Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Justiz- und Polizeidepartement EJPD

Bundesamt für Justiz BJ
Direktionsbereich Öffentliches Recht
Fachbereich Rechtsetzungsprojekte I

30. April 2024

Beurteilung der Angemessenheit – Vereinigte Staaten

Schaffung eines Datenschutzrahmens für die Übermittlung von Personendaten von der Schweiz an zertifizierte Organisationen in den Vereinigten Staaten (*Swiss-U.S. Data Privacy Framework*) – Beurteilung der Angemessenheit des Datenschutzes

BJ-D-72B33401/379

Inhaltsverzeichnis

1 Ausgangslage

1.1 Mit dem Datenschutzgesetz vom 25. September 2020 eingeführtes Verfahren der Angemessenheitsprüfung

Mit der neuen Datenschutzgesetzgebung, die seit dem 1. September 2023 in Kraft ist, wurde eine Änderung der Zuständigkeit eingeführt: Nach Artikel 16 Absatz 1 des Datenschutzgesetzes vom 25. September 2020 (DSG)[1] und Artikel 8 Absatz 1 der Datenschutzverordnung vom 31. August 2022 (DSV)[2] bestimmt der Bundesrat, ob ein Staat, ein Gebiet, ein spezifischer Sektor in einem Staat oder ein internationales Organ ein angemessenes Datenschutzniveau gewährleistet. Anhang 1 der DSV enthält eine Liste der Staaten, Gebiete, spezifischen Sektoren in einem Staat und internationalen Organe mit angemessenem Datenschutzniveau.

Zuständig für die Beurteilung der Angemessenheit des Datenschutzniveaus ist das Bundesamt für Justiz[3]; dabei geht es um eine rechtliche Beurteilung, die veröffentlicht wird.

1.2 Früherer Datenschutzrahmen und dessen Aufhebung

Unter dem (aufgehobenen) Datenschutzgesetz vom 19. Juni 1992 führte der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) eine indikative Liste von Staaten, die ein angemessenes Schutzniveau aufweisen.

Am 11. Januar 2017 hatte der EDÖB die Vereinigten Staaten in die Liste aufgenommen, und zwar für den Datenaustausch mit zertifizierten Unternehmen im Rahmen des *Swiss-U.S. Privacy Shield*. Für die EU galt mit den Vereinigten Staaten ein praktisch identischer Rahmen.

Mit Urteil vom 16. Juli 2020 qualifizierte der Europäische Gerichtshof (EuGH) im Fall *Schrems II* (Rechtssache C-311/18) den gewährten Schutz als unzureichend und erklärte damit den für die Übermittlung von Personendaten von der EU an die Vereinigten Staaten geltenden Mechanismus für ungültig. Zur Begründung hielt der EuGH fest, der Mechanismus lasse für die Überwachung durch die amerikanischen Geheimdienste unverhältnismässige Abweichungen vom Datenschutz zu und sehe für die betroffenen Personen keinen wirksamen Rechtsschutz vor.

Auch wenn die Entscheidung des EuGHs für die Schweiz rechtlich nicht bindend ist, sah sich der EDÖB veranlasst, die Aufnahme der Vereinigten Staaten in die von ihm geführte indikative Liste von Staaten mit angemessenem Schutzniveau erneut zu prüfen. Dies geschah mit Rücksicht auf das allgemeine Prinzip der Rechtsstaatlichkeit, das Bedürfnis nach Rechtssicherheit und auf den Umstand, dass der Rahmen für den Austausch von Personendaten zwischen der Schweiz und den Vereinigten Staaten praktisch identisch ist mit dem, der zwischen der EU und den Vereinigten Staaten galt. Am 8. September 2020 veröffentlichte der EDÖB

---

1 SR 235.1.

2 SR 235.11.

3 Gemäss Artikel 7 Absatz 1 Buchstabe d der Organisationsverordnung für das Eidgenössische Justiz- und Polizeidepartement (SR 172.213.1), übt es diese Aufgabe in Zusammenarbeit mit ebenfalls zuständigen Ämtern aus.

eine Stellungnahme, wonach die Vereinigten Staaten den Anforderungen an einen angemessenen Datenschutz im Sinne des Datenschutzgesetzes nicht genügen, und strich diese von der Liste. Aus diesem Grund nahm der Bundesrat die Vereinigten Staaten auch nicht in die Liste der Staaten in Anhang 1 der DSV auf, als die neue Gesetzgebung am 1. September 2023 in Kraft trat.

1.3 Schaffung eines Datenschutzrahmens für die Übermittlung von Personendaten von der Schweiz an zertifizierte Unternehmen in den Vereinigten Staaten

Nach Aufhebung des früheren Datenschutzrahmens und der Streichung der Vereinigten Staaten von der Liste des EDÖB fanden zwischen der Schweiz und den Vereinigten Staaten Gespräche statt, parallel zu denen zwischen der EU und den Vereinigten Staaten.

Diese Gespräche haben zu folgenden Ergebnissen geführt: Schaffung eines kommerziellen Rahmens für die zertifizierten Organisationen (Grundsätze, einschliesslich zusätzlicher Grundsätze des Datenschutzrahmens zwischen der Schweiz und den Vereinigten Staaten); Veröffentlichung verschiedener Dokumente durch die Regierung und die zuständigen Behörden der Vereinigten Staaten (Durchführungsverordnung 14086 vom 7. Oktober 2022, Vorschrift über das Gericht zur Datenschutzüberprüfung des Generalstaatsanwalts der Vereinigten Staaten vom 7. Oktober 2022; Richtlinie 126 der Nachrichtendienstgemeinschaft, die vom Büro der Direktorin des Nationalen Nachrichtendienstes [ODNI] am 6. Dezember 2022 erstellt wurde); Ernennung der Schweiz am 7. Juni 2024 als Staat, der vom zweistufigen Beschwerdemechanismus einschliesslich des Zugangs zum Gericht zur Datenschutzüberprüfung profitiert; Übergabe der Schreiben der Behörden der Vereinigten Staaten, in denen die eingegangenen Verpflichtungen bestätigt werden. Die genannten Unterlagen[4], die über die am Schluss dieses Dokuments aufgeführten Internetadressen zugänglich sind, bilden in ihrer Gesamtheit den Datenschutzrahmen für die Übermittlung von Personendaten von der Schweiz an die zertifizierten Organisationen in den Vereinigten Staaten (*Swiss-U.S. Data Privacy Framework [Swiss-U.S. DPF]*).

Gestützt auf die in der DSV festgelegten Beurteilungskriterien wird im Folgenden geprüft, ob die Vereinigten Staaten aufgrund der Gesamtheit der genannten Dokumente ein für die Übermittlung von Personendaten zwischen Verantwortlichen oder Auftragsbearbeitern in der Schweiz und zertifizierten Organisationen in den Vereinigten Staaten angemessenes Schutzniveau gewährleisten.

2 Kriterien zur Beurteilung der Angemessenheit

Artikel 8 DSV definiert verschiedene Kriterien, die bei der Beurteilung insbesondere zu berücksichtigen sind, nämlich:

a) die internationalen Verpflichtungen des Staates oder internationalen Organs, insbesondere im Bereich des Datenschutzes;
b) die Rechtsstaatlichkeit und die Achtung der Menschenrechte;
c) die geltende Gesetzgebung insbesondere zum Datenschutz sowie deren Umsetzung und die einschlägige Rechtsprechung;

[4] Die Dokumente sind nur auf Englisch verfügbar.

d) die wirksame Gewährleistung der Rechte der betroffenen Personen und des Rechtsschutzes;
e) das wirksame Funktionieren einer oder mehrerer unabhängiger Behörden, die im betreffenden Staat für den Datenschutz zuständig sind oder denen ein internationales Organ untersteht, und die über ausreichende Befugnisse und Kompetenzen verfügen.

Anhang 1 der DSV enthält die Liste der Staaten, Gebiete, spezifischen Sektoren in einem Staat und internationalen Organe, in denen ein angemessenes Datenschutzniveau gewährleistet ist. Die Liste ist rechtlich verbindlich.

Unter einem angemessenen Schutzniveau ist ein Niveau zu verstehen, das im Wesentlichen dem des schweizerischen Datenschutzrechts entspricht. Dabei geht es nicht darum, die jeweiligen Systeme Punkt für Punkt zu vergleichen, sondern zu entscheiden, ob das in einem Staat, einem Gebiet, einem spezifischen Sektor in einem Staat oder einem internationalen Organ geltende System insgesamt ein im Wesentlichen gleichwertiges Schutzniveau in Bezug auf den Inhalt der Rechte zum Schutz der Privatsphäre, deren Umsetzung und die bestehenden Kontrollmöglichkeiten bietet. In diesem Zusammenhang sind die unterschiedlichen rechtlichen und kulturellen Traditionen zwischen der Schweiz und einem Staat, einem Gebiet, einem spezifischen Sektor in einem Staat oder einem internationalen Organ, der bzw. das Gegenstand einer Angemessenheitsprüfung ist, zu berücksichtigen.

Nach Artikel 45 der Datenschutz-Grundverordnung[5] stellt die EU auf ganz ähnliche Kriterien ab, wenn sie die Angemessenheit des Schutzniveaus für Personendaten in einem Drittstaat beurteilt.

3 Kommerzieller Rahmen für die Übermittlung von Personendaten zwischen den Verantwortlichen und Auftragsbearbeitern in der Schweiz und den zertifizierten Organisationen in den Vereinigten Staaten

3.1 Anwendbare Gesetzgebung

3.1.1 Grundsätze des Datenschutzrahmens

Die Grundsätze, einschliesslich die zusätzlichen Grundsätze des Datenschutzrahmens für die Übermittlung von Personendaten von der Schweiz an zertifizierte Organisationen in den Vereinigten Staaten (im Folgenden: Grundsätze des *Swiss-U.S. DPF* oder Grundsätze)[6] beruhen auf einem Zertifizierungssystem, bei dem sich die Organisationen, d.h. die Unternehmen in den Vereinigten Staaten, die den Datenschutzrahmen für die Übermittlung von Personendaten in Anspruch nehmen möchten, verpflichten, eine Reihe von Grundsätzen zum Schutz der Privatsphäre zu beachten. Eine Zertifizierung unter dem *Swiss-U.S. DPF* setzt voraus, dass eine Organisation den Untersuchungs- und Durchsetzungsbefugnissen der Bundeshandelskommission (*Federal Trade Commission*) oder des Verkehrsministeriums (*U.S. Department*

[5] Vgl. Verordnung (EU) 2016/ 679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/ 46/ EG (Datenschutz-Grundverordnung) JO L 119 vom 4.5.2016, S. 1, einsehbar unter folgendem Link. EUR-Lex - 32016R0679 - EN - EUR-Lex (europa.eu).

[6] Die Internetadressen zu den Referenztexten finden sich am Schluss des vorliegenden Dokuments.

of Transportation) untersteht; die Organisation muss die Einhaltung der Grundsätze jährlich neu zertifizieren.

Die Grundsätze des *Swiss-U.S. DPF* definieren Personendaten als Daten über eine identifizierte oder identifizierbare Person, die in den Anwendungsbereich des DSG und seiner Verordnungen fallen und von einer Organisation in den Vereinigten Staaten aus der Schweiz empfangen und in irgendeiner Form gespeichert werden. Der Begriff der Bearbeitung wird seinerseits umschrieben als jeder Vorgang oder jede Reihe von Vorgängen im Zusammenhang mit Personendaten, durchgeführt mit oder ohne Einsatz automatisierter Verfahren, wie das Beschaffen, Speichern, Organisieren, Aufbewahren, Anpassen oder Verändern, Extrahieren, Abfragen, Verwenden, Bekanntgeben und Verbreiten oder das Löschen und Vernichten. Diese zentralen Begriffe werden also gleich definiert wie im schweizerischen Recht.

Die Grundsätze des *Swiss-U.S. DPF* garantieren die Einhaltung der wesentlichen datenschutzrechtlichen Grundsätze des schweizerischen Rechts, wie sie namentlich in Artikel 6 DSG umschrieben sind.

So müssen Personendaten rechtmässig und verhältnismässig bearbeitet werden, sie dürfen nur zu einem bestimmten Zweck beschafft und dann nur so verwendet werden, dass es mit diesem Zweck vereinbar ist. Im *Swiss-U.S. DPF* ergibt sich das vor allem aus dem Grundsatz der Datenintegrität und Zweckbindung (*Data Integrity and Purpose Limitation Principle*), aber auch aus dem Grundsatz der freien Wahlmöglichkeit (*Choice Principle*), wonach eine Organisation den betroffenen Personen die Möglichkeit geben muss zu entscheiden, ob ihre Personendaten an Dritte bekanntgegeben oder zu einem Zweck verwendet werden dürfen, der deutlich von dem abweicht, zu dem sie ursprünglich beschafft oder von diesen Personen nachträglich genehmigt wurde.

Die Personendaten müssen richtig und die Bearbeitung muss gemessen am Zweck, den sie verfolgt, verhältnismässig sein. Sie dürfen zudem nicht länger aufbewahrt werden als es zur Erreichung des Zwecks, für den sie beschafft wurden, nötig ist. Im *Swiss-U.S. DPF* ergibt sich das aus dem Grundsatz der Datenintegrität und Zweckbindung sowie aus dem Grundsatz der freien Wahlmöglichkeit.

Die Datensicherheit muss gewährleistet sein: Die Verantwortlichen und Auftragsbearbeiter müssen die Sicherheitsmassnahmen ergreifen, die mit Blick auf die mit der Bearbeitung verbundenen Risiken und die Art der bearbeiteten Daten vernünftig und geeignet sind. Im *Swiss-U.S. DPF* ergibt sich das aus dem Grundsatz der Sicherheit (S*ecurity Principle*).

Nach dem Grundsatz der Transparenz müssen die betroffenen Personen über die wesentlichen Merkmale der Bearbeitung ihrer Personendaten unterrichtet werden: Die Organisationen müssen insbesondere darüber informieren, dass sie dem *Swiss-U.S. DPF* unterstehen, welcher Art die beschafften Daten sind, welchen Zweck die Bearbeitung verfolgt, welche Rechte die betroffenen Personen haben und welche Rechtsmittel zur Verfügung stehen. Im *Swiss-U.S. DPF* ergibt sich das aus dem Grundsatz der Information (*Notice Principle*). Die Organisationen sind verpflichtet, ihre Datenschutzgrundsätze, in denen die Grundsätze des *Swiss-U.S. DPF* ihren Niederschlag finden, offenzulegen.

Den betroffenen Personen stehen gegenüber den Verantwortlichen und den Auftragsbearbeitern gewisse Ansprüche zu, insbesondere das Recht auf Auskunft, das Recht, sich der Bearbeitung zu widersetzen, und das Recht auf Berichtigung und Löschung der Daten. So haben die betroffenen Personen das Recht, sich ohne Angabe von Gründen bestätigen zu lassen,

dass sie betreffende Personendaten bearbeitet werden, und zu verlangen, dass ihnen diese Daten, die Informationen über den Zweck der Bearbeitung, die Arten der bearbeiteten Personendaten sowie deren Empfänger mitgeteilt werden. Dieses Auskunftsrecht kann nur ausnahmsweise, aus Gründen, welche vergleichbar sind mit denen, die das schweizerische Recht vorsieht, eingeschränkt werden, so wenn überwiegende Interessen eines Dritten es nötig machen. Darüber hinaus haben die betroffenen Personen das Recht, die Berichtigung unrichtiger Daten sowie die Löschung von Daten zu verlangen, die unter Verletzung der anwendbaren Grundsätze bearbeitet wurden. Im *Swiss-U.S. DPF* ergibt sich das aus dem Auskunftsgrundsatz (*Access Principle, Supplementary Principle on Access*).

Werden Personendaten zwischen einer zertifizierten Organisation und einem als Verantwortlicher oder Auftragsbearbeiter fungierenden Dritten weitergegeben, kommen nach dem Grundsatz über die Verantwortlichkeit der Weitergabe (*Accountability for Onward Transfer Principle*) besondere Regeln zur Anwendung: Eine solche Weitergabe darf nur für begrenzte und genau festgelegte Zwecke und auf vertraglicher Grundlage erfolgen, wobei der Vertrag vom Dritten verlangen muss, das gleiche Schutzniveau zu gewährleisten, das durch die Grundsätze garantiert wird.

Nach dem Grundsatz des Rechtsschutzes, der Durchsetzung und der Haftung (*Recourse, Enforcement and Liability Principle*) müssen die zertifizierten Organisationen wirksame Mechanismen schaffen, um die Einhaltung der Grundsätze sicherzustellen. Sie müssen auch Massnahmen treffen, um sich zu vergewissern, dass die Regelungen zum Schutz der Privatsphäre diesen Grundsätzen entsprechen und tatsächlich eingehalten werden. Dies kann durch ein System der Selbstkontrolle geschehen oder durch externe Überprüfungen.

Besondere Garantien kommen zur Anwendung, wenn es um die Bearbeitung besonders schützenswerter Personendaten in Sinn des schweizerischen Rechts geht: Die Organisationen müssen die ausdrückliche Einwilligung der betroffenen Personen einholen (sog. *opt-in*), wenn sie solche Daten an Dritte bekanntgeben oder sie für andere Zwecke verwenden wollen als die, für die sie beschafft wurden oder die diese Personen in Ausübung ihrer freien Wahlmöglichkeit nachträglich genehmigt haben. Allerdings ist die Einwilligung unter gewissen, eng umschriebenen Umständen, die mit den im schweizerischen Recht zugelassenen Ausnahmen vergleichbar sind, nicht erforderlich, so wenn überwiegende Interessen einer Drittperson es verlangen. Im *Swiss-U.S. DPF* ergeben sich die beschriebenen Anforderungen aus dem zusätzlichen Grundsatz über heikle Daten (*Supplemental Principle on Sensitive Data)*.

3.1.2 Anwendungsbereich

Der kommerzielle Rahmen gilt für Personendaten, die von der Schweiz an Organisationen in den Vereinigten Staaten übermittelt werden, die sich durch die Zertifizierung zur Einhaltung der Grundsätze verpflichtet haben (vgl. oben Ziff. 3.1.1).[7]

Der Rahmen ist auf Organisationen in den Vereinigten Staaten anwendbar, die als Verantwortliche i.S. von Artikel 5 Buchstabe j DSG oder als Auftragsbearbeiter i.S. von Artikel 5

[7] Ausgenommen sind Daten, die zum Zweck der Veröffentlichung, Verbreitung oder für andere Formen öffentlicher Kommunikation von journalistischem Material und von bereits veröffentlichten und aus Medienarchiven verbreiteten Informationen erhoben werden.

Buchstabe k DSG zu qualifizieren sind. Die Auftragsbearbeiter sind vertraglich zu verpflichten, nur auf Weisung des Verantwortlichen in der Schweiz zu handeln und diesen dabei zu unterstützen, Personen die Wahrnehmung ihrer Rechte im Rahmen der Grundsätze zu erleichtern.

3.2 Wirksamkeit der Garantien, Unabhängigkeit der Behörde, Rechtsschutz

3.2.1 Verwaltung des kommerziellen Rahmens, Zertifizierung und Überwachung

Die Verwaltung des kommerziellen Rahmens ist Sache des Handelsministeriums der Vereinigten Staaten (*U.S. Department of Commerce,* DoC).

Für eine Selbstzertifizierung oder eine spätere Rezertifizierung (auf jährlicher Basis) unter dem *Swiss-U.S. DPF* müssen die Organisationen öffentlich erklären, dass sie sich zur Einhaltung der Grundsätze verpflichten und dass sie ihre Datenschutzregelungen offenlegen und diese vollständig umsetzen. Sie sind verpflichtet, das DoC zudem insbesondere über die Zwecke, für die die Personendaten bearbeitet werden sollen, über den anwendbaren unabhängigen Beschwerdemechanismus und über das zuständige statutarische Kontrollorgan, das die Einhaltung der Grundsätze gewährleistet, zu informieren. Organisationen, die sich zum ersten Mal selbst zertifizieren, dürfen erst dann öffentlich darauf hinweisen, dass sie die Grundsätze einhalten, wenn das DoC sie in das Verzeichnis der teilnehmenden Organisationen aufgenommen hat, welches vom DOC geführt und der Öffentlichkeit zugänglich gemacht wird.

Das DoC übt auch eine Aufsichtsfunktion aus. Um eine korrekte Anwendung des *Swiss-U.S. DPF* sicherzustellen, führt es das erwähnte Verzeichnis der Organisationen, die sich gegenüber dem DoC selbst zertifiziert und sich zur Einhaltung der Grundsätze verpflichtet haben, und macht dieses der Öffentlichkeit zugänglich. Dies ermöglicht es, diese Organisationen als solche zu identifizieren. Das DoC führt ausserdem eine Liste der Organisationen, die aus dem Verzeichnis gestrichen worden sind, jeweils unter Angabe der Gründe für die Streichung. Das DoC wird diejenigen Organisationen aus dem Verzeichnis streichen, die sich freiwillig aus dem *Swiss-U.S. DPF* zurückziehen oder ihre jährliche Rezertifizierung gegenüber dem DoC nicht durchführen. Diese Organisationen müssen entweder die Grundsätze weiterhin auf die Personendaten anwenden, welche sie im Rahmen des *Swiss-U.S. DPF* erhalten haben und dem DoC jährlich bestätigen, dass sie sich dazu verpflichten (d.h. solange sie diese Daten aufbewahren), die Personendaten auf andere zulässige Weise geeignet schützen (z.B. durch einen Vertrag, der die Anforderungen der vom EDÖB genehmigten, ausgestellten oder anerkannten Standarddatenschutzklauseln vollständig umsetzt), oder die Daten zurückgeben oder löschen. Das DoC wird auch diejenigen Organisationen aus dem Verzeichnis streichen, die die Grundsätze wiederholt nicht eingehalten haben. Auch in diesem Fall müssen die Organisationen die Personendaten, die sie im Rahmen des *Swiss-U.S. DPF* erhalten haben, zurückgeben oder löschen.

Das DoC führt Kontrollen durch, um zu überprüfen, ob die Anforderungen an die Zertifizierung erfüllt werden, insbesondere ob die Grundsätze tatsächlich eingehalten werden. Dazu wird es stichprobenweise Kontrollen bei zufällig ausgewählten Organisationen durchführen, ebenso bei bestimmten Organisationen, wenn mögliche Probleme festgestellt werden, insbesondere wenn es Beschwerden erhält oder die Organisation Auskunftsersuchen nicht zufriedenstellend beantwortet. In gewissen Fällen kann die Organisation zur allfälligen Ergreifung von Zwangsmassnahmen an die zuständige Behörde verwiesen werden.

Das DoC wird auch Kontrollen durchführen, um sicher zu gehen, dass keine falschen Erklärungen über die Einhaltung der Grundsätze gemacht werden, insbesondere bei Organisationen, die aus dem Verzeichnis gestrichen worden sind. Gegebenenfalls kann sie die Angelegenheit an die zuständige Behörde überweisen, zur allfälligen Ergreifung von Zwangsmassnahmen.

3.2.2 Garantie der Einhaltung des Datenschutzrahmens

Die Teilhabe am kommerziellen Rahmen setzt voraus, dass die Organisationen der Gerichtsbarkeit der zuständigen Behörden der Vereinigten Staaten – der Bundeshandelskommission (*Federal Trade Commission*, FTC, nachstehend FT-Kommission) oder des Verkehrsministeriums (*U.S. Department of Transportation*, DoT) – unterstehen. Diese Behörden verfügen über die notwendigen Ermittlungs- und Durchsetzungskompetenzen, um die Einhaltung der Grundsätze wirksam sicherstellen zu können.[8]

Die FT-Kommission ist eine aus fünf Kommissarinnen und Kommissaren bestehende Behörde, die vom Präsidenten der Vereinigten Staaten ernannt werden; die Ernennung muss anschliessend durch den Senat bestätigt werden. Die Kommissarinnen und Kommissare, die während ihrer siebenjährigen Amtszeit keiner anderen Tätigkeit oder Anstellung nachgehen dürfen, können vom Präsidenten nur aus wichtigen Gründen ihres Amtes enthoben werden. Die FT-Kommission hat den Auftrag, die Öffentlichkeit vor irreführenden oder unfairen Handelspraktiken und unlauteren Wettbewerbsmethoden zu schützen. Sie kann Ermittlungen zur Einhaltung der Grundsätze sowie zu falschen Erklärungen über die Unterstellung unter den kommerziellen Rahmen führen. Sie kann Entscheidungen der Verwaltung oder der Bundesgerichte erwirken und die Einhaltung dieser Entscheidungen überwachen, indem sie Organisationen zur Herausgabe von Unterlagen zwingt, und sie kann den Rechtsweg beschreiten, um die Entscheidungen im Fall der Nichtbefolgung durchzusetzen.

Das DoT verfügt über die ausschliessliche Zuständigkeit zur Regelung der Datenschutzbestimmungen von Fluggesellschaften; geht es um Datenschutzbestimmungen von Reisebüros, die sich auf den Luftverkehr oder den Verkauf von Luftbeförderungsdienstleistungen beziehen, teilt sich das DoT die Zuständigkeit mit der FT-Kommission. Kann keine Einigung erzielt werden, kann das DoT einen unabhängigen und unparteiischen DoT-Verwaltungsrichter ersuchen, Unterlassungsanordnungen zu erlassen oder zivilrechtliche Sanktionen zu verhängen, oder es kann denselben Rechtsbehelf vor den Gerichten der Vereinigten Staaten einklagen.[9] Das DoT hat sich im Übrigen verpflichtet, Ermittlungen zu mutmasslichen Verstössen gegen die Grundsätze Priorität einzuräumen, bei falschen Erklärungen zur Unterstellung unter den kommerziellen Rahmen die Massnahmen zu ergreifen, die angezeigt sind, und dafür zu sorgen, dass die betreffenden Vollstreckungsverfügungen umgesetzt und veröffentlicht werden.

---

[8] Vgl. die Schreiben der FT-Kommission und des DoT, die über die am Schluss des vorliegenden Dokuments aufgeführten Internetadressen abgerufen werden können.

[9] Vgl. Regelungen über den Verkehr in Titel 49 des *United States Code* (U.S.C.), abrufbar unter: 49 USC Ch. 461: INVESTIGATIONS AND PROCEEDINGS (house.gov).

Die vorstehenden Ausführungen zeigen, dass die FT-Kommission und das DoT als unabhängige Kontrollbehörden qualifiziert werden können, die unter dem Aspekt eines angemessenen Schutzniveaus für Personendaten über hinreichende Befugnisse und Kompetenzen verfügen.

3.2.3 Rechtsschutz

Für ihre Zertifizierung müssen die Organisationen den Anforderungen des Grundsatzes des Rechtsschutzes, der Durchsetzung und der Haftung (*Recourse, Enforcement and Liability Principle*) (s.o. Ziff. 3.1.1) genügen, indem sie unabhängige, wirksame und leicht zugängliche Beschwerdemöglichkeiten vorsehen, die eine rasche und für die betroffene Person kostenlose Beilegung von Streitigkeiten erlauben.

Die Organisationen können unabhängige Beschwerdemöglichkeiten in der Schweiz oder in den Vereinigten Staaten wählen und sich für im Privatsektor erarbeitete Programme zum Schutz der Privatsphäre entscheiden, welche die Grundsätze in ihre Regelungen integriert haben, sowie gesetzliche oder reglementarische Überwachungsbehörden, die individuelle Beschwerden behandeln und Streitfälle beilegen können, oder sich verpflichten, mit dem EDÖB zusammenzuarbeiten.

Betroffene Personen können Beschwerden direkt bei der Organisation, bei einem von ihr bezeichneten unabhängigen Organ der Streitbeilegung oder beim EDÖB einreichen. Das DoC wird Organisationen, welche einen Streitfall nicht beilegen können, an das DoT oder die FT-Kommission verweisen. Die FT-Kommission und das DoT werden Hinweise auf die Nichteinhaltung der Grundsätze vorrangig behandeln. Betroffene Personen können Beschwerden auch über das Consumer Sentinel Netzwerk direkt bei der FT-Kommission einreichen oder die Webseite des DoT nutzen, um direkt Datenschutzbeschwerden gegen Fluggesellschaften und Ticketanbieter einzureichen.

Organisationen und verantwortliche unabhängige Beschwerdeinstanzen sind verpflichtet, die Beschwerden zügig zu behandeln. Hält sich eine Organisation nicht an die Entscheidung des unabhängigen Streitbeilegungsorgans oder der Regierungsstelle, kann das die Streichung aus dem vom DoC geführten und der Öffentlichkeit zugänglichen Verzeichnis zur Folge haben.

Betroffene Personen können auch Beschwerde beim EDÖB einreichen. Um die Behandlung der Beschwerden zu beschleunigen, steht zudem eine Kontaktstelle im DoT in direkter Verbindung zum EDÖB. So können betroffene Personen ihre Beschwerde direkt beim EDÖB einreichen und sie an das DoT, das den kommerziellen Rahmen verwaltet, weiterleiten lassen; auch das kann zur Streichung aus dem vom DoC geführten Verzeichnis führen.

Wurde ein Beschwerdefall nicht auf einem der beschriebenen Wege geklärt, kann die betroffene Person unter bestimmten Bedingungen die Möglichkeit eines verbindlichen Schiedsverfahrens in Anspruch nehmen, wie in Anhang I der Grundsätze beschrieben. Bei dieser Möglichkeit, die nur als letztes Mittel in Frage kommt, ist ein Schiedspanel aus – je nach Wunsch der Parteien – einem oder drei Mitgliedern befugt, individuelle, nicht geldwerte Abhilfemassnahmen anzuordnen, wie den Zugang zu den Personendaten, deren Korrektur, Löschung oder Rückgabe. Das DoT und die Schweiz werden gemeinsam eine Liste von Schiedsrichterinnen und -richtern erstellen, basierend auf den Kriterien Unabhängigkeit, Integrität und Erfahrung. Das internationale Zentrum für Streitbeilegung (*International Center for Dispute Resolution*, ICDR) der Amerikanischen Schiedsinstitution (*American Arbitration*

Association, AAA)[10] wird die Verwaltung der Schiedsfälle übernehmen. Die Verfahren vor dem Schiedspanel unterstehen einer Reihe von vereinbarten Schiedsregeln und einem Verhaltenskodex für die Schiedsrichterinnen und -richter. Die Durchsetzung der ergangenen Schiedssprüche kann vor den Gerichten der Vereinigten Staaten eingeklagt werden.[11]

Damit ist die Rechtsweggarantie gewährleistet, sobald die oben beschriebenen Rechtsbehelfe sicherstellen, dass Beschwerden über die Nichteinhaltung der Grundsätze des *Swiss-U.S. DPF* durch die zertifizierten Organisationen Gegenstand wirksamer Entscheidungen und Abhilfemechanismen sein werden.

4 Zugang der Behörden der Vereinigten Staaten zu den von der Schweiz übermittelten Personendaten

4.1 Zugang für Zwecke der Strafverfolgung

4.1.1 Anwendbare Gesetzgebung, Wirksamkeit der Garantien

Die Verfassung der Vereinigten Staaten garantiert, dass die Behörden nicht uneingeschränkt oder willkürlich Personendaten erfassen dürfen. Der 4. Zusatzartikel[12] bezweckt den Schutz der Privatsphäre und der Sicherheit des Individuums vor willkürlichen Übergriffen von Regierungsbeamtinnen und -beamten. Die rechtlichen Standards für den Erlass von Anordnungen sind sowohl bei physischen Durchsuchungen und Beschlagnahmungen als auch bei elektronisch gespeicherten Inhalten anwendbar. Auch wenn keine entsprechende Anordnung erforderlich ist, muss nach dem 4. Zusatzartikel jedes Handeln der Regierung angemessen sein.

Die Bundesstaatsanwältinnen und -staatsanwälte (*federal prosecutors*)[13] und die Strafermittlungsbeamtinnen und -beamten (*federal investigative agents*)[14] können zu Strafverfolgungszwecken (*criminal law enforcement*) Personendaten, die von zertifizierten Organisationen bearbeitet werden, nach den nachstehend beschriebenen Verfahren einsehen. Diese Verfahren kommen unabhängig von der Staatsangehörigkeit und dem Wohnort der betroffenen Personen zur Anwendung.

In Ermittlungen wegen bestimmter schwerer Straftaten kann eine *Grand Jury*, in der Regel auf Antrag einer Bundesstaatsanwältin oder eines Bundesstaatsanwalts, Anordnungen treffen

---

[10] Wenn der kommerzielle Rahmen in Kraft tritt, bietet die Internetseite des Zentrums kurze und klare Informationen zum Schiedsmechanismus und zum diesbezüglichen Antragsverfahren https://go.adr.org/sw-us_dpf_annexi.html.

[11] Vgl. Titel 9 des *United States Code* (U.S.C.), Schiedsverfahren, abrufbar unter: ARBITRATION (house.gov).

[12] Text der Verfassung der Vereinigten Staaten abrufbar unter: U.S. Senate: Constitution of the United States.

[13] Bundesstaatsanwältinnen und -staatsanwälte sind Beamtinnen und Beamte des Justizministeriums.

[14] Strafermittlungsbeamtinnen und -beamten sind dem Bundesamt für Ermittlungen (*Federal Bureau of Investigation*, FBI) angegliedert, das seinerseits zum Justizministerium gehört.

und Personen vorladen (*subpoenas*), um sie zu verpflichten, Geschäftsunterlagen, elektronisch gespeicherte Informationen oder sonstige materielle Beweismittel vorzulegen oder zur Verfügung zu stellen.[15] Zum selben Zweck können behördliche Anordnungen auch in Ermittlungen wegen Betrug im Gesundheitswesen, wegen Kindsmissbrauch, zum Schutz der Geheimdienste, wegen Verstössen gegen das Betäubungsmittelgesetz sowie bei Ermittlungen eines Generalinspektors oder einer Generalinspektorin zulässig sein. In beiden Fallgruppen müssen die Informationen für die Ermittlungen relevant sein, und die Anordnung muss angemessen, d.h. sie darf nicht übermässig, repressiv oder belastend sein; sie kann im Übrigen aus diesen Gründen angefochten werden.

Verschiedene Rechtsgrundlagen[16] ermächtigen die Strafverfolgungsbehörden, auf Kommunikationsdaten zuzugreifen. Ein Gericht kann die Erhebung in Echtzeit von nichtinhaltlichen Wähl-, Routing-, Anschluss- und Signalinformationen zu einer Telefonnummer oder E-Mail-Adresse genehmigen, wenn es feststellt, dass die Behörde eine mögliche Relevanz dieser Informationen für laufende strafrechtliche Ermittlungen bescheinigt hat. Der Einsatz von Tracking-Geräten kann für einen Zeitraum von höchstens 60 Tagen genehmigt und nur durch eine neue richterliche Anordnung verlängert werden. Ausserdem kann durch richterliche Anordnung der Zugang zu Kunden- und Verkehrsdaten sowie Kommunikationsinhalten erwirkt werden, die von Internetdienstanbietern, Telefongesellschaften und anderen dritten Dienstanbietern gespeichert werden; dabei stützt sich die Anordnung auf die Vermutung, dass die betreffenden Daten Beweise für eine Straftat liefern. Für Daten über registrierte Abonnentinnen und Abonnenten, IP-Adressen und Rechnungsdaten können die Strafverfolgungsbehörden entsprechende Anordnungen treffen. Für die meisten anderen gespeicherten nichtinhaltlichen Informationen können sie eine richterliche Anordnung einholen, wenn das Gericht überzeugt ist, dass die beantragten Informationen für laufende strafrechtliche Ermittlungen einschlägig und wichtig sind.

Auf richterliche Anordnung hin können die Strafverfolgungsbehörden auch drahtgebundene, mündliche oder elektronische Kommunikation in Echtzeit abhören. Die Anordnung stellt unter anderem fest, dass das Abhören oder elektronische Abfangen vermutlich Beweise für eine Straftat oder den Aufenthaltsort einer flüchtigen Person liefert.

Besteht die Vermutung, dass verwertbare Gegenstände gefunden werden könnten, etwa als Beweis für eine Straftat, kann das Gericht eine Durchsuchung oder Beschlagnahme anordnen. Werden auf diese Weise Beweise rechtswidrig erlangt, kann die betroffene Person verlangen, dass sie nicht verwertet werden, wenn sie in einem Strafverfahren vorgelegt werden sollten. Wird ein Dateninhaber, z.B. ein zertifiziertes Unternehmen, aufgrund eines Durchsuchungsbefehls zur Offenlegung von Daten verpflichtet, kann er diese Verpflichtung anfechten,

---

[15] Vgl. die bundesrechtlichen Regeln zum Strafverfahren (*Federal Rules of Criminal Procedure*), abrufbar unter: Current Rules of Practice & Procedure | United States Courts (uscourts.gov).

[16] Vgl. Titel 18 des *United States Code* (U.S.C.), Bestimmungen über die Straftaten und die Strafverfolgung (insbesondere die Art. 2510 ff., 2701 ff. und 3121 ff.), abrufbar unter: OLRC Home (house.gov).

unter anderem mit der Begründung, dass sie eine unbillige Härte (*unduly burdensome*) darstelle.[17]

Neben dem beschriebenen gesetzlichen Rahmen für den behördlichen Zugang zu Personendaten für Strafverfolgungszwecke hat der Generalstaatsanwalt (*Advocate General*) Leitlinien publiziert, die den Zugang zusätzlich einschränken und auch Bestimmungen zum Schutz der Privatsphäre enthalten. Das betrifft namentlich die Leitlinien für Inlandeinsätze des FBI[18], die unter anderem verlangen, dass die am wenigsten einschneidenden Ermittlungsmethoden angewendet werden, unter Berücksichtigung des Eingriffs in die Privatsphäre und einer potenziellen Rufschädigung.

Für auf die Gesetzgebung der Bundesstaaten gestützte Ermittlungen gelten vergleichbare Garantien. Die Strafverfolgungsbehörden greifen im Wesentlichen in gleicher Weise auf die Möglichkeit von Anordnungen und Vorladungen zurück wie oben für die Bundesbehörden beschrieben, zum Teil aber mit zusätzlichen, in Verfassung oder Gesetz der Bundesstaaten vorgesehenen Einschränkungen. In jedem Fall müssen die auf Stufe der Bundesstaaten geltenden Garantien denen der Verfassung der Vereinigten Staaten mindestens gleichwertig sein.

Ähnliche Garantien gelten auch für behördliche Anordnungen, die ergehen, um für zivilrechtliche oder regulatorische Zwecke – d.h. im öffentlichen Interesse – Zugang zu Daten zu erhalten, die sich im Besitz von Unternehmen in den Vereinigten Staaten befinden. Dabei dürfen die Behörden mit zivilrechtlichen und regulatorischen Aufgaben, Zugang nur zu Daten verlangen, die für Fragen relevant sind, welche in ihren Zuständigkeitsbereich fallen.[19] Der Empfänger einer solchen Anordnung kann deren Vollzug gerichtlich anfechten, da die Anordnung angemessen («*reasonable*») sein muss.[20] Auch wenn behördliche Anordnungen keiner vorgängigen gerichtlichen Genehmigung bedürfen, können sie trotzdem Gegenstand einer gerichtlichen Kontrolle werden, nämlich im Fall einer Anfechtung durch die betroffene Person, oder wenn die Behörde die Anordnung vor Gericht durchzusetzen will. Über diese allgemei-

---

[17] Vgl. die bundesrechtlichen Regeln zum Strafverfahren (*Federal Rules of Criminal Procedure*).

[18] Abrufbar unter: The Attorney General's Guidelines for Domestic FBI Operations (justice.gov).

[19] Der Oberste Gerichtshof der Vereinigten Staaten hat in dieser Hinsicht auch die Notwendigkeit betont, ein Gleichgewicht zwischen der Bedeutung des öffentlichen Interesses und der Bedeutung der Interessen der betroffenen Personen am Schutz ihrer Privatsphäre zu finden. Vgl. *Oklahoma Press Publishing Co. v. Walling*, 327 U.S. 186 (1946), abrufbar unter: U.S. Reports: Okla. Press Pub. Co. v. Walling, 327 U.S. 186 (1946).(loc.gov).

[20] Vgl. die oben im Zusammenhang mit Anordnungen im Strafprozess erwähnten Kriterien.

nen Garantien hinaus können sich aus gewissen Gesetzen spezifische, strengere Anforderungen ergeben.[21] In jedem Fall sind die Anforderungen des 4. Zusatzartikels zur Verfassung der Vereinigten Staaten zu erfüllen.

Ergänzend ist darauf hinzuweisen, dass die USA durch das Justizdepartement (DoJ) die oben beschriebenen Garantien und Zugangsbeschränkungen auch in einem Schreiben bestätigt haben.[22]

Die weitere Verwendung der beschafften Daten wird durch eine zentrale Richtlinie (Rundschreiben Nr. A-130 des Büros für Verwaltung und Budget [*Office of Management and Budget*, OMB])[23] geregelt, die von allen Bundesbehörden, einschliesslich den Strafverfolgungsbehörden, umgesetzt und eingehalten werden muss, wenn sie identifizierbare Personendaten bearbeiten. Die Behörden sind gehalten, die Erfassung, Beschaffung, Verwendung, Bearbeitung, Speicherung, Verwaltung, Verbreitung und Offenlegung identifizierbarer Personendaten auf das zu beschränken, was rechtlich zulässig, relevant und nach vernünftigem Ermessen für die ordnungsgemässe Erfüllung der der Behörde übertragenen Aufgaben erforderlich ist. Die Behörden müssen ein umfassendes Programm zum Schutz der Privatsphäre aufstellen (Risikomanagement, Verfahren zur Erkennung, Dokumentation und Meldung von Vorfällen, usw.).

Gestützt auf die Regelung über das E-Government (*E-Government Act*)[24] sind die Bundesbehörden verpflichtet, Massnahmen zum Schutz der Datensicherheit zu treffen, die dem Risiko und dem Umfang des Schadens Rechnung tragen, der durch unbefugten Zugang, unbefugte Verwendung, Verbreitung, Unterbrechung, Veränderung oder Vernichtung von Daten entstehen könnte. Sie müssen zudem einen IT-Beauftragten (*Chief Information Officer*) ernennen, der die Einhaltung der Anforderungen an die Datensicherheit gewährleistet und jährliche unabhängige Evaluationen durchführt. Analysen der Auswirkungen auf die Privatsphäre sind für alle Bundesbehörden vorgeschrieben, die neue IT-Technologien entwickeln oder anschaffen, mit denen Daten in identifizierbarer Form beschafft, aufbewahrt oder verbreitet werden, oder die eine neue Datenbeschaffung einführen.

Das OMB und das Nationale Institut für Normen und Technologie (*National Institute of Standards and Technology*, NIST) haben für die Bundesbehörden (einschliesslich Strafverfolgungsbehörden) verbindliche Normen entwickelt, welche die Mindestanforderungen an die Datensicherheit umschreiben. Dazu gehören Kontrollen des Datenzugangs, Sensibilisierung

---

[21] So können beispielsweise Finanzinstitute behördliche Anordnungen, die bezwecken, an gewisse Arten von Informationen heranzukommen, angefochten werden, unter Berufung auf das Gesetz über das Bankgeheimnis und die Ausführungsgesetzgebung, vgl. insbesondere Titel 31 des *United States Code* (U.S.C.), Regelung über Geld und Finanzen, abrufbar unter: OLRC Home (house.gov).

[22] Vgl. das Schreiben des DoJ, zugänglich über die am Schluss des vorliegenden Dokuments aufgeführten Internetadressen.

[23] Abrufbar unter: Review-Doc-2016--466-1.docx (archives.gov).

[24] Vgl. Titel 44, Kapitel 36 des *United States Code* (U.S.C.).

und Schulung, Notfallplanung, Reaktion auf Vorfälle, Prüfungs- und Rechenschaftsinstrumente, Gewährleistung der System- und Datenintegrität, die Evaluation der Sicherheits- und Datenschutzrisiken, usw.[25]

Nach den Vorschriften über Bundesdokumente[26] müssen Daten, die sich im Besitz von Bundesbehörden befinden, durch Massnahmen geschützt werden, welche die physische Unversehrtheit der Daten gewährleisten und einen unbefugten Zugriff verhindern.

Was die Datenaufbewahrung betrifft, sind die Bundesbehörden gehalten, Aufbewahrungsfristen festzulegen, die durch die Nationale Verwaltungsstelle für Archivgut und Unterlagen (*National Archives and Record Administration*)[27] genehmigt werden müssen. Die Dauer wird in Abhängigkeit verschiedener Faktoren bestimmt, wie etwa der Art der Ermittlungen oder der Relevanz der Beweismittel für die Ermittlungen.

4.1.2 Unabhängigkeit der Behörde, Rechtsschutz

4.1.2.1 Aufsicht

Die Tätigkeit der Bundesstrafverfolgungsbehörden steht unter der Aufsicht verschiedener Stellen.[28] Wie unter Ziffer 4.1.1 ausgeführt, handelt es sich dabei häufig um eine vorgängige Kontrolle durch Gerichte, welche die verschiedenen Massnahmen zur Datenbeschaffung genehmigen müssen. Darüber hinaus überwachen auch andere Organe die Tätigkeit der Strafverfolgungsbehörden. Richterliche wie nicht richterliche Organe bieten Gewähr für eine unabhängige Kontrolle.

In verschiedenen Behörden, die für die Strafverfolgung zuständig sind, gibt es Bürgerrechts- und Datenschutzbeauftragte (*Civil Liberties and Privacy Officers*, CLPO, nachstehend: CLP-Beauftragte).[29] Zu ihren Aufgaben gehört allgemein die Aufsicht über die Verfahren, mit denen sichergestellt werden soll, dass die betreffende Behörde die Belange des Datenschutzes und der bürgerlichen Freiheiten angemessen berücksichtigt und geeignete Vorkehrungen getroffen hat, um Beschwerden wegen Verletzung des Datenschutzes oder bürgerlicher Rechte zu behandeln. Die Verantwortlichen der einzelnen Behörden müssen dafür sorgen, dass die

---

[25] Vgl. das Rundschreiben Nr. A-130 des OMB; NIST SP 800-53, Rev. 5, Control Mappings to ISO/IEC 27001, Juli 2023, abrufbar unter: SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations | CSRC (nist.gov).

[26] Vgl. Titel 44, Kapitel 31 des *United States Code* (U.S.C.).

[27] Vgl. Titel 44, Kapitel 29 des *United States Code* (U.S.C.).

[28] Die unter Ziff. 4.1.2.1 erwähnten Mechanismen sind auch auf die Datenbeschaffung und -verwendung durch Bundesbehörden für zivil- oder aufsichtsrechtliche Zwecke anwendbar. Die Zivil- und Aufsichtsbehörden des Bundes unterstehen der Aufsicht ihrer jeweiligen Generalinspektorinnen und -inspektoren und des Kongresses.

[29] Vgl. Titel 42, Kapitel 21E des *United States Code* (U.S.C.).

CLP-Beauftragten über die notwendigen Unterlagen und Ressourcen verfügen, Zugang zum für die Erfüllung ihrer Aufgaben erforderlichen Material und Personal haben und über vorgeschlagene Änderungen der Datenschutzpolitik informiert und dazu konsultiert werden. Die CLP-Beauftragten haben dem Kongress regelmässig Bericht zu erstatten, der insbesondere Angaben zu Anzahl und Art der bei den Behörden eingegangenen Beschwerden und deren Ausgang, sowie zu den Auswirkungen der von den CLP-Beauftragten geleisteten Arbeit enthält.

Darüber hinaus kontrolliert eine unabhängige[30] Generalinspektorin[31] oder ein unabhängiger Generalinspektor die Aktivitäten des Justizdepartements, einschliesslich jene des FBI. Er oder sie führt unabhängige Untersuchungen, Audits und Inspektionen der Programme und Aktivitäten des DoJ durch,[32] hat Zugang zu sämtlichen Dossiers, Berichten, Audits, Überprüfungen, Dokumenten, Empfehlungen oder sonstigem einschlägigem Material, deren Herausgabe er/sie notfalls unter Strafandrohung anordnen kann, und kann Zeugenaussagen abnehmen. Wenn die Generalinspektorin oder der Generalinspektor unverbindliche Empfehlungen zu Abhilfemassnahmen ausspricht, werden seine Berichte in der Regel veröffentlicht und dem Kongress übermittelt, der dann seine Kontrollfunktion wahrnehmen kann. Die Generalinspektorin oder der Generalinspektor nimmt Beschwerden von Privatpersonen entgegen und prüft diese.

Weiter unterstehen Strafverfolgungsbehörden, die in der Terrorismusbekämpfung tätig sind, der Kontrolle der Stelle zur Überwachung der Privatsphäre und der bürgerlichen Freiheiten (*Privacy and Civil Liberties Oversight Board*, PCLOB, nachstehend: PCLO-Stelle). Die PCLO-Stelle ist eine unabhängige Behörde innerhalb der Exekutive, die sich aus fünf Mitgliedern zusammensetzt, die vom Präsidenten der USA mit Zustimmung des Senats für eine feste Amtszeit von sechs Jahren ernannt werden; ihm dürfen unter keinen Umständen mehr als drei Mitglieder derselben politischen Partei angehören.[33] Die Stelle ist mit Aufgaben im Bereich der Terrorismusbekämpfung und deren Umsetzung im Einklang mit dem Schutz der Privatsphäre und der bürgerlichen Freiheiten betraut. Sie hat Zugriff auf alle einschlägigen Dossiers, Berichte, Audits, Überprüfungen, Dokumente und Empfehlungen von Bundesbehörden, einschliesslich klassifizierter Informationen, und kann Zeugenaussagen abnehmen. Die Stelle erhält Berichte der CLP-Beauftragten verschiedener Bundesbehörden, kann Empfehlungen an Regierungs- und Strafverfolgungsbehörden abgeben, und erstattet den Ausschüssen des Kongresses und dem Präsidenten regelmässig Bericht. Die Berichte müssen wenn immer möglich veröffentlicht werden.

---

[30] Die Generalinspektorinnen und -inspektoren sind unkündbar und können nur durch den Präsidenten der Vereinigten Staaten ihres Amtes enthoben werden, wobei dieser dem Kongress schriftlich die Gründe für die Amtsenthebung mitteilen muss.

[31] Vgl. Titel 5, Teil I, Kapitel 4 des *United States Code* (U.S.C.).

[32] Vgl. den Strategieplan 2020-204 des Generalinspektors des DoJ, abrufbar unter: Strategic Plan Draft - To AIGs (justice.gov).

[33] Vgl. Titel 42, Kapitel 21E des *United States Code* (U.S.C.).

Schliesslich unterstehen die Tätigkeiten im Zusammenhang mit der Strafverfolgung der Kontrolle durch spezielle Kommissionen des Kongresses (die Rechtskommissionen des Repräsentantenhauses und des Senats). Diese Rechtskommissionen üben auf verschiedene Weise eine regelmässige Aufsicht aus, insbesondere durch Anhörungen, Untersuchungen, Überprüfungen und Berichte.

4.1.2.2 Rechtsschutz

Die Strafverfolgungsbehörden benötigen für die Beschaffung von Personendaten in den meisten Fällen eine vorgängige richterliche Genehmigung. Das gilt nicht für behördliche Anordnungen, die aber auf spezielle Situationen beschränkt sind und zumindest dann einer unabhängigen richterlichen Überprüfung unterliegen, wenn sie vor Gericht durchgesetzt werden sollen. Insbesondere können die Adressatinnen und Adressaten diese Anordnungen vor Gericht anfechten, mit der Begründung, sie seien nicht angemessen, d.h. übermässig, repressiv oder belastend. Die betroffenen Personen können bezüglich der Bearbeitung ihrer Personendaten Gesuche oder Beschwerden bei den Strafverfolgungsbehörden einreichen. Auf diesem Weg können sie namentlich den Zugang zu ihren Personendaten und deren Berichtigung verlangen.[34] Was die Tätigkeit im Zusammenhang mit der Terrorismusbekämpfung betrifft, können Betroffene auch Beschwerde bei den CLP-Beauftragten der Strafverfolgungsbehörden einreichen.[35]

Darüber hinaus bestehen mehrere gerichtliche Rechtsbehelfe gegen eine Behörde oder eine oder einen ihrer Beamtinnen oder Beamten, die Personendaten bearbeiten. Diese Rechtsbehelfe[36] stehen allen Personen unabhängig von ihrer Nationalität offen, wenn die jeweiligen Voraussetzungen erfüllt sind.

Nach den im Verwaltungsverfahrensrecht enthaltenen Bestimmungen über die gerichtliche Überprüfung[37] kann jede Person, die durch Entscheidungen einer Behörde einen Schaden erleidet, von einer solchen Entscheidung betroffen ist oder durch sie verletzt wird, Beschwerde vor Gericht einlegen. Das schliesst die Möglichkeit ein, dem Gericht zu beantragen, die Entscheidung, Feststellungen und Schlussfolgerungen der Behörde, die als willkürlich, mutwillig, ermessensmissbräuchlich oder sonstwie nicht rechtskonform anzusehen sind, für rechtswidrig zu erklären und aufzuheben.

Noch konkreter ist die Vertraulichkeit der elektronischen Kommunikation geregelt.[38] Die Regelung sieht ein System von gesetzlichen Rechten zum Schutz der Privatsphäre vor, und sie bestimmt den Zugriff der Strafverfolgungsbehörden auf den Inhalt telefonischer, mündlicher

---

[34] Vgl. Rundschreiben Nr. A-130 des OMB.

[35] Vgl. Titel 42, Kapitel 21 des *United States Code* (U.S.C.).

[36] Vgl. insbesondere die Regelungen über das Verwaltungsverfahren und die Transparenz (Titel 5 des *United States Code* [U.S.C.]) und die Regelung über die Vertraulichkeit elektronischer Kommunikation (Titel 18 des *United States Code* [U.S.C.]).

[37] Vgl. Titel 5 des *United States Code* (U.S.C.).

[38] Vgl. Titel 18, Teil I, Kapitel 121 des *United States Code* (U.S.C.).

und elektronischer Kommunikation, die von Drittanbieterinnen gespeichert wird. Der rechtswidrige Zugriff, der nicht gerichtlich genehmigt oder anderweitig erlaubt wurde, ist strafbar; betroffene Personen können vor einem amerikanischen Bundesgericht Klage auf zivilen und pönalen Schadenersatz erheben und eine gerechte Wiedergutmachung oder einen Feststellungsentscheid gegen eine Beamtin oder einen Beamten, die oder der vorsätzlich solche rechtswidrigen Handlungen begangen hat, oder gegen die Vereinigten Staaten erwirken.

Verschiedene weitere Regelungen[39] geben betroffenen Personen das Recht, eine Klage gegen eine Behörde oder einen amerikanischen Beamten wegen der Bearbeitung ihrer Personendaten zu erheben.

Schliesslich hat jede Person gestützt auf die Öffentlichkeitsgesetzgebung (Freedom of Information Act)[40] das Recht auf Zugang zu Informationen der Bundesbehörden, einschliesslich solchen, die Personendaten enthalten. Nach Ausschöpfung der verwaltungsinternen Rechtsmittel kann sie dieses Zugangsrecht vor Gericht geltend machen, es sei denn, die Informationen wären durch eine Ausnahme oder eine besondere, die Anwendung des Gesetzes ausschliessende Klausel vor der Veröffentlichung geschützt. In diesem Fall wird das Gericht prüfen, ob eine Ausnahmeregelung gilt bzw. von der zuständigen Behörde rechtmässig geltend gemacht wurde.

4.2 Zugang für Zwecke der nationalen Sicherheit

4.2.1 Anwendbare Gesetzgebung, Wirksamkeit der Garantien

Die Behörden der Vereinigten Staaten können für Zwecke der nationalen Sicherheit unter Einhaltung besonderer Bedingungen und Garantien Personendaten erheben, die von der Schweiz an zertifizierte Organisationen übermittelt wurden. Besonderes Augenmerk gilt hier der Beurteilung der Fernmeldeaufklärung (*signals intelligence*), bei der die elektronische Kommunikation und Daten aus Informationssystemen erhoben werden, die Personendaten enthalten können.

Gestützt auf die Durchführungsverordnung (*executive order*) EO 12333 von 1981[41] (nachstehend: EO 12333) über die Tätigkeit der Nachrichtendienste der Vereinigten Staaten können Personendaten auch ausserhalb der USA erhoben werden, also auch im Zuge ihrer Übermittlung von der Schweiz in die USA.

Sobald Personendaten bei in den Vereinigten Staaten zertifizierten Organisationen eingegangen sind, können die Nachrichtendienste Zugang zu diesen Daten verlangen, wenn das geltende Recht es erlaubt. Solche Datenerhebungen können insbesondere in der Gesetzgebung

---

[39] Namentlich die Regelungen über Telefonabhörungen und über Computerbetrug und -missbrauch (vgl. Titel 18 des *United States Code* (U.S.C.).

[40] Vgl. Titel 5 des *United States Code* (U.S.C.).

[41] Vgl. Executive Orders | National Archives.

über die Überwachung durch Auslandsgeheimdienste vorgesehen sein (*Foreign Intelligence Surveillance Act*, FISA, nachstehend FIS-Gesetz).[42]

Am 7. Oktober 2022 erliess der Präsident der Vereinigten Staaten die Durchführungsverordnung EO 14086[43] (nachstehend: EO 14086) über den Ausbau der Garantien im Bereich der Signalaufklärungsaktivitäten. Die EO 14086 ersetzt weitgehend[44] die Richtlinie 28 des Präsidenten (*Presidential Policy Directive*, PPD-28)[45], gilt für sämtliche Signalaufklärungsaktivitäten, also sowohl für die auf das FIS-Gesetz als auch für die auf die EO 12333 abgestützten Aktivitäten, und ist für die Gesamtheit der US-amerikanischen Nachrichtendienste verbindlich. Es legt Schranken und Garantien fest, welche jene im FIS-Gesetz und der EO 12333 vorgesehenen ergänzen, und führt einen neuen Rechtsschutzmechanismus ein, mit dem diese Garantien geltend gemacht und durchgesetzt werden können. Die Nachrichtendienste haben ihre Richtlinien und Verfahren aktualisiert, um sie mit der EO 14086 in Einklang zu bringen; dem Prozess gingen Konsultationen unter anderem des Generalstaatsanwalts, der ODNI CLP-Beauftragten und der PCLO-Stelle voraus, bevor die Neuerungen am 3. Juli 2023 publiziert wurden.[46]

Die EO 14086 enthält einen Katalog von Anforderungen, die für alle Tätigkeiten im Bereich der Signalaufklärung gelten. Die Tätigkeiten müssen gesetzlich vorgesehen sein oder auf einer Ermächtigung des Präsidenten beruhen und im Einklang mit der Gesetzgebung der Vereinigten Staaten, insbesondere der Verfassung, ausgeführt werden. Es sind geeignete Garantien vorzusehen, um sicherzustellen, dass bei der Planung solcher Tätigkeiten dem Schutz der Privatsphäre und dem Schutz der bürgerlichen Freiheiten aller natürlichen Personen, unabhängig von der Staatsangehörigkeit oder ihres Wohnsitzes, Rechnung getragen wird. Insbesondere muss vorgängig, auf der Grundlage einer sachgerechten Evaluation aller relevanten Faktoren, festgestellt worden sein, dass die Tätigkeiten notwendig sind, um eine anerkannte nachrichtendienstliche Priorität voranzubringen. Zudem müssen sie in einem angemessenen Verhältnis zu der anerkannten Aufklärungspriorität stehen, für die sie genehmigt wurden. Es ist mit anderen Worten eine Interessensabwägung vorzunehmen zwischen der Bedeutung der Tätigkeit für diese Priorität und den Auswirkungen auf die Privatsphäre und die bürgerlichen Freiheiten der betroffenen Personen.

Die beschriebenen Anforderungen werden noch durch Garantien verstärkt, die sicherstellen sollen, dass der Eingriff in die Rechte der Betroffenen nicht über das hinausgeht, was zur Erreichung eines legitimen Zwecks notwendig und verhältnismässig ist.

---

42 Vgl. Titel 50, Kapitel 36 des *United States Code* (U.S.C.).

43 Vgl. die am Schluss des vorliegenden Dokuments aufgeführten Internetadressen.

44 Die EO 14086 ersetzt das PPD-28 mit Ausnahme einiger spezifischer Bestimmungen (Teilwiderruf des PPD-28).

45 Vgl. Presidential Policy Directive -- Signals Intelligence Activities | whitehouse.gov (archives.gov).

46 Vgl. INTEL - ODNI Releases IC Procedures Implementing New Safeguards in Executive Order 14086.

Zunächst beschränkt die EO 14086 die Gründe, aus denen Fernmeldeaufklärungsdaten erhoben werden dürfen. Zum einen definiert die EO die legitimen Zwecke, die mit der Erhebung verfolgt werden können, darunter z.B. das Verständnis oder die Bewertung der Fähigkeiten, Absichten oder Aktivitäten ausländischer Organisationen, einschliesslich internationaler terroristischer Organisationen, die eine tatsächliche oder potenzielle Bedrohung für die nationale Sicherheit der Vereinigten Staaten darstellen. Zum anderen listet sie gewisse Ziele auf, die unter keinen Umständen verfolgt werden dürfen, darunter etwa das Ziel, die freie Äusserung von Ideen oder politischen Meinungen durch Private oder die Presse zu beschränken. Ausserdem darf die tatsächliche Datenerhebung nur erfolgen, um eine nachrichtendienstliche Priorität voranzubringen; solche Prioritäten werden von der Direktorin des Nationalen Nachrichtendienstes festgelegt, von den CLP-Beauftragten und vom ODNI evaluiert und anschliessend dem Präsidenten der Vereinigten Staaten zur Genehmigung vorgelegt. Dieses Verfahren bietet Gewähr dafür, dass die dem Schutz der Privatsphäre dienenden Aspekte berücksichtigt werden, wenn nachrichtendienstliche Prioritäten ausgearbeitet werden.

Ist eine Aufklärungspriorität festgelegt, wird anhand verschiedener Voraussetzungen entschieden, ob und in welchem Umfang Fernmeldeaufklärungsdaten erhoben werden dürfen, um diese Priorität zu fördern. Diese Voraussetzungen konkretisieren die allgemeinen Standards der EO 14086 zu Notwendigkeit und Verhältnismässigkeit. So dürfen die Fernmeldeaufklärungsdaten erst erhoben werden, nachdem auf der Grundlage einer sachgerechten Beurteilung aller relevanten Faktoren festgestellt worden ist, dass die Erhebung notwendig ist, um eine bestimmte nachrichtendienstliche Priorität voranzubringen. Um dieses Kriterium der Notwendigkeit beurteilen zu können, müssen die Nachrichtendienste die Verfügbarkeit, Umsetzbarkeit und Zulässigkeit anderer, weniger einschneidender Quellen und Methoden prüfen und ggf. diese prioritär zum Einsatz bringen.

Wird die Erhebung von Fernmeldeaufklärungsdaten als notwendig erachtet, muss sie so genau wie möglich auf die konkreten Bedürfnisse zugeschnitten werden. Um unverhältnismässige Eingriffe in die Privatsphäre und die bürgerlichen Freiheiten zu verhindern, d.h. um ein Gleichgewicht zwischen den Bedürfnissen der nationalen Sicherheit einerseits und dem Schutz der Privatsphäre und den bürgerlichen Freiheiten andererseits herzustellen, müssen alle relevanten Faktoren ausreichend berücksichtigt werden, wie etwa die Art des verfolgten Zwecks, die Eingriffsintensität der Erhebung, namentlich ihre Dauer, der mutmassliche Beitrag der Erhebung zur Erreichung des Zwecks, die realistischerweise zu erwartenden Folgen für die Betroffenen, sowie die Art und die Sensibilität der zu erhebenden Daten.

Eine Sammelerhebung von Fernmeldeaufklärungsdaten, d.h. die Beschaffung grosser Mengen von Fernmeldeaufklärungsdaten ohne Anwendung besonderer Suchbegriffe,[47] darf nur ausserhalb der Vereinigten Staaten auf der Grundlage der EO 12333 durchgeführt werden. Allerdings ist einer gezielten Erhebung der Vorzug zu geben. Nach der EO 14086 ist eine Sammelerhebung nur zulässig, wenn die für die Förderung einer validierten Aufklärungspriorität erforderlichen Informationen vernünftigerweise nicht durch eine gezielte Erhebung erlangt werden können, und es kommen besondere Garantien zur Anwendung: Es müssen geeignete Methoden und technische Massnahmen eingesetzt werden, um die erhobenen Daten

[47] Die Sammelerhebung ist zu unterscheiden von der allgemeinen und wahllosen Datenbeschaffung («Massenüberwachung»), bei der keine Einschränkungen und Garantien bestehen.

auf das zu beschränken, was für die Förderung einer validierten Aufklärungspriorität erforderlich ist, und um die Erhebung irrelevanter Informationen so gering wie möglich zu halten. Weiter wird die Verwendung von Informationen, die durch die Sammelerhebung gewonnen wurden, auf sechs vordefinierte Zwecke beschränkt, darunter der Schutz vor Terrorismus, ausländischer Spionage, Sabotage oder Mord. Schliesslich dürfen Fernmeldeaufklärungsdaten, die durch eine Sammelerhebung gewonnen wurden, nur dann abgefragt werden, wenn dies zur Förderung einer validierten Aufklärungspriorität erforderlich ist, und zwar in Verfolgung der sechs Ziele und im Einklang mit Strategien und Verfahren, die den Auswirkungen der Abfragen auf die Privatsphäre und die bürgerlichen Freiheiten aller Personen, unabhängig von ihrer Staatsangehörigkeit oder ihrem Wohnort, gebührend Rechnung tragen.

Zusätzlich zu den Anforderungen der EO 14086 unterliegt die Erhebung von Fernmeldeaufklärungsdaten, die an eine zertifizierte Organisation in den Vereinigten Staaten übermittelt werden, besonderen Einschränkungen und Garantien, die in Artikel 702 FIS-Gesetz geregelt sind. Nach dieser Bestimmung unterbreiten der Generalstaatsanwalt und die Direktorin des Nationalen Nachrichtendienstes dem für die Überwachung der Auslandgeheimdienste zuständigen Gericht (*Foreign Intelligence Surveillance Court*, FISC, nachstehend FIS-Gericht) jährliche Zertifizierungen, in denen die Kategorien der zu erhebenden Auslandsaufklärungsdaten bestimmt sind. Die Zertifizierungen sind mit Verfahren zur zielgenauen Erfassung, Minimierung und Datenabfrage einzureichen, die ebenfalls vom Gericht genehmigt werden und für die Nachrichtendienste rechtsverbindlich sind.

Das FIS-Gericht ist ein unabhängiges Gericht, dessen Entscheidungen vor dem für die Überwachung der Auslandsgeheimdienste zuständigen Rechtsmittelgericht (*Foreign Intelligence Surveillance Court of Review*, FISCR) und letztinstanzlich vor dem Obersten Gerichtshof der Vereinigten Staaten angefochten werden können.[48] Das FIS-Gericht wird von einer ständigen Expertengruppe unterstützt, die aus fünf Rechtsanwältinnen oder Rechtsanwälten und fünf Sachverständigen für nationale Sicherheit und Bürgerrechte besteht; so ist gewährleistet, dass Fragen zum Schutz der Privatsphäre angemessen berücksichtigt werden.

Zuständig für Entscheidungen über die individuelle, zielgenaue Datenerfassung ist die Nationale Sicherheitsbehörde (*National Security Agency*, NSA). Sie trifft die Auswahl der einzelnen Zielpersonen nach den vom FIS-Gericht genehmigten Verfahren für die zielgenaue Erfassung. Danach muss die NSA auf Grundlage der gesamten Umstände feststellen, dass die zielgenaue Datenerfassung gegen eine bestimmte Person wahrscheinlich zu Informationen der Auslandsaufklärung aus einer der Kategorien führen wird, die in einer Zertifizierung aufgeführt sind. Die zielgenaue Ausrichtung der Datenerhebung erfolgt über sogenannte Selektoren, die bestimmte Kommunikationsmittel wie die E-Mail-Adresse oder die Telefonnummer der Zielperson identifizieren, jedoch niemals Stichwörter oder Namen von Personen. Die NSA muss die faktischen Grundlagen für die Auswahl des Ziels dokumentieren und nach der erstmaligen Erfassung in regelmässigen Abständen bestätigen, dass die Vorgaben für die gezielte Erfassung weiterhin erfüllt sind, andernfalls die Erfassung einzustellen ist. Die Auswahl der einzelnen Zielpersonen durch die NSA und die Dokumentation jeder aufgezeichneten Be-

[48] Vgl. Titel 50, Kapitel 36 des *United States Code* (U.S.C.).

wertung und Begründung der Erfassung werden alle zwei Monate durch die für die Überwachung der Nachrichtendienste zuständigen Abteilungen des DoJ überprüft; diese sind verpflichtet, dem FIS-Gericht und dem Kongress jeden Verstoss zu melden.

Für die anderen Rechtsgrundlagen, welche die Erhebung von Personendaten vorsehen, die an zertifizierte Organisationen in den Vereinigten Staaten übermittelt werden, gelten andere Einschränkungen und Garantien. Im Allgemeinen ist die Sammelerhebung von Daten ausdrücklich verboten, vielmehr müssen besondere Suchbegriffe verwendet werden. Um eine individuelle elektronische Überwachung durchführen zu können, müssen die Nachrichtendienste einen Antrag beim FIS-Gericht stellen, in dem sie die Tatsachen und Umstände darlegen, die die Annahme rechtfertigen, dass ein hinreichender Verdacht besteht, die Einrichtung werde von einer ausländischen Macht oder einem Vertreter einer ausländischen Macht genutzt oder eine solche Nutzung stehe unmittelbar bevor. Das FIS-Gericht beurteilt unter anderem, ob gestützt auf die vorgelegten Tatsachen ernsthafte Gründe bestehen, die diesen Verdacht stützen. Ein Gesuch an das FIS-Gericht ist auch erforderlich für eine Hausdurchsuchung oder eine Durchsuchung des Eigentums, die zur Überprüfung oder Beschlagnahme von Informationen, Material oder Vermögensgegenständen führen soll, oder für die Installation von Geräten zur Telefonüberwachung und die Nachverfolgung und Registrierung von Kommunikation.

Für die Bearbeitung von Personendaten, die von den Nachrichtendiensten der Vereinigten Staaten im Rahmen der Fernmeldeaufklärung beschafft wurden, gelten im Übrigen verschiedene Garantien. Zunächst muss jeder Nachrichtendienst eine angemessene Datensicherheit gewährleisten und den Zugriff unbefugter Personen auf solche Personendaten verhindern. Der Datenzugriff ist auf dazu befugte und geschulte Mitarbeitende zu beschränken, die diese Informationen benötigen, um ihren Auftrag erfüllen zu können. Generell müssen die Nachrichtendienste für eine angemessene Schulung ihrer Mitarbeitenden sorgen. Weiter müssen sie die Standards der Gemeinschaft der Nachrichtendienste (*Intelligence Community*) zu Genauigkeit und Objektivität einhalten, insbesondere im Hinblick auf Datenqualität und Datenzuverlässigkeit, auf die Berücksichtigung anderer Informationsquellen und auf die Objektivität bei der Durchführung von Analysen. Was die Datenaufbewahrung betrifft, gelten unabhängig von der Nationalität der betroffenen Personen dieselben Fristen. Für die Verbreitung von Personendaten, die im Rahmen der Fernmeldeaufklärung erhoben wurden, gelten besondere Regeln. So dürfen Personendaten nicht einzig aufgrund der Staatsangehörigkeit oder des Wohnsitzstaates einer Person oder zum Zweck erhoben werden, die Anforderungen der EO 14086 zu umgehen. Um die Kontrolle, ob die anwendbaren rechtlichen Vorgaben eingehalten wurden, zu erleichtern und wirksame Rechtsbehelfe zur Verfügung zu stellen, ist schliesslich jeder Nachrichtendienst verpflichtet, eine angemessene Dokumentation über die Erhebung von Fernmeldeaufklärungsdaten zu führen. Zusätzlich zu den oben genannten Garantien der EO 14086, die bei Verwendung von im Rahmen der Fernmeldeaufklärung gewonnenen Informationen gelten, unterstehen die Nachrichtendienste noch allgemeineren Anforderungen in Bezug auf die Zweckbindung, Datenminimierung, -richtigkeit, -sicherheit, -aufbewahrung und -verbreitung, wie sie insbesondere aus der Weisung 1253 des Ausschusses für nationale Sicherheitssysteme (*Committee on National Security Systems,* CNSSi) betreffend Sicherheitskategorisierung und Kontrollauswahl für nationale Sicherheitssysteme (Security Categorization and Control Selection for National Security Systems), dem Rundschreiben Nr. A-130 des Büros für Verwaltung und Budget (OMB) und anderen Regelungen hervorgehen.

4.2.2 Unabhängigkeit der Behörde, Rechtsschutz

4.2.2.1 Aufsicht

Die Tätigkeiten der Nachrichtendienste werden durch verschiedene Organe beaufsichtigt. Zunächst verlangt die EO 14086, dass jeder Nachrichtendienst über hochrangige Rechtsbeauftragte und Beauftragte für Aufsicht und Compliance verfügt, um die Einhaltung des geltenden nationalen Rechts zu gewährleisten. Diese müssen insbesondere die Tätigkeiten im Rahmen der Fernmeldeaufklärung regelmässig überwachen und dafür sorgen, dass Verstösse behoben werden. Die Nachrichtendienste müssen diesen Beauftragten Zugang zu allen einschlägigen Informationen gewähren, damit sie ihre Aufsichtsaufgaben wahrnehmen können, und dürfen keine Massnahmen treffen, welche die Aufsichtstätigkeit behindern oder unangemessen beeinflussen. Darüber hinaus muss jeder schwerwiegende Verstoss, der von einem Beauftragten für Aufsicht oder einem anderen Mitarbeitenden festgestellt wird, unverzüglich der Leitung des Nachrichtendienstes und der Direktion des nationalen Nachrichtendienstes gemeldet werden; diese müssen dafür sorgen, dass alle erforderlichen Abhilfemassnahmen getroffen werden und eine Wiederholung solcher Verstösse verhindert wird.

Wie bei den Strafverfolgungsbehörden gibt es auch bei allen Nachrichtendiensten Datenschutz- und Bürgerrechtsbeauftragte (*Privacy and Civil Liberties Officers*, CLPOs, nachstehend: CLP-Beauftragte).[49] Ihre Befugnisse umfassen in der Regel die Aufsicht über Verfahren, mit denen sichergestellt werden soll, dass die betreffende Abteilung oder der betreffende Nachrichtendienst die Belange der Privatsphäre und der bürgerlichen Freiheiten hinreichend beachtet und geeignete Vorkehrungen getroffen hat, um Beschwerden von Einzelpersonen nachzugehen, die sich in ihrer Privatsphäre oder ihren Bürgerrechten verletzt glauben. Die Leitung des Nachrichtendiensts oder der betreffenden Abteilungen muss sicherstellen, dass die CLP-Beauftragten über die für die Erfüllung ihrer Aufgaben erforderlichen Ressourcen verfügen und Zugang zu den dafür nötigen Unterlagen und zum Personal haben, und dass sie über vorgeschlagene Änderungen der Datenschutzpolitik informiert und dazu konsultiert werden. Die CLP-Beauftragten erstatten dem Kongress und der PCLO-Stelle regelmässig Bericht, mit Angaben zu Anzahl und Art der bei der Abteilung oder beim Nachrichtendienst eingegangenen Beschwerden, mit einer Zusammenfassung über die Behandlung dieser Beschwerden, der durchgeführten Überprüfungen und Untersuchungen und der Auswirkungen der von den CLP-Beauftragten geleisteten Arbeit.

Weiter verfügt jeder Nachrichtendienst über einen unabhängigen Generalinspektor oder eine unabhängige Generalinspektorin, die unter anderem für die Aufsicht über die Auslandsaufklärung zuständig sind. Dem Büro der Direktorin des Nationalen Nachrichtendienstes (ODNI) ist ein Büro des Generalinspektors der Gemeinschaft der Nachrichtendienste (*Intelligence Community*) angegliedert, mit umfassenden Zuständigkeiten für die gesamte Gemeinschaft. Die Generalinspektorinnen und -inspektoren sind unabhängig und führen Audits und Untersuchungen der Programme und Aktivitäten des jeweiligen Nachrichtendienstes durch, unter anderem auch in Missbrauchsfällen oder bei Rechtsverletzungen. Sie haben Zugriff auf alle Archive, Berichte, Audits, Überprüfungen, Dokumente, Empfehlungen oder sonstiges einschlägiges Material, dessen Herausgabe sie nötigenfalls durch Verfügung anordnen können, und sie können Zeugenaussagen abnehmen. Fälle mutmasslicher Straftaten leiten sie

[49] Vgl. Titel 42 des *United States Code* (U.S.C.).

an die Strafverfolgungsbehörden weiter und geben der Leitung der Nachrichtendienste Empfehlungen für Abhilfemassnahmen ab. Solche Empfehlungen sind zwar nicht verbindlich, doch werden die Berichte, auch solche über die getroffenen (oder unterlassenen) Folgemassnahmen, regelmässig veröffentlicht und dem Kongress übermittelt, der auf dieser Grundlage seine eigene Kontrollfunktion wahrnehmen kann.

Ferner überwacht das Aufsichtsgremium der Nachrichtendienste (*Intelligence Oversight Board*, IOB [nachstehend IO-Gremium]), das im Beratungsgremium des Präsidenten für Nachrichtendienste (*President's Intelligence Advisory Board*, PIAB [nachstehend PIA-Gremium]) eingerichtet wurde, die Einhaltung der Verfassung und aller einschlägigen Vorschriften durch die Nachrichtendienste. Das PIA-Gremium besteht aus 16 Mitgliedern, die vom Präsidenten ernannt werden und nicht der Regierung der Vereinigten Staaten angehören dürfen. Das IO-Gremium besteht aus maximal fünf Mitgliedern, die vom Präsidenten aus den Reihen der Mitglieder des PIA-Gremiums ernannt werden. Nach der EO 12333 sind die Leiterinnen und Leiter aller Nachrichtendienste verpflichtet, dem IO-Gremium jede nachrichtendienstliche Tätigkeit zu melden, bei der Grund zur Annahme besteht, dass sie rechtswidrig sein oder eine Durchführungsverordnung (*Executive Order*) oder eine Präsidialrichtlinie (*Presidential Directive*) verletzen könnte. Das IO-Gremium ist seinerseits verpflichtet, den Präsidenten über nachrichtendienstliche Tätigkeiten zu informieren, die seiner Ansicht nach nationales Recht (namentlich Dekrete) verletzen und die vom Generalstaatsanwalt, der Direktorin des Nationalen Nachrichtendienstes oder der Leitung eines Nachrichtendienstes nicht angemessen behandelt werden. Darüber hinaus ist das IO-Gremium verpflichtet, den Generalstaatsanwalt über mögliche strafrechtlich relevante Verstösse zu informieren.

Ausserdem unterstehen die Nachrichtendienste der Aufsicht der PCLO-Stelle. Nach seinem Gründungsstatut ist diese Stelle mit Aufgaben im Bereich der Terrorismusbekämpfung und deren Umsetzung im Einklang mit dem Schutz der Privatsphäre und der bürgerlichen Freiheiten betraut. Bei der Überprüfung der Tätigkeit der Nachrichtendienste hat sie Zugriff auf sämtliche einschlägige Archive, Berichte, Audits, Analysen, Unterlagen, Schriftstücke und Empfehlungen, einschliesslich der Geheimhaltung unterliegende Informationen, und sie kann Zeugenaussagen abnehmen. Die Stelle kann Empfehlungen an die Behörden abgeben und erstattet den Ausschüssen des Kongresses und dem Präsidenten regelmässig Bericht. Die Berichte der PCLO-Stelle, einschliesslich der Berichte an den Kongress, müssen so weit wie möglich veröffentlicht werden. Die PCLO-Stelle übt auch spezifische Überwachungsfunktionen aus, soweit es um die Umsetzung der EO 14086 geht; hier prüft sie insbesondere, ob die Verfahren der Nachrichtendienste mit der EO vereinbar sind, und evaluiert, ob der Beschwerdemechanismus korrekt funktioniert (s. Ziff. 4.2.2.2).

Zusätzlich zu diesen Kontrollmechanismen der Exekutive nehmen spezielle Ausschüsse des Kongresses (Ausschüsse des Repräsentantenhauses und des Senats für Nachrichtendienste und Justiz [*House and Senate Intelligence and Judiciary Committees*]) Aufsichtsaufgaben über alle Formen der Auslandsaufklärung wahr. Die Mitglieder dieser Ausschüsse haben Zugriff auf Informationen, die der Geheimhaltung unterliegen, sowie auf nachrichtendienstliche Methoden und Programme. Die Ausschüsse üben ihre Aufsicht auf verschiedene Weise aus, insbesondere durch Anhörungen, Untersuchungen, Überprüfungen und Berichte. Die Ausschüsse des Kongresses erhalten regelmässig Berichte über nachrichtendienstliche Tätigkeiten, u.a. vom Generalstaatsanwalt, von der Direktorin des Nationalen Nachrichtendienstes, den Nachrichtendiensten und anderen Aufsichtsgremien (z.B. den Generalinspektorinnen und Generalinspektoren).

Generell unternimmt die Gemeinschaft der Nachrichtendienste (*Intelligence Community*) verschiedene Anstrengungen, um Transparenz in Bezug auf ihre Aufklärungsaktivitäten zu gewährleisten. So hat das ODNI im Jahr 2015 Grundsätze für die Transparenz der Nachrichtendienste und einen entsprechenden Umsetzungsplan verabschiedet.[50] In diesem Zusammenhang hat die *Intelligence Community* freigegebene Teile von Strategien, Verfahren, Aufsichtsberichten, etc. veröffentlicht und wird dies auch weiterhin tun.

Schliesslich unterliegt die Beschaffung von Personendaten gestützt auf das FIS-Gesetz auch der Aufsicht durch das FIS-Gericht. Dieses Gericht kann bei Bedarf den betreffenden Nachrichtendienst anweisen, Abhilfemassnahmen zu treffen. Die Massnahmen können individueller oder struktureller Natur sein und beispielsweise von der Einstellung der Datenerhebung über die Änderung der Erhebungspraxis bis hin zur Löschung rechtswidrig beschaffter Daten reichen. Darüber hinaus prüft das FIS-Gericht im Rahmen seiner jährlichen Kontrolle der Zertifizierungen, ob die vorgelegten Zertifizierungen den Anforderungen des FIS-Gesetzes entsprechen. Sind die von der Regierung beantragten Zertifizierungen nach FIS-Gesetz Abschnitt 702 unzureichend, insbesondere aufgrund gewisser Verstösse, kann es eine Mängelverfügung (*Deficiency Order*) erlassen, mit der die Regierung aufgefordert wird, den Mangel innerhalb von 30 Tagen zu beheben, oder von der Zertifizierung abzusehen bzw. diese nicht umzusetzen. Das FIS-Gericht evaluiert die festgestellten Mängel und kann Verfahrensänderungen oder zusätzliche Überwachung und Berichterstattung verlangen, um die Probleme zu lösen.

4.2.2.2 Rechtsschutz

Das amerikanische Recht kennt verschiedene Möglichkeiten, Klage vor einem unabhängigen und unparteiischen Gericht zu erheben. Auf diesem Weg können die betroffenen Personen Zugang zu ihren Personendaten erhalten, die Rechtmässigkeit des staatlichen Zugriffs auf ihre Daten überprüfen lassen und im Fall einer Verletzung Abhilfe erwirken, insbesondere dadurch, dass ihre Personendaten berichtigt oder gelöscht werden.

Die EO 14086 sieht einen besonderen Beschwerdemechanismus vor, ergänzt durch die Vorschrift des Generalstaatsanwalts der Vereinigten Staaten über das Gericht zur Datenschutzüberprüfung *(Data Protection Review Court*, DPRC, nachstehend DPR-Gericht) vom 7. Oktober 2022, in dem Beschwerden von betroffenen Personen im Zusammenhang mit der Fernmeldeaufklärung der Vereinigten Staaten bearbeitet und erledigt werden. Jede betroffene Person in der Schweiz hat das Recht, bei der Beschwerdestelle eine Beschwerde wegen mutmasslicher Verletzung des amerikanischen Rechts im Bereich der Funkaufklärung einzureichen, die ihre Privatsphäre oder ihre bürgerlichen Freiheiten beeinträchtigt. Diese Beschwerdemöglichkeit steht Personen aus den vom Generalstaatsanwalt bezeichneten Ländern oder Organisationen der regionalen Wirtschaftsintegration offen. Am 7. Juni 2024 wurde die Schweiz als zum Beschwerdemechanismus zugelassener Staat benannt.[51]

Eine in der Schweiz betroffene Person, die eine solche Beschwerde einlegen will, muss sie zunächst dem EDÖB als für den Datenschutz in der Schweiz zuständige, unabhängige und

---

[50] Vgl. The Principles of Intelligence Transparency for the IC (dni.gov).

[51] Vgl. die am Schluss des vorliegenden Dokuments aufgeführten Internetadressen zu den Referenztexten.

für die Übermittlung von Beschwerden im Rahmen des Rechtsbehelfsverfahrens geeignete Behörde unterbreiten. Dieses Vorgehen ermöglicht es den betroffenen Personen, sich an eine Behörde zu wenden, mit der sie in ihrer Sprache verkehren können. Um der Beschwerdestelle den Einstieg in die Prüfung zu ermöglichen, sind ihr Nachweise zu liefern, dass die Beschwerde eine natürliche Person betrifft, sowie gewisse Basisinformationen zu den Personendaten (wie E-Mailadresse oder Telefonnummer), welche mutmasslich an die Vereinigten Staaten übermittelt wurden. Weitere nötige Informationen umfassen die Mittel, mit denen die Daten mutmasslich übermittelt wurden, die Identität (soweit bekannt) der Regierungsstellen der Vereinigten Staaten, die verdächtigt werden, an der behaupteten Verletzung beteiligt gewesen zu sein, und die Art der beantragten Abhilfemassnahmen (z.B. Löschung der betreffenden Daten). Nicht erforderlich ist dagegen der Nachweis, dass Nachrichtendienste tatsächlich Personendaten beschafft haben, oder dass solche Daten Gegenstand einer Fernmeldeaufklärung waren. Der EDÖB nimmt die Beschwerde entgegen und prüft lediglich die Identität der natürlichen Person und ob alle Basisinformationen geliefert wurden. Ist das der Fall, übermittelt er die Beschwerde an die Beschwerdestelle in den Vereinigten Staaten.

Die Prüfung der Beschwerde obliegt zunächst dem CLP-Beauftragten (*Privacy and Civil Liberties Officer)* des ODNI (*Office of the Director of National Intelligence*) (nachstehend ODNI-CLPO), dessen Rolle und Befugnisse mit Blick auf die spezifischen, in der EO 14086 vorgesehenen Massnahmen erweitert wurden. Dazu enthält die vom ODNI erlassene Richtlinie 126 der Gemeinschaft der Nachrichtendienste[52] genauere Angaben zu den Verfahren, die bei der Umsetzung des Beschwerdemechanismus nach der EO 14086 zu beachten sind. Innerhalb der Gemeinschaft der Nachrichtendienste hat der ODNI-CLPO u.a. dafür zu sorgen, dass der Schutz der Privatsphäre und der bürgerlichen Freiheiten angemessen in die Strategien und Verfahren des ODNI und der Nachrichtendienste integriert wird und das ODNI die geltenden Anforderungen zum Schutz der Privatsphäre und der bürgerlichen Freiheiten erfüllt; ausserdem analysiert er die Auswirkungen auf die Privatsphäre. Der ODNI-CLPO kann nur aus wichtigen Gründen durch die Direktorin des Nationalen Nachrichtendienstes seines Amtes enthoben werden, d.h. wegen Fehlverhaltens, Begehung einer Straftat, Verletzung von Sicherheitsvorschriften, Pflichtversäumnis oder Unfähigkeit. Bei seiner Prüfung hat der ODNI-CLPO Zugang zu den Informationen, die für seine Beurteilung erforderlich sind, und er kann auf die (obligatorische) Unterstützung der CLP-Beauftragten der verschiedenen Nachrichtendienste zählen. Den Nachrichtendiensten ist es verboten, die Prüfung zu behindern oder ungebührlich zu beeinflussen. Das gilt auch für die Direktion des Nationalen Nachrichtendienstes, die nicht in die Prüfung eingreifen darf. Bei seiner Prüfung muss der ODNI-CLPO das Recht unparteiisch anwenden und sowohl die nationalen Sicherheitsinteressen in Bezug auf die nachrichtendienstlichen Aktivitäten als auch den Schutz der Privatsphäre berücksichtigen. Im Rahmen seiner Prüfung ermittelt der ODNI-CLPO, ob geltendes amerikanisches Recht verletzt wurde, und entscheidet gegebenenfalls über geeignete Abhilfemassnahmen. Dabei geht es um Massnahmen, mit denen eine nachgewiesene Verletzung vollständig behoben wird, z.B. die Einstellung der unrechtmässigen Datenerhebung, die Löschung unrechtmässig erhobener Daten, die Löschung der Ergebnisse unrechtmässig durchgeführter Abfragen von an sich rechtmässig erhobenen Daten, die Beschränkung des Zugriffs auf rechtmässig erhobene Daten auf angemessen geschulte Mitarbeitende oder die Rücknahme nachrichten-

[52] Vgl. die am Schluss des vorliegenden Dokuments aufgeführten Internetadressen zu den Referenztexten.

dienstlicher Berichte, die unrechtmässig erhobene oder verbreitete Daten enthalten. Die Entscheidungen des ODNI-CLPO über individuelle Beschwerden, einschliesslich der verfügten Abhilfemassnahmen, sind für die betroffenen Nachrichtendienste verbindlich, sofern nicht das DPR-Gericht, auf welches weiter unten eingegangen wird, nachträglich eine gegenteilige Entscheidung erlässt. Der ODNI-CLPO muss seine Prüfung dokumentieren und eine als vertraulich eingestufte Entscheidung vorlegen, in der er die Grundlage für seine Sachverhaltsfeststellungen, den Nachweis einer einschlägigen Rechtsverletzung und geeignete Abhilfemassnahmen erläutert. Ergibt die Prüfung, dass die Verletzung von einer Behörde begangen wurde, die unter der Aufsicht des FIS-Gerichts steht, muss der ODNI-CLPO ebenfalls einen vertraulichen Bericht an den Assistenz-Generalstaatsanwalt für nationale Sicherheit (*Assistant Attorney General for National Security*) abgeben, der seinerseits die Verletzung dem FIS-Gericht zu melden hat, das weitere Massnahmen ergreifen kann.

Nach Abschluss der Prüfung teilt der ODNI-CLPO der beschwerdeführenden Person über den EDÖB in einer standardisierten Antwort mit, dass die Prüfung keine einschlägigen Verletzungen ergeben hat, oder aber, dass er eine Entscheidung getroffen hat, die angemessene Abhilfemassnahmen erfordert. Mit diesem Vorgehen kann die Vertraulichkeit der Tätigkeiten im Interesse der nationalen Sicherheit gewahrt werden, und gleichzeitig der betroffenen Person eine Entscheidung eröffnet werden, die bestätigt, dass ihre Beschwerde ordnungsgemäss geprüft und beurteilt wurde. Diese Entscheidung ist anfechtbar. Zu diesem Zweck wird die betroffene Person über die Möglichkeit belehrt, das DPR-Gericht anzurufen und eine Überprüfung der Entscheidungen des ODNI-CLPO zu beantragen, sowie darüber, dass im Fall einer Beschwerde an das DPR-Gericht ein besonderer Anwalt oder eine besondere Anwältin bestellt wird, der oder die ihre Interessen vertritt und sicherstellt, dass das DPR-Gericht gut über den Sachverhalt und die Rechtslage in Bezug auf die Angelegenheit informiert ist.

Jede beschwerdeführende Person und jedes Mitglied der Gemeinschaft der Nachrichtendienste kann beim DPR-Gericht eine Überprüfung der Entscheidung des ODNI-CLPO beantragen. Beantragt ein Mitglied der Gemeinschaft der Nachrichtendienste eine Überprüfung, wird ebenfalls ein besonderer Anwalt oder eine besondere Anwältin ernannt, welcher oder welche die Interessen der beschwerdeführenden Person vertritt und sicherstellt, dass das DPR-Gericht gut über den Sachverhalt und die Rechtslage in Bezug auf die Angelegenheit informiert ist. Der Antrag muss innert 60 Tagen nach Erhalt der Mitteilung des ODNI-CLPO, dass die Überprüfung abgeschlossen ist, gestellt werden und alle Informationen enthalten, die die betroffene Person dem DPR-Gericht unterbreiten möchte, wie beispielsweise Argumente zu Rechtsfragen. Betroffene Personen in der Schweiz müssen ihr Gesuch wiederum über den EDÖB stellen, der den Überprüfungsantrag dann an das DPR-Gericht weiterleitet.

Das DPR-Gericht ist ein unabhängiges Rechtsprechungsorgan, eingesetzt durch den Generalstaatsanwalt gestützt auf die EO 14086. Es besteht aus mindestens sechs Richterinnen und Richtern, die vom Generalstaatsanwalt in Absprache mit der PCLO-Stelle, der Handelsministerin und der Direktorin des Nationalen Nachrichtendienstes für eine (erneuerbare) Amtszeit von vier Jahren ernannt werden. Die Ernennung erfolgt nach den Kriterien, welche die Exekutive bei der Beurteilung von Bewerbungen für das Amt einer Bundesrichterin oder eines Bundesrichters anwendet, unter Berücksichtigung der richterlichen Vorerfahrungen. Darüber hinaus müssen die Richterinnen und Richter aus der Rechtspraxis kommen (d.h. aktive Mitglieder der Anwaltskammer und zur Ausübung des Anwaltsberufs zugelassen sein) und über ausreichende Erfahrung in den Bereichen des Schutzes der Privatsphäre und der nationalen Sicherheit verfügen. Der Generalstaatsanwalt muss sicherstellen, dass mindestens die Hälfte der Richterinnen und Richter über richterliche Erfahrung verfügt, und dass alle

eine Zugangsberechtigung zu vertraulichen Informationen über die nationale Sicherheit haben. Ausserdem dürfen sie im Moment ihrer Ernennung und auch noch zwei Jahre davor nicht in der Exekutive beschäftigt gewesen sein. Ausser ihrer Funktion als Mitglieder des DPR-Gerichts dürfen sie während ihrer Amtszeit kein anderes offizielles Amt und keine andere offizielle Anstellung in der Regierung der Vereinigten Staaten innehaben. Die Unabhängigkeit in der Urteilsfindung wird durch verschiedene Garantien sichergestellt. Insbesondere darf die Exekutive (der Generalstaatsanwalt und die Nachrichtendienste) die gerichtliche Prüfung nicht behindern oder ungebührlich beeinflussen. Das DPR-Gericht selbst ist zu einer unparteiischen Rechtsprechung verpflichtet und arbeitet nach seinem eigenen, durch Mehrheit verabschiedeten Reglement. Eine Abberufung der Richterinnen und Richter ist nur durch den Generalstaatsanwalt und nur aus wichtigen Gründen möglich (Fehlverhalten, Begehen einer Straftat, Verletzung von Sicherheitsvorschriften, Pflichtversäumnis oder Unfähigkeit), und unter gebührender Berücksichtigung der für Bundesrichterinnen und Bundesrichter geltenden Standards, die in den Regeln über die richterliche Ethik und über die Unfähigkeit von Richterinnen und Richtern (*Rules for Judicial-Conduct and Judicial-Disability Proceedings*) festgelegt sind.[53]

Die Beschwerden an das DPR-Gericht werden von einem Panel aus drei Gerichtsmitgliedern, von denen eines den Vorsitz führt, geprüft, die nach dem Verhaltenskodex für Richter der Vereinigten Staaten (*Code of Conduct for U.S. Judges*) vorgehen müssen. Jedes Panel wird durch einen Spezialanwalt (*Special Advocate*) unterstützt, der Zugang zu allen den Fall betreffenden Informationen hat, einschliesslich solcher von vertraulicher Natur. Der Spezialanwalt stellt sicher, dass die Interessen der beschwerdeführenden Person vertreten werden und dass das Panel über alle relevanten Rechts- und Sachverhaltsfragen informiert ist. Sofern die beschwerdeführende Person einen Überprüfungsantrag stellt, kann der Spezialanwalt sie schriftlich um Informationen ersuchen, um seinen Standpunkt zum Überprüfungsantrag an das DPR-Gericht zu vertiefen. Das DPR-Gericht prüft die Entscheidungen des ODNI-CLPO sowohl hinsichtlich der Frage, ob geltendes amerikanisches Recht verletzt wurde, als auch hinsichtlich der Frage, welche Abhilfemassnahmen angemessen sind. Es stützt sich dabei mindestens auf die Untersuchungsakten des ODNI-CLPO und auf alle von der beschwerdeführenden Person, dem Spezialanwalt oder einem Nachrichtendienst vorgelegten Informationen und Stellungnahmen. Ein Panel des DPR-Gerichts hat Zugang zu allen für die Prüfung erforderlichen Informationen, die es über den ODNI-CLPO beschaffen kann.

Nach Abschluss seiner Prüfung kann das DPR-Gericht entscheiden, dass es keine Beweise für eine Fernmeldeaufklärung gibt, bei der Personendaten der beschwerdeführenden Person betroffen waren, dass die Feststellungen des ODNI-CLPO rechtlich korrekt und durch stichhaltige Beweise belegt sind, oder aber seine eigenen Entscheidungen treffen, wenn es mit denen des ODNI-CLPO nicht einverstanden ist. Trifft das DPR-Gericht eine Entscheidung, welche von jener des ODNI-CLPO abweicht, hat die Entscheidung des Gerichts Vorrang und ist für den ODNI-CLPO und die Nachrichtendienste verbindlich.

[53] Vgl. EO 14086 und Richtlinien des Generalstaatsanwalts, sowie die Webseite des DPR-Gerichts, auf der die amtierenden Richter und ihr Werdegang aufgeführt sind: https://www.justice.gov/opcl/redress-data-protection-review-court.

In allen Fällen trifft das DPR-Gericht eine schriftliche Entscheidung mit der Mehrheit der Stimmen. Ergibt die Prüfung eine Verletzung geltender Vorschriften, bestimmt es in seiner Entscheidung angemessene Abhilfemassnahmen, z.B. die Löschung unrechtmässig erhobener Daten, die Löschung der Ergebnisse unrechtmässiger Abfragen, die Beschränkung des Zugriffs auf rechtmässig erhobene Daten auf angemessen geschulte Mitarbeitende oder die Rücknahme von nachrichtendienstlichen Berichten, die unrechtmässig erhobene Daten enthalten oder auf rechtswidrige Weise verbreitet wurden. Die Entscheidung des DPR-Gerichts ist bezüglich der Beschwerde, die sie betrifft, verbindlich und endgültig. Ergibt die Prüfung, dass die Verletzung von einer Behörde begangen wurde, die unter der Aufsicht des FIS-Gerichts steht, muss der ODNI-CLPO auch einen vertraulichen Bericht an den Assistenz-Generalstaatsanwalt für nationale Sicherheit abgeben, der seinerseits die Verletzung an das FIS-Gericht meldet; dieses kann weitere Massnahmen ergreifen. Jede Entscheidung eines Panels des DPR-Gerichts wird dem ODNI-CLPO übermittelt. Wurde die gerichtliche Prüfung durch einen Antrag der beschwerdeführenden Person ausgelöst, wird diese über den EDÖB in einer standardisierten Antwort benachrichtigt, dass das DPR-Gericht das Verfahren abgeschlossen und die Prüfung keine einschlägigen Verletzungen ergeben hat, oder aber entschieden hat, dass angemessene Abhilfemassnahmen erforderlich sind. Das Büro für den Schutz der Privatsphäre und bürgerliche Freiheiten des Justizministeriums (*Office of Privacy and Civil Liberties of the DoJ*) archiviert alle vom DPR-Gericht geprüften Informationen und Entscheidungen, die künftigen Panels des Gerichts als unverbindliche Präjudizien zur Verfügung gestellt werden. Auch das Handelsministerium (DoC) führt ein Archiv mit allen Beschwerdeführerinnen und Beschwerdeführern, die eine Beschwerde eingereicht haben. Um die Transparenz zu erhöhen, muss das DoC mindestens alle fünf Jahre die zuständigen Nachrichtendienste kontaktieren, um sich zu vergewissern, dass die vom ODNI-CLPO oder vom DPR-Gericht geprüften Informationen freigegeben wurden. Ist dies der Fall, wird die betroffene Person über die zuständige Behörde informiert, dass die Informationen im Rahmen des geltenden Rechts zugänglich sind.

Schliesslich wird das ordnungsgemässe Funktionieren dieses Beschwerdemechanismus regelmässig und unabhängig evaluiert, und zwar durch eine jährliche Untersuchung durch die unabhängige PCLO-Stelle.[54] Diese prüft unter anderem, ob der ODNI-CLPO und das DPR-Gericht Beschwerden fristgerecht behandelt haben, ob sie vollständigen Zugang zu den erforderlichen Informationen hatten, ob im Verfahren die grundlegenden Garantien der EO 14086 korrekt berücksichtigt wurden und ob die Gemeinschaft der Nachrichtendienste die Entscheidungen des ODNI-CLPO und des DPR-Gerichts vollständig umgesetzt hat. Die PCLO-Stelle legt dem Präsidenten der Vereinigten Staaten, dem Generalstaatsanwalt, der Direktorin des Nationalen Nachrichtendienstes, den Leitungen der Nachrichtendienste, dem ODNI-CLPO und den Nachrichtendienstausschüssen des Kongresses einen Bericht über die Ergebnisse seiner Untersuchung vor; der Bericht wird in einer nicht vertraulichen Fassung auch veröffentlicht. Der Generalstaatsanwalt, die Direktorin des Nationalen Nachrichtendienstes, der ODNI-CLPO und die Leitungen der Nachrichtendienste sind verpflichtet, alle in diesen Berichten enthaltenen Empfehlungen umzusetzen oder ihnen in anderer Weise Folge zu geben. Darüber hinaus stellt die PCLO-Stelle jährlich eine öffentliche Bescheinigung aus, wonach die

[54] EO 14086 empfiehlt der PCLO-Stelle eine jährliche Überprüfung der Funktionsweise des Rechtsbehelfsmechanismus. Die PCLO-Stelle hat sich bereit erklärt, diese Überprüfungen vorzunehmen (vgl. Oversight Projects - PCLOB).

Beschwerden im Rahmen des Beschwerdemechanismus den Anforderungen der EO 14086 gemäss behandelt werden.

Neben dem spezifischen Beschwerdemechanismus nach der EO 14086 stehen den betroffenen Personen unabhängig von ihrer Nationalität und ihrem Wohnsitz auch Rechtsmittel vor den ordentlichen Gerichten der Vereinigten Staaten zur Verfügung. Insbesondere bieten das FIS-Gesetz und ein damit zusammenhängender Erlass betroffenen Personen folgende Möglichkeiten: Zivilklage gegen die Vereinigten Staaten auf Schadenersatz, wenn sie betreffende Informationen rechtswidrig und vorsätzlich verwendet oder offengelegt wurden; Schadenersatzklage gegen Regierungsbeamtinnen und -beamte der Vereinigten Staaten, die als Privatpersonen handeln; Anfechtung der Rechtmässigkeit der Überwachung, falls die Regierung beabsichtigt, aus der elektronischen Überwachung gewonnene Erkenntnisse in einem Gerichts- oder Verwaltungsverfahren in den Vereinigten Staaten gegen die betroffene Person zu verwenden oder offenzulegen. Eine allgemeinere Rekursmöglichkeit bietet das Verwaltungsverfahrensgesetz (*Administrative Procedure Act*). Danach kann jede Person, die durch Handlungen einer Behörde einen Schaden oder Nachteil erleidet, Beschwerde vor Gericht erheben.

Gestützt auf die Gesetzgebung über die Öffentlichkeit der Verwaltung[55] hat jede Person das Recht, Zugang zu Informationen von Bundesbehörden zu verlangen, auch solchen, die Personendaten enthalten. Dieser Zugang kann auch die Einleitung von Verfahren vor den ordentlichen Gerichten erleichtern, insbesondere mit Blick auf den Nachweis der Klagelegitimation. Die Behörden können Informationen zurückhalten, wenn gewisse, einzeln aufgezählte Ausnahmen vorliegen, darunter Informationen, die aus Gründen der nationalen Sicherheit der Geheimhaltung unterliegen, und Informationen über Ermittlungen der Strafverfolgungsbehörden. Betroffene, die mit einem abschlägigen Bescheid nicht einverstanden sind, können diesen anfechten, indem sie eine verwaltungsinterne und anschliessend eine gerichtliche Überprüfung vor den Bundesgerichten verlangen.

5 Andere Kriterien

5.1 Internationale Verpflichtungen

Den internationalen Verpflichtungen ist Rechnung zu tragen. Dabei sind nicht nur die Verpflichtungen im Bereich des Datenschutzes relevant, auch andere Verpflichtungen können in Betracht fallen, beispielsweise Übereinkommen zum Informationsaustausch.

Die Vereinigten Staaten sind Vertragspartei verschiedener internationaler Regelwerke, die Verpflichtungen zum Schutz der Privatsphäre und zum Schutz der Menschenrechte allgemein begründen.

Als Mitglied der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) beteiligen sich die Vereinigten Staaten an den Arbeiten zum Thema Data Governance und Schutz der Privatsphäre. Sie haben sich verpflichtet, den OECD-Rahmen für den Schutz der

[55] Vgl. Titel 5 des *United States Code* (U.S.C.).

Privatsphäre einzuhalten, insbesondere die OECD-Leitsätze zum Schutz der Privatsphäre[56]. Ausserdem haben sich die Vereinigten Staaten aktiv an der Ausarbeitung der Erklärung[57] beteiligt, die den Behördenzugriff auf Personendaten bei privaten Unternehmen regelt.

Die Vereinigten Staaten sind dem Übereinkommen des Europarats über die Cyberkriminalität (Budapest-Konvention)[58] beigetreten.

Sie sind weiter Mitglied der Asiatisch-Pazifischen Wirtschaftsgemeinschaft (APEC) und Partei des APEC-Datenschutzrahmens (*APEC Privacy Framework*)[59].

Überdies ist die FT-Kommission akkreditiertes Mitglied der Internationalen Konferenz der Datenschutzbeauftragten (*Global Privacy Assembly*)[60], während die PCLO-Stelle und der oder die Delegierte für Datenschutz und bürgerliche Freiheiten des Justizministeriums Beobachterstatus haben.

Auch bilaterale oder multilaterale Freihandelsabkommen oder Abkommen über den digitalen Handel können relevant sein, wenn sie Klauseln zum Schutz von Personendaten und zum grenzüberschreitenden Datenfluss enthalten. In diesem Zusammenhang können namentlich das Freihandelsabkommen zwischen den Vereinigten Staaten, Mexiko und Kanada sowie dasjenige zwischen den Vereinigten Staaten und Japan erwähnt werden.[61] Ausserdem beteiligen sich die Vereinigten Staaten ebenfalls an den Verhandlungen zu einem Abkommen über den digitalen Handel, die zurzeit auf eine gemeinsame Initiative von WTO-Mitgliedern geführt werden.[62]

5.2 Rechtsstaat

Die Vereinigten Staaten sind eine föderale Republik, bestehend aus 50 Bundesstaaten, zu denen noch verschiedene Aussengebiete hinzukommen. Regierungsform ist die Demokratie.

Die Aussenpolitik, das Militär, die Nachrichtendienste und der Aussenhandel sind Sache des Bundes. Die 50 Bundesstaaten sind in vielen anderen Bereichen zuständig, darunter Justiz, Bildung, usw.

---

[56] Abrufbar unter: OECD Legal Instruments.

[57] Abrufbar unter: OECD Legal Instruments.

[58] Abrufbar unter: STCE 185 - Convention sur la cybercriminalité (coe.int); SR 0.311.43.

[59] Abrufbar unter: APEC Privacy Framework.

[60] Vgl. Global Privacy Assembly.

[61] Vgl. Digital Trade & E-Commerce FTA Chapters | United States Trade Representative (ustr.gov).

[62] Vgl. WTO | Joint Initiative on E-Commerce.

Die Verfassung der Vereinigten Staaten stammt aus dem Jahr 1787 und ist damit die älteste noch geltende moderne Verfassung. Sie schreibt den Grundsatz der Gewaltenteilung fest: Die Legislative wird vom Kongress ausgeübt, der aus zwei Kammern besteht, dem Senat und dem Repräsentantenhaus; der Präsident und die Vizepräsidentin der Vereinigten Staaten leiten die Exekutive; der Oberste Gerichtshof ist das höchste Gericht der Vereinigten Staaten und behandelt als höchstes Berufungsgericht die Fälle der unteren Bundesgerichte sowie Fälle, die Fragen des Bundesrechts oder der Auslegung der Verfassung betreffen. Die Unabhängigkeit der Justiz ist verfassungsrechtlich verankert.

5.3 Menschenrechte

Was das Kriterium der Achtung der Menschenrechte betrifft, so muss dieses im Zusammenhang mit dem gesamten Rechtsrahmen eines Staates gesehen werden, insbesondere wenn es um den Schutz vor unverhältnismässigen Eingriffen in die Privatsphäre geht.

Die Verfassung der Vereinigten Staaten führt gewisse Grundrechte auf, welche die Behörden des Bundes und der Bundesstaaten nicht verletzen dürfen und von den Gerichten durchgesetzt werden. Diese Rechte spiegeln zum Teil die Menschenrechte wider, die in der Allgemeinen Erklärung der Menschenrechte[63] enthalten sind. Das gilt namentlich für die Meinungsfreiheit, die Glaubensfreiheit, die Versammlungsfreiheit, die Rechtsgleichheit und die Verfahrensgarantien.

Darüber hinaus hat sich der Oberste Gerichtshof in einer Reihe von Urteilen mit dem Schutz der Privatsphäre befasst, insbesondere im Zusammenhang mit dem Vierten Verfassungszusatz, der ein Recht auf Schutz vor unangemessenen Durchsuchungen und Beschlagnahmungen durch die Regierung vorsieht.[64]

6 Schlussfolgerung

Die vorstehenden Ausführungen zeigen, dass für den Zugriff der Strafverfolgungsbehörden oder der nationalen Sicherheitsbehörden der Vereinigten Staaten auf Personendaten, die von der Schweiz an zertifizierte Organisationen übermittelt wurden, ein rechtlicher Rahmen besteht. Der Rahmen umschreibt die Bedingungen, unter denen der Zugriff erfolgen kann, und stellt sicher, dass der Zugriff und die Weiterverwendung der Personendaten auf das beschränkt werden, was im öffentlichen Interesse erforderlich und verhältnismässig ist. Diese Garantien können von den betroffenen Personen auf dem zur Verfügung stehenden Rechtsweg geltend gemacht werden und sind somit wirksam.

Das Bundesamt für Justiz kommt deshalb gestützt auf die vorstehende Prüfung zum Schluss, dass die Vereinigten Staaten ein angemessenes Schutzniveau für Personendaten gewährleisten, die ein Verantwortlicher oder ein Auftragsbearbeiter in der Schweiz im Rahmen des *Swiss-U.S. DPF* an zertifizierte Organisationen in den Vereinigten Staaten übermittelt.

---

[63] Abrufbar unter: Allgemeine Erklärung der Menschenrechte.

[64] Vgl. *Griswold v. Connecticut, 381 US 479 (1965),* abrufbar unter*:* Griswold v. Connecticut, 381 U.S. 479 (1965), Justia US Supreme Court Center.

Entscheidet der Bundesrat gestützt auf die vorliegende Beurteilung im positiven Sinn, können zwischen Verantwortlichen und Auftragsbearbeitern in der Schweiz und zertifizierten Organisationen in den Vereinigten Staaten Personendaten übermittelt werden, ohne dass zusätzliche Garantien eingeholt werden müssten (vgl. Art. 16 Abs. 1 DSG).

Internetadressen der Referenztexte:

- Grundsätze, einschliesslich Zusatzgrundsätze, des für zertifizierte Organisationen in den Vereinigten Staaten geltenden kommerziellen Rahmens zwischen der Schweiz und den Vereinigten Staaten über den Datenschutz; Schreiben der folgenden Behörden, welche die eingegangenen Verpflichtungen bestätigen: Justizministerium (DoJ), Handelsministerium (*Secretary of Commerce*) (DoC), Internationale Handelsadministration (*International Trade Administration*, ITA), Bundeshandelskommission (*Federal Trade Commission*, FTC) und Verkehrsministerium (*Department of Transport*, DoT) sowie Schreiben des Büros der Direktorin des Nationalen Nachrichtendienstes (ODNI) im DoC: https://www.dataprivacyframework.gov/s/framework-text?tabset-c1491=3
- Durchführungsverordnung 14086 vom 7. Oktober 2022: https://www.state.gov/executive-order-14086-policy-and-procedures
- Vorschrift über das Gericht zur Datenschutzüberprüfung des Generalstaatsanwalts der Vereinigten Staaten (*U.S. Attorney General*), publiziert am 7. Oktober 2022: https://www.federalregister.gov/documents/2022/10/14/2022-22234/data-protection-review-court
- Richtlinie 126 der Gemeinschaft der Nachrichtendienste, erstellt am 6. Dezember 2022 durch das ODNI: https://www.dni.gov/files/documents/ICD/ICD_126-Implementation-Procedures-for-SIGINT-Redress-Mechanism.pdf
- Ernennung der Schweiz am 7. Juni 2024 als Staat, der vom zweistufigen Beschwerdemechanismus einschliesslich des Zugangs zum Gericht zur Datenschutzüberprüfung profitiert: https://www.justice.gov/opcl/media/1355326/dl?inline, siehe auch: https://www.justice.gov/opcl/executive-order-14086