschränken, was nach dem Verfassungsrecht von Kunden und Abonnenten von Internetanbietern verlangt wird. Das SCA sieht je nach Eingriffsintensität der Datenerhebung einen zunehmenden Schutz der Privatsphäre vor. Für Informationen zur Teilnehmerregistrierung, Internetprotokolladressen (IP-Adressen) und zugehörige Zeitstempel sowie Rechnungsdaten müssen Strafverfolgungsbehörden eine Vorladung einholen. Für die meisten anderen gespeicherten Informationen, die nicht zum Inhalt gehören, wie z. B. E-Mail-Header ohne Betreffzeile, müssen die Strafverfolgungsbehörden einem Richter konkrete Fakten vorlegen, die belegen, dass die angeforderten Informationen für eine laufende strafrechtliche Untersuchung relevant und wesentlich sind. Um den gespeicherten Inhalt elektronischer Kommunikation zu erhalten, müssen die Strafverfolgungsbehörden in der Regel eine richterliche Anordnung einholen, die sich auf wahrscheinliche Gründe für die Annahme stützt, dass das betreffende Konto Beweise für eine Straftat enthält. Das SCA sieht auch eine zivilrechtliche Haftung und strafrechtliche Sanktionen vor.[4]

Gerichtsbeschlüsse für die Überwachung gemäß dem Federal Wiretap Law: Darüber hinaus können die Strafverfolgungsbehörden drahtgebundene, mündliche oder elektronische Kommunikation in Echtzeit für strafrechtliche Ermittlungszwecke gemäß dem Federal Wiretap Law abhören. Siehe 18 U.S.C. §§ 2510-2523. Diese Befugnis steht nur auf der Grundlage einer gerichtlichen Anordnung zur Verfügung, in der ein Richter unter anderem feststellt, dass es einen wahrscheinlichen Grund für die Annahme gibt, dass die Abhörmaßnahme oder die elektronische Überwachung Beweise für ein Bundesverbrechen oder den Aufenthaltsort eines Flüchtigen, der vor der Strafverfolgung flieht, liefern wird. Das Gesetz sieht eine zivilrechtliche Haftung und strafrechtliche Sanktionen für Verstöße gegen die Abhörbestimmungen vor.

Durchsuchungsbefehl - Fed. R. Crim. P. Rule 41: Die Strafverfolgungsbehörden können Räumlichkeiten in den Vereinigten Staaten physisch durchsuchen, wenn sie von einem Richter dazu ermächtigt werden. Die Strafverfolgungsbehörden müssen dem Richter auf der Grundlage eines wahrscheinlichen Grundes nachweisen, dass eine Straftat begangen wurde oder im Begriff ist, begangen zu werden, und dass Gegenstände, die mit der Straftat in Verbindung stehen, wahrscheinlich an dem im Durchsuchungsbefehl angegebenen Ort gefunden werden. Von dieser Befugnis wird häufig Gebrauch gemacht, wenn eine physische Durchsuchung eines Grundstücks durch die Polizei erforderlich ist, weil die Gefahr besteht, dass Beweise vernichtet werden, wenn dem Unternehmen eine Vorladung oder eine andere Vorlageanordnung zugestellt wird. Eine Person, die einer Durchsuchung unterzogen wird oder deren Eigentum einer Durchsuchung unterzogen wird, kann die Unterdrückung von Beweisen beantragen, die bei einer rechtswidrigen Durchsuchung erlangt wurden oder daraus hervorgegangen sind, wenn diese Beweise in einem Strafverfahren gegen die betreffende Person verwendet werden. Siehe Mapp v. Ohio, 367 U.S. 643 (1961). Wenn ein Dateninhaber zur Offenlegung von Daten gemäß einer

[4] Darüber hinaus ermächtigt Abschnitt 2705(b) des SCA die Regierung, auf der Grundlage eines nachgewiesenen Bedarfs an Schutz vor Offenlegung eine gerichtliche Anordnung zu erwirken, die es einem Anbieter von

Kommunikationsdiensten untersagt, seine Nutzer freiwillig über den Erhalt eines SCA-Rechtsverfahrens zu informieren. Im Oktober 2017 gab der stellvertretende Generalstaatsanwalt Rod Rosenstein ein Memorandum an die Anwälte und Bediensteten des DOJ heraus, das Leitlinien enthält, um sicherzustellen, dass Anträge auf solche Schutzanordnungen auf die spezifischen Fakten und Anliegen einer Untersuchung zugeschnitten sind, und das eine allgemeine Obergrenze von einem Jahr festlegt, wie lange ein Antrag auf eine Verzögerung der Bekanntgabe gerichtet sein kann. Im Mai 2022 gab die stellvertretende Generalstaatsanwältin Lisa Monaco ergänzende Leitlinien zu diesem Thema heraus, in denen unter anderem DOJ-interne Genehmigungsanforderungen für Anträge auf Verlängerung einer Schutzanordnung über den ursprünglichen Einjahreszeitraum hinaus festgelegt und die Beendigung von Schutzanordnungen bei Abschluss einer Untersuchung vorgeschrieben wurden.

kann die gezwungene Partei die Offenlegungspflicht als unangemessen belastend anfechten. Siehe In re Application of United States, 610 F.2d 1148, 1157 (3d Cir. 1979) (mit der Feststellung, dass "ein ordnungsgemäßes Verfahren eine Anhörung zur Frage der Belastung erfordert, bevor eine Telefongesellschaft gezwungen wird, Unterstützung bei einem Durchsuchungsbefehl zu leisten"); In re Application of United States, 616 F.2d 1122 (9th Cir. 1980) (mit derselben Schlussfolgerung auf der Grundlage der Aufsichtsbefugnis des Gerichts).

DOJ-Richtlinien und -Vorschriften: Zusätzlich zu diesen verfassungsmäßigen, gesetzlichen und regelbasierten Beschränkungen des staatlichen Zugriffs auf Daten hat der Generalstaatsanwalt Richtlinien herausgegeben, die den Zugriff der Strafverfolgungsbehörden auf Daten weiter einschränken und die auch den Schutz der Privatsphäre und der bürgerlichen Freiheiten beinhalten. Die Richtlinien des Generalstaatsanwalts für inländische FBI-Operationen (September 2008) (im Folgenden "AG FBI-Richtlinien"), die unter http://www.justice.gov/archive/opa/docs/guidelines.pdf abrufbar sind, setzen beispielsweise Grenzen für den Einsatz von Ermittlungsmitteln zur Suche nach Informationen im Zusammenhang mit Untersuchungen, die Bundesverbrechen betreffen. Diese Richtlinien verlangen, dass das FBI die am wenigsten einschneidenden Ermittlungsmethoden einsetzt, die möglich sind, wobei die Auswirkungen auf die Privatsphäre und die bürgerlichen Freiheiten sowie die potenzielle Rufschädigung berücksichtigt werden. Ferner wird darauf hingewiesen, dass "es selbstverständlich ist, dass das FBI seine Ermittlungen und sonstigen Aktivitäten auf rechtmäßige und angemessene Weise durchführen muss, die die Freiheit und die Privatsphäre respektiert und unnötige Eingriffe in das Leben gesetzestreuer Menschen vermeidet". AG FBI Guidelines at 5. Das FBI hat diese Richtlinien durch den FBI Domestic Investigations and Operations Guide (DIOG) umgesetzt, der unter https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29 abrufbar ist, ein umfassendes Handbuch, das detaillierte Beschränkungen für den Einsatz von Ermittlungsinstrumenten und Leitlinien enthält, um sicherzustellen, dass die bürgerlichen Freiheiten und die Privatsphäre bei jeder Ermittlung geschützt werden. Weitere Regeln und Richtlinien, die Einschränkungen für die Ermittlungstätigkeit von Bundesstaatsanwälten vorschreiben, sind im Justizhandbuch enthalten, das ebenfalls online unter https://www.justice.gov/jm/justicemanual abrufbar ist.

Zivil- und Aufsichtsbehörden (öffentliches Interesse):

Auch der zivilrechtliche oder behördliche (d.h. im "öffentlichen Interesse" liegende) Zugang zu Daten, die sich im Besitz von Unternehmen in den Vereinigten Staaten befinden, ist erheblich eingeschränkt. Behörden mit zivil- und aufsichtsrechtlichen Zuständigkeiten können Unternehmen vorladen, um Geschäftsunterlagen, elektronisch gespeicherte Informationen oder andere materielle Gegenstände anzufordern. Diese Behörden sind bei der Ausübung ihrer administrativen oder zivilrechtlichen Vorladungsbefugnisse nicht nur durch ihre eigenen Gesetze eingeschränkt, sondern auch durch eine unabhängige gerichtliche Überprüfung der Vorladungen vor einer möglichen gerichtlichen Durchsetzung. Siehe z. B. Fed. R. Civ. P. 45. Die Behörden können nur Zugang zu Daten verlangen, die für Angelegenheiten relevant sind, die in ihren Regelungsbereich fallen. Darüber hinaus kann ein Empfänger einer behördlichen Vorladung die Durchsetzung dieser Vorladung vor Gericht anfechten, indem er Beweise dafür vorlegt, dass die Behörde nicht in Übereinstimmung mit grundlegenden Standards der Angemessenheit gehandelt hat, wie bereits erwähnt.

Es gibt weitere Rechtsgrundlagen für Unternehmen, um Datenanfragen von Verwaltungsbehörden anzufechten, die auf ihren spezifischen Branchen und den Arten von Daten, über die sie verfügen, basieren. So können beispielsweise Finanzinstitute gegen behördliche Vorladungen vorgehen, mit denen bestimmte Arten von Informationen als Verstöße gegen das Bankgeheimnisgesetz und seine Durchführungsbestimmungen angefordert werden. 31 U.S.C. § 5318; 31 C.F.R. Chapter X. Andere Unternehmen können sich auf den Fair Credit Reporting Act, 15 U.S.C. § 1681b, oder eine Reihe anderer branchenspezifischer Gesetze

berufen. Der Missbrauch der Vorladungsbefugnis einer Behörde kann zur Haftung der Behörde oder zur persönlichen Haftung der Behördenmitarbeiter führen. Siehe z. B. Right to Financial Privacy Act, 12 U.S.C. §§ 3401-3423. Die Gerichte in den Vereinigten Staaten sind somit die Wächter gegen unzulässige behördliche Anfragen und bieten eine unabhängige Aufsicht über die Maßnahmen der Bundesbehörden.

Schließlich ist jede gesetzliche Befugnis der Verwaltungsbehörden zur physischen Beschlagnahme

Aufzeichnungen eines Unternehmens in den Vereinigten Staaten im Rahmen einer behördlichen Durchsuchung müssen die Anforderungen des Vierten Verfassungszusatzes erfüllen. Siehe See v. City of Seattle, 387 U.S. 541 (1967).

Schlussfolgerung:

Alle Strafverfolgungs- und Regulierungsmaßnahmen in den Vereinigten Staaten müssen im Einklang mit dem geltenden Recht stehen, einschließlich der US-Verfassung, Statuten, Regeln und Vorschriften. Solche Aktivitäten müssen auch mit den geltenden Richtlinien übereinstimmen, einschließlich der Richtlinien des Generalstaatsanwalts, die die Strafverfolgungsaktivitäten des Bundes regeln. Der oben beschriebene Rechtsrahmen schränkt die Möglichkeiten der US-Strafverfolgungs- und Aufsichtsbehörden ein, Informationen von Unternehmen in den Vereinigten Staaten zu erlangen - unabhängig davon, ob die Informationen US-Personen oder Bürger ausländischer Staaten betreffen - und erlaubt darüber hinaus eine gerichtliche Überprüfung von Regierungsanfragen nach Daten gemäß diesen Behörden.

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

# ANHANG VII

BÜRO DES DIREKTORS DES NATIONALEN
GEHEIMDIENSTES BÜRO DES
GENERALANWALTS

WASHINGTON, DC 20511

9. Dezember 2022

Leslie B. Kiernan
Allgemeine
Rechtsberaterin
U.S. Handelsministerium
1401 Constitution Ave. NW
Washington, DC 20230

Sehr geehrte Frau Kiernan,

Am 7. Oktober 2022 unterzeichnete Präsident Biden die Executive Order 14086, *Enhancing Safeguards for United States Signals Intelligence Activities,* mit der die strengen Datenschutz- und Bürgerrechtsgarantien, die für US-Signaldienstaktivitäten gelten, verstärkt werden. Diese Schutzmaßnahmen beinhalten: die Forderung, dass nachrichtendienstliche Tätigkeiten zur Erreichung bestimmter legitimer Ziele durchgeführt werden müssen; das ausdrückliche Verbot solcher Tätigkeiten zur Erreichung bestimmter verbotener Ziele; die Einführung neuartiger Verfahren, die sicherstellen, dass nachrichtendienstliche Tätigkeiten zur Erreichung dieser legitimen Ziele beitragen und nicht zur Erreichung verbotener Ziele; die Vorschrift, dass nachrichtendienstliche Aktivitäten nur dann durchgeführt werden dürfen, wenn auf der Grundlage einer angemessenen Bewertung aller relevanten Faktoren festgestellt wurde, dass die Aktivitäten notwendig sind, um eine validierte nachrichtendienstliche Priorität voranzubringen, und nur in dem Umfang und auf eine Weise, die der validierten nachrichtendienstlichen Priorität, für die sie genehmigt wurden, angemessen ist; und die Anweisung an die Elemente des Nachrichtendienstes (Intelligence Communjty, IC), ihre Richtlinien und Verfahren zu aktualisieren, um die in der Executive Order geforderten Sicherheitsvorkehrungen für nachrichtendienstliche Aktivitäten zu berücksichtigen. Von besonderer Bedeutung ist, dass die Executive Order auch einen unabhängigen und verbindlichen Mechanismus einführt, der es Einzelpersonen aus "qualifizierten Staaten", die gemäß der Executive Order benannt sind, ermöglicht, Rechtsmittel einzulegen, wenn sie glauben, dass sie unrechtmäßigen US-Signalenachrichtendienstaktivitäten ausgesetzt waren, einschließlich Aktivitäten, die gegen die in der Executive Order enthaltenen Schutzbestimmungen verstoßen.

Präsident Bidens Erlass 14086 markiert den Höhepunkt von mehr als einem Jahr detaillierter Verhandlungen zwischen Vertretern der Europäischen

Kommission (EK) und den Vereinigten Staaten und legt die Schritte fest, die die Vereinigten Staaten unternehmen werden, um ihre Verpflichtungen aus dem EU-US-Datenschutzrahmen umzusetzen. Im Einklang mit dem kooperativen Geist, der zu dem Rahmenwerk geführt hat, haben Sie, soweit ich weiß, von der Europäischen Kommission zwei Fragenkomplexe erhalten, die Folgendes betreffen

wie der IK die Durchführungsverordnung umsetzen wird. Ich bin gerne bereit, diese Fragen mit diesem Schreiben zu beantworten.

*Abschnitt 702 des Foreign Intelligence Surveillance Act von 1978 (FISA-Abschnitt 702)*

Die erste Gruppe von Fragen betrifft FISA Abschnitt 702, der die Sammlung von Informationen über ausländische Geheimdienste durch die gezielte Ansprache von Nicht-US-Personen erlaubt, von denen man annimmt, dass sie sich außerhalb der Vereinigten Staaten befinden, und zwar mit der erzwungenen Unterstützung von Anbietern elektronischer Kommunikationsdienste. Die Fragen beziehen sich insbesondere auf das Zusammenspiel zwischen dieser Bestimmung und der Executive Order 14086 sowie auf die anderen Schutzmaßnahmen, die für Aktivitäten gemäß FISA Abschnitt 702 gelten.

Zunächst können wir bestätigen, dass der IStGH die in der Exekutivverordnung 14086 festgelegten Sicherheitsvorkehrungen auf die gemäß FISA-Abschnitt 702 durchgeführten Aktivitäten anwenden wird.

Darüber hinaus gelten für die Anwendung des FISA-Abschnitts 702 durch die Regierung zahlreiche weitere Sicherheitsvorkehrungen. So müssen beispielsweise alle Zertifizierungen des FISA-Abschnitts 702 sowohl vom Generalstaatsanwalt als auch vom Direktor der Nationalen Nachrichtendienste (DNI) unterzeichnet werden, und die Regierung muss alle derartigen Zertifizierungen dem Foreign Intelligence Surveillance Court (FISC) zur Genehmigung vorlegen, der sich aus unabhängigen, auf Lebenszeit ernannten Richtern zusammensetzt, die eine nicht verlängerbare siebenjährige Amtszeit haben. In den Bescheinigungen werden Kategorien von nachrichtendienstlichen Informationen aus dem Ausland genannt, die der gesetzlichen Definition von nachrichtendienstlichen Informationen aus dem Ausland entsprechen müssen, indem sie auf Nicht-US-Personen abzielen, von denen man annimmt, 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 Bescheinigung muss dem FISC in einem Antragspaket zur Genehmigung vorgelegt werden, das die Bescheinigungen des Generalstaatsanwalts und des DNI, eidesstattliche Erklärungen bestimmter Leiter von Nachrichtendiensten sowie für die Regierung verbindliche Verfahren zur gezielten Erfassung, Minimierung und Abfrage enthält. Die Targeting-Verfahren verlangen unter anderem, dass der IC auf der Grundlage der Gesamtheit der Umstände vernünftig einschätzen kann, dass das Targeting wahrscheinlich zur Sammlung von Informationen über ausländische Nachrichtendienste führen wird, die in einer Zertifizierung nach Abschnitt 702 des PISA aufgeführt sind.

Darüber hinaus muss der IStGH bei der Erhebung von Informationen gemäß FISA-Abschnitt 702: eine schriftliche Erläuterung der Grundlage für seine Einschätzung zum Zeitpunkt der Zielerfassung vorlegen, dass die Zielperson voraussichtlich ausländische nachrichtendienstliche Informationen, die in einer Bescheinigung nach PISA-Abschnitt 702 identifiziert wurden, besitzen, erhalten oder weitergeben wird; bestätigen, dass der in den Verfahren zur Zielerfassung nach PISA-Abschnitt 702 festgelegte Standard für die Zielerfassung 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 Summcuy ofNotable Section 702 Requirements,* at 2-3 (July 15, 2015).

Die Anforderung an den IK, seine Einschätzung, dass die Ziele des FISA-Abschnitts 702 den geltenden Zielnormen entsprechen, schriftlich festzuhalten und regelmäßig zu bestätigen, erleichtert dem FISC die Aufsicht über die zielgerichteten Aktivitäten des IK. Jede aufgezeichnete Beurteilung und Begründung der Zielsetzung wird alle zwei Monate von Anwälten des Justizministeriums (DOJ) überprüft, die diese Überwachungsfunktion unabhängig von den Operationen der Auslandsnachrichtendienste ausüben. Die Abteilung des DOJ, die diese Aufgabe wahrnimmt

Funktion ist dann gemäß einer seit langem bestehenden FISC-Regel dafür verantwortlich, dem FISC alle Verstöße gegen die geltenden Verfahren zu melden. Dank dieser Berichterstattung und regelmäßiger Treffen zwischen dem FISC und dieser DOJ-Abteilung zur Überwachung des FISA-Abschnitts 702 Targeting kann der FISC die Einhaltung des FISA-Abschnitts 702 Targeting und anderer Verfahren durchsetzen und auf andere Weise sicherstellen, dass die Aktivitäten der Regierung rechtmäßig sind. Insbesondere kann das FISC dies auf verschiedene Weise tun, unter anderem durch den Erlass verbindlicher Abhilfeentscheidungen, um die Befugnis der Regierung zur Datenerhebung gegen ein bestimmtes Ziel zu beenden oder die Datenerhebung nach FISA-Abschnitt 702 zu ändern oder zu verzögern. Der FISC kann die Regierung auch auffordern, weitere Berichte oder Informationen über die Einhaltung der Zielerfassungs- und anderer Verfahren vorzulegen oder Änderungen an diesen Verfahren zu verlangen.

*Die "Massenerhebung" von nachrichtendienstlichen Informationen*

Der zweite Fragenkomplex betrifft die "Massenerfassung" von nachrichtendienstlichen Signalen, die in der Executive Order 14086 definiert wird als "die genehmigte Erfassung großer Mengen nachrichtendienstlicher Signaldaten, die aufgrund technischer oder operativer Erwägungen ohne die Verwendung von Unterscheidungsmerkmalen (z. B. ohne die Verwendung spezifischer Identifikatoren oder Auswahlbegriffe) erfasst werden".

In Bezug auf diese Fragen stellen wir zunächst fest, dass weder das FISA noch die National Security Letters eine Massenerhebung zulassen. In Bezug auf FISA:

- Die Titel I und III des FISA, die die elektronische Überwachung bzw. die physische Durchsuchung genehmigen, erfordern eine gerichtliche Anordnung (mit begrenzten Ausnahmen, z. B. in Notfällen) und setzen immer einen hinreichenden Verdacht voraus, dass es sich bei der Zielperson um eine ausländische Macht oder einen Agenten einer ausländischen Macht handelt. *Siehe* 50 U.S.C. §§ 1805, 1824.

- Der USA FREEDOM Act von 2015 änderte Titel IV des FISA, der den Einsatz von Pen-Registern und Trap-and-Trace-Geräten auf richterliche Anordnung (außer in Notfällen) erlaubt, dahingehend, dass die Regierung verpflichtet ist, Anträge auf einen "spezifischen Auswahlbegriff" zu stützen. *Siehe* 50 U.S.C. § 1842(c)(3).

- Titel V des FISA, der es dem Federal Bureau of Investigation (FBI) gestattet, bestimmte Arten von Geschäftsunterlagen zu beschaffen, erfordert eine gerichtliche Anordnung auf der Grundlage eines Antrags, in dem dargelegt wird, dass "es spezifische und artikulierbare Fakten gibt, die Grund zu der Annahme geben, dass die Person, auf die sich die Unterlagen beziehen, eine ausländische Macht oder ein Agent einer ausländischen Macht ist". *Siehe* 50 U.S.C. § 1862(b)(2)(B).[1]

- Schließlich erlaubt FISA-Abschnitt 702 das "gezielte Anvisieren von Personen, die vernünftigerweise

[1] Von 2001 bis 2020 erlaubte Titel V des FISA dem FBI, beim FISC eine Genehmigung zur Beschaffung von "greifbaren Gegenständen" zu beantragen, die für bestimmte genehmigte Untersuchungen relevant sind.
*Siehe* USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272, § 215 (2001). Diese Diese Bestimmung, die inzwischen außer Kraft getreten ist und daher nicht mehr gilt, war die Grundlage für die massenhafte Erhebung von Telefonie-Metadaten durch die Regierung. Noch bevor die Bestimmung außer Kraft trat, wurde sie jedoch durch den USA FREEDOM Act dahingehend geändert, dass die Regierung einen Antrag an den FISC auf einen "spezifischen Auswahlbegriff" stützen muss. *Siehe* USA FREEDOM Act, Pub. L. No. 114-23, 129 Stat. 268, § I 03 (2015).

die sich vermutlich außerhalb der Vereinigten Staaten befinden, um Informationen über ausländische Geheimdienste zu erhalten". *Siehe* 50 U.S.C. § 188la(a). Wie das Privacy and Civil Liberties Oversight Board festgestellt hat, besteht die Datenerhebung der Regierung gemäß FISA Abschnitt 702 "ausschließlich darin, einzelne Personen ins Visier zu nehmen und die mit diesen Personen in Verbindung stehenden Kommunikationen zu erfassen, von denen die Regierung Grund zu der Annahme hat, dass sie bestimmte Arten von Auslandsnachrichten erhalten wird", so dass das "Programm nicht durch die Erfassung von Kommunikationen in großen Mengen funktioniert". Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act,* at 103 (July 2, 2014).[2]

In Bezug auf nationale Sicherheitsbriefe schreibt der USA FREEDOM Act von2015 eine "spezifische Auswahlfrist" für die Verwendung solcher Briefe 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 sieht die Executive Order 14086 vor, dass "die angestrebte Sammlung vorrangig zu erfolgen hat" und dass, wenn der IC eine Massenerhebung durchführt, die "Massenerhebung von Signalen nur auf der Grundlage der Feststellung genehmigt wird, dass die Informationen, die zur Förderung einer bestätigten nachrichtendienstlichen Priorität erforderlich sind, vernünftigerweise nicht durch eine gezielte Sammlung gewonnen werden können". *Siehe* Executive Order 14086, § 2(c)(ii)(A).

Für den Fall, dass der IK feststellt, dass die Massenerhebung diese Standards erfüllt, sieht die Executive Order 14086 zusätzliche Schutzmaßnahmen vor. Insbesondere verlangt die Executive Order, dass der IC bei der Durchführung von Massenerhebungen "angemessene Methoden und technische Maßnahmen anwendet, um die gesammelten Daten auf das zu beschränken, was notwendig ist, um eine validierte nachrichtendienstliche Priorität voranzubringen, und gleichzeitig die Sammlung nicht relevanter Informationen zu minimieren". *Siehe id.* Der Erlass besagt auch, dass "nachrichtendienstliche Tätigkeiten", zu denen auch die Abfrage von nachrichtendienstlichen Informationen gehört, die durch Massenerfassung gewonnen wurden, "nur dann durchgeführt werden, wenn auf der Grundlage einer angemessenen Bewertung aller relevanten Faktoren festgestellt wurde, dass die Tätigkeiten notwendig sind, um eine validierte nachrichtendienstliche Priorität voranzubringen". *See id.* § 2(a)(ii)(A). Der Erlass setzt diesen Grundsatz weiter um, indem er festlegt, dass der IStGH nur in großem Umfang erlangte, nicht minimierte Signalinformationen abfragen darf, um sechs zulässige Ziele zu verfolgen, und dass solche Abfragen gemäß Strategien und Verfahren durchgeführt werden müssen, die "die Auswirkungen [der Abfragen] auf die Privatsphäre und die bürgerlichen Freiheiten aller Personen angemessen berücksichtigen, unabhängig von ihrer Nationalität oder dem Ort, an dem sie sich aufhalten könnten". *Siehe id.* § 2(c)(iii)(D). Schließlich sieht die Anordnung die Handhabung, Sicherheit und Zugangskontrollen für die erhobenen Daten vor. *Siehe id.* § 2(c)(iii)(A) und§ 2(c)(iii)(B).

* * * * *

Wir hoffen, dass diese Klarstellungen hilfreich sind. Bitte zögern Sie nicht, sich mit uns in Verbindung zu setzen, wenn Sie weitere Fragen dazu haben, wie die US-Behörde

die Durchführungsverordnung 14086 umzusetzen gedenkt.

---

[2] Die Abschnitte 703 und 704, die den Internationalen Strafgerichtshof ermächtigen, im Ausland befindliche US-Personen ins Visier zu nehmen, erfordern eine gerichtliche Anordnung (außer in Notfällen) und setzen immer einen hinreichenden Grund für die Annahme voraus, dass es sich bei der Zielperson um eine ausländische Macht, einen Agenten einer ausländischen Macht oder einen Offizier oder Mitarbeiter einer ausländischen Macht handelt. *Siehe50U.S.C.§§* 1881b, 1881c.

Sincerely,

Christopher C.
Fonzone Allgemeiner
Rechtsbeistand

EUROPÄISCHE
KOMMISSION

Brüssel, 10.7.2023
K(2023) 4745 endgültig

ANHANG 8

**ANHANG**

***zum***

**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 EU-US-Datenschutzrahmen**

# ANHANG VIII

## Liste der Abkürzungen

Die folgenden Abkürzungen werden in diesem Beschluss verwendet:

| | |
|---|---|
| AAA | Amerikanische Vereinigung für Schiedsgerichtsbarkeit |
| AG-Verordnung | Verordnung des Generalstaatsanwalts über das Gericht für die Überprüfung des Datenschutzes |
| AGG-DOM | Rechtsanwalt General Leitlinien für Innerstaatliche FBI-Einsätze |
| APA | Verwaltungsverfahrensgesetz |
| CIA | Zentrale Intelligenz Agentur |
| CNSS | Ausschuss für nationale Sicherheitssysteme |
| Gerichtshof | Gerichtshof der Europäischen Union (EuGH) |
| Entscheidung | 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 EU-US-Datenschutzrahmen |
| DHS | Ministerium für Innere Sicherheit |
| DNI | Direktor des Nationalen Nachrichtendienstes |
| DoC | U.S. Handelsministerium |
| DoJ | U.S. Department of Justice |
| DoT | U.S. Department of Transportation |
| DPA | Datenschutzbehörde |
| DPF-Liste | Datenschutz-Rahmenliste |
| DPRC | Datenschutzprüfungsausschuss |
| ECOA | Gesetz über die Chancengleichheit im Kreditwesen |
| ECPA | Gesetz zum Schutz der Privatsphäre in der elektronischen Kommunikation |
| EEA | Europäischer Wirtschaftsraum |
| EO 12333 | Executive Order 12333 "Nachrichtendienstliche Tätigkeiten der Vereinigten Staaten". |
| EO 14086, die EO | Exekutiverlass 14086 "Verbesserung der Sicherheitsvorkehrungen für die Aktivitäten der US-Nachrichtendienste". |
| EU-U.S. DPF oder DPF | EU-US-Datenschutzrahmen |
| EU-U.S. DPF-Panel | EU-US-Datenschutzrahmen-Panel |
| FBI | Federal Bureau of Investigation |

| | |
|---|---|
| FCRA | Gesetz über faire Kreditauskunft |
| FISA | Foreign Intelligence Surveillance Act |
| FISC | Foreign Intelligence Surveillance Court |
| FISCR | Foreign Intelligence Surveillance Court of Review |
| FOIA | Gesetz über die Informationsfreiheit |
| FRA | Bundesarchivgesetz |
| FTC | U.S. Federal Trade Commission |
| HIPAA | Gesetz zur Übertragbarkeit und Rechenschaftspflicht von Krankenversicherungen |
| IZDR | Internationales Zentrum für Streitbeilegung |
| IOB | Intelligence Oversight Board |
| NIST | Nationales Institut für Normen und Technologie |
| NSA | Nationale Sicherheitsbehörde |
| NSL | Nationale Sicherheitserklärung(en) |
| ODNI | Büro des Direktors des Nationalen Nachrichtendienstes |
| ODNI CLPO, CLPO | Beauftragter für den Schutz der bürgerlichen Freiheiten des Direktors der nationalen Nachrichtendienste |
| OMB | Amt für Verwaltung und Haushalt |
| OPCL | Büro für Datenschutz und bürgerliche Freiheiten des Justizministeriums |
| PCLOB | Aufsichtsbehörde für Datenschutz und bürgerliche Freiheiten |
| PIAB | Nachrichtendienstlicher Beirat des Präsidenten |
| PPD 28 | Richtlinie 28 des Präsidenten |
| 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 und zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG |
| SAOP | Leitende Beamtin der Agentur für den Datenschutz |
| Die Grundsätze | EU-US-Datenschutzrahmenprinzipien |
| U.S. | Vereinigte Staaten |
| Gewerkschaft | Europäische Union |