EUROPÄISCHE
KOMMISSION

Brüssel, den 9.10.2024
COM(2024) 451 final

BERICHT DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT

über die erste regelmäßige Überprüfung der Funktionsweise des Angemessenheitsbeschlusses zum Datenschutzrahmen EU-USA

1. ERSTE REGELMÄSSIGE ÜBERPRÜFUNG – HINTERGRUND, VORBEREITUNG UND VORGEHENSWEISE

In ihrem Beschluss vom 10. Juli 2023 (im Folgenden „Angemessenheitsbeschluss“) stellte die Kommission fest, dass der Datenschutzrahmen EU-USA ein angemessenes Schutzniveau für personenbezogene Daten bietet, die aus der Europäischen Union an Organisationen in den Vereinigten Staaten von Amerika übermittelt werden.[1] Gemäß dem Angemessenheitsbeschluss muss die Kommission regelmäßige Überprüfungen durchführen, von denen die erste ein Jahr nach dem Tag der Bekanntgabe des Angemessenheitsbeschlusses an die Mitgliedstaaten stattfinden sollte. Mit dem vorliegenden Bericht wird diese erste Überprüfung abgeschlossen.

Wie in Erwägungsgrund 211 des Angemessenheitsbeschlusses gefordert, konzentrierte sich diese erste Überprüfung nach dem ersten Jahr der Anwendung des neuen Rahmens auf die Frage, ob alle im Rahmen vorgesehenen Elemente umgesetzt worden sind und wirksam funktionieren. Die Überprüfung erstreckte sich auf alle Aspekte der Funktionsweise des Rahmens, auch angesichts der rechtlichen Entwicklungen seit der Annahme des Angemessenheitsbeschlusses.

Zur Vorbereitung der Überprüfung holte die Kommission Informationen von einschlägigen Interessenträgern ein, insbesondere von Nichtregierungsorganisationen (NRO) mit Fachwissen im Bereich der digitalen Rechte und der Privatsphäre[2], von Organisationen, die im Rahmen des Datenschutzrahmens zertifiziert sind, über ihre Handelsverbände[3]sowie von den US-Behörden, die an der Umsetzung des Rahmens beteiligt sind. Darüber hinaus hat die Kommission im Rahmen einer spezifischen Aufforderung zur Stellungnahme auf dem Portal „Ihre Meinung zählt“ Rückmeldungen von der breiten Öffentlichkeit eingeholt.[4]

Am 18. und 19. Juli 2024 fand in Washington D.C. eine Überprüfungssitzung statt. Sie wurde vom EU-Kommissar für Justiz und Verbraucher, Didier Reynders, und der US-Handelsministerin Gina Raimondo eröffnet.[5]

---

[1] Durchführungsbeschluss (EU) 2023/1795 der Kommission vom 10. Juli 2023 gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates über die Angemessenheit des Schutzniveaus für personenbezogene Daten nach dem Datenschutzrahmen EU-USA.

[2] Die Kommission sandte neun NRO (Human Rights Watch, American Civil Liberties Union, Consumer Federation of America, Center for Digital Democracy, New America Open Technology Institute, Access Now, Electronic Frontier Foundation, Electronic Privacy Information Center und Center for Democracy and Technology) einen Fragebogen zu, der sich auf relevante Entwicklungen des Rechtsrahmens der USA, von Aufsichts- und Durchsetzungsmechanismen und die Funktionsweise von Beschwerdestellen konzentrierte. Am 9. Juli 2024 fand auch eine Onlinebesprechung der Kommissionsdienststellen und der Vertreter des Europäischen Datenschutzausschusses mit diesen nichtstaatlichen Organisationen statt.

[3] Die Kommission sandte neun Handelsverbänden (Software & Information Industry Association, U.S. Chamber of Commerce, Information Technology Industry Council, The Software Alliance, Centre for Information Policy Leadership, Interactive Advertising Bureau, United States Council for International Business, Computer and Communications Industry Association und Engine) einen Fragebogen zu, der sich auf die Erfahrungen der nach dem Datenschutzrahmen zertifizierten Unternehmen konzentrierte, insbesondere auf das Zertifizierungsverfahren, die Maßnahmen zur Einhaltung der Grundsätze des Datenschutzrahmens, Verfahren für die Bearbeitung von Anfragen und Beschwerden von Privatpersonen usw.

[4] Die eingegangenen Rückmeldungen sind unter folgendem Link abrufbar: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14379-Datenschutzrahmen-EU-USA-Bericht-der-Kommission-uber-die-Wirkungsweise-des-Rahmens_de.

[5] Die Überprüfungssitzung wurde nach Themen organisiert, wobei jeder Tagesordnungspunkt durch eine kurze Präsentation der zuständigen US-Behörde, des EU-Vertreters oder der Organisation vorgestellt wurde, gefolgt von einer ausführlichen Fragerunde. Die „kommerziellen Aspekte“ des Rahmens (d. h. die Anwendung und

Für die EU wurde die Überprüfung von Vertretern der Generaldirektion Justiz und Verbraucher der Europäischen Kommission sowie fünf vom Europäischen Datenschutzausschuss (EDSA) benannten Vertretern verschiedener nationaler Datenschutzbehörden und des Europäischen Datenschutzbeauftragten durchgeführt.[6] Aufseiten der USA nahmen Vertreter des Department of Commerce (Handelsministerium – DoC), des Außenministeriums, der Federal Trade Commission (Kartellbehörde – FTC), des Department of Transportation (Verkehrsministerium – DoT), des Office of the Director of National Intelligence (Büro des Direktors des Nationalen Nachrichtendienstes – ODNI), des Department of Justice (Justizministerium – DoJ), des Inspector General for the Intelligence Community (Generalinspekteur für die Intelligence Community) sowie Mitglieder des Privacy and Civil Liberties Oversight Board (Stelle zur Überwachung des Schutzes der Privatsphäre und der bürgerlichen Freiheiten – PCLOB) teil. Darüber hinaus stellten Vertreter von Organisationen, die unabhängige Streitbeilegungsdienste anbieten, und der American Arbitration Association (Amerikanischer Verband für Schiedsgerichtsbarkeit) während der einschlägigen Überprüfungssitzungen Informationen zur Verfügung. Zudem leisteten die nach dem Datenschutzrahmen zertifizierten Organisationen einen Beitrag zu der Überprüfung in der Form von Präsentationen zu der Frage, wie Unternehmen den Erfordernissen des Datenschutzrahmens genügen.

Darüber hinaus stützen sich die Erkenntnisse der Kommission auf öffentlich zugängliche Informationen wie Gerichtsentscheidungen, Durchführungsvorschriften und -verfahren der zuständigen US-Behörden, Berichte und Studien nichtstaatlicher Organisationen, Transparenzberichte zertifizierter Unternehmen, Jahresberichte unabhängiger Aufsichtsstellen sowie Medienberichte.

2. FESTSTELLUNGEN

2.1. Gewerbliche Aspekte

2.1.1. Zertifizierungsverfahren

Um personenbezogene Daten erhalten zu können, die auf der Grundlage des Datenschutzrahmens aus der EU übermittelt werden, muss ein US-Unternehmen gegenüber dem Handelsministerium seine Einhaltung spezifischer Datenschutzanforderungen (Grundsätze des Datenschutzrahmens) zertifizieren und anschließend jährlich neu zertifizieren lassen. Die Zertifizierung setzt voraus, dass ein Unternehmen den Ermittlungs- und Durchsetzungsbefugnissen der FTC oder des Verkehrsministeriums unterliegt, dass es öffentlich seine Bereitschaft zur Einhaltung der Grundsätze des Datenschutzrahmens erklärt, seine Datenschutzbestimmungen offenlegt und diese Anforderungen vollständig umsetzt.[7] Vor Abschluss einer Zertifizierung prüft das Handelsministerium, ob das Unternehmen alle Zertifizierungsanforderungen erfüllt hat.[8]

Durchsetzung der Anforderungen an nach dem Datenschutzrahmen zertifizierte Unternehmen) wurden am ersten Tag behandelt, während am zweiten Tag Fragen im Zusammenhang mit dem Zugang der Regierung zu personenbezogenen Daten erörtert wurden.

[6] Die Vertreter der Kommission und des EDSA kamen am 12. Juni und 10. Juli 2024 zusammen, um die Überprüfung vorzubereiten, die eingegangenen Beiträge zu erörtern und zu ermitteln, zu welchen Aspekten zusätzliche Informationen eingeholt und geklärt werden müssen.

[7] Anhang I Abschnitt I.2 des Angemessenheitsbeschlusses.

[8] Anhang III des Angemessenheitsbeschlusses.

In der Überprüfungssitzung erklärte das Handelsministerium, dass der Schwerpunkt in diesem ersten Jahr des Datenschutzrahmens auf der Einrichtung des Zertifizierungsverfahrens lag, einschließlich der Entwicklung spezieller IT-Tools, der Aktualisierung von Verfahren, der Zusammenarbeit mit Unternehmen und der Durchführung anderer Öffentlichkeitsarbeit/Sensibilisierungsmaßnahmen. Zum Zeitpunkt der Überprüfungssitzung waren mehr als 2 800 Unternehmen nach dem Datenschutzrahmen zertifiziert. Dies bedeutet, dass im ersten Jahr der Anwendung des Datenschutzrahmens mehr Unternehmen zertifiziert wurden als nach dem vorherigen Rahmen, dem Datenschutzschild, im ersten Jahr seines Bestehens.[9] Nach Angaben des Handelsministeriums sind 70 % der Teilnehmer KMU, und eine große Zahl von dem Datenschutzrahmen angehörenden Unternehmen (47 %) sind in der Informations-, Kommunikations- und Technologiebranche (IKT) tätig. Darüber hinaus sind 60 % der Unternehmen ausschließlich für Nicht-Personaldaten zertifiziert, 2,5 % ausschließlich für Personaldaten und 37,5 % für Personal- und Nicht-Personaldaten.

Das Handelsministerium hat die erforderlichen Verfahren für die Bearbeitung von Anträgen von Unternehmen angenommen. Die Unternehmen müssen ihre Zertifizierungsanträge auf der Website zum Datenschutzrahmen des Handelsministeriums (https://www.dataprivacyframework.gov/) einreichen. Sie enthält Informationen über die Teilnahme am Datenschutzrahmen[10] und über die Verpflichtungen des Unternehmens nach dem Rahmen[11]. Ein spezielles Team im Handelsministerium unter der Verantwortung eines speziellen Direktors für den Datenschutzrahmen ist für alle Aspekte im Zusammenhang mit dem Management und der Verwaltung des Datenschutzrahmens zuständig, einschließlich des Zertifizierungsverfahrens und der Überwachung der Einhaltung der Vorschriften. Jeder Antrag wird einem bestimmten Mitarbeiter zugewiesen, der während des gesamten Zertifizierungsverfahrens für das betreffende Unternehmen verantwortlich bleibt.

Um nach dem Datenschutzrahmen zertifiziert zu werden, reichen die Unternehmen ihren Antrag ein, einschließlich eines Entwurfs einer Datenschutzerklärung. Das Handelsministerium prüft, ob sie den einschlägigen Anforderungen des Datenschutzrahmens entspricht. Wenn Organisationen verschiedene Einheiten innerhalb einer Unternehmensgruppe (z. B. verschiedene Tochtergesellschaften) zertifizieren lassen möchten, fordert und überprüft das Handelsministerium entweder eine umfassende Datenschutzerklärung, in der alle zu erfassenden Unternehmen eindeutig angegeben sind, oder separate Strategien für jedes Unternehmen. Das Handelsministerium überprüft auch mit der im Antrag angegebenen unabhängigen Beschwerdestelle[12], ob sich die Organisation tatsächlich bei ihr registriert hat. Bei Unternehmen, die das Gremium der Datenschutzbehörde auswählen (z. B. weil sie Personaldaten verarbeiten), prüft das Handelsministerium, ob das Unternehmen die für die Inanspruchnahme des Gremiums erforderlichen Gebühren entrichtet hat. Erforderlichenfalls prüft das Handelsministerium auch, ob der Antragsteller in den Zuständigkeitsbereich der FTC oder des Verkehrsministeriums fällt (und daher berechtigt ist, sich dem Datenschutzrahmen anzuschließen).

[9] Im entsprechenden Zeitraum verfügten 2 400 Unternehmen über eine Zertifizierung im Rahmen des Datenschutzschilds.

[10] https://www.dataprivacyframework.gov/program-articles/How-to-Join-the-Data-Privacy-Framework-(DPF)-Program-(part%E2%80%931).

[11] https://www.dataprivacyframework.gov/key-requirements.

[12] Beschwerdestellen des privaten Sektors, mit denen die Beschwerden und Streitigkeiten jeder Person untersucht und zügig und ohne Kosten für die Person beigelegt werden.

Wenn alle Bedingungen erfüllt sind, teilt das Handelsministerium der Organisation mit, dass es seine Datenschutzerklärung unter Verweis auf den Datenschutzrahmen auf seiner Website veröffentlichen kann. Sobald die Datenschutzerklärung öffentlich ist, bestätigt das Handelsministerium die Zertifizierung und nimmt das Unternehmen in die Datenschutzrahmen-Liste auf seiner Website auf. Der Datenschutzrahmen kann herangezogen werden, um personenbezogene Daten aus der EU ab dem Zeitpunkt zu erhalten, zu dem das Handelsministerium die Organisation in diese Liste aufnimmt.[13]

Wie in der Überprüfungssitzung erläutert, haben die bisher vom Handelsministerium durchgeführten Kontrollen dazu geführt, dass 33 Anträge abgelehnt wurden, weil sie die Anforderungen des Datenschutzrahmens nicht erfüllten. Im Allgemeinen arbeitet das Handelsministerium mit dem Unternehmen zusammen, um etwaige Mängel zu beheben. Stellt das Handelsministerium Mängel fest, so teilt es dem Unternehmen mit, dass es diese beheben muss und dass das Ausbleiben einer Reaktion innerhalb einer bestimmten Frist, oder das Versäumnis, die Selbstzertifizierung gemäß den Verfahren des Handelsministeriums abzuschließen, dazu führt, dass der Antrag als zurückgezogen gilt. Wird die ursprüngliche Zertifizierung nicht innerhalb von zwölf Monaten abgeschlossen/geändert, betrachtet das Handelsministerium sie als zurückgezogen.

Die Frist für die jährliche Neuzertifizierung ist in der Datenschutzrahmen-Liste für jedes Unternehmen angegeben. Um die Unternehmen daran zu erinnern, dass eine erneute Zertifizierung beantragt werden muss, hat das Handelsministerium ein System eingerichtet, um daran zu erinnern, dass die Zertifizierung bald ausläuft. Organisationen erhalten einen Monat vor, dann zwei Wochen vor und schließlich einen Tag vor dem Fälligkeitstermin eine Erinnerung. Unternehmen, die ihre Zertifizierung auslaufen lassen, werden von der Datenschutzrahmen-Liste gestrichen. Wie in Anhang III des Angemessenheitsbeschlusses beschrieben, verfügt das Handelsministerium auf seiner Website über einen speziellen Abschnitt, in dem die US-Organisationen aufgeführt sind, die keine aktiven Teilnehmer mehr sind, und die jeweiligen Gründe für die Streichung der betreffenden Unternehmen (z. B. Auslaufen oder Ausscheiden) aus der Liste (im Folgenden „Liste der inaktiven Unternehmen“). Wenn Organisationen aus der Datenschutzrahmen-Liste gestrichen werden, weil ihre Zertifizierung ausgelaufen ist, setzt sich das Handelsministerium mit ihnen in Verbindung, um zu bestätigen, dass die Zertifizierung auslaufen soll oder ob stattdessen eine erneute Zertifizierung beabsichtigt ist, und im letzteren Fall zu überprüfen, ob sie während des Zeitraums, in dem sie nicht zertifiziert wurden, die Grundsätze des Datenschutzrahmens auf personenbezogene Daten angewandt haben, die sie im Rahmen des Datenschutzrahmens erhalten haben, und in Erfahrung zu bringen, welche Schritte sie unternehmen werden, um die offenen Fragen zu klären, die ihre Neuzertifizierung verzögert haben. Wenn Unternehmen dem Handelsministerium mitteilen, dass sie sich aus dem Datenschutzrahmen zurückziehen möchten, müssen sie dem Handelsministerium bestätigen, ob sie die im Rahmen des Datenschutzrahmens erhaltenen Daten zurückgeben oder löschen werden; ob sie sie behalten und die Grundsätze des Datenschutzrahmens weiterhin auf diese Daten anwenden werden (was jährlich zu bestätigen ist); oder ob sie sie behalten und andere Schutzvorkehrungen einführen (z. B. von der Europäischen Kommission angenommene Standardvertragsklauseln).

Aus den Rückmeldungen von Handelsverbänden und Unternehmen geht hervor, dass die nach dem Datenschutzrahmen zertifizierten Unternehmen eine Reihe von Maßnahmen ergriffen

[13] Anhang I Abschnitt I Absatz 3 des Angemessenheitsbeschlusses.

haben, um die Einhaltung der Grundsätze des Datenschutzrahmens sicherzustellen. Beispielsweise haben die Organisationen zur Einhaltung des Grundsatzes des Rechtsschutzes, der Durchsetzung und der Haftung interne Kontrollen durchgeführt, die entweder ihm Rahmen von Selbstbewertung oder von externen Compliance-Überprüfungen erfolgt sind. Die beiden unabhängigen Beschwerdestellen des privaten Sektors, die an der Überprüfungssitzung teilnahmen, erklärten, dass sie auch externe Compliance-Überprüfungen im Rahmen von Überprüfungen der Datenschutzerklärungen vornehmen, und eine der unabhängigen Beschwerdestellen des privaten Sektors erklärte, dass sie auch Prüfungen und Stichprobenkontrollen durchführt, wobei der Schwerpunkt beispielsweise auf den Grundsätzen des Auskunftsrechts, der Wahlmöglichkeit und der Weitergabe liegt. Darüber hinaus haben zertifizierte Unternehmen interne Compliance-Programme und Kontrollmechanismen entwickelt, Mitarbeiter geschult, Mechanismen eingeführt, die Privatpersonen die Ausübung ihrer Rechte ermöglichen, Datenschutz-Folgenabschätzungen durchgeführt und bestehende Verträge überprüft.

2.1.2. Überwachung der Einhaltung von Grundsätzen, falsche Angaben zur Beteiligung und Durchsetzung

Nach dem Datenschutzrahmen ist das Handelsministerium dafür zuständig, die Einhaltung der Grundsätze des Datenschutzrahmens durch den Einsatz verschiedener Instrumente zu überwachen, einschließlich Kontrollen von Amts wegen (auf eigene Initiative), Ad-hoc-Stichproben vor Ort und Fragebögen zur Einhaltung der Grundsätze. Dazu gehört auch die Aufdeckung und Handhabung von Fällen, in denen zu Unrecht eine Beteiligung an der Regelung geltend gemacht wird, z. B. durch Internetrecherchen.[14]

Um die Einhaltung der Grundsätze durch die Unternehmen des Datenschutzrahmens zu überwachen, hat sich das Handelsministerium im vergangenen Jahr hauptsächlich auf Ad-hoc-Webrecherchen und Kontrollen von (sozialen) Medien gestützt. Das Handelsministerium berichtete, dass es in diesem ersten Jahr keine Probleme in Bezug auf die Einhaltung der Grundsätze des Datenschutzrahmens festgestellt und keine Unternehmen für etwaige Durchsetzungsmaßnahmen an die FTC oder das Verkehrsministerium verwiesen hat. Außerdem hat es eine spezielle Kontaktstelle eingerichtet, um die Zusammenarbeit mit den Datenschutzbehörden zu erleichtern und Beschwerden von Privatpersonen und Verweise von anderen Behörden (z. B. Datenschutzbehörden oder der FTC) entgegenzunehmen. Im vergangenen Jahr gingen jedoch keine Verweise oder Beschwerden ein. Während im ersten Jahr der Anwendung des Datenschutzrahmens der Schwerpunkt auf der Einrichtung des Rahmens und des Zertifizierungsverfahrens lag, erklärte das Handelsministerium in der Überprüfungssitzung, dass es plant, die Konformitätsprüfungen mit automatisierten Mitteln durchzuführen, um sie systematischer zu gestalten, und dass es derzeit die hierfür erforderlichen IT-Instrumente entwickelt.

Die Kommission erkennt an, dass das Handelsministerium seine Anstrengungen in diesem ersten Jahr auf die Einrichtung des Rahmens und des Zertifizierungsverfahrens konzentrieren musste. Es ist wichtig, dass das Handelsministerium seine Anstrengungen zur Überwachung und Überprüfung der Einhaltung der Grundsätze in Zukunft verstärkt, was erforderlich ist, um

[14] Siehe Anhang III des Angemessenheitsbeschlusses. Falsche Angaben können z. B. entstehen, wenn ein Unternehmen behauptet, am Datenschutzrahmen teilzunehmen, und es entweder nie mit dem Zertifizierungsverfahren begonnen hat oder es begonnen, jedoch nicht beendet hat oder seine Zertifizierung ausgelaufen ist.

ein anhaltend hohes Maß an Einhaltung des Rahmens sicherzustellen und Fälle aufzudecken, in denen weitere Durchsetzungsmaßnahmen erforderlich sind, einschließlich möglicher falscher Angaben zur Beteiligung von Unternehmen. In diesem Zusammenhang begrüßt die Kommission, dass das Handelsministerium seine Absicht bekräftigt hat, (automatisierte) Instrumente zu entwickeln und zu nutzen, um Compliance-Probleme und falsche Angaben wirksamer und systematischer zu ermitteln, und ist der Ansicht, dass dies Teil umfassenderer Bemühungen sein sollte, die verschiedenen ihm zur Verfügung stehenden Instrumente (z. B. Stichprobenkontrollen, Fragebögen zur Überprüfung der Einhaltung der Grundsätze, Auskunftsersuchen usw.) stärker zu nutzen, auch um die Einhaltung spezifischer Anforderungen des Datenschutzrahmens zu überprüfen.[15]

Organisationen des Datenschutzrahmens unterliegen der Gerichtsbarkeit der FTC und des Verkehrsministeriums. Während der Überprüfungssitzung bestätigte das Verkehrsministerium, dass alle Verfahren eingerichtet sind, um geeignete Durchsetzungsmaßnahmen zu ergreifen. Es erklärte ferner, dass nur sehr wenige Unternehmen, die seiner Gerichtsbarkeit unterliegen, dem Datenschutzrahmen beigetreten seien (d. h. einige wenige Verkaufsstellen von Flugtickets, aber keine Fluggesellschaften). Die FTC bestätigte, dass sie bei jeder ihrer Datenschutzuntersuchungen systematisch auf Verstöße gegen den Datenschutzrahmen überprüft. Bislang hat die FTC keine Verweise von anderen Behörden erhalten. Bei der Kommission sind einige Beschwerden eingegangen, in denen auf den Datenschutzrahmen Bezug genommen wird, wobei zwei von ihnen Unternehmen betrafen, die auf der „Liste der inaktiven Unternehmen“ stehen, zwei Unternehmen betrafen, die nicht am Datenschutzrahmen beteiligt waren, und eine davon keine personenbezogenen Daten betraf, die aus der EU übermittelt wurden. Zum Zeitpunkt der Erstellung dieses Berichts hatte die FTC keine Beschlüsse zur Durchsetzung der Einhaltung des Datenschutzrahmens erlassen, obwohl sie bestätigte, dass mehrere Unternehmen, die über eine Zertifizierung nach dem Datenschutzrahmen verfügen, derzeit untersucht werden.

Die Kommission begrüßt, dass die FTC bei allen Datenschutzuntersuchungen systematisch überprüft, ob gegen den Datenschutzrahmen verstoßen wurde. Da die weitere Wirksamkeit des Datenschutzrahmens von seiner konsequenten Durchsetzung abhängt, wird erwartet, dass die FTC ihre Untersuchungsbefugnisse innerhalb des Rahmens weiter ausüben wird, unter anderem durch proaktive Sweep-Maßnahmen, die sich auf die Einhaltung bestimmter Anforderungen des Datenschutzrahmens und/oder bestimmte Sektoren konzentrieren.

2.1.3. Bearbeitung von Beschwerden

Der Datenschutzrahmen bietet Privatpersonen in der EU unterschiedliche Rechtsbehelfsmöglichkeiten bei Verstößen gegen die Grundsätze des Datenschutzrahmens durch zertifizierte Organisationen.[16] Dazu gehört auch, die Lösung durch direkten Kontakt mit einer Organisation des Datenschutzrahmens weiterzuverfolgen, die der betroffenen Person innerhalb von 45 Tagen eine Antwort geben muss. Privatpersonen können auch eine Beschwerde bei einer unabhängigen Beschwerdestelle einreichen, die von einer Organisation benannt wurde, um Beschwerden zu untersuchen und beizulegen. Je nach den Umständen könnte es sich dabei entweder um eine Stelle zur alternativen Streitbeilegung oder um eine

[15] Beispielsweise in Bezug auf Weitergabe, indem von der Möglichkeit nach Grundsatz 3 Buchstabe b des Datenschutzrahmens Gebrauch gemacht wird, eine Zusammenfassung oder ein Exemplar der einschlägigen Datenschutzbestimmungen in Verträgen zu Weitergaben anzufordern.

[16] Siehe Abschnitt 2.4 des Angemessenheitsbeschlusses.

Datenschutzbehörde handeln[17]. Wenn die Beschwerde der betroffenen Person durch keine der anderen zur Verfügung stehenden Rechtsbehelfe zufriedenstellend beigelegt werden konnte, können Privatpersonen als letztes Mittel ein verbindliches Schiedsverfahren vor dem Datenschutzrahmen-Panel einleiten.

2.1.3.1. Bearbeitung von Beschwerden durch Unternehmen

Aus den Antworten von Handelsverbänden und Unternehmen auf die von der Kommission übermittelten Fragebögen geht hervor, dass nur sehr wenige – wenn überhaupt – Beschwerden von Privatpersonen über die Nichteinhaltung der Grundsätze des Datenschutzrahmens bei den im Rahmen des Datenschutzrahmens zertifizierten Unternehmen eingegangen sind. Gleichzeitig haben die Unternehmen verschiedene Verfahren und Instrumente eingeführt, die es Privatpersonen ermöglichen, ihre Rechte wahrzunehmen und Beschwerden einzureichen, unter anderem über webbasierte Formulare, E-Mails und Telefon.

2.1.3.2. Unabhängige Beschwerdestelle

Die während der Überprüfungssitzung eingegangenen Rückmeldungen und die von den Handelsverbänden übermittelten Informationen deuten darauf hin, dass es nur sehr wenige Beschwerden über unabhängige Beschwerdestellen gegeben hat. Zu den von den Unternehmen ausgewählten unabhängigen Beschwerdestellen gehören BBB National Programs, JAMS, TRUSTe und VeraSafe. Gemäß dem Datenschutzrahmen müssen die unabhängigen Beschwerdestellen einen Jahresbericht mit zusammengefassten statistischen Angaben zur Inanspruchnahme ihrer Streitbeilegungsdienste veröffentlichen. Zum Zeitpunkt der Annahme des vorliegenden Berichts hatten alle betroffenen unabhängigen Beschwerdestellen ihre Jahresberichte veröffentlicht.[18]

Darüber hinaus stellten BBB und VeraSafe in der Überprüfungssitzung ausführlich ihre Tätigkeiten im letzten Jahr vor. Sie berichteten über einen Anstieg der Zahl der Wirtschaftsteilnehmer, die ihre Dienstleistungen im Vergleich zu früheren Rahmen in Anspruch nahmen, und wiesen darauf hin, dass sie einige Beschwerden erhalten hatten, obwohl die überwiegende Mehrheit nicht zulässig war. So gingen bei BBB 87 Beschwerden von EU-Bürgerinnen und Bürgern ein, von denen nur zwei für eine Beilegung zulässig waren. Obwohl BBB erläuterte, dass Beschwerden im Durchschnitt innerhalb von fünf Geschäftstagen

[17] Die dem Datenschutzrahmen angehörenden Organisationen sind verpflichtet, bei der Prüfung und Klärung einer Beschwerde durch eine nationale Datenschutzbehörde mitzuwirken, wenn es um Personaldaten geht, die im Rahmen eines Beschäftigungsverhältnisses erhoben wurden, oder wenn sie sich freiwillig der Kontrolle durch die Datenschutzbehörden unterstellt haben.

[18] ANA – https://www.ana.net/content/show/id/accountability-dpf-consumers;
BBB National Programs – https://assets.bbbprograms.org/docs/default-source/eu-privacy-shield/dpf_periodicalreport_072024.pdf; ICDR – AAA – https://go.adr.org/rs/294-SFS-516/images/Data%20Privacy%20Framework%20IRM%20Program%20Report%202023-2024%20FINAL.pdf?version=0;
Insights association – https://www.insightsassociation.org/Portals/INSIGHTS/Insights%20Association%20DPF%20Services%20Program%202024%20Annual%20Report_Final_1.pdf;
JAMS – https://www.jamsadr.com/files/Uploads/Documents/2024-Annual-Report-DPF-Cases.pdf;
Privacy Trust DPF Services – https://privacytrust.com/fserve/PrivacyTrust_Dispute_Resolution_Report_2023_2024.pdf;
TRUSTe Dispute Resolution – https://trustarc.com/wp-content/uploads/2024/07/2024-Independent-Recourse-Mechanism-Annual-Report.pdf;
VeraSafe – https://verasafe.com/wp-content/uploads/2020/06/VeraSafe-DPF-Dispute-Resolution-Program-Annual-Report-2024.pdf.

bearbeitet werden, wurden diese beiden Beschwerden schließlich aufgrund einer fehlenden Antwort der Privatpersonen geschlossen. VeraSafe erhielt 26 Beschwerden, von denen sechs zulässig waren. Zwei von diesen betrafen Anträge auf Zugang und Löschung und wurden beigelegt, zwei sind noch anhängig und zwei wurden entweder zurückgezogen oder abgeschlossen, weil die Person nicht geantwortet hatte. Beide unabhängigen Beschwerdestellen erklärten, dass sie sich bemühen, Beschwerden in der Sprache der betreffenden Person zu beantworten.

Dem Datenschutzrahmen angehörende Unternehmen, die aus der EU übermittelte Personaldaten verarbeiten, müssen die EU-Datenschutzbehörden als ihre unabhängigen Beschwerdestellen für diese Daten auswählen, während sie für andere Arten von personenbezogenen Daten, die auf der Grundlage des Datenschutzrahmens übermittelt werden, die EU-Datenschutzbehörden auf freiwilliger Basis als unabhängige Beschwerdestellen auswählen können. Mehr als die Hälfte der zum Zeitpunkt der Überprüfung im Rahmen des Datenschutzrahmens zertifizierten Unternehmen entschied sich für diese Lösung[19], was zu begrüßen ist. Seit der Annahme des Angemessenheitsbeschlusses hat der EDSA die Geschäftsordnung für das „informelle Gremium der EU-Datenschutzbehörden“ angenommen. Das Gremium ist zuständig für die verbindliche Beratung der US-Organisationen bei ungeklärten Beschwerden von Privatpersonen über den Umgang mit personenbezogenen Daten, die aus der EU im Rahmen des Datenschutzrahmens übermittelt wurden. Gemäß seiner Geschäftsordnung setzt sich das Gremium aus einer Datenschutzbehörde, die als federführende Datenschutzbehörde fungiert, und anderen benannten mitprüfenden Datenschutzbehörden zusammen.[20] Es erteilt innerhalb von 60 Tagen nach Eingang einer Beschwerde über den Datenschutzrahmen verbindliche Ratschläge. Der EDSA hat auch ein Muster für Beschwerdeformulare für die Einreichung von Beschwerden bei Datenschutzbehörden[21] sowie „FAQs for European individuals“ (FAQs für europäische Privatpersonen)[22] und Unternehmen[23] zum Datenschutzrahmen veröffentlicht. Das Gremium hatte zum Zeitpunkt der Überprüfung keine Beschwerden erhalten.

2.1.3.3. Das verbindliche Schiedsverfahren

Das International Centre for Dispute Resolution (Internationales Zentrum für Streitbeilegung – ICDR), die internationale Abteilung der American Arbitration Association, wurde vom Handelsministerium mit der Durchführung von verbindlichen Schiedsverfahren beauftragt. Nach der Annahme des Angemessenheitsbeschlusses wählte das Handelsministerium zusammen mit der Kommission elf Schiedsrichter mit Erfahrung im Bereich des Schutzes der Privatsphäre und mit unterschiedlichem Hintergrund aus, darunter Schiedsgerichtsbarkeit,

[19] Kurz nach dem Datum der Überprüfungssitzung wurde auf der Website des Datenschutzrahmens angegeben, dass 1 511 der 2 892 Teilnehmer eine EU-Datenschutzbehörde als Beschwerdestelle hatten.
[20] Am 17. April 2024 nahm der EDSA die Geschäftsordnung des informellen Gremiums der EU-Datenschutzbehörden gemäß dem Datenschutzrahmen EU-USA an. Sie ist hier abrufbar: https://www.edpb.europa.eu/system/files/2024-04/dpf_rules-of-procedure_informal-panel-dpas_en.pdf.
[21] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-template-complaint-form_de.
[22] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-faq-european-individuals_de.
[23] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-faq-european-businesses_de.

Justiz, Wissenschaft und Zivilgesellschaft[24]. Darüber hinaus wurden die Schiedsregeln[25] für das Datenschutzrahmen-Panel und ein Verhaltenskodex für Schiedsrichter[26] angenommen, die alle auf der ICDR-Website abrufbar sind. Zum Zeitpunkt der Überprüfung war das Schiedsverfahren noch nicht von einer Person in der EU ausgelöst worden.

2.1.4. Leitlinien, Zusammenarbeit und Sensibilisierung

Seit Inkrafttreten des Datenschutzrahmens hat das Handelsministerium verschiedene Sensibilisierungsmaßnahmen durchgeführt, indem es Roadshows, Webinare und Konferenzen, die Kontaktaufnahme zu Handelsverbänden und die direkte Interaktion mit mehr als 3 000 Unternehmen organisiert hat, um Informationen über den Datenschutzrahmen bereitzustellen. Es hat auch Leitlinien veröffentlicht, u. a. in Form von häufig gestellten Fragen, die sich an Privatpersonen sowie an Unternehmen aus der EU und den USA richten.[27] Der EDSA wiederum hat Beschwerdeformulare und häufig gestellte Fragen für Privatpersonen und Unternehmen entwickelt. Ebenso veröffentlichte die Kommission bei der Annahme ihres Angemessenheitsbeschlusses Fragen und Antworten sowie ein Informationsblatt zum Datenschutzrahmen.[28]

Gleichzeitig ergab die Überprüfungssitzung, dass mehr getan werden muss, um Privatpersonen zu sensibilisieren und den Unternehmen Leitlinien an die Hand zu geben. Die von Unternehmen und unabhängigen Beschwerdestellen eingegangenen Beiträge sowie die sehr geringe Zahl von Beschwerden deuten darauf hin, dass sich Privatpersonen möglicherweise nicht immer ihrer Rechte und/oder des Verfahrens zur Ausübung dieser Rechte bewusst sind. Während der Überprüfungssitzung bekundete das Handelsministerium sein Interesse an einer Zusammenarbeit mit den Datenschutzbehörden der EU, um das Bewusstsein der EU-Bürgerinnen und -Bürger für den Rahmen zu schärfen. Die Kommission fördert solche Initiativen und unternimmt auch Schritte, um Privatpersonen besser zu informieren, unter anderem durch die Bereitstellung zusätzlicher Informationen über den Datenschutzrahmen auf ihrer Website, z. B. durch die Aufnahme von Links und Verweisen auf einschlägige Leitfäden, die vom EDSA, dem Handelsministerium und anderen US-Behörden angenommen wurden.

Was die Leitlinien zu den Grundsätzen des Datenschutzrahmens betrifft, einigten sich die Vertreter des EDSA in der Überprüfungssitzung darauf, in den kommenden Monaten zusammenzuarbeiten, um weitere Klarstellungen zum Begriff der Personaldaten im Rahmen des Datenschutzrahmens und zu den spezifischen Verpflichtungen, die für die Verarbeitung solcher Daten gelten, bereitzustellen. Es wurden verschiedene Elemente untersucht, die in diese Leitlinien aufzunehmen sind. In diesen Leitlinien könnten beispielsweise bestimmte praktische Szenarien behandelt werden, in denen Beschäftigtendaten im Rahmen des Datenschutzrahmens verarbeitet würden (z. B. durch einen Cloud-Anbieter), und es könnte erläutert werden, welche Verpflichtungen des Datenschutzrahmens für solche Szenarien relevant wären. Darüber hinaus könnte es Unternehmen, die Beschäftigtendaten von EU-Bürgerinnen und -Bürgern erhalten (diese Daten allerdings nicht unbedingt im Rahmen eines Beschäftigungsverhältnisses verwenden), nahelegen, das Gremium der Datenschutzbehörden als ihre unabhängige

[24] https://go.adr.org/DPF_Arbitrator_Bios.html.
[25] https://go.adr.org/rs/294-SFS-516/images/IC.DR-AAA_EU-US_DPF_AnnexI_Arbitration_Rules.pdf.
[26] https://go.adr.org/rs/294-SFS-516/images/Code_of_Conduct_for_Arbitrators_Appointed_to_EU-US_DPF_AnnexI_Arbitrations.pdf.
[27] Siehe z. B. https://www.dataprivacyframework.gov/US-Businesses.
[28] https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_de.

Beschwerdestelle auszuwählen. Dadurch würde sichergestellt, dass sich diese Privatpersonen an eine Behörde wenden können, die in ihrer Nähe ist und erforderlichenfalls mit den geltenden nationalen Rechtsvorschriften, die für Personaldaten gelten, besser vertraut ist.

Ein spezifischer Aspekt, bei dem weitere Leitlinien (auch auf der Grundlage von Beiträgen von Handelsverbänden) nützlich erscheinen, betrifft die Anforderungen des Datenschutzrahmens an Weitergaben. Darüber hinaus wies das Handelsministerium darauf hin, dass geprüft werden sollte, ob einige Sektoren von zusätzlichen Leitlinien für die Anwendung der Grundsätze des Datenschutzrahmens auf ihre Tätigkeiten profitieren könnten, z. B. im Bereich der Gesundheitsforschung und der Finanzdienstleistungen.

Die Kommission begrüßt die Bereitschaft beider Seiten, Leitlinien auszuarbeiten, und erwartet, dass die Arbeiten zu den oben genannten Themen in Kürze aufgenommen werden.

Ganz allgemein wurden mehrere Verfahren eingerichtet, um den Austausch und die Zusammenarbeit zwischen den US-Behörden und den Datenschutzbehörden sicherzustellen, unter anderem durch die Benennung spezieller Kontaktstellen innerhalb der FTC und des Handelsministeriums, die sich mit Anfragen und Verweisen der Datenschutzbehörden befassen.

2.1.5. Relevante Entwicklungen im US-Rechtssystem

Seit der Annahme des Angemessenheitsbeschlusses gab es im US-Rechtsrahmen im Bereich der Privatsphäre eine Reihe von Entwicklungen. Dazu gehören Entwicklungen in den Bereichen Gesetzgebung, Regulierung und Rechtsprechung. Sie deuten im Allgemeinen auf eine zunehmende Konvergenz zwischen den Ansätzen der EU und der USA in Bezug auf bestimmte Herausforderungen im Bereich der Privatsphäre hin, unter anderem durch die Verwendung ähnlicher Rechtsbegriffe. Einige dieser Entwicklungen sind im Gange und müssen weiter beobachtet werden.

Auf Bundesebene hat der Präsident mehrere Executive Orders (Durchführungsverordnungen – EO) erlassen, die für die Verwendung personenbezogener Daten relevant sind. Insbesondere verbietet oder begrenzt die Executive Order 14117 vom 28. Februar 2024[29] Transaktionen mit bestimmten Kategorien sensibler personenbezogener Daten (z. B. Gesundheitsdaten, biometrische Identifikatoren, Daten zur menschlichen Genomik) mit Unternehmen in einigen „problematischen Ländern“[30]. Mit der angenommenen Verordnung wird der Justizminister angewiesen, Verordnungen vorzuschlagen, die zum Zeitpunkt der Annahme des vorliegenden Berichts noch erlassen werden müssen, um ihre Umsetzung näher zu erläutern. Darüber hinaus konzentriert sich die Executive Order 14110 vom 30. Oktober 2023 über künstliche Intelligenz[31] auf die Entwicklung sicherer und vertrauenswürdiger künstlicher Intelligenz. Mehrere Bundesbehörden werden verpflichtet, KI-bezogene Sicherheitsstandards und -

[29] https://www.federalregister.gov/documents/2024/03/01/2024-04573/preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related.

[30] Dazu gehören, wie vom Justizminister in einer am 3. Mai 2024 veröffentlichten Advance Notice of Proposed Rulemaking (Vorabmitteilung vorgeschlagener Regelungen) vorgeschlagen, China, Kuba, Hongkong und Macau, Iran, Nordkorea und Venezuela. Siehe https://www.federalregister.gov/documents/2024/03/05/2024-04594/national-security-division-provisions-regarding-access-to-americans-bulk-sensitive-personal-data-and.

[31] https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence.

leitlinien zu entwickeln, unter anderem zu spezifischen KI-Risiken für die Privatsphäre und zu Techniken zur Wahrung der Privatsphäre.

Was die gesetzgeberische Arbeit betrifft, so wurden in den letzten Jahren zwar auf Bundesebene Gesetzentwürfe zum Datenschutz in den Kongress eingebracht, aber 20 US-Staaten haben bis Juli 2024 umfassende Datenschutzgesetze erlassen, von denen acht in Kraft getreten sind: Kalifornien, Colorado, Oregon, Virginia, Connecticut, Utah, Texas und Florida. Darüber hinaus haben 17 US-Staaten Rechtsvorschriften erlassen, die sich mit der automatisierten Verarbeitung (oder zumindest mit einigen Formen davon) befassen und generell Widerspruch für bestimmte Arten der Entscheidungsfindung auf der Grundlage von „Profiling“ zulassen[32].

In Bezug auf die Entwicklungen in der Rechtsprechung haben mehrere Vertreter der Zivilgesellschaft auf das jüngste Urteil des Obersten Gerichtshofs in der Rechtssache Loper Bright Enterprises gegen Raimondo (vom 28. Juni 2024) hingewiesen. Mit diesem Urteil wird die frühere Rechtsprechung zur Chevron-Doktrin außer Kraft gesetzt, wonach die Gerichte den Grundsatz der Zurückhaltung auf die vernünftige Auslegung des Rechts durch eine Regulierungsbehörde anwenden, wenn in einem von dieser Behörde durchgesetzten Gesetz Unklarheiten bestehen. Insbesondere haben einige NRO Bedenken hinsichtlich der Auswirkungen dieses Urteils des Obersten Gerichtshofs auf die Regelungsbefugnis der FTC im Bereich des Schutzes der Privatsphäre geäußert, räumten jedoch ein, dass es möglicherweise keine oder nur begrenzte Auswirkungen auf ihre Durchsetzungsbefugnisse geben könnte. In der Überprüfungssitzung teilte die FTC mit, dass es noch früh sei, um die genauen Auswirkungen dieses Urteils zu erkennen. Gleichzeitig erklärte sie, dass die FTC im Rahmen einer anderen Befugnis des FTC-Gesetzes Regeln erlässt als andere Verwaltungsbehörden und dass die Chevron-Doktrin für sie weniger relevant ist. Das kürzlich ergangene Urteil könnte daher in diesem Bereich nur begrenzte Auswirkungen haben.

Darüber hinaus informierte die FTC über die jüngsten Entwicklungen bei ihrem Ansatz für automatisierte Verarbeitung und künstliche Intelligenz. Dazu gehören die Annahme einer gemeinsamen Erklärung mit anderen Durchsetzungsbehörden gegen Diskriminierung und Voreingenommenheit in automatisierten Systemen[33] sowie mehrere Durchsetzungsmaßnahmen, bei denen sich die FTC unter anderem auf die Transparenz, die Fairness der automatisierten Verarbeitung und die Fähigkeit von Privatpersonen, die Ergebnisse anzufechten, konzentriert. Der bemerkenswerteste Fall in diesem Zusammenhang ist der Beschluss der FTC gegen Rite Aid vom März 2024, mit dem ein fünfjähriges Verbot des

[32] Es gibt zwar Unterschiede zwischen den verschiedenen Staaten, was unter „Profiling“ zu verstehen ist, doch wird Profiling im Allgemeinen definiert als jede Form der automatisierten Verarbeitung personenbezogener Daten zur Bewertung, Analyse oder Vorhersage personenbezogener Aspekte im Zusammenhang mit der wirtschaftlichen Lage, der Gesundheit, den persönlichen Vorlieben, den Interessen, der Zuverlässigkeit, dem Verhalten, dem Aufenthaltsort oder den Bewegungen einer identifizierten oder identifizierbaren natürlichen Person. In der Regel können Verbraucher Profiling widersprechen. Folgende Staaten haben Rechtsvorschriften zu Profiling ausgearbeitet: Colorado (Colo. Rev. Stat. Ann. § 6-1-1306), Connecticut (Conn. Gen. Stat. Ann. § 42-518), Delaware (Del. Code Ann. Tit. 6, § 12D-104), Florida (Fla. Stat. Ann. § 501.705), Indiana (Ind. Code Ann. § 24-15-3-1), Kentucky (Ky. Rev. Stat. Ann. § 367.3615), Maryland (Maryland Online Data Privacy Act von 2024, erlassen am 9. Mai 2024), Minnesota (Minn. Ann. § 325O.07), Montana (Mont. Code Ann. § 30-14-2808), Nebraska (Neb. Rev. Stat. Ann. § 87-1107), New Hampshire (N.H. Rev. Stat. Ann. § 507-H:4), New Jersey (N.J. Stat. Ann. § 56:8-166.8), Oregon (Or. Rev. Stat. Ann. § 646A.574), Rhode Island (Rhode Island Data Transparency and Privacy Protection Act, erlassen am 29. Juni 2024), Tennessee (Tenn. Code Ann. § 47-18-3304), Texas (Tex. Bus. & Com. Code Ann. § 541.051) und Virginia (Va. Code Ann. § 59.1-577).

[33] https://files.consumerfinance.gov/f/documents/cfpb_joint-statement-enforcement-against-discrimination-bias-automated-systems_2023-04.pdf.

Einsatzes von Gesichtserkennungstechnologie für Sicherheitszwecke durch dieses Unternehmen verhängt wurde.[34] Insbesondere stellte die FTC fest, dass Rite Aid keine angemessenen Maßnahmen ergriffen hat, um fehlerhafte Ergebnisse zu verhindern und die Verbraucher über die verwendete Technologie zu informieren. Generell erläuterte die FTC bei der Überprüfungssitzung ihre derzeitigen Prioritäten und insbesondere in den Bereichen, die ihrer Ansicht nach einen proaktiveren Durchsetzungsansatz erfordern. Dazu gehören der Schutz sensibler Daten (z. B. Gesundheitsdaten, biometrische Daten, Geolokalisierung)[35], der Schutz von Kindern[36] und Minderjährigen im Internet und die Datensicherheit[37].

Die Kommission wird diese und andere Entwicklungen in den USA weiterhin aufmerksam verfolgen, insbesondere alle weiteren Schritte auf dem Weg zu einem umfassenden Datenschutzgesetz auf Bundesebene und die möglichen Auswirkungen der jüngsten Rechtsprechung des Obersten Gerichtshofs auf die Rolle der FTC im Bereich der Privatsphäre.

Die Kommission begrüßt die Informationen der FTC über ihre jüngsten Durchsetzungsmaßnahmen und aktuellen Prioritäten, die weitgehend den Trends und Prioritäten bei der Durchsetzung des Datenschutzes in Europa entsprechen. Die FTC beteiligt sich auch aktiv an dem Netzwerk, in dem Länder zusammenkommen, die von einem Angemessenheitsbeschluss der EU profitieren, den die Kommission im März 2024 auf den Weg gebracht hat.[38] Diese stärkere Konvergenz dürfte eine engere Zusammenarbeit zwischen den für die Durchsetzung des Datenschutzes zuständigen Stellen beiderseits des Atlantiks fördern und erleichtern, insbesondere in Fragen, die für das Funktionieren des Datenschutzrahmens relevant sind.

2.2. Aspekte im Zusammenhang mit dem Zugang zu und der Verwendung von im Rahmen des Datenschutzrahmens EU-USA durch US-Behörden übermittelten personenbezogenen Daten

Der Angemessenheitsbeschluss enthält eine detaillierte Bewertung der Vorschriften für die Erhebung und Verwendung personenbezogener Daten, die aus der EU an nach dem Datenschutzrahmen zertifizierte Unternehmen übermittelt werden, durch US-Behörden, insbesondere für Zwecke der Strafverfolgung und der nationalen Sicherheit. Wie von den US-Behörden in der Überprüfungssitzung bestätigt wurde, gab es seit der Annahme des Angemessenheitsbeschlusses im ersten Jahr des Datenschutzrahmens keine relevanten

[34] https://www.ftc.gov/legal-library/browse/cases-proceedings/2023190-rite-aid-corporation-ftc-v.

[35] Siehe z. B. die jüngste Anordnung der FTC gegen X-Mode wegen des Verkaufs und der Weitergabe sensibler Standortdaten (https://www.ftc.gov/system/files/ftc_gov/pdf/X-ModeSocialDecisionandOrder.pdf) und gegen Monument wegen der Weitergabe sensibler Gesundheitsdaten an Dritte zu Marketingzwecken (https://www.ftc.gov/system/files/ftc_gov/pdf/MonumentOrderFiled.pdf).

[36] So hat die FTC vor Kurzem eine Untersuchung angekündigt, die zu einer Klage gegen TikTok und dessen Muttergesellschaft, Bytedance, wegen angeblicher Verletzung des Rechts auf Privatsphäre von Kindern führte. Beide Unternehmen seien ihrer Verpflichtung, die Eltern zu benachrichtigen und ihre Zustimmung einzuholen, bevor personenbezogene Daten von Kindern unter 13 Jahren erhoben und verwendet werden, nicht nachgekommen (https://www.ftc.gov/news-events/news/press-releases/2024/08/ftc-investigation-leads-lawsuit-against-tiktok-bytedance-flagrantly-violating-childrens-privacy-law).

[37] Siehe Überblick über die jüngsten Durchsetzungsmaßnahmen in dem FTC 2023 Privacy and Data Security Update (Aktualisierung zu Privatsphäre und Datensicherheit der FTC 2023): https://ec.europa.eu/commission/presscorner/detail/de/mex_24_1307.

[38] Siehe https://ec.europa.eu/commission/presscorner/detail/de/mex_24_1307. Im Anschluss an die Sitzung im März 2024 wurde beschlossen, eine Reihe thematischer Sitzungen abzuhalten. Die erste fand im Juli 2024 statt und konzentrierte sich auf die Entwicklung von Instrumenten, die kleine und mittlere Unternehmen bei der Einhaltung der Datenschutzgesetze unterstützen können.

Entwicklungen in Bezug auf den Rechtsrahmen, der für den Zugang zu Daten zu Strafverfolgungs- oder Regulierungszwecken gilt. Aus diesem Grund betreffen die nachstehenden Feststellungen nur Entwicklungen im Bereich der nationalen Sicherheit.

Die Schlussfolgerungen im Angemessenheitsbeschluss über den Zugang von Nachrichtendiensten zu Daten stützen sich auf die Analyse der Bedingungen und Beschränkungen, die für Signalaufklärungstätigkeiten nach mehreren einschlägigen Rechtsvorschriften gelten – insbesondere Abschnitt 702 des Foreign Intelligence Surveillance Act (Gesetz über die Überwachung der Auslandsgeheimdienste – FISA) und Executive Order 12333[39] –, ergänzt und gestärkt durch die Executive Order 14086 on Enhancing Safeguards for United States Signals Intelligence (Durchführungsverordnung zur Verbesserung der Schutzmaßnahmen für Signalaufklärungsdienste der Vereinigten Staaten – EO 14086), die am 7. Oktober 2022 vom Präsidenten der Vereinigten Staaten angenommen wurde. Die in der EO 14086 festgelegten Garantien gelten für alle US-amerikanischen Signalaufklärungstätigkeiten, unabhängig davon, auf welche rechtliche Befugnis sich diese Tätigkeiten stützen und wo sie stattfinden, und schützen die Daten von Nicht-US-Bürgerinnen und -Bürgern (einschließlich Europäerinnen und Europäern).[40] Mit der EO 14086 wurde auch eine neue Beschwerdestelle eingeführt, bei der diese verbindlichen Garantien von Privatpersonen in der EU geltend gemacht und durchgesetzt werden können.

In den folgenden Abschnitten werden die Schritte, die die US-Behörden seit der Annahme des Angemessenheitsbeschlusses unternommen haben, um der EO 14086 nachzukommen, sowie relevante Entwicklungen in Bezug auf den oben genannten Rechtsrahmen beschrieben.

2.2.1. Relevante Entwicklungen in Bezug auf den US-Rechtsrahmen

2.2.1.1. Umsetzung der Executive Order 14086 durch Nachrichtendienste

Die mit der EO 14086 eingeführten Einschränkungen und Garantien ergänzen die in Abschnitt 702 FISA und in der EO 12333 vorgesehenen Einschränkungen und Garantien. Sie sind für alle Nachrichtendienste verbindlich und wurden durch die von den einzelnen Behörden festgelegten Strategien und Verfahren weiter umgesetzt.

Im Rahmen der ersten Überprüfung bestätigten die US-Behörden, dass die EO 14086 seit ihrer Annahme nicht geändert wurde. Darüber hinaus wurde klargestellt, dass der US-Präsident nicht von der in den Abschnitten 2(b)(i)(B) und 2(b)(ii)(C) der EO 14086 vorgesehenen Befugnis Gebrauch gemacht hat, die Liste der legitimen Ziele, die mit der Erhebung von Signalaufklärungsdaten verfolgt werden können, oder die Liste der Zwecke, für die durch Sammelerhebung gewonnene Daten verwendet werden dürfen, zu aktualisieren.[41] Um

[39] Weitere Maßnahmen, die nach dem FISA in Bezug auf aus der EU übermittelte Daten ergriffen werden können, sind die individualisierte elektronische Überwachung (Abschnitt 105 FISA), die Durchsuchung (Abschnitt 302 FISA), der Einsatz von Geräten zur Rufnummernerfassung von ausgehenden und eingehenden Anrufen (Abschnitt 402 FISA) und die Erhebung von Geschäftsunterlagen bei bestimmten Unternehmen (Beförderungsunternehmen, öffentliche Einrichtungen, Mietwagenfirmen oder Lagerhäuser, Abschnitt 501 FISA). Diese verschiedenen Rechtsgrundlagen werden im Angemessenheitsbeschluss eingehend analysiert (Erwägungsgründe 142-152).

[40] Weitere Informationen sind Abschnitt 3.2.1.2 des Angemessenheitsbeschlusses zu entnehmen.

[41] Zu diesen legitimen Zielen/Zwecken gehören beispielsweise der Schutz vor Spionage, Sabotage, Ermordung oder andere nachrichtendienstliche Tätigkeiten, die durch eine ausländische Regierung, Organisation oder Person oder in deren Namen oder mit deren Unterstützung durchgeführt werden; Schutz vor Terrorismus, Geiselnahme und Gefangennahme von Personen durch oder im Namen einer ausländischen Regierung, Organisation oder Person.

spezifischere nachrichtendienstliche Prioritäten festzulegen, für die Signalaufklärungsdaten erhoben werden dürfen, wurde mit der EO 14086 ein besonderes Verfahren eingeführt. Insbesondere muss der ODNI Civil Liberties Protection Officer (Bürgerrechtsbeauftragter des Nationalen Nachrichtendienstes – ODNI CLPO) konsultiert werden, um für jede Priorität zu beurteilen, ob sie 1) einem oder mehreren der in der EO aufgeführten legitimen Ziele dient; 2) nicht dazu bestimmt und voraussichtlich nicht dazu führen wird, Signalaufklärungsdaten für ein in der EO aufgeführtes verbotenes Ziel zu erheben, und 3) unter gebührender Berücksichtigung der Privatsphäre und der bürgerlichen Freiheiten aller Personen festgelegt wurde.[42] Der ODNI CLPO bestätigte in der Überprüfungssitzung, dass er die von dem Direktor des Nationalen Nachrichtendienstes im Rahmen des National Intelligence Priorities Framework 2023 vorgeschlagenen Prioritäten überprüft hat, zu dem Schluss gekommen ist, dass sie die oben genannten Anforderungen erfüllen, und dass er seine Schlussfolgerung dem Direktor des Nationalen Nachrichtendienstes (DNI) mitgeteilt hat, der wiederum die Prioritäten dem Präsidenten zur Validierung vorlegte. Der ODNI CLPO veranstaltete auch Schulungen zu den Anforderungen der EO 14086 für Teile der Intelligence Community, die an der Entwicklung von nachrichtendienstlichen Prioritäten beteiligt sind.

Darüber hinaus haben die US-Behörden im vergangenen Jahr weitere praktische Schritte unternommen, um die EO 14086 in ihrem täglichen Betrieb umzusetzen. Insbesondere haben die Nachrichtendienste weitere interne Strategien und Leitlinien für die Anwendung der EO eingeführt, z. B. interne Verfahren (durch interne Genehmigungsanforderungen, dokumentierte Zugangskontrollen, sodass nur Personen, die ordnungsgemäß geschult wurden und über die erforderlichen Aufgabenanforderungen verfügen, Zugang zu den Informationen haben usw.), um sicherzustellen, dass die Anforderungen an die Notwendigkeit und Verhältnismäßigkeit sowohl bei der gezielten Erhebung als auch bei der Sammelerhebung eingehalten werden.[43] Darüber hinaus wurden Schulungen zur EO 14086 für das Personal verschiedener Nachrichtendienste (z. B. NSA, CIA, FBI) angeboten, einschließlich jährlicher und Ad-hoc-Schulungen, die vom ODNI CLPO organisiert werden, sowie verpflichtender Schulungen für alle neuen Mitarbeiter, die die Arbeit beim ODNI aufnehmen.

Die Kommission begrüßt die verschiedenen Maßnahmen zur Umsetzung und Gewährleistung der Einhaltung der EO 14086. Mit zunehmender Erfahrung bei der praktischen Anwendung der Schutzmaßnahmen der EO würde die Kommission es begrüßen, wenn bei künftigen Überprüfungen konkrete Beispiele dafür erörtert werden könnten, wie die EO in der Praxis (unter Wahrung der geltenden Vertraulichkeitserwägungen) angewandt wird.

2.2.1.2. Erneute Genehmigung von Abschnitt 702 FISA

Abschnitt 702 FISA gestattet die gezielte Überwachung von Nicht-US-Bürgerinnen und -Bürgern, die sich mit hinreichender Bestimmtheit außerhalb der Vereinigten Staaten aufhalten, um Auslandsaufklärungsdaten zu erlangen. Die Erhebung erfolgt auf der Grundlage jährlicher Zertifizierungen, die dem Foreign Intelligence Surveillance Court (Gericht zur Überwachung der Auslandsgeheimdienste – FISC) vorgelegt und von diesem genehmigt wurden. In diesen Zertifizierungen werden spezifische Kategorien der zu erhebenden Auslandsaufklärungsdaten aufgeführt. Am 21. Juli 2023 gab das ODNI bekannt, dass es drei genehmigte Zertifizierungen nach Abschnitt 702 FISA gibt, die die folgenden Kategorien von Auslandsaufklärungsdaten

[42] Abschnitt 2(b)(iii) EO 14086.

[43] Siehe https://www.intel.gov/ic-on-the-record-database/results/oversight/1278-odni-releases-ic-procedures-implementing-new-safeguardsin-executive-order-14086, veröffentlicht am 3. Juli 2023.

abdecken: 1) ausländische Regierungen und mit diesen verbundene Organisationen, 2) Terrorismusbekämpfung und 3) Bekämpfung der Proliferation.[44] Die Zertifizierungen müssen auch vom FISC genehmigte Verfahren zur zielgenauen Erfassung und zur Minimierung der Datenmenge umfassen.[45] Die zielgenaue Erfassung wird insbesondere durchgeführt, indem US-Unternehmen, die die FISA-Definition des Begriffs „electronic communication service provider“ (Anbieter elektronischer Kommunikationsdienste – ECSP) erfüllen, aufgefordert werden, elektronische Kommunikationsdaten für Mitteilungen an oder von „Selektoren“ offenzulegen, die ein bestimmtes Kommunikationskonto, z. B. eine Telefonnummer oder eine E-Mail-Adresse, identifizieren. Die US-Regierung hat eine Reihe von Materialien zu Abschnitt 702 FISA veröffentlicht, um die Öffentlichkeit über die Funktionsweise der Überwachungsprogramme, die geltenden Anforderungen, den Schutz der Privatsphäre sowie über die Rolle des FISC zu informieren.[46]

Aufgrund einer Verfallsklausel sollte Abschnitt 702 FISA Ende 2023 auslaufen, sofern er nicht vom Kongress erneut genehmigt würde. Nach einer vorübergehenden erneuten Genehmigung ohne Änderungen verabschiedete der Kongress am 19. April 2024 das Reforming Intelligence and Securing America Act (Gesetz zur Reform der Nachrichtendienste und zur Sicherung Amerikas – RISAA), mit dem Abschnitt 702 FISA für einen Zeitraum von zwei Jahren erneut genehmigt und mehrere Änderungen eingeführt wurden. Es ist grob zu unterscheiden zwischen: 1) Änderungen des Umfangs der nach Abschnitt 702 FISA zulässigen Überwachungstätigkeiten und 2) institutionellen und verfahrenstechnischen Änderungen.

Änderungen des Umfangs der nach Abschnitt 702 FISA zulässigen Überwachungstätigkeiten

Durch das RISAA wurden drei wesentliche Änderungen am Umfang der Überwachungstätigkeiten vorgenommen, die nach Abschnitt 702 FISA durchgeführt werden können.

Erstens wurde die sogenannte „about collection“ endgültig verboten.[47] Dies bezieht sich auf die Sammlung von Mitteilungen, bei denen der Selektor nach Abschnitt 702 (z. B. eine E-Mail-Adresse) nicht in den Feldern „an“ oder „von“ der Mitteilung erscheint, sondern ein Verweis auf einen solchen Selektor in der Mitteilung enthalten ist (z. B. E-Mail-Mitteilungen, die nicht an die oder von der ausgewählten E-Mail-Adresse gesendet werden, sondern bei denen die ausgewählte E-Mail-Adresse im E-Mail-Text oder Fließtext enthalten ist). Während eine solche Erhebung bereits nach einer Änderung des FISA im Jahr 2018 ausgeschlossen wurde, sah das Gesetz nach einem spezifischen Genehmigungsverfahren unter Beteiligung des FISC und des Kongresses noch die Möglichkeit vor, die „about collection“ in Zukunft wieder aufzunehmen. Mit der letzten Änderung durch das RISAA ist diese Möglichkeit nicht mehr gegeben.

Zweitens wurde die Definition des Begriffs „Auslandsaufklärungsdaten“ um Informationen über Maßnahmen zur Drogenbekämpfung erweitert.[48] Während der Überprüfungssitzung erklärten die US-Behörden, dass dies aufgrund der derzeitigen Opioidkrise und der

[44] https://www.intelligence.gov/ic-on-the-record-database/results/1307-release-of-documents-related-to-the-2023-fisa-section-702-certifications.

[45] Solche Verfahren begrenzen die Erhebung von Daten in Bezug auf einen bestimmten Zweck der Auslandsaufklärung, beschränken den Zugang zu Datenbanken, in denen nach Abschnitt 702 FISA erlangte Informationen gespeichert werden (auch durch Zugangskontrollen), und sehen Beschränkungen für die Verwendung, Speicherung und Verbreitung solcher Informationen vor.

[46] https://www.intel.gov/foreign-intelligence-surveillance-act.

[47] Abschnitt 22 RISAA.

[48] Abschnitt 23 RISAA.

zunehmenden Bedrohung der nationalen Sicherheit durch internationale Drogenhändler und -hersteller eingeführt wurde. Vor diesem Hintergrund wurde bestätigt, dass dieser Begriff unter mehrere der in der EO 14086 aufgeführten legitimen Ziele fällt, nämlich das Verständnis oder die Bewertung der Fähigkeiten, Absichten oder Aktivitäten ausländischer Organisationen, die eine tatsächliche oder potenzielle Bedrohung für die nationale Sicherheit der USA oder ihrer Verbündeten darstellen, das Verständnis oder die Bewertung transnationaler Bedrohungen, die sich auf die globale Sicherheit auswirken, einschließlich Risiken für die öffentliche Gesundheit sowie der Schutz vor grenzüberschreitenden kriminellen Bedrohungen.[49]

Drittens wurde durch das RISAA die Definition des Begriffs „Anbieter elektronischer Kommunikationsdienste“ (ECSP) erweitert, wodurch der Kreis der Unternehmen erweitert wurde, die nach Abschnitt 702 FISA zur Bereitstellung von Informationen verpflichtet sein können.[50] Die Begriffsbestimmung umfasst nun andere Dienstleister, die „Zugang zu Geräten haben, die für die Übertragung oder Speicherung von drahtgebundener oder elektronischer Kommunikation verwendet werden oder verwendet werden können“, wobei öffentliche Unterkünfte, Wohnungen, gemeinschaftliche Einrichtungen und Gastronomieeinrichtungen ausdrücklich ausgenommen sind. In einem Schreiben an den Kongress verwies das Justizministerium auf diese Änderung als technische Änderung, mit der eine „extrem kleine“ Zahl von Technologieunternehmen abgedeckt werden soll, die nach jüngsten Entscheidungen des FISC und des Foreign Intelligence Surveillance Court of Review (Rechtsmittelgericht für Entscheidungen im Bereich der Überwachung der Auslandsgeheimdienste – FISCR) von der früheren Definition von ECSP nicht erfasst wurden.[51] In demselben Schreiben verpflichtete sich das Justizministerium, den Anwendungsbereich einzuschränken und diese Definition ausschließlich auf die Art des Dienstleisters anzuwenden, um den es in dem Rechtsstreit ging, der zu der Entscheidung des FISC führte. Folglich werden die betroffenen Unternehmen in einem als Verschlusssache eingestuften Anhang für den Kongress genannt. Mehrere NRO, darunter diejenigen, die im Rahmen der Überprüfung Rückmeldungen gaben, äußerten Bedenken hinsichtlich dieser Ausweitung und brachten vor, dass sie potenziell viele US-Unternehmen betreffen könnte (da viele von ihnen irgendeine Art von Diensten anbieten und Zugang zu Kommunikationsausrüstung haben). Angesichts dieser Bedenken wurde mit Unterstützung der Intelligence Community eine weitere Änderung in einem Entwurf des Intelligence Authorisation Act for Fiscal Year 2025 (Gesetz über die Geheimdienstgenehmigung für das Steuerjahr 2025) vorgeschlagen, der derzeit dem Kongress vorliegt. Diese Änderung würde, wenn sie vom Kongress verabschiedet würde, sicherstellen, dass die zusätzlichen Unternehmen, die unter die Definition von ECSP fallen, nur auf die in den oben genannten Entscheidungen des FISC genannten Unternehmen beschränkt wären. In dem Gesetzentwurf ist auch vorgesehen, dass jede an ein solches Unternehmen gerichtete Richtlinie dem FISC gemeldet werden muss, damit dieses prüfen kann, ob das Unternehmen tatsächlich in den Anwendungsbereich fällt. In seinem Schreiben an den Kongress verpflichtete sich das Justizministerium, dem Kongress alle sechs Monate über jede Anwendung der aktualisierten Definition Bericht zu erstatten, damit der Kongress die angemessene Aufsicht über die enge Anwendung der Definition ausüben kann.

[49] Abschnitt 2(b)(ii)(A)(2), (3) und (10) EO 14086.
[50] Abschnitt 25 RISAA.
[51] https://www.justice.gov/opa/media/1348621/dl?inline. Siehe die Entscheidung des FISC von 2022 (https://www.intel.gov/assets/documents/702%20Documents/declassified/2022-FISC-ECSP-OPINION.pdf) und das Urteil des FISCR, mit dem diese Entscheidung bestätigt wurde (https://www.intel.gov/assets/documents/702%20Documents/declassified/2023_FISC-R_ECSP_Opinion.pdf).

Wichtig ist, dass in der Überprüfungssitzung von den US-Behörden und vom PCLOB bestätigt wurde, dass alle Garantien der EO 14086 weiterhin uneingeschränkt für die gesamte Datenerhebung und -nutzung nach Abschnitt 702 FISA gelten, auch nach diesen Änderungen. Während das RISAA den Kreis der Unternehmen, die eine Anordnung erhalten können, etwas erweitert, schränkt es die Ausübung von Rechten nicht ein. Dennoch wird es wichtig sein, weitere Entwicklungen (Gesetzgebung und Berichterstattung) zu beobachten und Informationen über die Anwendung dieser neuen Vorschriften in der Praxis zu erhalten. Dazu gehören beispielsweise die Auswirkungen der Erweiterung der Definitionen von Auslandsaufklärung und ECSP auf die Zahl der Ziele nach Abschnitt 702 FISA (wie vom ODNI jährlich mitgeteilt, siehe unten zur Transparenz). Der künftige Folgebericht zum jüngsten PCLOB-Bericht zu Abschnitt 702 FISA (siehe unten) sollte in dieser Hinsicht besonders aussagekräftig sein.

Institutionelle und verfahrenstechnische Änderungen

In Bezug auf institutionelle und verfahrenstechnische Änderungen wurden durch das RISAA mehrere Verfahren kodifiziert, die bereits in der Praxis angewandt wurden, und es wurden neue Garantien eingeführt. Während einige davon nur US-Bürgerinnen und -Bürger betreffen, erhöhen mehrere Änderungen den Schutz sowohl für US- als auch für Nicht-US-Bürgerinnen und -Bürger, deren Daten nach Abschnitt 702 FISA erhoben werden können[52], und sind daher für die Funktionsweise des Datenschutzrahmens relevant.

Erstens wurden eine Reihe zusätzlicher Rechenschafts-, Aufsichts- und Berichtspflichten eingeführt. Insbesondere muss das FBI-Personal nun jährlich zu den Regeln für die Abfrage von nach Abschnitt 702 FISA erlangten Informationen geschult werden.[53] Das FBI ist auch verpflichtet, dem Kongress über seine Abfragetätigkeiten (z. B. die Zahl der Abfragen unter Verwendung von „Batch-Job-Technologien“, d. h. die Nutzung mehrerer Abfragebegriffe als Teil einer einzigen Abfrage) und über die Maßnahmen zur Rechenschaftspflicht zu berichten, die ergriffen wurden, um die Einhaltung der rechtlichen Abfrageanforderungen sicherzustellen (Abschnitte 11-12 RISAA). Darüber hinaus wird der Generalinspektor des Justizministeriums angewiesen, einen Bericht über die Einhaltung der Abfrageanforderungen durch das FBI zu erstellen (Abschnitt 9 RISAA). Um die Transparenz der Verfahren vor dem FISC zu erhöhen, sind das ODNI und der Justizminister nun verpflichtet, die Überprüfung von Entscheidungen des FISC zur Freigabe innerhalb von 180 Tagen abzuschließen (Abschnitt 7 RISAA). Darüber hinaus müssen die Niederschriften aller Anhörungen vor dem FISC und dem FISCR (Gericht, bei dem Entscheidungen des FISC angefochten werden können) aufbewahrt und dem Kongress übermittelt werden (Abschnitt 8 RISAA).

Zweitens wurden mit dem RISAA weitere Beschränkungen für die Verwendung der nach Abschnitt 702 FISA erhobenen Daten durch das FBI eingeführt. Abschnitt 2(d) RISAA sieht

[52] Darüber hinaus wurden durch das RISAA einige Änderungen in Bezug auf die herkömmliche individuelle elektronische Überwachung gemäß Abschnitt 105 FISA eingeführt (auf der Grundlage einer Anordnung des FISC, die erlassen wird, wenn der Standard eines hinreichenden Verdachts erfüllt ist). Ein Antrag eines Nachrichtendienstes beim Justizminister auf Anordnung einer individuellen elektronischen Überwachung erfordert nun eine eidesstattliche Erklärung, die die Annahme begründet, dass die Voraussetzungen des Abschnitts 105 FISA erfüllt sind (Abschnitt 6(a) RISAA). Die mögliche Dauer der elektronischen Überwachung ausländischer Mächte oder Agenten ausländischer Mächte wurde von 120 Tagen auf ein Jahr verlängert (Abschnitt 6(g) RISAA).

[53] Abschnitt 2(d) RISAA.

vor, dass eine Abfrage unter Verwendung der „Batch-Technologie“ nur nach Einholung der Zustimmung eines Anwalts innerhalb des FBI erfolgen kann, es sei denn, es liegen außergewöhnliche Umstände vor. Darüber hinaus ist es dem FBI nun untersagt, nach Abschnitt 702 FISA erlangte, nicht minimierte Informationen automatisch zu prüfen, und es muss stattdessen sicherstellen, dass die Analysten die Suche nach solchen Informationen aktiv auswählen müssen. Darüber hinaus ist es dem FBI durch RISAA untersagt, Abfragen durchzuführen, die ausschließlich dazu dienen, Beweise für kriminelle Aktivitäten zu finden und zu extrahieren (es sei denn, es besteht berechtigter Grund zu der Annahme, dass sie dazu beitragen könnten, eine Gefahr für Leben oder schwere Körperschäden abzuschwächen oder zu beseitigen, oder wenn dies erforderlich ist, um den Offenlegungspflichten in einem Rechtsstreit nachzukommen).[54] Darüber hinaus ist es dem FBI untersagt, nicht minimierte Daten in Analyseregister aufzunehmen, es sei denn, die betroffene Person ist für eine bestehende nationale Sicherheitsuntersuchung relevant.[55]

Drittens wurden einige Bestimmungen über den Status und die Rolle Amici Curiae vor dem FISC geändert[56]. Die Amici werden als Sachverständige benannt, die das Gericht (und das FISCR) in Fragen im Zusammenhang mit dem Schutz der Privatsphäre und der bürgerlichen Freiheiten unterstützen oder bei der Klärung technologischer Fragen in Bezug auf Anwendungen einer bestimmten Regierung behilflich sind. Während das FISA zuvor verlangte, dass Amici über Fachwissen in den Bereichen Privatsphäre und bürgerliche Freiheiten, Sammlung nachrichtendienstlicher Erkenntnisse, Kommunikationstechnologie oder anderen relevanten Bereiche verfügten, erfordert es nun grundsätzlich Fachwissen in den Bereichen Privatsphäre und bürgerliche Freiheiten und Sammlung nachrichtendienstlicher Erkenntnisse. Das Gericht hatte bereits die Möglichkeit, in allen Fällen, die es für angemessen hielt, einen Amicus zu bestellen, und war dazu verpflichtet, wenn es um eine neue oder bedeutsame Rechtsauslegung ging. Nach der erneuten Genehmigung ist das FISC nun auch verpflichtet, einen Amicus zu benennen, wenn die Genehmigung von Zertifizierungen nach Abschnitt 702 FISA und begleitender Verfahren (z. B. Verfahren für eine zielgenaue Erfassung) ersucht wird, es sei denn, es stellt fest, dass dies nicht angemessen ist oder wahrscheinlich zu einer unangemessenen Verzögerung führen würde.[57] Darüber hinaus kann das Gericht nun entscheiden, einen oder mehrere Amici statt nur eine Person zu ernennen. Ferner wird klargestellt, dass die von den Amici bereitzustellenden Informationen „auf die vom Gericht ermittelten spezifischen Probleme“ beschränkt sein müssen, auch wenn die Bereiche, zu denen sich die Amici äußern können, weiterhin weit gefasst sind (d. h. rechtliche Argumente und Informationen im Zusammenhang mit dem Schutz der Privatsphäre und der bürgerlichen Freiheiten von US-Bürgerinnen und -Bürgern, nachrichtendienstliche Sammlung, Kommunikationstechnologien oder andere relevante Bereiche).

Schließlich wird in Abschnitt 18 RISAA eine „FISA-Reformkommission“ eingesetzt, die sich unter anderem aus Mitgliedern des Kongresses, dem Vorsitz des PCLOB, dem ersten stellvertretenden Direktor des Nationalen Nachrichtendienstes, dem stellvertretenden

[54] Abschnitt 3(a) RISAA.

[55] Abschnitt 3(b) RISAA. Wenn dies aufgrund dringender Umstände erforderlich ist, kann der Direktor des FBI eine Ausnahme von dieser Bestimmung beschließen, die dem Kongress mitgeteilt werden muss.

[56] Zur Klarstellung: Diese Änderungen berühren nicht den Status und die Rolle der Spezialanwälte vor dem Data Protection Review Court (Datenschutzüberprüfungsgericht – DPRC), wie die USA in der Überprüfungssitzung bestätigt haben.

[57] Abschnitt 5(b) RISAA.

Justizminister sowie weiteren vom Kongress zu ernennenden Mitgliedern[58] zusammensetzt, um zusätzliche FISA-Reformen zu empfehlen.

Die Kommission wird die weiteren Entwicklungen in Bezug auf Abschnitt 702 FISA genau verfolgen, auch im Zusammenhang mit den Aufsichtstätigkeiten des PCLOB (siehe unten), der Arbeit der Reformkommission und der bevorstehenden Überprüfung des FISA nach zwei Jahren.

2.2.1.3. Überwachungstätigkeiten in der Praxis: Zahlen und Trends

Der Annual Statistical Transparency Report Regarding the Intelligence Community's Use of National Security Surveillance Authorities for Calendar Year 2023 des ODNI (Jährlicher statistischer Transparenzbericht des ODNI über den Einsatz nationaler Sicherheitsüberwachungsbehörden durch die Intelligence Community für das Kalenderjahr 2023 – veröffentlicht im April 2024)[59] zeigt, dass die Zahl der Ziele nach Abschnitt 702 FISA von 245 073 im Kalenderjahr 2022 auf 268 590 im Kalenderjahr 2023 gestiegen ist. In dem Bericht wird erläutert, dass Schwankungen bei der Zahl der Ziele auf eine Vielzahl von Gründen zurückzuführen sein können, darunter Änderungen der operativen Prioritäten, Weltereignisse, technische Fähigkeiten, Verhalten der Ziele und Veränderungen im Telekommunikationssektor. Aus dem Bericht geht auch hervor, dass keine Nicht-US-Bürgerinnen und -Bürger (im Vergleich zu einem im Jahr 2021 und keinem im Jahr 2022) gemäß Abschnitt 402 FISA (Einsatz von Geräten zur Rufnummernerfassung von ausgehenden und eingehenden Anrufen) ins Visier genommen wurden, während sechs Anordnungen (gegenüber elf Anordnungen in den Jahren 2021 und 2022) für sechs Ziele (gegenüber 13 im Jahr 2021 und elf im Jahr 2022) gemäß Abschnitt 501 FISA (Zugang zu Geschäftsunterlagen von Beförderungsunternehmen, Mietwagenfirmen oder Lagerhäusern) erlassen wurden, die 5 412 eindeutige Kennungen (gegenüber 23 157 im Jahr 2021 und 55 431 im Jahr 2022) betrafen, die für die Übermittlung der aufgrund dieser Anordnungen erhobenen Informationen verwendet wurden.

Aus dem jährlichen Bericht zum Foreign Intelligence Surveillance Act (FISA-Bericht) an den Kongress geht hervor, dass im Kalenderjahr 2023 beim FISC 327 Anträge auf elektronische Überwachung und/oder Durchsuchungen für Auslandsaufklärungszwecke gemäß Abschnitt 105 bzw. 302 FISA gestellt wurden.[60] Die Gesamtzahl der Zielpersonen lag zwischen 500 und 999. In Bezug auf National Security Letters (NSL) ist dem Bericht zu entnehmen, dass 10 115 Anfragen (mit Ausnahme von Anfragen nach reinen Teilnehmerinformationen) nach Informationen über Nicht-US-Bürgerinnen und -Bürger gestellt wurden, die 3 033 verschiedene Nicht-US-Bürgerinnen und -Bürger betrafen.[61]

Mehrere nach dem Datenschutzrahmen zertifizierte Unternehmen (z. B. Google und Meta) machen von der im US-Recht vorgesehenen Möglichkeit Gebrauch, Transparenzberichte zu veröffentlichen, die Aufschluss über die Zahl der FISA- und NSL-Anfragen geben, die sie in

[58] In Abschnitt 18 ist ausdrücklich eine Vertretung von außerhalb des Kongresses vorgeschrieben.
[59] https://www.dni.gov/files/CLPT/documents/2024_ASTR_for_CY2023.pdf.
[60] https://www.justice.gov/nsd/media/1350236/dl?inline.
[61] Diese Zahlen sind im Vergleich zum vorangegangenen Berichtsjahr (2022) weitgehend stabil geblieben. Im Vergleich dazu gab es 317 endgültige Anträge beim FISC auf elektronische Überwachung und/oder Durchsuchungen für Auslandsaufklärungszwecke im Jahr 2022. Die Gesamtzahl der Personen, die von Anordnungen zur elektronischen Überwachung betroffen waren, lag zwischen 0 und 499. Im Jahr 2022 stellte das FBI 9 103 NSL-Anfragen zu Nicht-US-Bürgerinnen und -Bürgern (mit Ausnahme von Anfragen nach reinen Teilnehmerinformationen). Quelle: https://irp.fas.org/agency/doj/fisa/2022rept.pdf.

einem bestimmten Berichtszeitraum erhalten haben. Zum Zeitpunkt der Erstellung dieses Berichts lagen die Statistiken zu FISA-Anfragen nach Juli 2023 noch nicht vor. Beispielsweise hat Google zwischen Juli und Dezember 2023 500 bis 999 NSL-Anfragen erhalten, die 2 000 bis 2 499 Konten betrafen.[62] Meta berichtete, dass es im selben Berichtszeitraum 0 bis 499 NSL-Anfragen erhalten hat, die 500 bis 999 Konten betrafen.[63] Die Zahlen sind in den letzten Jahren relativ stabil geblieben. Um die Transparenz weiter zu erhöhen, veröffentlichen einige Unternehmen (z. B. Google) proaktiv NSL, die sie erhalten haben, sobald die Geheimhaltungsbeschränkungen aufgehoben werden.[64]

2.2.1.4. Sonstige Entwicklungen

Im Rahmen der Vorbereitung der Überprüfung haben mehrere NRO Fragen zu neuen Formen der Datenerfassung von US-Nachrichtendiensten durch den Erwerb von Daten von kommerziellen Unternehmen, insbesondere von Datenvermittlungsunternehmen, aufgeworfen. Sie erklärten, dass die auf dieser Grundlage erhobenen Daten zwar weiterhin im Einklang mit anderen Anforderungen verarbeitet werden müssen, z. B. auch gemäß der EO 12333[65], der Erwerb jedoch außerhalb des Rahmens von FISA und EO 14086 erfolgt.

In diesem Zusammenhang sei daran erinnert, dass jede Art der freiwilligen Weitergabe von Daten an Dritte im Rahmen des Datenschutzrahmens mehreren detaillierten Bedingungen unterliegt. Erstens kann eine zertifizierte Organisation keine Daten an Dritte weitergeben (die nicht als Beauftragter/Auftragsverarbeiter handeln), ohne die betroffenen Personen zu informieren und ihr die Wahl zu lassen.[66] Zweitens dürfen Weitergaben gemäß dem Grundsatz der Verantwortlichkeit für die Weitergabe nur 1) für begrenzte und genau festgelegte Zwecke, 2) auf der Grundlage eines Vertrags zwischen der Organisation, die dem Datenschutzrahmen EU-USA angehört, und dem Dritten und 3) nur durchgeführt werden, wenn dieser Vertrag den Dritten verpflichtet, das gleiche Schutzniveau zu gewährleisten, das durch die Grundsätze garantiert wird.[67]

Darüber hinaus hat die FTC, wie auch in der Überprüfungssitzung erörtert, Durchsetzungsmaßnahmen gegen Datenvermittlungsunternehmen ergriffen, die sensible Verbraucherdaten verkaufen. So erließ die FTC in einem Verfahren gegen X-Mode und dessen Nachfolger Outlogic am 9. Januar 2024 eine Anordnung, mit der dem Unternehmen untersagt wurde, Geolokalisierungsdaten an Dritte zu verkaufen und Daten, die es unrechtmäßig verwendet und weitergegeben hatte, zu löschen. Die Untersuchung der FTC ergab unter anderem, dass das Unternehmen die Privatpersonen nicht vollständig über die Verwendung und den Verkauf ihrer Geolokalisierungsdaten informierte, es versäumte, Maßnahmen zu ergreifen, um Einzelpersonen die Möglichkeit zu geben, Tracking zu verweigern, die Verwendung der Daten zu potenziell diskriminierenden Zwecken gestattete und die Nutzung solcher Informationen durch Dritte nicht einschränkte.[68] Die Kommission geht davon aus, dass die

[62] https://transparencyreport.google.com/user-data/us-national-security.
[63] https://transparency.meta.com/reports/government-data-requests/country/US/.
[64] https://transparencyreport.google.com/user-data/us-national-security.
[65] Siehe z. B. Abschnitt 2.4 der EO 12333 zu Erhebungsmethoden.
[66] Siehe Erwägungsgrund 40 des Angemessenheitsbeschlusses.
[67] Siehe Erwägungsgrund 38 des Angemessenheitsbeschlusses.
[68] https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-order-prohibits-data-broker-x-mode-social-outlogic-selling-sensitive-location-data.

FTC denselben Ansatz verfolgen wird, wenn im Rahmen des Datenschutzrahmens zertifizierte Unternehmen Daten unter Verstoß gegen die oben genannten Bestimmungen weitergeben.

Schließlich sei darauf hingewiesen, dass das ODNI im Mai 2024 den Intelligence Community Policy Framework for Commercially Available Information[69] (Strategierahmen der Intelligence Community für kommerziell verfügbare Informationen) herausgegeben hat. Dieser Rahmen enthält eine Reihe von Grundsätzen und Anforderungen, die Nachrichtendienste bei der Erhebung und bei der Nutzung von Daten im Zusammenhang mit einer Handelstransaktion befolgen sollten, unter anderem um die Risiken für die Privatsphäre und die bürgerlichen Freiheiten so gering wie möglich zu halten.

2.2.2. Unabhängige Aufsicht

Die Tätigkeiten der US-Nachrichtendienste unterliegen der Aufsicht verschiedener Stellen, darunter Datenschutz- und Bürgerrechtsbeauftragte, Generalinspekteure, der Kongress und das PCLOB. Insbesondere verlangt die EO 14086, dass jeder Nachrichtendienst über hochrangige Beamte für Recht, Aufsicht und Compliance verfügt, um die Einhaltung der geltenden US-Rechtsvorschriften zu gewährleisten. Diese Aufsichtsfunktion wird von Beauftragten, die für die Einhaltung der Vorschriften zuständig sind, sowie von den Datenschutz- und Bürgerrechtsbeauftragen und den Generalinspekteuren wahrgenommen.[70] Sie müssen die Tätigkeiten im Rahmen der Signalaufklärung regelmäßig überwachen und dafür sorgen, dass Verstöße abgestellt werden. Die Nachrichtendienste müssen diesen Beamten Zugang zu allen einschlägigen Daten gewähren, damit sie ihre Aufsichtsaufgaben wahrnehmen können, und dürfen keine Maßnahmen treffen, die ihre Aufsichtstätigkeit behindern oder unangemessen beeinflussen.

Der General Counsel of the Office of the Intelligence Community Inspector General (Generalberater des Generalinspektors des Büros der Intelligence Community – ICIG) im ODNI, der über eine umfassende Zuständigkeit für die gesamte Intelligence Community verfügt und befugt ist, Beschwerden oder Informationen über mutmaßliches rechtswidriges Verhalten oder Amtsmissbrauch zu untersuchen, nahm an der Überprüfungssitzung teil. Er bestätigte, dass der ICIG im Rahmen seiner Aufsichtstätigkeit systematisch die Einhaltung der EO 14086 überprüft. Ferner verwies er auf die jüngsten Aufsichtstätigkeiten anderer Generalinspekteure der Intelligence Community, die in regelmäßigen Berichten genauer dargelegt werden. So informierte der Generalinspektor der NSA in seinem halbjährlichen Bericht an den Kongress für April bis September 2023[71] über eine Bewertung eines internen

[69] https://www.dni.gov/files/ODNI/documents/CAI/Commercially-Available-Information-Framework-May2024.pdf. Die Nachrichtendienste müssen den Rahmen seit August 2024 einhalten.

[70] Jeder Nachrichtendienst verfügt über einen Generalinspekteur, der rechtlich unabhängig ist und für die Durchführung von Überprüfungen und Untersuchungen im Zusammenhang mit den von der jeweiligen Behörde für Zwecke der nationalen Sicherheit durchgeführten Tätigkeiten zuständig ist. Sie haben Zugang zu allen relevanten (auch als Verschlusssache eingestuften) Materialien, erforderlichenfalls durch Anordnungen, und können aussagen. Die Generalinspekteure leiten Fälle mutmaßlicher strafrechtlicher Verstöße an die Strafverfolgungsbehörden weiter und geben den Leitern der Nachrichtendienste Empfehlungen für Abhilfemaßnahmen. Obwohl ihre Empfehlungen nicht verbindlich sind, werden ihre Berichte, einschließlich über Folgemaßnahmen (oder deren Fehlen), in der Regel veröffentlicht und dem Kongress übermittelt. Siehe hierzu Fußnote 136 des Angemessenheitsbeschlusses zur Rolle des Generalinspekteurs.

[71] https://oig.nsa.gov/reports/Article/3609957/semiannual-report-to-congress-1-april-2023-to-30-september-2023/.

Kontrollrahmens der NSA für Entscheidungen und Anfragen zur Zielerfassung. Er kam zu dem Schluss, dass dieser Rahmen ordnungsgemäß funktioniert und die Einhaltung der Gesetze, Richtlinien und politischen Maßnahmen zum Schutz der bürgerlichen Freiheiten und der Privatsphäre sicherstellt. In demselben Bericht wird auch eine Untersuchung erwähnt, bei der der Missbrauch eines Signalaufklärungsinstruments für unbefugte Zwecke durch einen NSA-Mitarbeiter aufgedeckt wurde.

Nach der EO 14086 ist das PCLOB[72] mit spezifischen Aufsichtsfunktionen betraut[73]. Der Vorsitz des PCLOB und seine drei Mitglieder nahmen an der Überprüfungssitzung teil und teilten mit, dass das PCLOB die Nachrichtendienste im April 2023 zu den Entwürfen ihrer Strategien und Verfahren zur Umsetzung der EO 14086 beraten hat und zur Benennung der Richter und Spezialanwälte des DPRC konsultiert worden war. Darüber hinaus leitete die Stelle ein Aufsichtsprojekt ein, um 1) die Umsetzung der aktualisierten Strategien und Verfahren zu überprüfen, die von den Nachrichtendiensten angenommen wurden, um sicherzustellen, dass sie mit der EO im Einklang stehen, und 2) eine jährliche Überprüfung der Funktionsweise der neuen Beschwerdestelle (siehe unten) durchzuführen.[74] Die PCLOB-Mitglieder bestätigten, dass es beabsichtigt, beide Überprüfungen in naher Zukunft durchzuführen. In Bezug auf Rechtsbehelfe erklärten sie, dass sich die Überprüfung des PCLOB auf die Strategien und Verfahren zur Einrichtung der Stelle konzentrieren wird, wenn keine Beschwerden eingehen.

In Bezug auf andere Aufsichtstätigkeiten legte das PCLOB am 28. September 2023 einen Bericht zu Abschnitt 702 FISA vor.[75] Dieser Bericht ist eine Folgemaßnahme zu einem früheren Bericht aus dem Jahr 2014 und enthält aktualisierte sachliche und rechtliche Informationen über die Funktionsweise von Überwachungsprogrammen nach Abschnitt 702 FISA. Der Bericht enthält auch Empfehlungen zur Einhaltung der geltenden Anforderungen durch die Nachrichtendienste und Vorschläge an den Kongress, mehrere Aspekte von Abschnitt 702 FISA im Zusammenhang mit seiner erneuten Genehmigung weiter zu stärken (u. a. durch Kodifizierung der in der EO 14086 aufgeführten legitimen Ziele für Überwachungstätigkeiten).[76] Während der Überprüfungssitzung teilte das PCLOB mit, dass es bald Antworten von Nachrichtendiensten zur Umsetzung seiner Empfehlungen erhalten wird, die in einen künftigen Folgebericht einfließen werden. Weitere laufende Aufsichtsprojekte betreffen die Bekämpfung des Terrorismus im Inland und seine Auswirkungen auf die

[72] Das PCLOB ist eine unabhängige Stelle, die mit Aufgaben im Bereich der Terrorismusbekämpfung und deren Umsetzung betraut ist, wobei der Schutz der Privatsphäre und der bürgerlichen Freiheiten im Vordergrund steht. Sie kann auf alle relevanten Informationen (einschließlich Verschlusssachen) zugreifen, Anhörungen durchführen und Zeugenaussagen hören. Sie kann Empfehlungen an die Strafverfolgungsbehörden und Nachrichtendienste richten und erstattet dem Kongress und dem Präsidenten regelmäßig Bericht. Die Berichte werden so weit wie möglich öffentlich zugänglich gemacht.

[73] https://documents.pclob.gov/prod/Documents/EventsAndPress/834a1977-f420-4b2a-ae93-8a522b2c7c74/Trans-Atlantic%20Data%20Privacy%20Framework%20EO%20press%20release%20(FINAL)%20-%20Completed%20508%20-%2010202022.pdf.

[74] https://www.pclob.gov/OversightProjects/Details/1115.

[75] https://documents.pclob.gov/prod/Documents/OversightReport/8ca320e5-01d3-4d6a-8106-3384aad6ff31/2023%20PCLOB%20702%20Report%20-%20Nov%2017%202023%20-%201446.pdf.

[76] Die Kommission stellt fest, dass einige dieser Empfehlungen in das RISAA aufgenommen wurden, darunter die Empfehlung zur „about collection“ oder die Empfehlung zur Stärkung der Rolle der FISC-Sachverständigen (Amici).

Privatsphäre und die bürgerlichen Freiheiten sowie die Erhebung von Open-Source- oder kommerziell verfügbaren Daten durch das FBI.[77]

Schließlich brachten die im Rahmen der Überprüfung konsultierten NRO ihre Besorgnis darüber zum Ausdruck, dass die Amtszeit mehrerer PCLOB-Mitglieder in naher Zukunft enden wird und das PCLOB möglicherweise nicht beschlussfähig sein könnte. Insbesondere ist die Amtszeit des Vorsitzes abgelaufen, und der Zeitraum, in dem er kommissarisch tätig sein kann, endet im Januar 2025; gleichzeitig ist ein weiterer Sitz nicht besetzt, und ein dritter Sitz wird ebenfalls im Januar nächsten Jahres frei. In der Überprüfungssitzung erklärten die Mitglieder, dass sie nicht erwarten, dass das PCLOB seine Beschlussfähigkeit verliert, da für den derzeit unbesetzten Sitz bereits eine Nominierung erfolgt ist (und die Bestätigung durch den Senat aussteht).[78] Sie betonten ferner, dass selbst wenn der Ausschuss seine Beschlussfähigkeit verlieren würde, dies seine Fähigkeit, weiterhin Aufsichtsprojekte durchzuführen, nicht beeinträchtigen würde. Angesichts der wichtigen Rolle des PCLOB bei der Überprüfung der Umsetzung der EO 14086 wird die Kommission den Stand künftiger freier Sitze und Nominierungen/Ernennungen aufmerksam verfolgen.

2.2.3. Rechtsbehelfe

Mit der EO 14086, ergänzt durch eine Verordnung des Justizministers, wurde eine neue Beschwerdestelle eingeführt, um qualifizierte Beschwerden von Privatpersonen über US-amerikanische Signalaufklärungstätigkeiten zu bearbeiten und zu klären.[79] Jede Person in der EU hat das Recht, bei der Beschwerdestelle eine Beschwerde wegen einer mutmaßlichen Verletzung des US-Rechts im Bereich der signalerfassenden Aufklärung (z. B. EO 14086 Abschnitt 702 FISA, EO 12333) im Hinblick auf die Übermittlung von personenbezogenen Daten in die USA einzureichen, die ihre Interessen in Bezug auf Privatsphäre und bürgerliche Freiheiten beeinträchtigt. Privatpersonen können eine Beschwerde bei einer Datenschutzbehörde in einem EU-Mitgliedstaat einreichen, die die Beschwerde über das Sekretariat des EDSA an die Beschwerdestelle weiterleitet. Die Beschwerdestelle besteht aus zwei Ebenen, wobei die erste Prüfung von Beschwerden durch den ODNI CLPO durchgeführt wird und Privatpersonen die Möglichkeit haben, die Entscheidung des CLPO vor einem unabhängigen DPRC anzufechten. Nach Abschluss der Überprüfung durch ODNI CLPO oder DPRC werden die Privatpersonen über die nationale Behörde informiert, dass „bei der Überprüfung entweder keine einschlägigen Verstöße festgestellt wurden oder der ODNI CLPO/das DPRC eine Feststellung getroffen hat, die angemessene Abhilfemaßnahmen erfordert“. Die Beschlüsse des ODNI CLPO und des DPRC sind für Nachrichtendienste verbindlich.

Seit der Annahme des Angemessenheitsbeschlusses wurden weitere Schritte unternommen, damit die Beschwerdestelle voll funktionsfähig wird.

Was die Einrichtung des DPRC betrifft, so wurden am 14. November 2023 acht Richter (d. h. zwei Richter mehr als die erforderliche Mindestanzahl nach der EO 14086, ergänzt durch die Vorschriften des Justizministers in 28 C.F.R. § 201.3(a)) zum Gericht berufen.[80] Sie wurden

[77] https://www.pclob.gov/OversightProjects.
[78] https://documents.pclob.gov/prod/Documents/EventsAndPress/deb9cd13-12af-4250-998e-a520a2419a6b/PCLOB%20nominee%20press%20release%206-13-24.pdf.
[79] Erwägungsgründe 176-194 des Mehrheitsbeschlusses.
[80] https://www.justice.gov/opa/pr/attorney-general-merrick-b-garland-announces-judges-data-protection-review-court.

auf der Grundlage der in der EO 14086 festgelegten Kriterien und im Einklang mit dem darin festgelegten Verfahren, auch nach Konsultation u. a. des PCLOB, ernannt.[81] Dazu gehören ehemalige Richter des Federal District Court (Bundesbezirksgericht) und des Court of Appeals (Berufungsgericht), ein ehemaliger US-Justizminister und ein ehemaliges Mitglied des PCLOB. Wie in der EO gefordert, verfügen mindestens die Hälfte der Richter über vorherige juristische Erfahrung. Darüber hinaus wurden im April 2024 zwei Spezialanwälte – Rechtspraktiker, die sowohl auf dem Gebiet der Privatsphäre als auch der nationalen Sicherheit tätig sind – ernannt, um die Interessen von Privatpersonen vor dem DPRC zu vertreten. In der Überprüfungssitzung wurde bestätigt, dass alle Richter und Sonderanwälte die höchste Sicherheitsberechtigung erhalten haben und daher bei der Wahrnehmung ihrer Aufgaben für das DPRC Zugang zu Verschlusssachen haben können. Das DPRC hatte auch eine Reihe häufig gestellter Fragen veröffentlicht, die weitere Informationen über seine Rolle, Unabhängigkeit und Funktionsweise enthalten.[82]

Was die Bearbeitung von Beschwerden betrifft, so hat das ODNI am 6. Dezember 2022 die Intelligence Community Directive 126 (Richtlinie zur Intelligence Community 126) angenommen, in der verschiedene Aspekte des Verfahrens für die Untersuchung von und Entscheidung über Beschwerden im Einzelnen geregelt werden (durch Festlegung von Fristen, Einrichtung eines sicheren elektronischen Speichers und von Kommunikationskanälen, Verpflichtung des CLPO und der Intelligence Community zur Zusammenarbeit mit dem PCLOB im Rahmen der jährlichen Überprüfung der Beschwerdestelle usw.).[83] Diese Richtlinie gilt für die gesamte US-Intelligence Community und wurde durch weitere interne Verfahren ergänzt, die von einzelnen Nachrichtendiensten für ihre Zusammenarbeit mit dem ODNI CLPO im Zusammenhang mit der Bearbeitung einer Beschwerde angenommen wurden (z. B. Entwicklung eines sicheren Speichers für den Austausch von Beschwerden und reaktionsfähigen Dokumenten sowie sichere Kommunikation zwischen den zuständigen Stellen). Das DPRC wird in den kommenden Monaten auch detailliertere Vorschriften für die Bearbeitung von Beschwerden und andere Verfahrensaspekte erlassen.

In der Europäischen Union und den Vereinigten Staaten wurden eine Reihe zusätzlicher Maßnahmen ergriffen, um die breite Öffentlichkeit zu informieren und die Einreichung und Bearbeitung von Beschwerden zu erleichtern. Dazu gehören die Annahme eines Informationsvermerks über die neue Beschwerdestelle[84], eines Musters für Beschwerdeformulare (das von allen Datenschutzbehörden in ihre Landessprachen übersetzt und veröffentlicht werden soll)[85] und einer Geschäftsordnung, die die Zusammenarbeit zwischen den nationalen Aufsichtsbehörden und dem Sekretariat des EDSA regelt[86], durch den

[81] Abschnitt 3(d)(A) EO 14086.
[82] https://www.justice.gov/opcl/dprc-resources.
[83] https://www.dni.gov/files/documents/ICD/ICD_126-Implementation-Procedures-for-SIGINT-Redress-Mechanism.pdf.
[84] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/information-note-data-protection-framework-redress_de.
[85] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/template-complaint-form-us-office-director-national_de.
[86] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/rules-procedure-data-protection-framework-redress_de.

EDSA. Ebenso veröffentlichte das ODNI häufig gestellte Fragen und ein Merkblatt zur neuen Beschwerdestelle und beteiligte sich an Sensibilisierungsmaßnahmen.[87]

Darüber hinaus haben der EDSA und die zuständigen US-Behörden im vergangenen Jahr bei mehreren operativen Aspekten eng zusammengearbeitet. Wie in der Überprüfungssitzung bestätigt wurde, richteten sie insbesondere einen verschlüsselten Kommunikationskanal ein, um Beschwerden nationaler Behörden in der EU an das EDSA-Sekretariat, vom EDSA-Sekretariat an den ODNI CLPO und an das Office of Privacy and Civil Liberties (Büro für Datenschutz und Bürgerrechte – OPCL) des Justizministeriums sowie zwischen dem ODNI CLPO und anderen Behörden auf US-Seite (z. B. dem DPRC) zu übermitteln. Darüber hinaus erläuterte der ODNI CLPO, dass weitere interne Verfahren für die Zusammenarbeit einzelner Nachrichtendienste mit dem ODNI CLPO in Bezug auf die Bearbeitung von Beschwerden eingeführt wurden.

Schließlich teilte das OPCL, das für das DPRC administrative Unterstützung erbringt, auch mit, dass das DPRC im Rahmen seiner eigenen Haushaltslinie tätig ist und über die erforderlichen Einrichtungen zur Wahrnehmung seiner Aufgaben verfügt, einschließlich gesicherter Computer und Laptops, Telefone usw. Darüber hinaus hat das Handelsministerium, wie in der EO 14086 gefordert, die erforderlichen Maßnahmen ergriffen, unter anderem durch die Einrichtung eines verschlüsselten Kommunikationskanals mit dem ODNI CLPO, um eine Liste aller eingegangenen qualifizierten Beschwerden zu führen. Das Handelsministerium wird sich regelmäßig mit dem ODNI CLPO in Verbindung setzen, um zu klären, ob Informationen im Zusammenhang mit einer Einzelbeschwerde freigegeben wurden. In diesem Fall setzt das Handelsministerium die betroffene Person davon in Kenntnis, damit sie Zugang zu diesen Informationen erhalten kann.

Zum Zeitpunkt der Überprüfungssitzung waren keine Beschwerden bei den EU-Aufsichtsbehörden eingegangen und die neue Beschwerdestelle war noch nicht tätig geworden.

3. SCHLUSSFOLGERUNG

Auf der Grundlage der bei dieser ersten Überprüfung gesammelten Informationen kommt die Kommission zu dem Schluss, dass die US-Behörden die erforderlichen Strukturen und Verfahren eingerichtet haben, um sicherzustellen, dass der Datenschutzrahmen wirksam funktioniert. In diesem Zusammenhang würdigt die Kommission die sehr gute Zusammenarbeit mit den US-Behörden bei der Durchführung der Überprüfung.

Während sich diese erste Überprüfung natürlich auf die Kontrolle konzentrierte, ob alle konstitutiven Elemente des Rahmens vorhanden sind, erweisen sich die Erfahrungen mit der praktischen Anwendung der Garantien, die sowohl für die Verarbeitung von Daten durch zertifizierte Unternehmen als auch für den Zugang zu Daten durch Behörden gelten, nach nur einem Jahr des Betriebs zwangsläufig als begrenzt. Die Kommission wird daher die einschlägigen Entwicklungen in den nächsten Monaten und Jahren genau beobachten und dabei besonderes Augenmerk auf 1) die anstehenden Berichte des PCLOB über die Umsetzung der EO 14086 und die Funktionsweise der Beschwerdestelle der Signalaufklärung, insbesondere

[87] https://www.dni.gov/files/CLPT/documents/Fact_Sheets/The_Role_of_the_ODNI_CLPO_FAQs.pdf und https://www.dni.gov/files/CLPT/documents/Fact_Sheets/Data_Privacy_Framework.pdf.

des DPRC, 2) mögliche weitere Änderungen von Abschnitt 702 FISA und 3) die Nominierung und Ernennung von Mitgliedern des PCLOB zur Besetzung frei werdender Sitze legen.

Um eine kontinuierliche und wirksame Funktionsweise zu gewährleisten, hält die Kommission ferner Folgendes für wichtig:

- Wie in der Überprüfungssitzung angekündigt, macht das Handelsministerium umfassenderen Gebrauch von den verschiedenen im Datenschutzrahmen vorgesehenen Instrumenten zur Überwachung der Einhaltung der Grundsätze durch die Unternehmen und zur Aufdeckung falscher Angaben zur Beteiligung,
- die FTC entwickelt ihren proaktiven Ansatz bei der Untersuchung und Durchsetzung der Einhaltung der Grundsätze des Datenschutzrahmens durch zertifizierte Unternehmen weiter, und
- das Handelsministerium, die FTC und die EU-Datenschutzbehörden entwickeln gemeinsame Leitlinien zu Kernanforderungen im Rahmen der Grundsätze des Datenschutzrahmens, z. B. in Bezug auf Personaldaten und Weitergabe.

Angesichts dieses Ergebnisses der Überprüfung und wie in Erwägungsgrund 211 des Angemessenheitsbeschlusses vorgesehen, hält es die Kommission für angemessen, die nächste regelmäßige Überprüfung nach drei Jahren durchzuführen. So sollte es möglich sein, mehr Erfahrungen mit der praktischen Anwendung des Datenschutzrahmens zu sammeln und die oben genannten anstehenden Entwicklungen zu berücksichtigen. Die Kommission wird daher gemäß Artikel 3 Absatz 4 des Angemessenheitsbeschlusses den EDSA und den nach Artikel 93 Absatz 1 der Datenschutz-Grundverordnung eingesetzten Ausschuss zur Häufigkeit künftiger Überprüfungen konsultieren.