Stellungnahme 5/2023 zum Entwurf eines Durchführungsbeschlusses der Europäischen Kommission über die Angemessenheit des Schutzes personenbezogener Daten im Rahmen des Datenschutzrahmens EU-USA

Angenommen am 28. Februar 2023

Zusammenfassung

Am 13. Dezember 2022 veröffentlichte die Europäische Kommission den Entwurf eines Angemessenheitsbeschlusses („Beschlussentwurf") mit Anhängen. Diese enthalten einen neuen Rahmen für den transatlantischen Austausch personenbezogener Daten, den Datenschutzrahmen EU-USA („DSR"), der an die Stelle des früheren EU-US-Datenschutzschilds treten soll, der mit Urteil des Europäischen Gerichtshofs („EuGH") in der Rechtssache Schrems II vom 16. Juli 2020 für ungültig erklärt wurde. Zentraler Bestandteil des DSR sind die Grundsätze des Datenschutzrahmens EU-USA, einschließlich der ergänzenden Grundsätze (im Folgenden zusammen „DSR-Grundsätze").

Gemäß Artikel 70 Absatz 1 Buchstabe s der Verordnung (EU) 2016/679[1] des Europäischen Parlaments und des Rates (im Folgenden „DSGVO") ersuchte die Kommission den Europäischen Datenschutzausschuss (im Folgenden „EDSA") um eine Stellungnahme zu dem Beschlussentwurf.

Auf der Grundlage des Beschlussentwurfs bewertete der EDSA die Angemessenheit des in den USA gewährten Schutzniveaus. Der EDSA bewertete sowohl die gewerblichen Aspekte als auch den Zugang zu und die Verwendung von personenbezogenen Daten, die von Behörden in der EU in die USA übermittelt werden.

Der EDSA trug dem geltenden Rechtsrahmen der EU für den Datenschutz gemäß der DSGVO sowie den Grundrechten auf Privatleben und Datenschutz Rechnung, die in den Artikeln 7 und 8 der Charta der Grundrechte der Europäischen Union und in Artikel 8 der Europäischen Menschenrechtskonvention verankert sind. Er berücksichtigte ferner das in Artikel 47 der Charta verankerte Recht auf einen wirksamen Rechtsbehelf und ein unparteiisches Gericht sowie die Rechtsprechung zu den verschiedenen Grundrechten.

Darüber hinaus hat der EDSA die Anforderungen der vom EDSA angenommenen Referenzgrundlage für Angemessenheit[2] berücksichtigt.

Das Hauptziel des EDSA besteht darin, gegenüber der Kommission eine Stellungnahme zur Angemessenheit des Schutzniveaus für Personen abzugeben, deren personenbezogene Daten in die USA übermittelt werden. Es ist darauf hinzuweisen, dass der EDSA nicht erwartet, dass der US-Datenschutzrahmen das europäische Datenschutzrecht nachbildet.

Der EDSA weist jedoch darauf hin, dass Artikel 45 DSGVO und die Rechtsprechung des EuGH verlangen, dass die Rechtsvorschriften des Drittstaats betroffenen Personen ein Schutzniveau bieten, das dem in der EU garantierten Schutzniveau der Sache nach gleichwertig ist, damit davon ausgegangen werden kann, dass sie ein angemessenes Schutzniveau bieten.

1.1. Allgemeine Datenschutzaspekte

Im DSR ist vorgesehen, dass die Einhaltung der DSR-Grundsätze durch DSR-Organisationen in einigen Fällen eingeschränkt werden kann (z. B. in dem Umfang, der erforderlich ist, um einer gerichtlichen Anordnung nachzukommen oder um dem öffentlichen Interesse gerecht zu werden). Um die Auswirkungen dieser Ausnahmen auf das Schutzniveau für betroffene Personen besser ermitteln zu

[1] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. L 119 vom 4.5.2016, S. 1.

[2] Artikel-29-Datenschutzgruppe, Referenzgrundlage für Angemessenheit, WP 254 rev.01, 28. November 2017, zuletzt überarbeitet und angenommen am 6. Februar 2018, gebilligt vom EDSA am 25. Mai 2018 (im Folgenden „Referenzgrundlage für Angemessenheit").

können, empfiehlt der EDSA der Kommission, in dem Beschlussentwurf den Anwendungsbereich der Ausnahmen einschließlich der nach US-Recht anwendbaren Garantien klarzustellen.

Der EDSA stellt fest, dass es aufgrund der Struktur der Anhänge und ihrer Nummerierung schwierig ist, Informationen zu finden und darauf zu verweisen. Dies trägt zu einer insgesamt komplexen Darstellung des neuen Rahmens bei, der in seinen Anhängen Dokumente von unterschiedlicher rechtlicher Bedeutung zusammenfasst, und ist möglicherweise einem guten Verständnis der DSR-Grundsätze durch betroffene Personen, DSR-Organisationen und Datenschutzbehörden der EU nicht förderlich. Der EDSA betont ferner, dass Terminologie im gesamten DSR kohärent verwendet werden sollte. Ebenso fehlt es an Begriffsbestimmungen für einige wesentliche Ausdrücke.[3]

Der EDSA begrüßt die Aktualisierungen der DSR-Grundsätze[4], die den verbindlichen Rechtsrahmen für DSR-Organisationen bilden werden, stellt jedoch fest, dass die DSR-Grundsätze, an die sich die DSR-Organisationen halten müssen, trotz einiger Änderungen und zusätzlicher Erläuterungen in den Erwägungsgründen des Beschlussentwurfs im Wesentlichen unverändert gegenüber den Grundsätzen des Datenschutzschilds (auf die sich die gemeinsamen jährlichen Überprüfungen der Artikel-29-Datenschutzgruppe („WP29“) und des EDSA stützten) sind. Die DSR-Grundsätze entsprechen ferner weitgehend denen des Entwurfs des Datenschutzschilds, auf den die Artikel-29-Datenschutzgruppe ihre Stellungnahme aus dem Jahr 2016[5] stützte. In Bezug auf die im Wesentlichen unveränderten DSR-Grundsätze hält der EDSA es nicht für erforderlich, alle zuvor von der Artikel-29-Datenschutzgruppe vorgebrachten Bemerkungen zu wiederholen. Der EDSA hat beschlossen, sich auf spezifische Aspekte zu konzentrieren, die er heute angesichts der Entwicklung des rechtlichen und technologischen Umfelds für noch wichtiger hält.

So stellt der EDSA beispielsweise fest, dass einige Bedenken, die zuvor von der Artikel-29-Datenschutzgruppe und dem EDSA im Zusammenhang mit den Grundsätzen des Datenschutzschilds angesprochen wurden, nach wie vor bestehen. Diese betreffen insbesondere die Rechte betroffener Personen (z. B. einige Ausnahmen vom Auskunftsrecht sowie die Fristen und Modalitäten für das Widerspruchsrecht), das Fehlen wichtiger Definitionen, die mangelnde Klarheit in Bezug auf die Anwendung der DSR-Grundsätze auf Auftragsverarbeiter und die weit gefasste Ausnahme für öffentlich zugängliche Informationen.[6]

Der EDSA möchte ferner erneut darauf hinweisen, dass das Schutzniveau für Personen, deren Daten übermittelt werden, nicht durch Weiterleitungen durch den ursprünglichen Empfänger der übermittelten Daten untergraben werden darf.[7] Der EDSA fordert die Kommission erneut auf, klarzustellen, dass die Garantien, die der ursprüngliche Empfänger dem Einführer in dem Drittland auferlegt, vor einer Weiterübermittlung im Rahmen des DSR im Lichte der Rechtsvorschriften des Drittlandes wirksam sein müssen.

Rasche Entwicklungen im Bereich der automatisierten Entscheidungsfindung und der Erstellung von Profilen – zunehmend mithilfe von KI-Technologien – erfordern besondere Aufmerksamkeit. Der EDSA

[3] Dies gilt für die Ausdrücke „Verarbeiter“ und „Auftragsverarbeiter“. Darüber hinaus muss mit den US-Behörden noch der Begriff der „Personaldaten“ erörtert werden.
[4] Zum Beispiel die Klarstellung, dass es sich bei verschlüsselten Daten um personenbezogene Daten handelt.
[5] Stellungnahme 01/2016 der Artikel-29-Datenschutzgruppe zum Entwurf eines Angemessenheitsbeschlusses zum EU-US-Datenschutzschild, angenommen am 13. April 2016 (im Folgenden „WP29, Stellungnahme 01/2016“).
[6] EU-US-Datenschutzschild – Dritte jährliche gemeinsame Überprüfung, Bericht des EDSA, angenommen am 12. November 2019, Nr. 11.
[7] DSGVO-Referenzgrundlage für Angemessenheit, 3.A.9.

begrüßt die Bezugnahmen der Kommission auf spezifische Garantien, die in verschiedenen Bereichen in den einschlägigen US-Rechtsvorschriften vorgesehen sind.[8] Das Schutzniveau für natürliche Personen scheint jedoch je nachdem, ob überhaupt sektorspezifische Vorschriften auf die jeweilige Situation Anwendung finden, und wenn ja, welche, unterschiedlich auszufallen. Der EDSA ist der Auffassung, dass besondere Vorschriften für die automatisierte Entscheidungsfindung erforderlich sind, um ausreichende Garantien zu bieten, einschließlich des Rechts der Person, die zugrunde liegende Logik zu kennen, die Entscheidung anzufechten und ein menschliches Eingreifen zu erwirken, wenn die Entscheidung sie erheblich beeinträchtigt.

Der EDSA weist auf die Bedeutung einer wirksamen Aufsicht über den DSR und seiner wirksamen Durchsetzung hin und ist der Auffassung, dass Konformitätsprüfungen in Bezug auf substanziellere Anforderungen von entscheidender Bedeutung sind. Diese Aspekte werden vom EDSA genau überwacht, auch im Rahmen der regelmäßigen Überprüfungen. Der EDSA nimmt die erneuerten Zusagen zur Kenntnis, die in den Schreiben der Kartellbehörde (Federal Trade Commission, im Folgenden „FTC")[9] und des Verkehrsministeriums (Department of Transportation, im Folgenden „DoT")[10] in Bezug auf die Durchsetzung gemacht wurden, z. B. im Hinblick auf die Priorisierung der Untersuchung mutmaßlicher Verstöße gegen den DSR.

Der EDSA stellt fest, dass betroffenen Personen aus der EU sieben Rechtsmittelwege zur Verfügung stehen, wenn ihre personenbezogenen Daten unter Verstoß gegen den DSR verarbeitet werden. Diese Rechtsbehelfsverfahren entsprechen denen des früheren Datenschutzschilds, zu denen sich die Artikel-29-Datenschutzgruppe geäußert hatte.[11] Die Wirksamkeit dieser Rechtsbehelfsverfahren wird vom EDSA genau überwacht, auch im Rahmen der regelmäßigen Überprüfungen.

1.2. Zugang zu und Verwendung von aus der Europäischen Union übermittelten personenbezogenen Daten durch Behörden in den USA

In ihrem Beschlussentwurf kommt die Europäische Kommission zu dem Schluss, dass „jeder im öffentlichen Interesse, insbesondere für Zwecke der Strafverfolgung und der nationalen Sicherheit, erfolgende Eingriff durch US-Behörden in die Grundrechte von Personen, deren personenbezogene Daten gemäß dem Datenschutzrahmen EU-USA aus der Union in die Vereinigten Staaten übermittelt werden, auf das zur Erreichung des betreffenden legitimen Ziels unbedingt erforderliche Maß beschränkt wird und dass ein wirksamer Rechtsschutz gegen solche Eingriffe besteht".[12]

Zu ihrer Schlussfolgerung gelangt die Europäische Kommission nach einer umfassenden Bewertung der Executive Order 14086 Enhancing Safeguards for United States Signals Intelligence Activities (Durchführungsverordnung über die Verbesserung der Garantien für signalerfassende Aufklärungstätigkeiten der USA) (EO 14086). Die EO 14086 wurde vom amerikanischen Präsidenten am 7. Oktober 2022 nach Verhandlungen zwischen der Europäischen Kommission und der US-Regierung unterzeichnet, nachdem der Gerichtshof der Europäischen Union (EuGH) den früheren Angemessenheitsbeschluss betreffend den sogenannten Datenschutzschild für ungültig erklärt hatte.

Der EDSA würde es begrüßen, wenn Bedingung nicht nur für das Inkrafttreten, sondern auch für die Annahme des Beschlusses unter anderem die Annahme aktualisierter Strategien und Verfahren zur Umsetzung der EO 14086 durch alle US-Nachrichtendienste wäre. Der EDSA empfiehlt der

[8] Beschlussentwurf, Erwägungsgrund 35.
[9] Beschlussentwurf, Anhang IV.
[10] Beschlussentwurf, Anhang V.
[11] Siehe insbesondere WP29, Stellungnahme 01/2016, Abschnitt 2.2.6 Buchstabe a.
[12] Beschlussentwurf, Erwägungsgrund 195.

Kommission, diese aktualisierten Strategien und Verfahren zu bewerten und diese Bewertung dem EDSA mitzuteilen.

In Bezug auf den Zugang staatlicher Stellen zu personenbezogenen Daten, die in die USA übermittelt wurden, konzentrierte sich der EDSA bei seiner Analyse auf die Bewertung der neuen EO 14086, da mit dieser Durchführungsverordnung die vom EuGH in seinem Schrems-II-Urteil, mit dem er den früheren Angemessenheitsbeschluss für ungültig erklärte, festgestellten Defizite wirksam angegangen und behoben werden sollen.

Der EDSA erkennt an, dass der US-Rechtsrahmen für signalerfassende Aufklärungstätigkeiten durch die Annahme der EO 14086 geändert wurde, und betrachtet die in dieser Durchführungsverordnung enthaltenen zusätzlichen Garantien als erhebliche Verbesserung. Mit der EO 14086 werden die Begriffe der Erforderlichkeit und der Verhältnismäßigkeit in den US-Rechtsrahmen für die Signalaufklärung eingeführt und wird für den Fall, dass die EU als zugelassene Organisation der regionalen Wirtschaftsintegration benannt werden sollte, ein neues Rechtsbehelfsverfahren für EU-Bürger geschaffen. Nach Ansicht des EDSA ist das neue Rechtsbehelfsverfahren deutlich besser als das frühere sogenannte Ombudspersonverfahren im Rahmen des Datenschutzschilds. Im Gegensatz zum früheren Rechtsrahmen, der, wie der EuGH ausdrücklich festgestellt hat, keine Rechte für EU-Bürger begründete, werden mit der neuen EO 14086 solche Ansprüche geschaffen, und sie bietet mehr Garantien für die Unabhängigkeit des Data Protection Review Court (Datenschutzüberprüfungsgericht) und wirksamere Befugnisse zur Abstellung von Verstößen.

Beim Vergleich der in der EO 14086 enthaltenen zusätzlichen Garantien mit dem, was der EDSA zu den wesentlichen europäischen Garantien (EEG) als dem auf der Grundlage der Rechtsprechung des EuGH und des Europäischen Gerichtshofs für Menschenrechte (EGMR) ausgearbeiteten Standard formuliert hat, hat der EDSA in seiner Bewertung immer noch eine Reihe von Punkten ermittelt, die zusätzliche Klarstellungen erfordern oder Anlass zu Bedenken geben. Diese Punkte zeigen, dass der EDSA zwar seine Stellungnahme auf das Schrems-II-Urteil gestützt hat, der Umfang der Bewertung des EDSA jedoch zwangsläufig Erwägungen umfasst, die über die spezifischen Feststellungen im Schrems-II-Urteil hinausgehen.

Der EDSA hält eine weitere Klärung von Fragen für erforderlich, insbesondere in Bezug auf die „vorübergehende Sammelerhebung“ und die weitere Speicherung und Verbreitung von Daten, die (in großen Mengen) im US-Rechtsrahmen erhoben werden.

Da die Prüfung der Gleichwertigkeit der Sache nach kein Identitätstest ist und die im neuen Rechtsrahmen für die Signalaufklärung vorgesehenen Garantien gestärkt wurden, widmet sich der EDSA schwerpunktmäßig einer Bewertung der Garantien in ihrer Gesamtheit, wobei ein ganzheitlicher Ansatz verfolgt wird, der die Garantien für den gesamten Verarbeitungszyklus, von der Erhebung von Daten bis zur Verbreitung von Daten, einschließlich der Elemente Aufsicht und Rechtsschutz, abdeckt.

In diesem Zusammenhang hebt der EDSA folgende Feststellungen hervor:

Der EDSA erkennt zwar an, dass mit der EO 14086 die Begriffe der Erforderlichkeit und Verhältnismäßigkeit in den Rechtsrahmen für die Signalaufklärung eingeführt werden, betont jedoch, dass die Auswirkungen dieser Änderungen in der Praxis genau überwacht werden müssen, einschließlich der Überprüfung der internen Strategien und Verfahren zur Umsetzung der Garantien der Durchführungsverordnung auf Behördenebene.

Der EDSA begrüßt ferner, dass die EO 14086 eine Liste spezifischer Zwecke enthält, für die eine Erhebung möglich bzw. nicht möglich ist, und stellt fest, dass die Ziele angesichts neuer Erfordernisse

der nationalen Sicherheit durch zusätzliche – nicht unbedingt öffentliche – Ziele aktualisiert werden können.

Als Defizit im derzeitigen Rahmen hat der EDSA insbesondere festgestellt, dass der US-Rechtsrahmen, wenn er die Erhebung von Daten in großen Mengen gemäß Executive Order 12333 zulässt, nicht das Erfordernis einer vorherigen Genehmigung durch eine unabhängige Behörde enthält, wie dies in der jüngsten Rechtsprechung des EGMR gefordert wird, und dass er auch keine systematische unabhängige Ex-post-Überprüfung durch ein Gericht oder eine gleichwertige unabhängige Stelle vorsieht. In Bezug auf die vorherige unabhängige Genehmigung der Überwachung nach § 702 FISA bedauert der EDSA, dass das FISA-Gericht (im Folgenden „FISC") einen Programmantrag auf Einhaltung der EO 14086 bei der Zertifizierung des Programms, mit dem das Abheben auf Nicht-US-Personen genehmigt wird, nicht prüft, obwohl die Nachrichtendienste, die das Programm durchführen, an das Programm gebunden sind. Nach Auffassung des EDSA sollten die in dieser Durchführungsverordnung enthaltenen zusätzlichen Garantien dessen ungeachtet auch vom FISC berücksichtigt werden. Der EDSA erinnert daran, dass Berichte des Privacy and Civil Liberties Oversight Board (PCLOB) besonders nützlich für die Beantwortung der Frage wären, wie die Garantien der EO 14086 umgesetzt werden und wie diese Garantien angewandt werden, wenn Daten gemäß § 702 FISA und EO 12333 erhoben werden.

In Bezug auf das Rechtsbehelfsverfahren erkennt der EDSA erhebliche Verbesserungen in Bezug auf die Befugnisse des Datenschutzüberprüfungsgerichts (Data Protection Review Court, im Folgenden „DPRC") und dessen größere Unabhängigkeit im Vergleich zu derjenigen der Ombudsperson an. Des Weiteren erkennt der EDSA die im neuen Rechtsbehelfsverfahren vorgesehenen zusätzlichen Garantien an, wie etwa die Rolle der Sonderanwälte, die sich für das Interesse des Beschwerdeführers einsetzen, sowie die Überprüfung des Rechtsbehelfsverfahrens durch den PCLOB. Unter Berücksichtigung der Natur der nationalen Sicherheit und der in der EO 14086 vorgesehenen Garantien hegt der EDSA dennoch Bedenken bezüglich der allgemeinen Anwendung der Standardantwort des DPRC, in der es dem Beschwerdeführer mitteilt, dass entweder keine unter die Durchführungsverordnung fallenden Verstöße festgestellt wurden oder dass eine Entscheidung getroffen wurde, die eine angemessene Abhilfe erfordert, und dass dies zusammen betrachtet nicht angefochten werden kann. Angesichts der Bedeutung des Rechtsbehelfsverfahrens fordert der EDSA die Kommission auf, die Funktionsweise dieses Verfahrens in der Praxis genau zu überwachen.

Der EDSA erwartet von der Kommission, dass sie ihrer Zusage, den Angemessenheitsbeschluss aus Dringlichkeitsgründen auszusetzen, aufzuheben oder zu ändern, nachkommen wird, insbesondere wenn die US- Exekutive beschließen würde, die in der Durchführungsverordnung enthaltenen Garantien einzuschränken. [13]

Alles in allem begrüßt der EDSA die erheblichen Verbesserungen, die die EO im Vergleich zum vorherigen Rechtsrahmen bietet, insbesondere im Hinblick auf die Einführung der Grundsätze der Erforderlichkeit und Verhältnismäßigkeit und des individuellen Rechtsbehelfsverfahrens für betroffene Personen in der EU. Angesichts der geäußerten Bedenken und der erforderlichen Klarstellungen schlägt der EDSA vor, diesen Bedenken Rechnung zu tragen und die Kommission um die erbetenen Klarstellungen zu ersuchen, um die Grundlage für den Beschlussentwurf zu festigen und eine genaue Überwachung der konkreten Umsetzung dieses neuen Rechtsrahmens, insbesondere der darin vorgesehenen Garantien, bei künftigen gemeinsamen Überprüfungen sicherzustellen.

[13] Beschlussentwurf, Erwägungsgrund 212.

Inhaltsverzeichnis

Der Europäische Datenschutzausschuss —

Der Europäische Datenschutzausschuss hat folgende Erklärung angenommen:

Gestützt auf Artikel 70 Absatz 1 Buchstabe s der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (im Folgenden „DSGVO“)[1],

gestützt auf das EWR-Abkommen und insbesondere Anhang XI und Protokoll 37, zuletzt geändert durch den Beschluss des Gemeinsamen EWR-Ausschusses Nr. 154/2018 vom 6. Juli 2018[2],

gestützt auf Artikel 12 und Artikel 22 seiner Geschäftsordnung –

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

1 EINLEITUNG

1.1 US-Datenschutzrahmen

1. Die Vereinigten Staaten (im Folgenden „USA“) und die Europäische Union (im Folgenden „EU“) verfolgen unterschiedliche Ansätze in Bezug auf den Schutz der Privatsphäre und den Datenschutz. Während der Schutz der Privatsphäre und der Datenschutz in der EU in den Artikeln 7 und 8 der Charta der Grundrechte der Europäischen Union garantiert sind, wird der Datenschutz in den USA im Allgemeinen unter dem Gesichtspunkt des Verbraucherschutzes behandelt. Infolgedessen unterscheiden sich die Regulierungsansätze in den USA und in der EU.[3]

2. Im Gegensatz zum umfassenden Ansatz der EU, der mit der DSGVO verfolgt wird, gibt es in den USA auf Bundesebene kein umfassendes allgemeines Datenschutzgesetz. Der Schutz der Privatsphäre in den USA wird eher mithilfe eines sektoralen und bundesstaatlichen Ansatzes verwirklicht. So unterliegen beispielsweise bestimmte Sektoren spezifischen Rechtsakten, wie z. B. dem

   - Health Insurance Portability and Accountability Act (Gesetz über die Übertragbarkeit und Rechenschaftspflicht der Krankenversicherung) (HIPAA)[4]

[1] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), ABl. L 119 vom 4.5.2016, S. 1.

[2] Soweit in dieser Stellungnahme auf „Mitgliedstaaten“ Bezug genommen wird, ist dies als Bezugnahme auf „EWR-Mitgliedstaaten“ zu verstehen.

[3] Siehe auch den am 13. Dezember 2022 veröffentlichten Entwurf eines Durchführungsbeschlusses der Europäischen Kommission gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates über die Angemessenheit des Schutzes personenbezogener Daten im Rahmen des Datenschutzrahmens EU-USA (im Folgenden „Beschlussentwurf“), Anhang I Abschnitt I.

[4] Der Health Insurance Portability and Accountability Act (HIPAA) von 1996 ist ein Bundesgesetz der USA. In ihm sind nationale Standards zum Schutz sensibler Gesundheitsdaten der Patienten festgelegt. Ziel des HIPAA ist es,

- Children's Online Privacy Protection Act (Gesetz zum Schutz der Online-Privatsphäre von Kindern) (COPPA)[5]
- Gramm-Leach-Bliley Act (GLBA)[6]

3. Im Bereich des Zugangs staatlicher Stellen zu personenbezogenen Daten, die aus der EU in die USA übermittelt werden, gilt eine Reihe unterschiedlicher Rechtsgrundlagen, Beschränkungen und Garantien. Die rechtlichen Verfahren für den Zugang zu Informationen zu Zwecken der Strafverfolgung gehen zurück entweder auf die Verfassung der USA (Vierter Zusatzartikel), auf Gesetzesrecht und Verfahrensrecht oder auf Leitlinien und Strategien des Justizministeriums auf Ebene des Bundes oder der Bundesstaaten. Der Zugang zu Informationen zu Zwecken der nationalen Sicherheit wird durch mehrere Rechtsinstrumente geregelt, insbesondere durch das Gesetz zur Überwachung ausländischer Nachrichtendienste (Foreign Intelligence Surveillance Act, FISA), die Executive Order 12333, die kürzlich erlassene Executive Order 14086 sowie die Verordnung des Generalstaatsanwalts („AG-Verordnung")[7] zur Einrichtung eines Datenschutz-Überprüfungsgerichts (Data Protection Review Court, im Folgenden „DPRC").

4. Am 13. Dezember 2022 legte die Kommission ihren Entwurf eines Durchführungsbeschlusses der Kommission gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates über die Angemessenheit des Schutzes personenbezogener Daten im Rahmen des Datenschutzrahmens EU-USA (im Folgenden „Beschlussentwurf") vor, der in seinem Anhang den Datenschutzrahmen EU-USA enthält. Aus den oben dargelegten Gründen stützt sich der Beschlussentwurf nicht auf einen spezifischen und umfassenden föderalen Rechtsrahmen, sondern auf den DSR.

5. Der DSR funktioniert wie folgt: „Das US-Handelsministerium (im Folgenden „das Ministerium") gibt im Rahmen seiner gesetzlichen Befugnis, den internationalen Handel zu unterstützen, zu fördern und zu entwickeln (15 U.S.C. § 1512), die Grundsätze des Datenschutzrahmens EU-USA heraus, einschließlich

---

die Gesundheitsdaten natürlicher Personen angemessen zu schützen und gleichzeitig den Verkehr von Gesundheitsdaten für die Bereitstellung und Förderung einer hochwertigen Gesundheitsversorgung zu ermöglichen. Der HIPAA regelt die Verwendung und Offenlegung von Gesundheitsdaten durch Einrichtungen, die den Datenschutzbestimmungen unterliegen. Er enthält ferner Standards für das Recht natürlicher Personen auf Kenntnis und Kontrolle der Verwendung ihrer Gesundheitsdaten.
https://www.hhs.gov/hipaa/for-professionals/privacy/index.html; https://www.justice.gov/opcl/privacy-act-1974.

[5] Mit dem COPPA soll vorrangig Eltern die Kontrolle darüber verschafft werden, welche personenbezogenen Daten ihrer Kinder unter 13 Jahren von Betreibern für Kinder gestalteter Websites und Online-Dienste (einschließlich mobiler Apps und IoT-Geräten wie intelligentem Spielzeug) oder allgemeinen Publikumswebsites erhoben werden. Der COPPA verlangt, dass diese Betreiber die Eltern in Kenntnis setzen und ihre nachprüfbare Einwilligung einholen. Dies gilt auch für Daten ausländischer Kinder, wenn die Websites oder Dienste in den USA betrieben werden und dem COPPA unterliegen. Gleichzeitig gelten die Vorschriften auch für Websites und Dienstleistungen mit Sitz im Ausland, wenn diese sich an Kinder in den USA richten. Siehe: https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions#A.%20General%20Questions und Beschlussentwurf, Anhang IV, S. 3.

[6] Eines der Ziele des Gramm-Leach-Bliley Act ist der Schutz der Privatsphäre der Verbraucher im Finanzsektor. Der GLBA verpflichtet Finanzinstitute, ihren Kunden ihre Praxis des Informationsaustauschs zu erläutern und Vorkehrungen zum Schutz von Kundeninformationen zu treffen (z. B. für Unternehmen, die von der FTC nach der FTC Safeguards Rule reguliert werden). https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act

[7] Attorney General Order Nr. 5517-2022, mit der Vorschriften des US-Justizministeriums geändert werden, wie von der EO 14086 genehmigt und angeordnet.

der ergänzenden Grundsätze (im Folgenden zusammen ‚Grundsätze') und Anhang I der Grundsätze (im Folgenden ‚Anhang I')."[8]

6. Die Ausarbeitung der „Grundsätze" (im Folgenden „DSR-Grundsätze") erfolgte nach Konsultation der Europäischen Kommission (im Folgenden „Kommission"), der Industrie und anderer Interessenträger mit dem Ziel, Handel und Gewerbe zwischen der EU und den USA zu erleichtern[9] und gleichzeitig sicherzustellen, dass betroffene Personen ein Schutzniveau erhalten, das dem in der EU garantierten Schutzniveau der Sache nach gleichwertig ist.

7. Die DSR-Grundsätze werden als „Schlüsselkomponente" des DSR beschrieben. Einerseits bieten sie einen „gebrauchsfertigen" Mechanismus für Datenübermittlungen aus der EU in die USA. Andererseits werden personenbezogene Daten, die aus der EU in die USA übermittelt werden, nach den Vorgaben des EU-Rechts mit Garantien versehen und geschützt.

8. Der DSR gilt nur für US-Organisationen, die sich gemäß den Anforderungen des Rahmens selbst zertifiziert haben („DSR-Organisationen"). Dies ist derzeit nur möglich, wenn sie in die Zuständigkeit der Kartellbehörde (Federal Trade Commission, im Folgenden „FTC") oder des Verkehrsministeriums (Department of Transportation, im Folgenden „DoT") fallen. In Zukunft könnten weitere gesetzliche Einrichtungen mit der Befugnis zur Überwachung der Umsetzung der DSR-Grundsätze in einen künftigen Anhang aufgenommen werden.

9. In den DSR-Grundsätzen wird erläutert, dass die Bedingungen des Rahmens durchsetzbar sind durch i) die FTC nach Section 5 des Federal Trade Commission Act (FTC Act), der unlautere oder irreführende Handlungen im Handel oder sich auf diesen auswirkende entsprechende Handlungen verbietet[10], ii) das DoT nach 49 U.S.C: § 41712, das es einem Luftfahrtunternehmen oder Flugscheinvermittler verbietet, eine unlautere oder irreführende Praxis im Luftverkehr für den Verkauf oder die Beförderung im Luftverkehr auszuüben, oder iii) nach anderen Gesetzen oder Vorschriften, nach denen solche Handlungen verboten sind.

10. In den DSR-Grundsätzen wird darauf hingewiesen, dass weder die DSGVO in ihrer Anwendung betroffen ist noch bestehende Datenschutzverpflichtungen, die ansonsten nach US-Recht angewendet werden, durch die DSR-Grundsätze eingeschränkt werden.

1.2 Umfang der Bewertung durch den EDSA

11. Der Beschlussentwurf spiegelt die Bewertung des DSR durch die Kommission wider, die das Ergebnis der Gespräche mit der US-Regierung ist. Gemäß Artikel 70 Absatz 1 Buchstabe s DSGVO wird erwartet, dass der EDSA eine Stellungnahme zu den Feststellungen der Kommission in Bezug auf die Angemessenheit des Schutzniveaus in einem Drittland abgibt und sich erforderlichenfalls darum bemüht, Vorschläge zur Lösung aller Probleme zu unterbreiten.

12. Der EDSA begrüßt die Aktualisierungen der DSR-Grundsätze[11], die den verbindlichen Rechtsrahmen für DSR-Organisationen bilden werden. Der EDSA stellt jedoch fest, dass die DSR-Grundsätze im

[8] Beschlussentwurf, Anhang I Abschnitt I.
[9] Ebenda.
[10] 15 U.S.C. § 45 (a).
[11] Zum Beispiel die Klarstellung, dass es sich bei verschlüsselten Daten um personenbezogene Daten handelt.

Wesentlichen dieselben sind wie die Grundsätze des Datenschutzschilds[12] (auf denen die jährlichen gemeinsamen Überprüfungen durch die Artikel-29-Datenschutzgruppe („WP29“) und den EDSA beruhten). Die DSR-Grundsätze entsprechen ferner weitgehend denen des Entwurfs des Datenschutzschilds, auf den die Artikel-29-Datenschutzgruppe ihre Stellungnahme von 2016[13] stützte (im Folgenden „WP 29, Stellungnahme 01/2016“). In Bezug auf die im Wesentlichen unveränderten DSR-Grundsätze hält der EDSA es nicht für erforderlich, alle zuvor von der Artikel-29-Datenschutzgruppe vorgebrachten Bemerkungen zu wiederholen. Der EDSA hat beschlossen, sich auf spezifische Aspekte zu konzentrieren, die er heute angesichts der Entwicklung des rechtlichen und technologischen Umfelds für noch wichtiger hält.

13. Darüber hinaus befasst sich ein sehr wichtiger Teil der Analyse im Einklang mit der Rechtsprechung des EuGH[14] mit der rechtlichen Regelung für den Zugang staatlicher Stellen zu personenbezogenen Daten, die in die USA übermittelt werden.

14. Bei seiner Bewertung berücksichtigte der EDSA den geltenden europäischen Datenschutzrahmen, einschließlich der Artikel 7, 8 und 47 der Charta der Grundrechte der Europäischen Union (im Folgenden „Charta“), die das Recht auf Privat- und Familienleben, das Recht auf Schutz personenbezogener Daten bzw. das Recht auf einen wirksamen Rechtsbehelf und ein unparteiisches Gericht schützen, sowie Artikel 8 der Europäischen Menschenrechtskonvention (EMRK) zum Schutz des Privat- und Familienlebens. Darüber hinaus berücksichtigte der EDSA die Anforderungen der DSGVO, der einschlägigen Rechtsprechung und der vom EDSA angenommenen Referenzgrundlage für Angemessenheit (im Folgenden „DSGVO-Referenzgrundlage für Angemessenheit“)[15].

15. Ziel dieser Prüfung ist es, der Kommission eine Stellungnahme zur Bewertung der Angemessenheit des durch den DSR gebotenen Schutzniveaus vorzulegen. Der Begriff „angemessenes Schutzniveau“, der bereits in der Richtlinie 95/46/EG existierte, wurde vom EuGH weiterentwickelt. Daher ist es wichtig, an den vom EuGH in seinen Urteilen Schrems I[16] (Ungültigerklärung der „Safe Harbour-Regelung“) und Schrems II[17] (Ungültigerklärung des Datenschutzschilds) festgelegten Standard zu erinnern.

16. In seinem Urteil Schrems I hat der EuGH entschieden, dass das „Schutzniveau“ in dem Drittland zwar dem in der EU garantierten „der Sache nach gleichwertig“ sein muss, dass aber „sich die Mittel, auf die das Drittland insoweit zurückgreift, um ein solches Schutzniveau zu gewährleisten, von denen unterscheiden können, die in der Union herangezogen werden“[18]. Das Ziel ist also nicht, die

[12] Durchführungsbeschluss (EU) 2016/1250 der Kommission vom 12. Juli 2016 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes, ABl. L 207 vom 1.8.2016, S. 1.

[13] Stellungnahme 01/2016 der Artikel 29-Datenschutzgruppe zum Entwurf eines Angemessenheitsbeschlusses zum EU – US Datenschutzschild, angenommen am 13. April 2016 (im Folgenden „WP29, Stellungnahme 01/2016“).

[14] Insbesondere: Urteil des Gerichtshofs vom 6. Oktober 2015, Maximilian Schrems/Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:650, und Urteil des Gerichtshofs vom 16. Juli 2020, Data Protection Commissioner/Facebook Ireland Limited und Maximillian Schrems, C-311/18, ECLI:EU:C:2020:559.

[15] Artikel-29-Datenschutzgruppe, Referenzgrundlage für Angemessenheit, WP 254 rev.01, 28. November 2017, zuletzt überarbeitet und angenommen am 6. Februar 2018, gebilligt vom EDSA am 25. Mai 2018 (im Folgenden „DSGVO-Referenzgrundlage für Angemessenheit“).

[16] EuGH, Schrems I, Urteil des Gerichtshofs vom 6. Oktober 2015, Maximilian Schrems/Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:650 (im Folgenden „EuGH, Urteil Schrems I“).

[17] Urteil des Gerichtshofs vom 16. Juli 2020, Data Protection Commissioner/Facebook Ireland Limited und Maximillian Schrems, C-311/18, ECLI:EU:C:2020:559 (im Folgenden „EuGH, Urteil Schrems II“).

[18] EuGH, Urteil Schrems I, Rn. 73–74.

europäischen Vorschriften Punkt für Punkt wiederzugeben, sondern vielmehr die wesentlichen Kernanforderungen der zu prüfenden Vorschriften festzulegen. Angemessenheit kann durch eine Kombination von gegenüber den Betroffenen eingeräumten Rechten, bestimmten Pflichten für die Stellen, bei denen die Daten verarbeitet werden oder in deren Zuständigkeit die Verarbeitung der Daten fällt, und die Aufsicht durch unabhängige Behörden erreicht werden. Datenschutzvorschriften sind allerdings nur dann wirksam, wenn sie durchsetzbar sind und in der Praxis eingehalten werden. Daher sind bei der Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation nicht nur die geltenden Vorschriften zu beachten, sondern auch das System, mit dem die Wirksamkeit der Regeln gesichert werden soll. Effiziente Durchsetzungsmechanismen sind für die Wirksamkeit von Datenschutzvorschriften von wesentlicher Bedeutung.[19]

17. In seiner Entscheidung Schrems II befand der EuGH, dass die Gesetze, auf deren Grundlage amerikanische Nachrichtenbehörden auf in die USA übermittelte Daten zugreifen dürfen (Section 702 FISA/EO 12333), die in den Artikeln 7 und 8 der Charta der Grundrechte der Europäischen Union („Charta“) verankerten Rechte unverhältnismäßig einschränken und damit nicht Anforderungen erfüllt würden, die den im Unionsrecht nach Artikel 52 Absatz 1 Satz 2 der Charta bestehenden Anforderungen der Sache nach gleichwertig wären.[20]

18. Darüber hinaus stellte der EuGH fest, dass der frühere Rechtsrahmen keine Garantien bietet, die den in Artikel 47 der Charta geforderten der Sache nach gleichwertig sind, da der Ombudsmechanismus keinen Ausgleich bieten kann, da weder die PPD-28 noch die EO 12333 Nicht-US-Personen einen wirksamen Rechtsbehelf gewähren.[21] Der Ombudsperson fehle es an Unabhängigkeit von der Exekutive und an der Befugnis, verbindliche Entscheidungen gegenüber US-Nachrichtendiensten zu treffen.[22]

19. Mit der EO 14086, die im Wesentlichen die PPD-28 ersetzt, wurden zwei neue Anforderungen in das US-Recht eingeführt, die Elemente des Urteils des EuGH in der Rechtssache Schrems II aufgreifen: Auf der einen Seite dürfen Signalaufklärungstätigkeiten nur in dem Umfang durchgeführt werden, in dem dies erforderlich ist, um eine validierte nachrichtendienstliche Prioritätensammlung voranzubringen, und nur in dem Umfang und in einer Weise, die in einem angemessenen Verhältnis zu der validierten nachrichtendienstlichen Priorität steht; und auf der anderen Seite wird ein Rechtsbehelfsverfahren eingeführt.

20. In dieser Stellungnahme bewertet der EDSA insbesondere, inwieweit der DSR sowie die kürzlich erlassene EO 14086 den Feststellungen des EuGH in seinem Urteil wirksam Rechnung tragen.

1.3 Allgemeine Bemerkungen und Bedenken

1.3.1 Beurteilung des innerstaatlichen Rechts

21. Der EDSA geht davon aus, dass sich die im Beschlussentwurf enthaltene Bewertung auf die DSR-Grundsätze bezieht. Dennoch würde der EDSA einige Informationen über den US-amerikanischen Rechtsrahmen begrüßen, in dem die DSR-Organisationen tätig sind. Sie würden ein besseres Verständnis der Wechselwirkung zwischen dem DSR und dem US-Recht ermöglichen. So wird beispielsweise in Anhang I 1[23] festgestellt, dass die DSR-Grundsätze „die ansonsten nach US-Recht

[19] DSGVO-Referenzgrundlage für die Angemessenheit, S. 3.
[20] EuGH, Urteil Schrems II, Rn. 184–185.
[21] EuGH, Urteil Schrems II Rn. 192.
[22] EuGH, Urteil Schrems II Rn. 195.
[23] Beschlussentwurf, Anhang I Abschnitt I letzter Satz.

geltenden Datenschutzverpflichtungen nicht einschränken“, ohne dass diese Verpflichtungen beschrieben werden.

1.3.2 Internationale Verpflichtungen der USA

22. Gemäß Artikel 45 Absatz 2 Buchstabe c DSGVO und der DSGVO-Referenzgrundlage für die Angemessenheit berücksichtigt die Kommission bei der Prüfung der Angemessenheit des von einem Drittland gebotenen Schutzniveaus unter anderem die von dem Drittland eingegangenen internationalen Verpflichtungen oder andere Verpflichtungen, die sich aus der Teilnahme des Drittlands an multilateralen oder regionalen Systemen insbesondere in Bezug auf den Schutz personenbezogener Daten ergeben, sowie die Umsetzung dieser Verpflichtungen.

23. Die USA sind Vertragspartei mehrerer internationaler Übereinkommen, die das Recht auf Privatsphäre garantieren, wie des Internationalen Pakts über bürgerliche und politische Rechte (Artikel 17), des Übereinkommens über die Rechte von Menschen mit Behinderungen (Artikel 22) und des Übereinkommens über die Rechte des Kindes (Artikel 16). Darüber hinaus halten sich die USA als OECD-Mitglied an den OECD-Datenschutzrahmen, insbesondere an die Leitlinien für den Schutz der Privatsphäre und den grenzüberschreitenden Verkehr personenbezogener Daten. Am 14. Dezember 2022 wurde die „Erklärung der OECD über den Zugang staatlicher Stellen zu personenbezogenen Daten im Besitz von Privatunternehmen“ von Ministern und hochrangigen Vertretern der OECD-Mitglieder und der Europäischen Union angenommen. Die USA sind ferner Vertragspartei des Budapester Übereinkommens über Computerkriminalität.

24. Darüber hinaus sind die USA Mitglied des „Cross-Border Privacy Rules“ (CBPR)-Systems für die Asiatisch-Pazifische Wirtschaftskooperation (im Folgenden „APEC“), bei dem es sich um eine staatlich unterstützte Datenschutzzertifizierung handelt, mit der Unternehmen die Einhaltung international anerkannter Datenschutzvorschriften nachweisen können. Diese Datenschutzbestimmungen wurden von führenden APEC-Vertretern gebilligt.

25. Der EDSA nimmt ferner die Beteiligung der USA als Beobachterstaat an der Arbeit des Beratenden Ausschusses des Übereinkommens Nr. 108 des Europarats zur Kenntnis.

26. Des Weiteren nimmt der EDSA zur Kenntnis und begrüßt das kontinuierliche Engagement der US-Behörden in dem 2021 neu eingeführten Format des „Roundtable of G7 Data Protection and Privacy Authorities“ (G7 DPA-Roundtable), zu dem unabhängige Datenschutz- und Datenschutzaufsichtsbehörden der G7-Länder eingeladen werden. In diesem Zusammenhang haben sie beispielsweise das Kommuniqué des jüngsten Rundtischgesprächs der G7-Datenschutzbehörden[24] unterstützt, das am 8. September 2022 in Bonn (Deutschland) verabschiedet wurde und in dem das Konzept des „Data Free Flow with Trust“ im Mittelpunkt stand.

1.3.3 Fortschritte im Bereich der US-Datenschutzvorschriften

27. Der EDSA nimmt insbesondere die Entwicklungen bei den Datenschutzvorschriften auf Ebene der Bundesstaaten in den USA zur Kenntnis. Der EDSA begrüßt die Annahme von Datenschutzgesetzen, die

[24] Roundtable der G7-Datenschutzbehörden, Förderung des freien Datenverkehrs mit Vertrauen und Wissensaustausch über die Aussichten für internationale Datenräume, 8. September 2022, https://www.bfdi.bund.de/SharedDocs/Downloads/EN/G7/Communique-2022.pdf?__blob=publicationFile&v=1.

bis 2023 in fünf Staaten (Kalifornien, Colorado, Connecticut, Virginia und Utah) in Kraft getreten sind oder in Kraft treten werden[25]..

28. Der EDSA stellt ferner fest, dass in vielen anderen US-Bundesstaaten bereits entsprechende Initiativen für weitere bundesstaatliche Gesetze eingeleitet wurden.

29. Darüber hinaus begrüßt der EDSA ausdrücklich die Bemühungen in Bezug auf die parteiübergreifende Initiative für ein föderales Datenschutzgesetz, den American Data Privacy and Protection Act (ADPPA).

1.3.4 Anwendungsbereich des Beschlussentwurfs

30. Gemäß Artikel 1 des Beschlussentwurfs kommt die Kommission zu dem Schluss, dass die USA ein angemessenes Schutzniveau für personenbezogene Daten gewährleisten, die aus der EU an Organisationen in den Vereinigten Staaten übermittelt werden, die in der „Liste des Datenschutzrahmens" aufgeführt sind, die gemäß Anhang I Abschnitt I.3 vom US-Handelsministerium (Department of Commerce, „DoC") geführt und öffentlich zugänglich gemacht wird.[26]

31. Der DSR steht Unternehmen zur Verfügung, die in die Zuständigkeit der FTC oder des DoT fallen. Es wird darauf hingewiesen, dass andere US-amerikanische Rechtsorgane mit ähnlichen Befugnissen in Zukunft hinzugefügt werden können[27].

1.3.5 Einschränkungen der Pflicht zur Einhaltung der DSR-Grundsätze

32. In Anhang I Abschnitt I.5 ist vorgesehen, dass die Einhaltung der DSR-Grundsätze durch DSR-Organisationen unter anderem beschränkt werden kann i) auf das Maß, das erforderlich ist, um einer gerichtlichen Anordnung nachzukommen oder Anforderungen des öffentlichen Interesses, der Strafverfolgung[28] oder der nationalen Sicherheit[29] zu erfüllen (auch wenn Gesetze oder Regierungsverordnungen widersprüchliche Pflichten begründen), und ii) durch Gesetz, gerichtliche Anordnung oder Regierungsverordnung, mit der ausdrückliche Genehmigungen geschaffen werden, unter der Voraussetzung, dass eine DSR-Organisation bei der Ausübung einer solchen Genehmigung nachweisen kann, dass ihre Nichteinhaltung der DSR-Grundsätze auf das Maß beschränkt ist, das erforderlich ist, um den durch eine solche Genehmigung geförderten übergeordneten berechtigten Interessen gerecht zu werden.

33. Ohne umfassende Kenntnis des US-Rechts sowohl auf Ebene des Bundes als auch auf Ebene der Bundesstaaten ist es für den EDSA schwierig, den Umfang der in diesem Absatz aufgeführten Ausnahmen im Einzelnen zu bewerten. Daher empfiehlt der EDSA der Kommission, in den

[25] California Consumer Privacy Act (2018; in Kraft getreten am 1. Januar 2020); California Privacy Rights Act (2020; vollständig in Kraft getreten am 1. Januar 2023); Colorado Privacy Act (2021; tritt in Kraft am 1. Juli 2023); Connecticut Data Privacy Act (2022; tritt in Kraft am 1. Juli 2023); Virginia Consumer Data Protection Act (2021; in Kraft getreten am 1. Januar 2023); Utah Consumer Privacy Act (2022; tritt in Kraft am 31. Dezember 2023).

[26] Beschlussentwurf, Schlussbemerkungen, Artikel 1, S. 57. Der EDSA geht davon aus, dass der Beschlussentwurf nicht für Übermittlungen von Einrichtungen, die ihren Sitz außerhalb der EU haben, aber gemäß Artikel 3 Absatz 2 DSGVO der DGSVO unterliegen, an zertifizierte Einrichtungen in den USA gilt.

[27] Beschlussentwurf, Anhang I, Abschnitt I.2.

[28] Weitere Anmerkungen zur Verwendung von unter den Datenschutzrahmen EU-USA fallenden personenbezogenen Daten zu Strafverfolgungszwecken finden sich in Abschnitt 3.1 der vorliegenden Stellungnahme.

[29] Weitere Anmerkungen zur Verwendung von unter den Datenschutzrahmen EU-USA fallenden personenbezogenen Daten für Zwecke der nationalen Sicherheit finden sich in Abschnitt 3.2 der vorliegenden Stellungnahme.

Beschlussentwurf eine Klarstellung des Anwendungsbereichs der Ausnahmen, einschließlich der nach US-Recht anwendbaren Garantien, aufzunehmen, um die Auswirkungen dieser Ausnahmen auf das Schutzniveau für betroffene Personen besser zu umreißen. Der EDSA betont ferner, dass die Kommission über die Anwendung und Annahme von Gesetzen oder Regierungsverordnungen, die sich auf die Einhaltung der DSR-Grundsätze auswirken würden, unterrichtet werden und diese überwachen sollte.

1.3.6 Änderungen in Bezug auf den „Datenschutzschild"

34. Der EDSA begrüßt die Anstrengungen, die unternommen wurden, um den Anforderungen des Schrems-II-Urteils nachzukommen. Dennoch hätte es der EDSA begrüßt, wenn weitere Probleme, die i) in der Stellungnahme 01/2016 der Artikel-29-Datenschutzgruppe und ii) bei den bisher durchgeführten gemeinsamen Überprüfungen[30] festgestellt wurden, auch bei den Verhandlungen über den DSR behandelt worden wären.

35. Der EDSA stellt ferner fest, dass die DSR-Grundsätze, an die sich die DSR-Organisationen halten müssen, trotz einiger Änderungen und zusätzlicher Erläuterungen in den Erwägungsgründen des Beschlussentwurfs im Wesentlichen gegenüber den Grundsätzen des Datenschutzschilds unverändert sind.

1.3.7 Mangelnde Klarheit in den Dokumenten des DSR

36. Der EDSA stellt fest, dass es aufgrund der Struktur der Anhänge und ihrer Nummerierung schwierig ist, die Informationen zu finden und darauf zu verweisen. Dies trägt zu einer insgesamt komplexen Darstellung des neuen Rahmens bei, der in seinen Anhängen Dokumente von unterschiedlicher rechtlicher Bedeutung zusammenfasst, und ist möglicherweise einem guten Verständnis der DSR-Grundsätze durch betroffene Personen, DSR-Organisationen und Datenschutzbehörden in der EU nicht förderlich.

37. Der EDSA betont ferner, dass die Terminologie im gesamten DSR kohärent verwendet werden sollte. Dies ist derzeit, beispielsweise beim Begriff „Verarbeitung", nicht der Fall. In einigen Teilen des DSR werden nämlich einige Arten von Datenverarbeitungsvorgängen aufgeführt, anstatt den Begriff „Verarbeitung" zu verwenden. Dies kann zu Rechtsunsicherheit und möglichen Lücken im Schutz führen.[31]

38. Der EDSA begrüßt, dass einige der verwendeten Begriffe im DSR definiert werden.[32] Dies gilt jedoch nicht für einige andere wesentliche Begriffe wie zumindest „Verarbeiter" oder „Auftragsverarbeiter", die nach Ansicht des EDSA eine klare und spezifische Definition in Anhang I Abschnitt I 8 des DSR

[30] Jährliche Überprüfungen: EU-US-Datenschutzschild – Erste jährliche gemeinsame Überprüfung, WP 255, Bericht der Artikel-29-Datenschutzgruppe, angenommen am 28. November 2017 (im Folgenden „Erster gemeinsamer Überprüfungsbericht"); EU-US-Datenschutzschild – Zweite jährliche gemeinsame Überprüfung, Bericht des EDSA, angenommen am 22. Januar 2019 (im Folgenden „Zweiter gemeinsamer Überprüfungsbericht"); EU-US-Datenschutzschild – Dritte jährliche gemeinsame Überprüfung, Bericht des EDSA, angenommen am 12. November 2019 (im Folgenden „Dritter gemeinsamer Überprüfungsbericht").

[31] Beispielsweise wären i) nach dem Wortlaut von Anhang I Abschnitt III.6 f des Beschlussentwurfs die DSR-Grundsätze nur anwendbar, wenn die Organisation die empfangenen Daten „speichert, verwendet oder offenlegt" (d. h. nicht bei anderen Vorgängen, die unter den Begriff „Verarbeitung" fallen, wie das Erheben, Aufzeichnen, Verändern, Auslesen, Abfragen, Löschen) und wäre ii) gemäß Anhang I Abschnitt II.4 a des Beschlussentwurfs die Datensicherheit nur für die „Erstellung, Pflege, Nutzung oder Verbreitung" personenbezogener Informationen vorgeschrieben.

[32] Beschlussentwurf, Anhang I Abschnitt I 8.

rechtfertigen und auf die sich die USA und die EU einigen, um zu einem späteren Zeitpunkt Verwirrung bei DSR-Organisationen, die sich auf den DSR stützen, den Aufsichtsbehörden und der breiten Öffentlichkeit zu vermeiden.

39. Im Hinblick auf die unterschiedliche Auslegung des Begriffs „Personaldaten“ in der EU und den USA stimmt der EDSA dem dritten Überprüfungsbericht der Kommission zu, dem zufolge die Gespräche mit den US-Behörden fortgesetzt werden sollten[33].

2 ALLGEMEINE ASPEKTE DES DATENSCHUTZES

2.1 Inhaltliche Grundsätze

2.1.1 Begriffe

40. Der DSGVO-Referenzgrundlage für Angemessenheit zufolge sollten im System eines Drittlands grundlegende Datenschutzbegriffe und/oder -grundsätze bestehen. Die in der DSGVO verwendete Terminologie muss darin zwar nicht übernommen werden, doch sie sollten Begriffe, die im europäischen Datenschutzrecht verankert sind, widerspiegeln und mit diesen ihnen im Einklang stehen. Die DSGVO enthält beispielsweise folgende wichtige Begriffe: „personenbezogene Daten“, „Verarbeitung personenbezogener Daten“, „für die Verarbeitung Verantwortlicher“, „Auftragsverarbeiter“, „Empfänger“ und „sensible Daten“. Der EDSA begrüßt, dass der DSR genauso wie der Datenschutzschild Definitionen der Begriffe „personenbezogene Daten“, „Verarbeitung“ und „Verantwortlicher“ enthält.

41. Der EDSA stellt fest, dass unklar bleibt, inwieweit die DSR-Grundsätze auf DSR-Organisationen anwendbar sind, die personenbezogene Daten für Zwecke der „bloßen Verarbeitung“ (sogenannte „Verarbeiter“ oder „Auftragsverarbeiter“) erhalten. Der DSR unterscheidet nicht zwischen DSR-Grundsätzen, die für Verarbeiter gelten, und DSR-Grundsätzen, die für Verantwortliche gelten, und mehrere der Verpflichtungen in den DSR-Grundsätzen sind für Verarbeiter/Auftragsverarbeiter nicht angemessen. Beispielsweise sollte ein Verarbeiter/Auftragsverarbeiter nicht in der Lage sein, natürlichen Personen alle Elemente der vollständigen Mitteilung gemäß dem Mitteilungsgrundsatz (z. B. die Zwecke, für die er personenbezogene Daten über sie erhebt und verwendet) zur Verfügung zu stellen[34], da ein Verarbeiter/Auftragsverarbeiter die Mittel und Zwecke der Verarbeitung nicht allein bestimmen kann[35].

2.1.2 Grundsatz der Zweckbindung

42. Die DSGVO-Referenzgrundlage für Angemessenheit sieht im Einklang mit der DSGVO vor, dass personenbezogene Daten für einen bestimmten Zweck verarbeitet werden und folglich nur insoweit verwendet werden sollten, als das dem Zweck der Verarbeitung nicht entgegensteht.

---

[33] Dritter gemeinsame Überprüfungsbericht, S. 5, 15 f. und 30; siehe ferner die Arbeitsunterlage der Kommissionsdienststellen zum Bericht der Kommission an das Europäische Parlament und den Rat über die dritte jährliche Überprüfung der Funktionsweise des EU-US- Datenschutzschilds, S. 17 f.

[34] Beschlussentwurf, Anhang I Abschnitt II.1 a.

[35] Siehe auch die Stellungnahme 01/2016 der Artikel-29-Datenschutzgruppe, S 16.

43. Der Grundsatz der Datenintegrität und Zweckbindung besagt, dass eine Organisation personenbezogene Daten nicht in einer Weise verarbeiten darf, die mit den Zwecken, für die sie erhoben oder die anschließend von der natürlichen Person genehmigt wurden, unvereinbar ist.[36] Der EDSA stellt fest, dass im Rahmen der Grundsätze der Mitteilung, der Wahlmöglichkeit und der Datenintegrität und Zweckbindung unterschiedliche Begrifflichkeiten verwendet werden. Wie von der Artikel-29-Datenschutzgruppe festgestellt, und ungeachtet nützlicher Klarstellungen in den Erwägungsgründen des Beschlussentwurfs, werden im DSR Ausdrücke wie „verschiedene Zwecke", „wesentlich unterschiedliche Zwecke" oder „eine Verwendung, die nicht mit … übereinstimmt" ohne klare Begriffsbestimmung verwendet, was zu Rechtsunsicherheit führen könnte.

2.1.3 Recht auf Auskunft, Berichtigung, Löschung und Widerspruch

44. Im DSR werden die Rechte betroffener Personen auf Auskunft, Berichtigung und Löschung im Zusammenhang mit dem Auskunftsgrundsatz behandelt.[37]

45. Im Vergleich zum Datenschutzschild hat sich am Auskunftsgrundsatz nichts geändert. Folglich bleiben einige der in der Stellungnahme 01/2016 der Artikel-29-Datenschutzgruppe geäußerten Bedenken nach wie vor bestehen, wie nachstehend ausgeführt wird.

46. In Bezug auf das Auskunftsrecht natürlicher Personen hält es der EDSA für notwendig, erneut darauf hinzuweisen, dass die Einzelheiten der Verpflichtung, Anfragen von natürlichen Personen zu beantworten, besser im Haupttext des Grundsatzes stehen sollten (bisher werden sie noch immer nur in einer Fußnote beschrieben[38]).). Außerdem sollte klar sein, dass Auskunft in dem Umfang gewährt werden sollte, in dem eine DSR-Organisation personenbezogene Daten verarbeitet, und nicht nur, wenn sie sie „speichert".[39] Nach Ansicht des EDSA könnte der derzeitige Wortlaut zu einer engen Auslegung des Auskunftsrechts führen.

47. In Bezug auf die Liste der Ausnahmen vom Recht auf Auskunft[40] sei angemerkt, dass nach wie vor bei einigen tendenziell eher den Interessen der DSR-Organisationen Rechnung getragen wird. Der EDSA ist nach wie vor besorgt darüber, dass in diesen Fällen offenbar keine Verpflichtung besteht, die Rechte und Interessen des Einzelnen zu berücksichtigen.[41]

48. Eine weitere Ausnahme, die der Artikel-29-Datenschutzgruppe schon früher Anlass zu Bedenken gegeben hat[42] und die dem EDSA zu weit gefasst erscheint, ist die Ausnahme vom Auskunftsrecht bei öffentlich zugänglichen Informationen und Informationen aus öffentlichen Registern[43]. Der EDSA hat wiederholt darauf hingewiesen, dass betroffene Personen nach EU-Recht stets das Recht auf Auskunft über ihre Daten haben, unabhängig davon, ob die personenbezogenen Daten veröffentlicht wurden oder nicht. Sollten Auskunftsersuchen mit der Begründung abgelehnt werden, die Daten stammten aus öffentlich zugänglichen Quellen oder öffentlichen Registern, würden die betroffenen Personen nicht mehr in der Lage sein, die Richtigkeit der Daten zu kontrollieren und zu kontrollieren, ob die Daten überhaupt rechtmäßig öffentlich zugänglich gemacht wurden.

---

[36] Beschlussentwurf, Anhang I Abschnitt II.5.
[37] Beschlussentwurf, Anhänge I Abschnitte II.6 und III.8 a i.
[38] Beschlussentwurf, Anhang I Abschnitt III 8 a i 1. - Fußnote 14.
[39] Beschlussentwurf, Anhang I Abschnitt III.8 d ii.
[40] Beschlussentwurf, Anhang I Abschnitt III.8 e.
[41] Stellungnahme 01/2016 der Artikel-29-Datenschutzgruppe Nr. 2.2.5.
[42] Stellungnahme 01/2016 der Artikel-29-Datenschutzgruppe Nr. 2.2.9.
[43] Beschlussentwurf, Anhang I, Abschnitt III.15.d-e.

49. Der EDSA erinnert daran, dass das Recht auf Auskunft in Artikel 8 Absatz 2 der Charta verankert ist. Obwohl es sich dabei nicht um ein absolutes Recht handelt, ist es für das Recht auf Schutz personenbezogener Daten von grundlegender Bedeutung, da es die Ausübung der anderen Rechte der betroffenen Person, wie Berichtigung und Löschung, sowie das Widerspruchsrecht ermöglicht.[44]

50. Zusätzlich zu dem Recht auf Auskunft, Berichtigung und Löschung sollte die betroffene Person das Recht haben, aus zwingenden berechtigten Gründen in Verbindung mit ihrer Situation und unter bestimmten Umständen, die im Rechtsrahmen des Drittlands festgelegt sind, der Verarbeitung ihrer Daten jederzeit zu widersprechen.[45]

51. Mit dem Grundsatz der Wahlmöglichkeit sieht der DSR ein Recht auf Widerspruch (Opt-out) gegen die Offenlegung personenbezogener Daten gegenüber einem Dritten oder gegen die Verwendung personenbezogener Daten für einen wesentlich anderen Zweck vor[46]. Darüber hinaus haben natürliche Personen das Recht, jederzeit der Nutzung ihrer personenbezogenen Daten für Zwecke der Direktwerbung zu widersprechen.[47] Abgesehen von den Zwecken der Direktwerbung sind die Modalitäten, insbesondere die Fristen für die Ausübung des Widerspruchsrechts, nicht im Einzelnen festgelegt. Daher ersucht der EDSA die Kommission um eine Klarstellung, wie natürliche Personen ihr Widerspruchsrecht ausüben können.

52. Wie schon die Artikel-29-Datenschutzgruppe in ihrer Stellungnahme 01/2016 ist auch der EDSA der Ansicht, dass ein einfacher Verweis auf das Bestehen dieses Rechts in den Datenschutzbestimmungen nicht ausreichen kann. Eine individuelle Möglichkeit zur Ausübung dieses Rechts sollte nicht nur im Falle der Offenlegung oder Weiterverwendung personenbezogener Informationen angeboten werden. Der EDSA betont, dass im DSR ein allgemeines Widerspruchsrecht aus zwingenden berechtigten Gründen in Verbindung mit der besonderen Situation der betroffenen Person eingeräumt werden sollte. Der EDSA empfiehlt, dass ein solches Widerspruchsrecht jederzeit garantiert wird und dass dieses Recht nicht auf die Nutzung der Daten für die Direktwerbung beschränkt ist.[48]

53. In Bezug auf Personaldaten begrüßt der EDSA die Klarstellungen der Kommission in Bezug auf die Anwendung der Grundsätze der Bekanntmachung und der Wahlmöglichkeit in Fällen, in denen eine zertifizierte US-Organisation beabsichtigt, Personaldaten für einen anderen, nicht beschäftigungsbezogenen Zweck wie Marketingmitteilungen zu verwenden.[49] Der EDSA bleibt jedoch bei seiner Auffassung, dass die Weiterverarbeitung von Personaldaten für nicht beschäftigungsbezogene Zwecke in den meisten Fällen als unvereinbar mit dem ursprünglichen Zweck angesehen wird und dass die Einwilligung selten völlig freiwillig sein wird, wenn sie im Beschäftigungskontext erfolgt.

54. Der EDSA bekräftigt ferner die Bedenken der Artikel-29-Datenschutzgruppe in Bezug auf die Ausnahme von den Grundsätzen der Bekanntmachung und Wahlmöglichkeit von Personaldaten „in dem Umfang und für den Zeitraum, der erforderlich ist, um zu vermeiden, dass die Fähigkeit der Organisation, Beförderungen, Ernennungen oder andere ähnliche Beschäftigungsentscheidungen zu treffen, beeinträchtigt wird“[50], die dem EDSA als weitgefasst und vage erscheint.[51]

---

[44] Stellungnahme 01/2016 der Artikel-29-Datenschutzgruppe Nr. 2.2.5.
[45] DSGVO-Referenzgrundlage für Angemessenheit, Abschnitt 3.A.8.
[46] Beschlussentwurf, Anhang I Abschnitt II.2.a.
[47] Beschlussentwurf, Anhang I Abschnitt III.12.a.
[48] Stellungnahme 01/2016 der Artikel-29-Datenschutzgruppe Nr. 2.2.2.
[49] Beschlussentwurf, Anhang I Abschnitt III 9 b i und Erwägungsgrund 15 und Fußnote 27.
[50] Beschlussentwurf, Anhang I, III.9.b.iv.
[51] Stellungnahme 01/2016 der Artikel-29-Datenschutzgruppe Nr. 2.2.7.

2.1.4 Einschränkungen bei der Weiterleitung von Daten

55. Die Weiterleitung der personenbezogenen Daten durch den ursprünglichen Empfänger der ursprünglichen Datenübermittlung sollte nur zulässig sein, wenn der weitere Empfänger (d. h. der Empfänger der weitergeleiteten Daten) ebenfalls Vorschriften (einschließlich vertraglicher Bestimmungen) unterliegt und dadurch ein angemessenes Schutzniveau gewährleistet und die einschlägigen Anweisungen für die Verarbeitung von Daten im Namen des für die Verarbeitung Verantwortlichen befolgt. Das Schutzniveau natürlicher Personen, deren Daten übermittelt werden, darf durch die Weiterleitung der Daten nicht untergraben werden. Der ursprüngliche Empfänger von aus der EU übermittelten Daten ist verpflichtet sicherzustellen, dass ohne Vorliegen eines Angemessenheitsbeschlusses geeignete Garantien für die Weiterleitung der Daten gegeben sind. Solche Weiterleitungen von Daten sollten nur für begrenzte und bestimmte Zwecke erfolgen und solange es eine Rechtsgrundlage für die Verarbeitung gibt.[52]

56. Nach dem Grundsatz der Rechenschaftspflicht für Weiterleitungen des DSR können Weiterleitungen nur für begrenzte und festgelegte Zwecke auf der Grundlage eines Vertrags zwischen der DSR-Organisation und dem Dritten (oder einer vergleichbaren Vereinbarung innerhalb einer Unternehmensgruppe) und nur dann erfolgen, wenn dieser Vertrag den Dritten verpflichtet, dasselbe Schutzniveau zu bieten, wie es durch die DSR-Grundsätze garantiert wird.[53]

57. Der EDSA möchte erneut auf die in der Stellungnahme 01/2016 der Artikel-29-Datenschutzgruppe geäußerten Bedenken hinsichtlich der Ausnahme von der Notwendigkeit von Verträgen für konzerninterne Übermittlungen zwischen Verantwortlichen hinweisen.[54] Mit Blick auf Personaldaten versteht der EDSA nach wie vor nicht die Gründe für die Befreiung von der Verpflichtung zum Abschluss eines Vertrags mit dem Verantwortlichen eines Dritten im Falle einer Weiterleitung für „gelegentliche beschäftigungsbezogene betriebliche Erfordernisse".[55]

58. Darüber hinaus möchte der EDSA die Forderung der Artikel-29-Datenschutzgruppe[56] wiederholen, dass dem Rahmen angehörende Organisationen verpflichtet sein müssen, vor der Weitergabe zu bewerten, ob die verpflichtenden Anforderungen der nationalen Gesetzgebung des Drittlandes, die für den Empfänger gelten, nicht die Kontinuität des Schutzes der betroffenen Personen untergraben, deren Daten übermittelt werden[57].

---

[52] DSGVO-Referenzgrundlage für Angemessenheit, Abschnitt 3.A.9.
[53] Beschlussentwurf, Anhang I Abschnitt II.3.
[54] Beschlussentwurf, Anhang I Abschnitt III 10 b i, in dem auf „andere konzerninterne Instrumente (z. B. Compliance- und Kontrollprogramme)" Bezug genommen wird, die offenbar nicht verbindlich sein müssen.
[55] Beschlussentwurf, Anhang I Abschnitt III 9 e i, in dem auf Beispiele wie Versicherungsschutz verwiesen wird.
[56] Stellungnahme 01/2016 der Artikel-29-Datenschutzgruppe Nr. 2.2.3, S. 23.
[57] Vor dem Hintergrund des *Schrems-II*-Urteils hat der EDSA die Verpflichtungen für Datenexporteure und -importeure in Bezug auf Weiterübermittlungen in einer Reihe von Leitlinien und Empfehlungen weiter präzisiert: vgl. EDSA, Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten (Fassung 2.0, angenommen am 18. Juni 2021); Empfehlungen 02/2020 zu den wesentlichen europäischen Garantien in Bezug auf Überwachungsmaßnahmen (angenommen am 10. November 2020); Leitlinien 04/2021 über Verhaltensregeln als Instrument für Übermittlungen (Fassung 2.0, angenommen am 22. Februar 2022); Empfehlungen 01/2022 zum Antrag auf Genehmigung und zu den Elementen und Grundsätzen, die in verbindlichen internen Datenschutzvorschriften des Verantwortlichen zu finden sind (angenommen am 14. November 2022); Leitlinien 07/2022 zur Zertifizierung als Instrument für Übermittlungen (angenommen nach öffentlicher Konsultation am 14. Februar 2023).

59. Der EDSA vertritt die Auffassung, dass Weiterübermittlungen personenbezogener Daten in Drittländer Eingriffe in die Grundrechte natürlicher Personen mit sich bringen könnten, und fordert die Kommission auf, klarzustellen, dass die vom ursprünglichen Empfänger dem Importeur im Drittland auferlegten Garantien vor dem Hintergrund der Rechtsvorschriften des Drittlandes wirksam sein müssen und vor der Weiterleitung im Rahmen des DSR zu prüfen sind[58].

2.1.5 Automatisierte Entscheidungsfindung und Profiling

60. Entscheidungen, die allein auf der Grundlage der automatisierten Verarbeitung (automatisierte Entscheidungen im Einzelfall) einschließlich Profiling beruhen, die eine rechtliche Wirkung für die betroffene Person entfalten oder sie erheblich beeinträchtigen, sind nur unter bestimmten Bedingungen zulässig, die im Rechtsrahmen des Drittlands festzulegen sind. Im europäischen Rahmen umfassen diese Bedingungen zum Beispiel das Erfordernis, die ausdrückliche Einwilligung der betroffenen Person einzuholen, oder die Notwendigkeit einer solchen Entscheidung zum Abschluss eines Vertrags. Steht die Entscheidung nicht im Einklang mit den im Rechtsrahmen des Drittlands festgelegten Bedingungen, sollte die betroffene Person das Recht haben, ihr nicht zu unterliegen. In jedem Fall sollten nach dem Recht des Drittlands die erforderlichen Garantien gewährleistet werden, einschließlich des Rechts auf Unterrichtung über die besonderen Gründe, die der Entscheidung und der angewandten Logik zugrunde liegen, um unrichtige und unvollständige Angaben zu berichtigen und die Entscheidung anzufechten, falls sie auf der Grundlage einer falschen Sachlage getroffen wurde.[59]

61. Der DSR sieht keine spezifischen rechtlichen Garantien für den Fall vor, dass natürliche Personen Entscheidungen unterworfen sind, die eine rechtliche Wirkung für sie entfalten oder sie erheblich beeinträchtigen und die ausschließlich auf einer automatisierten Verarbeitung von Daten beruhen, die dazu bestimmt ist, bestimmte persönliche Aspekte der Person zu bewerten, wie etwa ihre Arbeitsleistung, ihre Kreditwürdigkeit, ihre Zuverlässigkeit oder ihr Verhalten.

62. Wie bereits in der Stellungnahme 01/2016 der Artikel-29-Datenschutzgruppe und vom EDSA in seinen früheren Stellungnahmen zu den Angemessenheitsbeschlüssen betreffend Japan und Südkorea[60], dargelegt, stellt der EDSA fest, dass rasche Entwicklungen im Bereich der automatisierten Entscheidungsfindung und des Profiling – zunehmend mithilfe von KI-Technologien – in dieser Hinsicht besondere Aufmerksamkeit erfordern.[61]

63. Der EDSA nimmt die Argumente der Kommission zur Kenntnis, wonach das Fehlen spezifischer Vorschriften für die automatisierte Entscheidungsfindung im DSR das Schutzniveau in Bezug auf in der Union erhobene personenbezogene Daten wahrscheinlich nicht beeinträchtigen wird (da jede auf einer automatisierten Verarbeitung beruhende Entscheidung in der Regel von dem Verantwortlichen in der Union getroffen würde, der eine direkte Beziehung zu der jeweiligen betroffenen Person hat)[62].. Nach Ansicht des EDSA kann jedoch nicht ausgeschlossen werden, dass ein in den USA ansässiger

[58] Stellungnahme 01/2016 der Artikel-29-Datenschutzgruppe Nr. 2.2.3, S. 23.
[59] DSGVO-Referenzgrundlage für Angemessenheit, Abschnitt 3.B.3.
[60] EDSA, Stellungnahme 28/2018 zum Entwurf eines Durchführungsbeschlusses der Europäischen Kommission über die Angemessenheit des Schutzes personenbezogener Daten in Japan, angenommen am 5. Dezember 2018; EDSA, Stellungnahme 32/2021 zum Entwurf eines Durchführungsbeschlusses der Europäischen Kommission über die Angemessenheit des Datenschutzniveaus in der Republik Korea, angenommen am 24. September 2021.
[61] Vgl. u. a. Rechtssache C-634/21, OQ/Land Hessen (SCHUFA Holding u. a.), Vorabentscheidungsersuchen (anhängig).
[62] Beschlussentwurf, Erwägungsgründe 33 und 34.

Verantwortlicher für Daten, die im Rahmen des Beschlussentwurfs übermittelt werden (z. B. im Zusammenhang mit Beschäftigung, zur Bewertung der Leistung am Arbeitsplatz, zur Versicherung oder zur Wohnung), automatisierte Entscheidungsfindung nutzen könnte.

64. Der EDSA begrüßt die Bezugnahmen der Kommission auf spezifische Garantien, die in verschiedenen Bereichen in den einschlägigen US-Rechtsvorschriften vorgesehen sind.[63] Für den EDSA scheint das Schutzniveau für natürliche Personen jedoch je nachdem, ob überhaupt sektorspezifische Vorschriften auf die vorliegende Situation Anwendung finden, und wenn ja, welche, unterschiedlich auszufallen. Es besteht die Gefahr, dass einige Situationen nicht erfasst werden, da sie nicht in den Anwendungsbereich der genannten Rechtsakte fallen. Darüber hinaus wird der Inhalt der Rechte des Einzelnen in Bezug auf die automatisierte Entscheidungsfindung in den verschiedenen Rechtsakten unterschiedlich beschrieben.

65. Vor diesem Hintergrund ist der EDSA der Auffassung, dass im DSR spezifische Vorschriften für die automatisierte Entscheidungsfindung erforderlich sind, um ausreichende Garantien zu bieten, einschließlich des Rechts der natürlichen Person, die zugrunde liegende Logik zu kennen, die Entscheidung anzufechten und ein menschliches Eingreifen zu erwirken, wenn die Entscheidung sie erheblich beeinträchtigt[64].

2.2 Verfahrens- und Durchsetzungsmechanismen

66. Der EDSA stellt fest, dass sich der DSR weiterhin auf ein System der Selbstzertifizierung stützt, auch wenn die Kommission es als „Zertifizierungssystem" bezeichnet.

67. Der EDSA erinnert an die Verbesserungen, die im Laufe der bisher durchgeführten gemeinsamen Überprüfungen erzielt wurden. Beispielsweise in Bezug auf die Rolle des Handelsministeriums, das Selbst(re)zertifizierungsverfahren ..., die Überwachung der Einhaltung der DSR-Grundsätze durch die Unternehmen (z. B. durch Stichproben, die Verwendung von Compliance-Fragebögen) und die Ermittlung und Bekämpfung falscher Teilnahmebehauptungen (z. B. durch Internetrecherchen).

68. Gleichzeitig hatten die Artikel-29-Datenschutzgruppe und der EDSA Bedenken hinsichtlich eines gewissen Mangels an Aufsicht über die Einhaltung der Anforderungen des Datenschutzschilds geäußert.[65] Insbesondere stimmt der EDSA den Feststellungen der Kommission nach der dritten jährlichen Überprüfung des Datenschutzschilds zu, dass sich die Stichprobenkontrollen des Handelsministeriums tendenziell auf formale Anforderungen beschränken (z. B. ausbleibende Antworten seitens benannter Kontaktstellen oder Unzugänglichkeit der Datenschutzbestimmungen eines Unternehmens im Internet)[66]. Nach Auffassung des EDSA kommt Konformitätsprüfungen in Bezug auf inhaltliche Anforderungen entscheidende Bedeutung zu.

69. Der EDSA weist ferner darauf hin, wie wichtig eine wirksame Aufsicht (auch über die Einhaltung wesentlicher Anforderungen) und die Durchsetzung des DSR sind. Dieser Aspekt wird vom EDSA genau überwacht, auch im Rahmen der regelmäßigen Überprüfungen.

---

[63] Beschlussentwurf, Erwägungsgrund 35.
[64] Siehe auch Dritter gemeinsamer Überprüfungsbericht, Nr. 76.
[65] Dritter gemeinsamer Überprüfungsbericht, Nr. 7.
[66] Bericht der Kommission an das Europäische Parlament und den Rat zur dritten jährlichen Überprüfung der Funktionsweise des EU-US-Datenschutzschilds (23.10.2019, COM(2019) 495 final), S. 4.

70. Was die Durchsetzung anbelangt, so nimmt der EDSA die in den Schreiben der FTC[67] und des DoT[68] erneuerten Zusagen zur Kenntnis, der Untersuchung mutmaßlicher Verstöße gegen den DSR Vorrang einzuräumen, geeignete Durchsetzungsmaßnahmen gegen Unternehmen zu ergreifen, die falsche oder irreführende Behauptungen über die Beteiligung machen, Durchsetzungsanordnungen im Zusammenhang mit Verstößen gegen den DSR zu überwachen und mit den Datenschutzbehörden in der EU zusammenzuarbeiten. In diesem Zusammenhang erkennt der EDSA auch an, dass die FTC erklärt hat, sie erwarte, ihre Durchsetzungsbemühungen weiter auf wesentliche Verstöße gegen den DSR zu konzentrieren, und sie beabsichtige, (auch) aus eigener Initiative Ermittlungen durchzuführen. Diese Aspekte werden vom EDSA, auch im Rahmen der regelmäßigen Überprüfungen, genau überwacht.

2.3 Rechtsschutzverfahren

71. Der EDSA begrüßt, dass im Beschlussentwurf die sieben Rechtsmittelwege klar dargelegt werden, die betroffene Personen in der EU beschreiten können, wenn ihre personenbezogenen Daten unter Verstoß gegen den DSR verarbeitet werden.[69]

72. Diese verschiedenen Rechtsbehelfsverfahren werden im Einklang mit den Anforderungen des Grundsatzes des Rechtsschutzes, der Durchsetzung und der Haftung und des ergänzenden Grundsatzes 11 betreffend „Streitbeilegung und Durchsetzung" des Handelsministeriums eingerichtet und in Anhang I des Beschlussentwurfs aufgeführt.[70]

73. Wie die Kommission in ihrem Beschlussentwurf betont, „sollten der betroffenen Person wirksame verwaltungsrechtliche und gerichtliche Rechtsbehelfe zur Verfügung gestellt werden".[71] Dies entspricht dem Erfordernis des Artikels 45 Absatz 2 Buchstabe a DSGVO, wonach die Kommission bei ihrer Prüfung der Angemessenheit des gebotenen Schutzniveaus in einem Drittland insbesondere „wirksame verwaltungsrechtliche und gerichtliche Rechtsbehelfe für betroffene Personen, deren personenbezogene Daten übermittelt werden", zu berücksichtigen hat.[72] Auf dieses Erfordernis wird auch in der DSGVO-Referenzgrundlage für Angemessenheit hingewiesen.[73]

74. Der EDSA stellt fest, dass diese Rechtsschutzverfahren mit denen des früheren Datenschutzschilds identisch sind, zu denen sich die Artikel-29-Datenschutzgruppe bereits geäußert hatte.[74]

75. Mit Blick auf das Schiedsverfahren stellt der EDSA fest, dass diese Option im Hinblick auf die Ausnahmen von den DSR-Grundsätzen nicht verfügbar ist[75], und verweist daher auf seine Anmerkungen unter Nr. 33.

[67] Beschlussentwurf, Anhang IV.
[68] Beschlussentwurf, Anhang V.
[69] Beschlussentwurf, Erwägungsgrund 67.
[70] Beschlussentwurf, Anhang I Abschnitte II.7 und III.11 und Anhang I zu Anhang I.
[71] Beschlussentwurf, Erwägungsgrund 64.
[72] Siehe auch Erwägungsgrund 141 DSGVO, in dem auf Artikel 47 der Charta der Grundrechte über das Recht auf einen wirksamen gerichtlichen Rechtsbehelf in der EU Bezug genommen wird.
[73] DSGVO-Referenzgrundlage für Angemessenheit, S. 8.
[74] Siehe insbesondere die Stellungnahme 01/2016 der Artikel-29-Datenschutzgruppe Abschnitt 2.2.6 a.
[75] Beschlussentwurf, Anhang I zu Anhang I Abschnitt A.

76. Mit Blick auf weitere Rechtsmittel, die nach dem US-Recht offenstehen, würde der EDSA des Weiteren nähere Einzelheiten zu den erwähnten Rechtsvorschriften begrüßen[76] und verweist auf seine Anmerkungen in Absatz 21.

77. Darüber hinaus begrüßt der EDSA das Schreiben der FTC, in dem diese ihre Absicht darlegt, eng mit den Datenschutzbehörden in der EU zusammenzuarbeiten.[77] Der EDSA begrüßt ferner die vorrangige Behandlung von Beschwerden durch die FTC, auch wenn damit für die betroffene Person möglicherweise nicht sichergestellt ist, dass ihre Beschwerde auf jeden Fall bearbeitet wird.

78. In Bezug auf die Möglichkeit, dass natürliche Personen in bestimmten Fällen Beschwerden bei einer Datenschutzbehörde in der EU einreichen können, würde der EDSA nähere Informationen zu den Fragen begrüßen, i) ob die Möglichkeit für Datenschutzbehörden in der EU, in Sachen Abhilfe- oder Ausgleichsmaßnahmen zu beraten, auch Empfehlungen bezüglich Geldbußen oder den Einsatz von Untersuchungsbefugnissen umfasst, und ii) in welchem Umfang Maßnahmen der Datenschutzbehörden in der EU als Beweis für Durchsetzungsmaßnahmen der FTC oder des DoT berücksichtigt würden[78].

79. Die Wirksamkeit der Rechtsschutzverfahren wird vom EDSA, auch im Rahmen der regelmäßigen Überprüfungen, genau überwacht.

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

3.1 Zugang und Nutzung für Strafverfolgungszwecke

3.1.1 Der Zugang von Strafverfolgungsbehörden zu personenbezogenen Daten sollte auf der Grundlage klarer, präziser und zugänglicher Vorschriften erfolgen.

80. Der EDSA begrüßt die im Beschlussentwurf enthaltenen, im Vergleich zum vorherigen Angemessenheitsbeschluss detaillierteren Informationen und Erläuterungen in Bezug auf den Zugang zu personenbezogenen Daten und deren Nutzung durch US-Behörden für Strafverfolgungszwecke. Der Beschlussentwurf enthält in seinem Anhang VI auch ein Schreiben des US-Justizministeriums, Abteilung Strafangelegenheiten, „mit einem kurzen Überblick über die wichtigsten Ermittlungsinstrumente, die verwendet werden, um Geschäftsdaten und andere Aufzeichnungen von Unternehmen in den Vereinigten Staaten für Zwecke der Strafverfolgung oder (zivile und regulatorische) Zwecke des öffentlichen Interesses zu erhalten, einschließlich der von diesen Behörden festgelegten Zugangsbeschränkungen“. Dem Schreiben zufolge werden alle darin beschriebenen rechtlichen Verfahren genutzt, um Informationen von Unternehmen in den USA zu erhalten, unabhängig von der Staatsangehörigkeit oder dem Wohnsitz der betroffenen Person, und gehen entweder direkt auf die US-Verfassung (Vierter Zusatzartikel), auf das Gesetzesrecht und das Verfahrensrecht oder auf Leitlinien und Strategien des Justizministeriums zurück. Dieser Überblick deckt nicht die von den Strafverfolgungsbehörden bei Terrorismus und anderen Ermittlungen im

[76] Beschlussentwurf, Erwägungsgrund 85.
[77] Beschlussentwurf, Anhang IV.
[78] Beschlussentwurf, Anhang I Abschnitt III 5 b iii.

Bereich der nationalen Sicherheit verwendeten Ermittlungsinstrumente im Bereich der nationalen Sicherheit ab.[79]

81. Der EDSA stellt fest, dass in dem Beschlussentwurf und seinem Anhang VI in erster Linie die Strafverfolgungs- und Regulierungsbehörden[80] des Bundes behandelt werden und nicht ausdrücklich auf die Gesetzesvorschriften der Bundesstaaten Bezug genommen wird, in denen diese Verfahren zur Einholung von Informationen vorgesehen sind. In Anhang VI heißt es ferner: „Es gibt weitere Rechtsgrundlagen, auf denen Unternehmen Datenanfragen von Verwaltungsbehörden aufgrund ihres spezifischen Wirtschaftszweigs und der Art der ihnen vorliegenden Daten anfechten können", und es werden darüber hinaus mehrere nicht erschöpfende Beispiele wie der Bank Secrecy Act und seine Durchführungsbestimmungen[81], der Fair Credit Reporting Act[82] und der Right to Financial Privacy Act[83] genannt. Der EDSA stellt fest, dass die für einen bestimmten Antrag auf Zugang geltende Rechtsgrundlage von der Art der angeforderten Daten, der Art des Unternehmens, der Art der rechtlichen Verfahren (strafrechtliche, verwaltungsrechtliche, mit anderen öffentlichen Interessen zusammenhängende Verfahren) und der Art der Stelle, die den Zugang beantragt, abhängt. Da alle geltenden Vorschriften zur Beschränkung des Zugangs von Strafverfolgungsbehörden zu Daten, die in die USA übermittelt werden, auf der Verfassung, auf dem Gesetz und auf transparenten Strategien des Justizministeriums beruhen, erkennt der EDSA die Zugänglichkeit dieser Vorschriften an und ersucht die Kommission, dieses Element im Beschlussentwurf zu berücksichtigen. Aus Anhang VI geht hervor, dass diese Vorschriften unabhängig von der Staatsangehörigkeit oder dem Wohnsitz der betroffenen Person gelten und im Allgemeinen den Anforderungen des Vierten Zusatzartikels gerecht werden (obwohl sie oft auch darüber hinausgehen und zusätzliche Schutzbestimmungen vorsehen).

82. Abschließend stellt der EDSA fest, dass die im Beschlussentwurf enthaltene Bewertung des Zugangs von Strafverfolgungsbehörden des Bundes im Vergleich zum vorherigen Angemessenheitsbeschluss detaillierter ausfällt. Was den Zugang von Strafverfolgungsbehörden der Bundesstaaten anbelangt, nimmt der EDSA auch zur Kenntnis, dass gemäß Anhang VI Schutzmaßnahmen nach bundesstaatlichem Recht mindestens denen der US-Verfassung einschließlich, wenn auch nicht ausschließlich, des Vierten Zusatzartikels, gleichwertig sein müssen. Der EDSA fordert die Kommission auf, das Element des Schutzes nach bundesstaatlichem Recht bei künftigen Überprüfungen vertieft zu prüfen.

3.1.2 Die Erforderlichkeit und Verhältnismäßigkeit in Bezug auf die berechtigten Ziele muss nachgewiesen werden

83. Der EDSA nimmt zur Kenntnis, dass ein Antrag auf Zugang zu Daten für Strafverfolgungszwecke im Allgemeinen als berechtigtes Ziel angesehen werden kann. Gleichzeitig sind solche Eingriffe jedoch nur zulässig, wenn sie erforderlich und verhältnismäßig sind.[84]

---

[79] Beschlussentwurf, Fußnote 1 zu Anhang VI.
[80] Siehe Beschlussentwurf, Erwägungsgründe 90-93.
[81] 31 U.S.C. § 5318; 31 C.F.R. Kapitel X
[82] 15 U.S.C. § 1681b
[83] 12 U.S.C. §§ 3401–3423
[84] Siehe Urteil des Gerichtshofs vom 6. Oktober 2020 in den verbundenen Rechtssachen C-511/18, C-512/18 und C-520/18, La Quadrature du Net u. a., ECLI:EU:C:2020:791 (im Folgenden „EuGH, Urteil La Quadrature du Net"), Rn. 140. Siehe auch EDSB, Beurteilung der Erforderlichkeit von Maßnahmen, die das Grundrecht auf Schutz personenbezogener Daten einschränken: Ein Toolkit, 11. April 2017 und EDSB Leitlinien für die Bewertung der

84. Nach ständiger Rechtsprechung des EuGH verlangt der Grundsatz der Verhältnismäßigkeit, dass gesetzgeberische Maßnahmen, die in das Recht auf Achtung des Privatlebens und das Recht auf Schutz personenbezogener Daten eingreifen, „geeignet sind, die mit der fraglichen Regelung zulässigerweise verfolgten Ziele zu erreichen, und nicht die Grenzen dessen überschreiten, was zur Erreichung dieser Ziele geeignet und erforderlich ist“.[85] Daher erfolgt die Prüfung der Erforderlichkeit und Verhältnismäßigkeit grundsätzlich immer in Bezug auf eine spezifische gesetzlich vorgesehene Maßnahme.

85. Die US-Behörden geben in Anhang VI an, dass Bundesstaatsanwälte und Ermittlungsbeauftragte des Bundes Zugang zu Dokumenten und sonstigen Informationen von Organisationen erhalten können, und zwar durch „mehrere Arten verbindlicher rechtlicher Verfahren, darunter Zeugenladungen durch eine Grand Jury, Zeugenladungen durch Verwaltungsbehörden und Durchsuchungsanordnungen“, und dass sie andere Mitteilungen „gemäß den für Strafverfolgung zuständigen Abhör- und Pen Register-Behörden des Bundes“ erlangen können.[86] Außerdem können Stellen mit zivilen und regulatorischen Zuständigkeiten gegenüber Organisationen die Vorlage von „Geschäftsaufzeichnungen, elektronisch gespeicherten Daten und anderen materiellen Beweismitteln“ verlangen.[87] Die Verfahren selbst werden ebenfalls in den Erwägungsgründen 90-93 des Beschlussentwurfs erläutert. Der EDSA stellt in diesem Zusammenhang eine positive Entwicklung in der US-Rechtsprechung in Bezug auf elektronisch gespeicherte Informationen fest, auf die im Beschlussentwurf Bezug genommen wird.[88]

86. In Anhang VI ist ferner festgelegt, dass diese rechtlichen Verfahren diskriminierungsfrei sind und im Allgemeinen dazu genutzt werden, Informationen von „Unternehmen“ in den USA zu erhalten, unabhängig davon, ob sie innerhalb des Datenschutzrahmens EU-USA zertifiziert sind oder nicht, und „ungeachtet der Staatsangehörigkeit oder des Wohnsitzes der betroffenen Person“.

87. Darüber hinaus enthält Anhang VI Feststellungen zu den Garantien nach dem Vierten Zusatzartikel der US-Verfassung, wonach bei Durchsuchungen und Beschlagnahmen durch Strafverfolgungsbehörden grundsätzlich eine gerichtliche Anordnung erforderlich ist, wenn Gründe und Besonderheiten nachgewiesen werden, und verweist auf die Tatsache, dass die Strafverfolgung in Ausnahmefällen, in denen das Erfordernis einer Anordnung nicht gilt, einer Plausibilitätsprüfung nach dem Vierten Zusatzartikel unterliegt.[89] Eine Person, die Gegenstand einer Durchsuchung ist oder deren Vermögensgegenstände Gegenstand einer Durchsuchung sind, kann die Nichtigkeit von Beweismitteln beantragen, die bei einer unrechtmäßigen Durchsuchung erlangt oder gewonnen wurden, wenn diese Beweismittel während eines Strafverfahrens gegen sie eingereicht werden.[90]

Verhältnismäßigkeit von Maßnahmen, die die Grundrechte auf Privatsphäre und den Schutz personenbezogener Daten einschränken, 19. Dezember 2019.

[85] Siehe Urteil des Gerichtshofs vom 8. April 2014 in den verbundenen Rechtssachen C-293/12 und C-594/12, Digital Rights Ireland, ECLI:EU:C:2014:238 (im Folgenden „EuGH, Urteil Digital Rights Ireland“), Rn. 46 und die dort angeführte Rechtsprechung.

[86] Beschlussentwurf, Anhang VI, S. 2.

[87] Beschlussentwurf, Anhang VI, S. 4.

[88] Siehe Beschlussentwurf, Fußnote 146. In einem Urteil von 2018 bekräftigte der Oberste Gerichtshof der USA, dass eine Durchsuchungsanordnung oder ausnahmsweise Durchsuchungsgenehmigung auch für Strafverfolgungsbehörden erforderlich ist, um auf historische Aufzeichnungen zum Standort von Mobiltelefonen zuzugreifen, die einen umfassenden Überblick über die Bewegungen eines Nutzers bieten, und dass der Nutzer in Bezug auf den Schutz solcher Informationen ein angemessenes Maß an Privatsphäre erwarten dürfen (Timothy Ivory Carpenter gegen Vereinigte Staaten von Amerika, Nr. 16-402, 585 U.S. (2018)).

[89] Siehe Beschlussentwurf, Anhang VI, S. 2.

[90] Siehe Beschlussentwurf, Erwägungsgrund 90.

88. Abschließend stellt der EDSA fest, dass das System von Ermittlungsinstrumenten, das verwendet wird, um Geschäftsdaten und andere Datenbestände von Unternehmen in den USA für Zwecke der Strafverfolgung oder des öffentlichen Interesses – einschließlich Zugangsbeschränkungen und -garantien – zu erlangen, ein umfassendes, aber auch komplexes System von Maßnahmen darstellt, das unter anderem den föderalen Charakter der US-Regierung widerspiegelt.

89. Somit könne davon ausgegangen werden, dass das System von Ermittlungsmaßnahmen im Bereich der Strafverfolgung in den USA im Allgemeinen den Anforderungen der Erforderlichkeit und Verhältnismäßigkeit in Bezug auf die Grundrechte auf Privatleben und Datenschutz genügt.

3.1.3 Es sollte eine unabhängige Aufsicht bestehen

90. Der EDSA nimmt gebührend zur Kenntnis, dass die meisten der im Beschlussentwurf und in Anhang VI beschriebenen Verfahren eine Gerichtsentscheidung voraussetzen, bevor die Behörden Zugang zu Daten erhalten (z. B. gerichtliche Anordnungen für Pen Register und Trap and Traces[91], gerichtliche Überwachungsanordnungen nach dem Federal Wiretap Law[92], Durchsuchungsanordnungen – Bundesstrafverfahrensordnung, Regel 41[93]). Es scheint jedoch, dass nicht alle das vorherige Hinzuziehen eines Gerichts erfordern. So können z. B. Zivil- und Regulierungsbehörden „Vorladungen aussprechen“.[94] In diesen Fällen besteht jedoch die Möglichkeit einer nachträglichen gerichtlichen Kontrolle der Angemessenheit der Vorladung, da „ein Empfänger einer Vorladung durch die Verwaltung die Vollstreckung dieser Vorladung vor Gericht anfechten kann“[95].

91. Darüber hinaus wird in dem Beschlussentwurf die Aufsicht über die Strafverfolgungsbehörden des Bundes durch verschiedene Stellen beschrieben, von der internen Kontrolle durch die Datenschutzbeauftragten bis hin zur externen Kontrolle durch den Inspector General und spezielle Ausschüsse im US-Kongress.[96] Die Europäische Kommission legt differenzierte und detaillierte Informationen vor und gelangt generell zu nachvollziehbaren Schlussfolgerungen. Daher verzichtet der EDSA darauf, die Tatsachenfeststellungen und -bewertungen in dieser Stellungnahme wiederzugeben.

92. Auf der Grundlage der verfügbaren Informationen stellt der EDSA fest, dass in Bezug auf den Zugang der Strafverfolgungsbehörden zu Daten, die sich im Besitz von Unternehmen in den USA befinden, ein relativ solider unabhängiger Aufsichtsmechanismus vorhanden ist.

3.1.4 Den Betroffenen müssen wirksame Rechtsbehelfe zur Verfügung stehen

93. Nach der Rechtsprechung des EuGH muss eine natürliche Person einen wirksamen Rechtsbehelf einlegen können, damit sie von ihren Rechten Gebrauch machen kann, wenn diese ihrer Auffassung nach nicht geachtet werden oder wurden. Der EuGH erklärte in der Rechtssache Schrems I, dass „eine Regelung, die keine Möglichkeit für den Bürger vorsieht, mittels eines Rechtsbehelfs Zugang zu den ihn betreffenden personenbezogenen Daten zu erlangen oder ihre Berichtigung oder Löschung zu erwirken, den Wesensgehalt des in Art. 47 der Charta verankerten Grundrechts auf wirksamen gerichtlichen Rechtsschutz verletzt. Nach Art. 47 Abs. 1 der Charta hat nämlich jede Person, deren durch das Recht der Union garantierte Rechte oder Freiheiten verletzt worden sind, das Recht, nach

[91] Siehe Beschlussentwurf, Erwägungsgrund 92.
[92] Siehe Beschlussentwurf, Anhang VI, S. 3.
[93] Siehe Beschlussentwurf, Erwägungsgrund 90 und Anhang VI, S. 3.
[94] Siehe Beschlussentwurf, Anhang VI, S. 4, sowie Erwägungsgrund 91.
[95] Siehe Beschlussentwurf, Anhang VI, S. 4, sowie Erwägungsgrund 91.
[96] Siehe Beschlussentwurf, Erwägungsgründe 103–106.

Maßgabe der in diesem Artikel vorgesehenen Bedingungen bei einem Gericht einen wirksamen Rechtsbehelf einzulegen."[97]

94. Der Beschlussentwurf[98] und dessen Anhang VI enthalten weitere Informationen über mögliche Rechtsbehelfe, die sich aus dem Gesetzesrecht ergeben und natürlichen Personen zur Verfügung stehen, wenn Behörden unrechtmäßigen Zugang zu ihren Daten erhalten.

95. Diesbezüglich sieht nach Auffassung der Kommission[99], 5 U.S.C. § 702 (Administrative Procedure Act (APA)) vor, dass eine Person, die aufgrund des Handelns einer Behörde einen Rechtsirrtum erleidet oder durch das Handeln einer Behörde im Sinne eines einschlägigen Gesetzes beeinträchtigt oder geschädigt wurde, Anspruch auf gerichtliche Überprüfung hat.

96. Darüber hinaus sieht der Stored Communications Act (SCA) (erlassen als Titel II des Electronic Communications Privacy Act) vor, dass jede Person, die durch einen Verstoß gegen dieses Kapitel, bei dem das den Verstoß begründende Verhalten wissentlich oder vorsätzlich erfolgte, geschädigt wurde, im Rahmen einer Zivilklage von der Person oder Einrichtung (außer den Vereinigten Staaten), die diesen Verstoß begangen hat, gegebenenfalls eine angemessene Entschädigung fordern kann.[100] Darüber hinaus kann jede Person, die durch einen vorsätzlichen Verstoß gegen dieses Kapitel oder gegen Kapitel 119 geschädigt wurde, vor dem United States District Court eine Klage gegen die Vereinigten Staaten auf Schadensersatz erheben.[101]

97. Darüber hinaus enthält der Beschlussentwurf auch Informationen über das Recht auf Zugang zu Aufzeichnungen von Bundesbehörden gemäß dem Freedom of Information Act (FOIA)[102] und mehreren anderen Gesetzen, die natürlichen Personen das Recht einräumen, gegen eine US-Behörde oder einen US-Beamten in Bezug auf die Verarbeitung ihrer personenbezogenen Daten Klage zu erheben, wie den Wiretap Act, den Computer Fraud and Abuse Act, den Federal Torts Claim Act, den Right to Financial Privacy Act und den Fair Credit Reporting Act.[103]

98. Der EDSA begrüßt die Klarstellungen der Kommission bezüglich der Zahl der Rechtsmittelwege, die natürliche Personen beschreiten können. Der EDSA fordert die Kommission ferner auf, weiter zu klären, ob diese Rechtsbehelfe es der betroffenen Person ermöglichen, „Zugang zu den sie betreffenden personenbezogenen Daten zu erhalten oder die Berichtigung oder Löschung dieser Daten zu erwirken", wie vom EuGH gefordert.

3.1.5 Weiterverwendung der erhobenen Daten

3.1.5.1 Weiterverwendung von übermittelten Daten, auf die Strafverfolgungsbehörden in den USA zugreifen

99. Der EDSA begrüßt, dass in dem Beschlussentwurf auch die Weiterverwendung der Daten geprüft wird, auf die Strafverfolgungsbehörden in den USA zugreifen. Der EDSA bedauert allerdings, dass nur ein Beispiel für die Grundlagen angeführt wird, auf denen die Daten weiter verbreitet werden dürfen.[104]

[97] EuGH, Urteil Schrems I, Rn. 95.
[98] Siehe Beschlussentwurf, Erwägungsgründe 107 bis 112.
[99] Siehe Beschlussentwurf, Erwägungsgrund 109.
[100] 18 U.S.C. § 2707
[101] 18 U.S.C. § 2712
[102] Siehe Beschlussentwurf, Erwägungsgrund 111.
[103] Siehe Beschlussentwurf, Erwägungsgrund 112.
[104] Siehe Beschlussentwurf, Erwägungsgrund 102.

In diesem Zusammenhang empfiehlt der EDSA der Kommission, in den Beschlussentwurf weitere Klarstellungen zu den Grundsätzen und Garantien für die Weiterverwendung von Daten aufzunehmen, wie sie im Privacy Act (5 U.S.C. 552a) enthalten sind.[105]

3.1.5.2 Weiterübermittlungen in Länder außerhalb der USA

100. Der EDSA stellt ferner fest, dass die Europäische Kommission auch Weiterübermittlungen von Strafverfolgungsbehörden in den USA an Behörden in Drittländern angesprochen hat, aber auch hier nur in Bezug auf die Attorney General Guidelines for Domestic FBI Operations (Allgemeine Leitlinien des Generalstaatsanwalts für FBI-Operationen im Inland, AGG-DOM).[106] Nach Auffassung des EDSA sind solche Informationen und Bewertungen von wesentlicher Bedeutung, um eine umfassende Bewertung des Schutzniveaus zu ermöglichen, das durch den US-Rechtsrahmen und die Verfahrensweisen in Bezug auf die internationale Offenlegung und Weiterverwendung gewährt wird. Da die Kommission insgesamt nur ein – begrenztes – Beispiel zum Thema Weiterübermittlung in Länder außerhalb der USA angeführt hat, ersucht der EDSA die Kommission, die geltenden Vorschriften und Garantien für die Weiterübermittlung, die Weiterverwendung und die Offenlegung personenbezogener Daten, die für Strafverfolgungszwecke in den USA erhoben und anschließend an Drittländer übermittelt werden, auch im Rahmen internationaler Abkommen, weiter zu präzisieren.

3.2 Zugriff und Nutzung für Zwecke der nationalen Sicherheit

101. Generell räumt der EDSA ein, dass Staaten in Fragen der nationalen Sicherheit über einen weiten Ermessensspielraum verfügen, was auch vom EGMR anerkannt wird. Der EDSA erinnert ferner daran, dass – wie in seinen aktualisierten Empfehlungen zu den wesentlichen europäischen Garantien für Überwachungsmaßnahmen[107] betont – in Artikel 6 Absatz 3 des Vertrags über die Europäische Union festgelegt ist, dass die in der EMRK verankerten Grundrechte allgemeine Grundsätze des EU-Rechts darstellen. Wie der EuGH in seiner Rechtsprechung in Erinnerung gerufen hat, stellt die EMRK jedoch, solange die Union ihr nicht beigetreten ist, kein Rechtsinstrument dar, das formell in die Unionsrechtsordnung übernommen wurde.[108] Somit ist das in Artikel 45 DSGVO geforderte Niveau des Schutzes der Grundrechte auf der Grundlage der Bestimmungen dieser Verordnung im Licht der in der Charta der Grundrechte der Europäischen Union verankerten Grundrechte zu bestimmen. Allerdings haben nach Artikel 52 Absatz 3 der Charta der Grundrechte der Europäischen Union die darin enthaltenen Rechte, die den durch die EMRK garantierten Rechten entsprechen, die gleiche Bedeutung und Tragweite, wie sie ihnen in der EMRK verliehen wird. Folglich muss, wie vom EuGH ausgeführt, die Rechtsprechung des EGMR zu Rechten, die auch in der EU-Charta vorgesehen sind, als Mindestschutzstandard für die Auslegung der entsprechenden Rechte in der EU-Charta berücksichtigt werden.[109] In Artikel 52 Absatz 3 letzter Satz der Charta heißt es jedoch: „Diese Bestimmung steht dem nicht entgegen, dass das Recht der Union einen weiter gehenden Schutz gewährt."

102. Daher hat der EDSA bei der folgenden Bewertung die Rechtsprechung des EGMR insofern berücksichtigt, als die EU-Charta in ihrer Auslegung durch den EuGH kein höheres Schutzniveau vorsieht, das andere Anforderungen als die Rechtsprechung des EGMR vorschreibt.

---

[105] Siehe Attorney General Guidelines for Domestic FBI Operations (Allgemeine Leitlinien des Generalstaatsanwalts für FBI-Operationen im Inland) (AGG-DOM), S. 36, Punkt B 1 g.

[106] Siehe Beschlussentwurf, Erwägungsgrund 102.

[107] Siehe EDSA, Empfehlungen 02/2020 zu den wesentlichen europäischen Garantien in Bezug auf Überwachungsmaßnahmen.

[108] Siehe EuGH, Urteil Schrems II, Rn. 98.

[109] Siehe EuGH, Urteil La Quadrature du Net, Rn. 124.

103. Mehrere Rechtsinstrumente sehen die Möglichkeit vor, Daten für US-Nachrichtendienste im US-Rechtsrahmen zu erheben, weiter abzurufen und zu verarbeiten.

104. Wie die Europäische Kommission in ihrem Beschlussentwurf ausgeführt hat, „können US-Nachrichtendienste Zugang zu personenbezogenen Daten beantragen, die zu Zwecken der nationalen Sicherheit an Organisationen in den Vereinigten Staaten übermittelt wurden, und zwar nur, wenn dies gesetzlich, insbesondere nach dem Foreign Intelligence Surveillance Act (FISA) oder nach Rechtsvorschriften, die den Zugang mittels National Security Letters (NSL) gestatten, zulässig ist".[110] „US-Nachrichtendienste haben auch die Möglichkeit, personenbezogene Daten außerhalb der Vereinigten Staaten zu erheben, wozu auch personenbezogene Daten während der Übermittlung aus der Union in die Vereinigten Staaten gehören können" gemäß Executive Order 12333 (EO 12333).[111]

105. In Bezug auf die spezifischen Datenerhebungsregelungen, insbesondere Section 702 FISA und EO 12333, sieht die EO 14086 nun neue Vorschriften vor, um die Sicherheitsvorkehrungen für die US-amerikanischen Signalaufklärungstätigkeiten zu verbessern. Diese allgemeinen Vorschriften gelten horizontal und müssen „weiterhin durch Strategien und Verfahren der Behörden umgesetzt werden, mit denen sie in konkrete Anweisungen für den Alltagsbetrieb umgesetzt werden".[112] Die EO 14086 ersetzte größtenteils die frühere Presidential Policy Directive 28 („PPD-28").[113]

106. Um den rechtlichen Rahmen für die Erhebung von, den Zugang zu und die Weiterverarbeitung von Daten für Zwecke der nationalen Sicherheit zu bewerten, ist es daher wichtig, den spezifischen Rechtsrahmen für die Erhebung von Daten innerhalb und außerhalb der USA zu prüfen, d. h. Section 702 FISA und EO 12333, die sich als solche seit der letzten Überprüfung des Datenschutzschilds nicht geändert haben, wobei zu berücksichtigen ist, dass die neue Executive Order 14086 Garantien vorsieht, die auch im Zusammenhang mit der Erhebung von Daten auf der Grundlage spezifischer Texte wie Section 702 FISA und EO 12333 umzusetzen sind.

3.2.1 Garantie A – Die Verarbeitung sollte im Einklang mit dem Gesetz stehen und auf klaren, präzisen und zugänglichen Vorschriften beruhen

107. Für seine Bewertung des allgemeinen Aufbaus der Datenerhebung zum Zwecke der nationalen Sicherheit möchte der EDSA auf die erste der vier sogenannten „wesentlichen europäischen Garantien" hinweisen, die eine „auf klaren, präzisen und zugänglichen Vorschriften beruhende Datenverarbeitung" vorsieht [114].

108. Nach ständiger Rechtsprechung des EuGH muss jede Einschränkung des Rechts auf Schutz personenbezogener Daten gesetzlich vorgesehen sein, und die gesetzliche Grundlage für den Eingriff in ein solches Recht muss selbst den Umfang der Einschränkung der Ausübung des betreffenden Rechts

[110] Siehe Beschlussentwurf, Erwägungsgrund 115.
[111] Siehe Beschlussentwurf, Erwägungsgrund 117.
[112] Siehe Beschlussentwurf, Erwägungsgrund 120.
[113] Mit dieser Executive Order wird die PPD-28 aufgehoben, mit Ausnahme der Abschnitte 3 und 6 dieser Directive und des als Verschlusssache eingestuften Anhangs dieser Directive, die in Kraft bleiben. Siehe das Memorandum des Präsidenten zur nationalen Sicherheit vom 7. Oktober 2022.
[114] Empfehlungen 02/2020 zu den wesentlichen europäischen Garantien für Überwachungsmaßnahmen, angenommen am 10. November 2020. Siehe Rn. 175 und 180 Schrems II sowie Gutachten 1/15 (PNR-Abkommen EU-Kanada) vom 26. Juli 2017, Rn. 139 und die dort angeführte Rechtsprechung.

festlegen.[115] Der Gerichtshof erinnerte auch daran, dass „die Regelung nach nationalem Recht bindend sein [muss]".[116] Diesbezüglich wird in der Rechtsprechung des EGMR klargestellt, dass der Begriff „Recht" im materiellen und nicht im formellen Sinne zu verstehen ist. Dies kann auch den Erlass nachrangiger Gesetze und Vorschriften durch berufsständische Regulierungsstellen im Rahmen unabhängiger Rechtsetzungsbefugnisse umfassen, die ihnen vom Parlament übertragen wurden, und sogar ungeschriebenes Recht. Um „gesetzlich" zu sein, muss eine Norm zumindest angemessen zugänglich und hinreichend präzise formuliert sein.[117]

109. Der erforderliche Grad an Genauigkeit ist im Verhältnis zum Umfang der Einschränkung des Rechts zu messen.[118] In Bezug auf die „Vorhersehbarkeit" des Gesetzes wies der EGMR im Urteil in der Rechtssache *Zakharov* ferner darauf hin, dass im Zusammenhang mit geheimen Überwachungsmaßnahmen wie der Überwachung von Kommunikation „Vorhersehbarkeit nicht bedeuten [kann], dass eine Person vorhersehen kann, wann die Behörden ihre Kommunikation wahrscheinlich abfangen, damit sie ihr Verhalten entsprechend anpassen kann". Klare und detaillierte Regeln für geheime Überwachungsmaßnahmen sind jedoch unerlässlich, um dem Risiko der Willkür vorzubeugen, wenn eine der Exekutive übertragene Befugnis geheim ausgeübt wird. „Das innerstaatliche Recht muss hinreichend klar sein, um den Bürgern einen angemessenen Hinweis darauf zu geben, unter welchen Umständen und unter welchen Voraussetzungen die Behörden befugt sind, auf solche Maßnahmen zurückzugreifen."[119]

110. Darüber hinaus stellte der EuGH klar, dass sich die Bewertung des anwendbaren Drittlandsrechts darauf konzentrieren sollte, ob natürliche Personen es vor Gericht geltend machen und sich darauf berufen können. Die betroffenen Personen gewährten Rechte sollten insbesondere vor Gericht durchsetzbar sein, und natürliche Personen müssen Rechte erhalten, die gegenüber Behörden durchsetzbar sind[120], was im Zusammenhang mit der vorherigen PPD-28 nicht der Fall war. Die EO 14086, die nach dem Verständnis des EDSA in der amerikanischen Rechtsordnung die gleiche Rechtswirkung hat wie PPD-28 (d. h. für die Exekutive verbindlich ist), sieht nun vor Gericht durchsetzbare Ansprüche gegen Behörden vor. Eine detaillierte Bewertung der neuen durchsetzbaren Rechte betroffener Personen findet sich im Abschnitt über Rechtsbehelfe.

111. Die Erwägungsgründe 114–152 des Beschlussentwurfs und Anhang VII enthalten eine zusammenfassende Darstellung einiger Aspekte des geltenden Rechtsrahmens, wie Einschränkungen bei der Erhebung, Einschränkungen für Speicherung und Verbreitung, Einhaltung von Vorschriften und Aufsicht, Transparenz und Rechtsschutz. Das US-amerikanische Rechtssystem für nachrichtendienstliche Tätigkeiten besteht aus einer Reihe verschiedener Dokumente, darunter Berichte, Strategien und Verfahren einzelner Behörden. In diesem Zusammenhang konzentriert sich der EDSA in seiner Bewertung auf eine begrenzte Zahl von Fragen, die er für wesentlich hält.

112. Gemäß den Erwägungsgründen 115 bis 119 des Beschlussentwurfs darf ein Zugriff nationaler Sicherheitsbehörden der USA auf übermittelte personenbezogene Daten nur erfolgen nach dem FISA, nach anderen gesetzlichen Vorschriften (12 U.S.C. § 3414, 15 U.S.C. § 1681u-1681v und 18 U.S.C.

[115] Siehe Urteil des EuGH, Schrems II, Rn. 174–175 und die dort angeführte Rechtsprechung. Zum Zugang von Behörden der Mitgliedstaaten siehe auch Rechtssache C-623/17, Privacy International, ECLI:EU:C:2020:790 (im Folgenden „EuGH, Urteil Privacy International"), Rn. 65, und EuGH, Urteil La Quadrature du Net, Rn. 175.
[116] EuGH, Urteil Privacy International, Rn. 68.
[117] EGMR, Sunday Times/Vereinigtes Königreich (Nr. 1), 26. April 1979, CE:ECHR:1979:0426JUD000653874 (im Folgenden „EGMR, Urteil Sunday Times/Vereinigtes Königreich Nr. 1"), Rn. 49.
[118] EGMR, Urteil Sunday Times/Vereinigtes Königreich Nr. 1, Rn. 49.
[119] EGMR, Zakharov/Russland, 4. Dezember 2015 (im Folgenden „EGMR, Urteil Zakharov"), Rn. 229.
[120] EuGH, Urteil Schrems II, Rn. 181.

§ 2709) oder, wenn es um personenbezogene Daten während der Übermittlung geht, auf der Grundlage der EO 12333. Aus den Erwägungsgründen 116 und 118 des Beschlussentwurfs geht hervor, dass die Kommission ihre Bewertung im Zusammenhang mit dem Zugriff der nationalen Sicherheitsbehörden der USA auf personenbezogene Daten auf die Sections 105, 302, 402, 501 und 702 FISA (ausländische nachrichtendienstliche Tätigkeiten gegen außerhalb der USA ansässige Nicht-US-Personen) und auf die EO 12333 (ausländische nachrichtendienstliche Tätigkeiten in Bezug auf personenbezogene Daten während der Übermittlung) konzentriert. Die Stellungnahme des EDSA beschränkt sich daher auf die Bewertung dieser Bestimmungen durch die Kommission unter Berücksichtigung der in der EO 14086 festgelegten Beschränkungen und Garantien.[121]

113. In diesem Zusammenhang sei darauf hingewiesen, dass alle im Beschlussentwurf genannten Rechtsinstrumente für die breite Öffentlichkeit (innerhalb und außerhalb der USA) zugänglich und online verfügbar sind. Darüber hinaus sind die in der EO festgelegten Anforderungen für die gesamte Intelligence Community bindend[122] und gelten bereichsübergreifend für alle Tätigkeiten der Auslandsaufklärung.

114. Der Begriff „Signalaufklärung" ist in der EO 14086 nicht definiert. Letztere verweist auf die Begriffsbestimmungen in der EO 12333 für die Festlegung des Umfangs von Auslandsaufklärung und Spionageabwehr, die weit gefasst sind. In diesem Zusammenhang weist der EDSA darauf hin, dass die EO 12333 seit der Einführung des FISA nur für die Erhebung von Daten außerhalb des Hoheitsgebiets der USA verwendet werden kann, doch erinnert der EDSA daran, dass die EO 12333 selbst, die unverändert geblieben ist, keine ausreichenden Angaben über ihren geografischen Geltungsbereich, den Umfang, in dem Daten erhoben, gespeichert oder weiter verbreitet werden können, oder über die Art der Straftaten, die zu einer Überwachung führen können, oder die Art der Informationen, die erhoben oder verwendet werden können, enthält. Grundsätzlich kann jede Erhebung von Auslandsaufklärungsdaten im Rahmen der EO 12333 nach dem Ermessen des US-Präsidenten erfolgen.[123] Nach dem Verständnis des EDSA besteht jedoch der Hauptzweck der EO 14086 darin, die Grenzen für die Erhebung und Verarbeitung personenbezogener Daten im Rahmen der Auslandsaufklärung festzulegen, unabhängig davon, welches Überwachungsprogramm verwendet wird und wo Daten erlangt werden. Der EDSA geht daher davon aus, dass die in der EO 14086 vorgesehenen zusätzlichen Garantien auch bei Überwachungsprogrammen angewandt werden, die für personenbezogene Daten während der Übermittlung im Rahmen des EO 12333 gelten.[124]

115. In diesem Zusammenhang werden in der EO 14086 zwölf legitime Ziele aufgeführt, die bei der Datenerhebung durch Signalaufklärung verfolgt werden sollten, fünf Ziele, für die keine Signalaufklärung durchgeführt werden darf[125], sowie sechs legitime Ziele für die Nutzung von in großen Mengen erhobenen Daten[126]. Während einige von ihnen recht detailliert sind (z. B. „Rettung von Geiseln"), sind andere allgemeiner gehalten (z. B. „globale Sicherheit"). Die EO 14086 enthält auch eine Liste verbotener Ziele, zu denen insbesondere die Unterdrückung oder Einschränkung „berechtigter

121 Mit dieser Executive Order wird die PPD-28 aufgehoben, mit Ausnahme der Abschnitte 3 und 6 dieser Directive und des als Verschlusssache eingestuften Anhangs dieser Directive, die in Kraft bleiben. Siehe Memorandum des Präsidenten zur nationalen Sicherheit vom 7. Oktober 2022

122 Siehe Beschlussentwurf, Erwägungsgrund 120.

123 Gemäß Artikel II der US-Verfassung fällt die Verantwortung für die Gewährleistung der nationalen Sicherheit, insbesondere die Sammlung von Erkenntnissen durch Auslandsaufklärung, in die Zuständigkeit des Präsidenten als Oberbefehlshaber der Streitkräfte.

124 Siehe Beschlussentwurf, Erwägungsgrund 134.

125 Siehe Executive Order 14086 („EO 14086"), Section 2 b ii A, 1 bis 5.

126 Siehe Beschlussentwurf, Erwägungsgrund 134, und EO 14086, Section 2 c ii.

Datenschutzinteressen" gehört.[127] Die EO 14086 sieht ferner die Möglichkeit für den Präsidenten der Vereinigten Staaten vor, weitere Ziele in die Liste aufzunehmen, für die die Erhebung zulässig ist, die auf Beschluss des Präsidenten nicht für die Öffentlichkeit freigegeben werden könnten, wenn er der Auffassung ist, dass dies eine Gefahr für die nationale Sicherheit der Vereinigten Staaten darstellen würde.[128] Solche Aktualisierungen dürfen nur „unter Berücksichtigung neuer Erfordernisse der nationalen Sicherheit" genehmigt werden.

116. Die Ziele allein können von den Nachrichtendiensten nicht zur Rechtfertigung der Erhebung von Daten im Rahmen von Signalaufklärung herangezogen werden, sondern müssen für operative Zwecke in konkreteren Prioritäten begründet werden, für die Signalaufklärungsdaten erhoben werden dürfen. In der EO 14086 ist das Verfahren für die Validierung der Prioritäten festgelegt, für die Signalaufklärungsdaten erhoben werden dürfen.[129] Der EDSA geht davon aus, dass sich das Verfahren zur Festlegung der validierten nachrichtendienstlichen Prioritäten grundsätzlich auf den Director of the Intelligence Community (Direktor der Gesamtheit der Nachrichtendienste) stützt, und erkennt an, dass es in der Regel die Bewertung des Civil Liberties Protection Officer (CLPO) of the Office of the Director of National Intelligence (Beauftragter für den Schutz der bürgerlichen Freiheiten des Amtes des Direktors des nationalen Nachrichtendienstes) umfassen sollte, der der Direktor nicht zustimmen muss; in diesem Fall muss es „die Bewertung des CLPO und die Ansichten des Direktors bei der Vorlage des National Intelligence Priorities Framework (Nationaler Rahmen für Prioritäten im Bereich der Nachrichtengewinnung) (NIPF) beim Präsidenten umfassen".[130]

117. Der EDSA stellt jedoch auch fest, dass diese Prioritäten gemäß der Definition des Begriffs „validated intelligence priority" (validierte nachrichtendienstliche Priorität) für die „meisten Tätigkeiten der Vereinigten Staaten zur Erhebung von Signalaufklärungsdaten"[131] jeweils Prioritäten bedeuten, die gemäß Section 2 b iii der EO (siehe vorstehender Absatz) validiert wurden. Das Validierungsverfahren kann sich in einigen Fällen unter „eng umrissenen Umständen" von diesem Verfahren unterscheiden; in diesem Fall kann der Präsident oder der Leiter eines Elements der Intelligence Community gemäß den Kriterien in Section 2 b iii A Absätze 1 bis 3, die die angemessene Berücksichtigung der Privatsphäre und der bürgerlichen Freiheiten aller Personen vorsieht, jedoch ohne Beteiligung des CLPO, „soweit möglich" eine Priorität festlegen.

118. In der EO 14086 wird darüber hinaus betont, dass „Tätigkeiten zur Erhebung von Signalaufklärungsdaten so exakt zugeschnitten wie möglich sein müssen", um einer validierten nachrichtendienstlichen Priorität zu dienen, und dass die „Intelligence Community die Verfügbarkeit, Durchführbarkeit und Angemessenheit anderer, weniger einschneidender Quellen prüft" und allgemeine Anforderungen an die Erforderlichkeit und Verhältnismäßigkeit formuliert.[132]

119. Darüber hinaus begründet die EO 14086 in Section 5 h das Recht, beim CLPO zulässige Beschwerden einzureichen und eine Überprüfung der Entscheidungen des CLPO durch den Data Protection Review Court im Einklang mit dem in Section 3 dieser EO vorgesehenen Rechtsschutzverfahren zu erwirken.

120. In Bezug auf die Art der nachrichtendienstlichen Operationen, die angeordnet werden können, scheint der Wortlaut des FISA klarer und präziser als der der EO 12333. FISA und EO 12333 müssen nun vor

[127] Siehe EO 14086, Section 2 b ii A 2.
[128] Siehe EO 14086, Section 2 b i B.
[129] Siehe Beschlussentwurf, Erwägungsgrund 129.
[130] Siehe EO 14086, Section 2 b iii B.
[131] Siehe EO 14086, Section 4 n.
[132] Siehe EO 14086, Section 2 c i A und B.

dem Hintergrund der EO 14086 und insbesondere unter Berücksichtigung u. a. der Grundsätze der Erforderlichkeit und Verhältnismäßigkeit angewandt werden.

121. Die in der EO 14086 festgelegten Anforderungen müssen durch behördliche Strategien und Verfahren näher umgesetzt und für den Alltagsbetrieb konkretisiert werden. In diesem Zusammenhang setzt die EO 14086 den US-Nachrichtendiensten eine Frist von höchstens einem Jahr für die Aktualisierung ihrer bestehenden Strategien und Verfahren (d. h. bis zum 7. Oktober 2023), um sie mit den Anforderungen der EO in Einklang zu bringen. Solche aktualisierten Strategien und Verfahren müssen in Absprache mit dem Attorney General, dem CLPO und dem Privacy and Civil Liberties Oversight Board (PCLOB) entwickelt und so weit wie möglich öffentlich zugänglich gemacht werden. [133]

122. Der EDSA würde es begrüßen, wenn Bedingung nicht nur für das Inkrafttreten, sondern auch für die Annahme des Beschlusses unter anderem die Annahme aktualisierter Strategien und Verfahren zur Umsetzung der EO 14086 durch alle US-Nachrichtendienste wäre. Der EDSA empfiehlt der Kommission, diese aktualisierten Strategien und Verfahren zu bewerten und diese Bewertung dem EDSA mitzuteilen.

123. Schließlich stellt der EDSA in Bezug auf die Speicherung der übermittelten Daten, die einmal zu Zwecken der nationalen Sicherheit erhoben wurden, fest, dass die EO 14086 sicherstellt, dass die für personenbezogene Daten von US-Bürgern geltenden Vorschriften auch für personenbezogene Daten von Nicht-US-Bürgern gelten. [134] Aus dem Beschlussentwurf geht hervor, dass diese Vorschriften in Section 309 des Intelligence Authorisation Act for Fiscal Year 2015 enthalten sind[135], in dem für jede nichtöffentliche Telefon- oder elektronische Kommunikation, die ohne Einwilligung der Person erlangt wurde, grundsätzlich eine maximale Speicherfrist von fünf Jahren festgelegt ist. Der EDSA empfiehlt der Kommission in diesem Zusammenhang, in dem Beschluss mehr Klarheit in Bezug auf ihre Bewertung der für personenbezogene Daten von US-Bürgern geltenden Vorschriften zu schaffen.

3.2.2 Garantie B – Nachweis der Erforderlichkeit und Verhältnismäßigkeit im Hinblick auf die verfolgten legitimen Ziele

3.2.2.1 Horizontale Garantien in der neuen Executive Order 14086 – Erforderlichkeit und Verhältnismäßigkeit

124. Die neue EO 14086, die generell die PPD-28 ersetzt, zielt darauf ab, Vorschriften zur Verbesserung der Garantien für Signalaufklärungstätigkeiten der Vereinigten Staaten festzulegen, die von den Elementen der Intelligence Community in ihren internen Strategien und Verfahren weiter umgesetzt werden sollen.

125. Mit der EO 14086 werden zwei neue Anforderungen in das US-Recht eingeführt, die den Anforderungen entsprechen, auf die der EuGH in seinem Schrems-II-Urteil hingewiesen hat, nämlich dass Signalaufklärungstätigkeiten nur insoweit durchgeführt werden dürfen, als dies erforderlich ist, um eine validierte nachrichtendienstliche Prioritätensammlung voranzubringen, und nur in dem Umfang und in einer Weise, die in einem angemessenen Verhältnis zu der validierten nachrichtendienstlichen Priorität stehen. [136]

[133] Siehe EO 14086, Section 2 c iv B und C.
[134] Beschlussentwurf, Erwägungsgrund 150.
[135] Beschlussentwurf, Fußnote 272.
[136] Siehe EO 14086, Section 2 a ii A und B.

126. Nach dem Verständnis des EDSA wurden diese Elemente aufgenommen, um den Grundsätzen der Erforderlichkeit und Verhältnismäßigkeit Rechnung zu tragen, die im EU-Recht und in der Rechtsprechung des EuGH und des EGMR vorgesehen sind und sicherstellen sollen, dass die Erhebung und Verarbeitung von Daten auf das erforderliche und verhältnismäßige Maß beschränkt wird.

127. In diesem Zusammenhang erinnert der EDSA an das für die Validierung nachrichtendienstlicher Prioritäten vorgesehene Verfahren sowie auf die mögliche Ausnahmeregelung (siehe Ziffern 116, 117).

128. Darüber hinaus stellt der EDSA fest, dass diese in der EO genannten Grundsätze der Erforderlichkeit und Verhältnismäßigkeit innerhalb eines Jahres in den Strategien und Verfahren jedes einzelnen Nachrichtendienstes operationalisiert und umgesetzt werden müssen.[137]

3.2.2.2 Besondere Garantien für die Erhebung von Signalaufklärungsdaten

129. Der EDSA stellt ferner fest, dass die EO 14086 Einschränkungen hinsichtlich der Ziele vorsieht, zu denen personenbezogene Daten im Zusammenhang mit Signalaufklärung erhoben bzw. nicht erhoben werden können.[138]

130. Der EDSA begrüßt, dass nach der EO die gezielte Erhebung von Daten Vorrang vor der Erhebung von Daten in großen Mengen hat.[139] Im Zusammenhang mit der Erhebung von Signalaufklärungsdaten enthält die EO eine Liste von 12 Zielen, für die Daten erhoben werden können, die in nachrichtendienstlichen Prioritäten näher zu begründen sind (siehe Ziffer 117), sowie eine Liste mit fünf Zielen, für die keine Maßnahmen zur Erhebung von Signalaufklärungsdaten durchgeführt werden dürfen.[140] Grundsätzlich sind diese Bestimmungen eine Garantie dafür, dass die Erforderlichkeit der Erhebung von Daten gewährleistet ist.

131. Der EDSA erinnert jedoch daran, dass in der EO 14086 auch vorgesehen ist, dass der Präsident der Vereinigten Staaten weitere Ziele in die Liste aufnehmen kann (siehe Ziffern 114 und 115).[141]

3.2.2.3 Besondere Garantien für die Erhebung von Daten in großen Mengen

132. Dem Urteil des EuGH in der Rechtssache Schrems I zufolge „verlangt der Schutz des Grundrechts auf Achtung des Privatlebens auf Unionsebene…, dass sich die Ausnahmen vom Schutz personenbezogener Daten und dessen Einschränkungen auf das absolut Notwendige beschränken“[142], und der Gerichtshof befand dort, dass „eine Regelung, die es den Behörden gestattet, generell auf den Inhalt elektronischer Kommunikation zuzugreifen, den Wesensgehalt des durch Art. 7 der Charta garantierten Grundrechts auf Achtung des Privatlebens [verletzt]“.

133. In der Rechtssache Schrems II[143] unterstrich der Gerichtshof, wie bereits erwähnt, im Hinblick auf seine Analyse der Sammelerhebung vor dem Hintergrund sowohl der EO 12333 als auch der PPD-28 insbesondere in den Randnummern 183 bis 185 Folgendes: „Hinsichtlich dieser im Rahmen der auf die E.O. 12333 gestützten Überwachungsprogramme bestehenden Möglichkeit, auf Daten während ihrer Übermittlung in die Vereinigten Statten zuzugreifen, ohne dass dieser Zugriff irgendeiner gerichtlichen

[137] Siehe EO 14086, Section 2 c iv B.
[138] Siehe EO 14086, Section 2 b i A, 1 bis 12
[139] Siehe EO 14086, Section 2 c ii A.
[140] Siehe EO 14086, Section 2 b ii A, 1 bis 5.
[141] Siehe EO 14086, Section 2 b i B.
[142] EuGH, Urteil Schrems I, Rn. 92.
[143] Siehe EuGH, Urteil Schrems II.

Kontrolle unterläge, besteht jedenfalls keine hinreichend klare und präzise Eingrenzung des Umfangs einer solchen Sammelerhebung personenbezogener Daten. “

134. Der EDSA stellt daher fest, dass der EuGH die Sammelerhebung nicht grundsätzlich ausgeschlossen hat, sondern in seiner Schrems-II-Entscheidung die Auffassung vertrat, dass eine solche Sammelerhebung nur dann rechtmäßig ist, wenn eine hinreichend klare und präzise Eingrenzung des Umfangs einer Sammelsammlung gegeben ist.

135. Der EDSA erkennt ferner an, dass die EO 14086 zwar die PPD-28 ersetzt, jedoch neue Garantien und Beschränkungen für die Erhebung und Verwendung von Daten vorsieht, die außerhalb der USA erhoben werden, da die Beschränkungen des FISA oder anderer spezifischerer US-Gesetze nicht gelten.

136. In Bezug auf die Sammelerhebung von Daten nimmt der EDSA zur Kenntnis, dass nach der EO 14086 Sammelerhebungen weiterhin zulässig sind. Tatsächlich betont der EDSA, dass sich an der Definition des Begriffs „Sammelerhebung“ gegenüber der vorherigen PPD-28 nicht geändert hat: „Sammelerhebungen von Signalaufklärungsdaten: die genehmigte Erhebung großer Mengen von Signalaufklärungsdaten, die aus technischen oder operativen Gründen ohne den Einsatz von Diskriminanten (z. B. ohne Verwendung spezifischer Kennungen oder Auswahlbegriffe) erlangt werden.“[144]

137. Seit dem Schrems-II-Urteil hat der Gerichtshof die für die Sammelerhebung erforderlichen Garantien noch nicht genau festgelegt. Der EDSA erinnert jedoch daran, dass der EGMR wichtige Entscheidungen zur Sammelerhebung und zu den einschlägigen Garantien in diesem Zusammenhang erlassen hat.

138. Der EDSA weist darauf hin, dass Sammelerhebungen, die die Erhebung großer Datenmengen ohne Diskriminanten ermöglichen, für natürliche Personen ein höheres Risiko[145] darstellen als eine gezielte Erhebung und daher zusätzliche Garantien erforderlich machen.

139. Der EDSA stellt ferner fest, dass der EuGH weitere Rechtsprechung zur Vorratsspeicherung von Verkehrs- und Standortdaten und zum anschließenden Zugriff auf diese von Telekommunikationsbetreibern gespeicherten Daten, auch zu Zwecken der nationalen Sicherheit, entwickelt hat, die, auch wenn sie in diesem Zusammenhang nicht als unmittelbar anwendbar angesehen werden kann, in gewissem Maße für die vorliegende Bewertung der Sammelerhebung im Zusammenhang mit der EO 12333 relevant sein könnte.

1) <u>Zweckbindung</u>

140. Der EO zufolge sollten Sammelerhebungen nur dann erfolgen, wenn festgestellt wurde, dass „die Informationen, die erforderlich sind, um eine validierte nachrichtendienstliche Priorität voranzubringen, nach vernünftigem Ermessen nicht durch gezielte Erhebung erlangt werden können“[146], und dass „das Element der Intelligence Community angemessene Methoden und technische Maßnahmen anwendet, um die erhobenen Daten auf das Maß zu beschränken, das erforderlich ist, um eine validierte nachrichtendienstliche Priorität voranzubringen, während

[144] Siehe EO 14086, Section 4 b.

[145] Siehe beispielsweise EGMR (Große Kammer), Big Brother Watch u. a./Vereinigtes Königreich, 25. Mai 2021 (im Folgenden „EGMR, Urteil Big Brother Watch“), Erwägungsgrund 363, wo der Gerichtshof feststellt, dass er „nicht davon überzeugt [ist], dass der Erwerb verbundener Kommunikationsdaten durch massenhaftes Abfangen notwendigerweise weniger einschneidend ist als die Beschaffung von Inhalten“.

[146] EO 14086, Section 2 c ii A.

gleichzeitig die Erhebung nicht relevanter Informationen minimiert wird“[147]. Zusätzlich zu diesen Garantien erkennt der EDSA auch an, dass aus Sammelerhebungen stammende Daten zur Verwirklichung eines oder mehrerer der sechs aufgeführten Ziele verwendet werden müssen.[148] Der EDSA betont ferner, dass diese Ziele zwar detaillierter sind als die in der früheren PPD-28, die im Wesentlichen durch die EO 14086 ersetzt wurde, dass aber der Umfang dieser Erhebungsmöglichkeiten potenziell weit gefasst ist, d. h. große Datenmengen umfasst.

141. Der EDSA erinnert weiter daran, dass die EO 14086 dem Präsidenten der Vereinigten Staaten auch die Möglichkeit einräumt, weitere Ziele in die Liste aufzunehmen (siehe Ziffer 115).[149]

2) <u>Vorherige unabhängige Genehmigung</u>

142. Der EDSA betont, dass der EGMR der vorherigen unabhängigen Genehmigung im Zusammenhang mit der Sammelerhebung von Daten für Zwecke der nationalen Sicherheit große Bedeutung beimisst. Der Gerichtshof befand nämlich insbesondere, dass „um das Risiko eines Missbrauchs der Befugnis zur Massenüberwachung so gering wie möglich zu halten, der Gerichtshof der Auffassung ist, dass das Verfahren ‚Ende-zu-Ende-Schutzmaßnahmen‘ unterliegen muss, was bedeutet, dass auf nationaler Ebene in jeder Phase des Verfahrens die Erforderlichkeit und Verhältnismäßigkeit der ergriffenen Maßnahmen zu beurteilen ist; dass Massenüberwachung von Anfang an einer unabhängigen Genehmigung unterliegen sollte, wenn Gegenstand und Umfang der Maßnahme festgelegt werden, und dass die Operation unter Aufsicht erfolgen und einer unabhängigen Ex-post-Überprüfung unterzogen werden sollte. Nach Auffassung des Gerichtshofs handelt es sich hierbei um grundlegende Garantien, die den Eckpfeiler eines jeden mit Artikel 8 konformen Systems für Massenüberwachung bilden werden.“[150]

143. Der EDSA nimmt ferner die folgende Randnummer dieses Urteils der Großen Kammer zur Kenntnis, in der der Straßburger Gerichtshof weiter hervorhebt, dass er „mit der Kammer übereinstimmt, dass die richterliche Genehmigung zwar ein wichtiger Schutz gegen Willkür‘ ist, aber keine „notwendige Anforderung“ ist (siehe Rn. 318–320 des Urteils der Kammer). Dennoch sollte eine Massenüberwachung von einer unabhängigen Stelle genehmigt werden, also von einer Stelle, die von der Exekutive unabhängig ist“[151].

144. In diesem Zusammenhang stellt der EDSA fest, dass die EO eine solche unabhängige vorherige Genehmigung für die Sammelerhebung nicht vorsieht und dass dies auch in der EO 12333 nicht vorgesehen ist (siehe weiter unten den Abschnitt über die EO 12333).

3) <u>Vorschriften für die Speicherung</u>

145. Der EDSA erinnert daran, dass eine weitere wichtige Reihe von Garantien die Vorschriften für die Dauer der Erhebung und Speicherung von Daten sind. In diesem Zusammenhang betonte der EGMR, dass „im innerstaatlichen Recht eine Begrenzung der Dauer des Abfangens, des Verfahrens für die Prüfung, Verwendung und Speicherung der erlangten Daten, der Vorsichtsmaßnahmen bei der Übermittlung der Daten an andere Parteien und der Umstände, unter denen abgefangene Daten gelöscht oder

[147] EO 14086, Section 2 c ii A.
[148] EO 14086, Section 2 c ii B.
[149] Siehe EO 14086, Section 2 c ii C.
[150] Siehe EGMR, Urteil Big Brother Watch, Rn. 350.
[151] Siehe EGMR, Urteil Big Brother Watch, Rn. 351.

vernichtet werden können oder müssen, festgelegt werden sollte“[152], da diese Garantien „für die Massenüberwachung gleichermaßen relevant sind“[153].

146. In diesem Zusammenhang geht der EDSA davon aus, dass die EO Vorschriften für die Vorratsspeicherung von Daten für personenbezogene Daten, die durch Signalaufklärung, einschließlich großer Datenmengen, erhoben wurden, vorsieht.[154] Der EDSA stellt fest, dass gemäß Section 2 c iii A der EO 14086 jedes Element der Intelligence Community, das personenbezogene Daten verarbeitet, die im Rahmen der Signalaufklärung erhoben wurden, Strategien und Verfahren festlegen und anwenden muss, die darauf abzielen, die Verbreitung und Speicherung personenbezogener Daten, die durch Signalaufklärung erhoben wurden, auf ein Mindestmaß zu beschränken. Diese Vorschriften sehen jedoch keine spezifische Speicherfrist vor, sondern beziehen sich allgemein auf dieselben Vorschriften, wie sie für die Vorratsspeicherung von Daten über US-Bürger und für Situationen gelten, in denen keine endgültige Speicherfrist festgelegt wurde. Der EDSA befürchtet daher, dass diese Aufbewahrungsfristen, wie für gezielte Erhebungen (siehe Ziffer 122), in dieser EO in Bezug auf mit Sammelerhebungen erhobene Daten nicht klar definiert sind. Er fordert die Kommission auf, ihre Bewertung der Erforderlichkeit und Verhältnismäßigkeit der für US-Bürger geltenden Speicherfristen und die verfügbaren Informationen über Speicherfristen in der Praxis, wenn nach US-Recht keine endgültige Speicherfrist festgelegt wurde, mitzuteilen, da der Beschlussentwurf an diese allgemeine Regel lediglich in einem kurzen Absatz[155] und in einer Fußnote[156] erinnert, anhand derer nicht festgestellt werden kann, ob diese Speicherfristen erforderlich und verhältnismäßig sind. Da dies, wie vom EGMR betont, eine entscheidende Garantie dafür ist, dass betroffene Personen ihre Rechte in einem Kontext ausüben können, in dem zunächst einmal eine besonders einschneidende Maßnahme zur Erhebung ihrer Daten ergriffen wird, fordert der EDSA die Europäische Kommission auf, weitere Erläuterungen zu den unterschiedlichen Speicherfristen in der Praxis zu geben.

4) Garantien für die „Verbreitung“

147. Ferner erinnert der EDSA daran, dass der EGMR zur Gewährleistung der Wirksamkeit der Erforderlichkeit und Verhältnismäßigkeit sowie des Grundsatzes der Zweckbindung auch die Bedeutung gesetzlicher Vorschriften über die weitere Verbreitung der, auch durch Sammelerhebungen, erhobenen Daten anerkannt hat.[157]

148. Nach Section 2 c iii A 1 c der EO 14086 dürfen Informationen über Nicht-US-Bürger, die durch Signalaufklärungstätigkeiten erhoben wurden, nur verbreitet werden, wenn eine befugte und angemessen geschulte Person Grund zu der Annahme hat, dass die personenbezogenen Daten angemessen geschützt sein werden und der Empfänger Kenntnis von den Informationen haben muss.

149. In Anbetracht dessen geht der EDSA davon aus, dass die Bestimmungen über die Verbreitung gemäß der EO 14086 kein ausdrückliches Verbot der Verbreitung für andere Zwecke als Zwecke der nationalen Sicherheit vorsehen, wenn es um die Weitergabe an zuständige US-Behörden geht.[158] Der EDSA fordert die Kommission auf, die in diesem Fall geltenden Vorschriften und Garantien weiter zu präzisieren.

[152] Siehe EGMR, Urteil Big Brother Watch, Rn. 348.
[153] Siehe EGMR, Urteil Big Brother Watch, Rn. 348.
[154] Siehe EO 14086, Section 2 c iii A 2 a bis c.
[155] Siehe Beschlussentwurf, Nr. 150.
[156] Siehe Beschlussentwurf, Fußnote 271.
[157] Siehe EGMR, Urteil Big Brother Watch, Rn. 348.
[158] Siehe EO 14086, Section 2 c iii A 1.

150. Der EDSA befürchtet daher, dass die von den zuständigen Behörden der Intelligence Community erlangten Daten dann im Rahmen strafrechtlicher Ermittlungen zum Zwecke der Bekämpfung von Kriminalität, einschließlich schwerer Straftaten, an die zuständigen US-Behörden weitergegeben werden könnten, wodurch den Strafverfolgungsbehörden ohne weitere spezifische Einschränkungen die Möglichkeit gegeben würde, Daten zu erlangen, deren direkte Erhebung ihnen untersagt gewesen wäre, und fordert die Kommission auf, diesen Punkt weiter zu prüfen.

151. Im spezifischen Kontext der Weiterübermittlung (Verbreitung an Empfänger außerhalb der Regierung der Vereinigten Staaten, einschließlich an eine ausländische Regierung oder internationale Organisation[159]) erinnert der EDSA daran, dass seiner Auffassung nach der Datenschutz auch im Zusammenhang mit Weiterübermittlungen, einschließlich im Bereich der nationalen Sicherheit, gewahrt werden sollte.[160]

152. In diesem Zusammenhang sieht die EO einige Garantien vor, nämlich die Verpflichtung, vor der Verbreitung der Daten dem Zweck der Verbreitung – ohne jedoch ausdrücklich zu verlangen, dass der Zweck der Verbreitung auch dem Schutz der nationalen Sicherheit dienen sollte –, der Art und dem Umfang der zu verbreitenden personenbezogenen Daten und den möglicherweise nachteiligen Folgen für die betroffene(n) Person(en) gebührend Rechnung zu tragen.

153. Der EDSA erkennt zwar an, dass einige dieser Garantien, insbesondere die Berücksichtigung der „möglicherweise nachteiligen Folgen“[161] für die betroffene(n) Person(en), einige Anforderungen der EMRK widerspiegeln, betont jedoch auch, dass der Straßburger Gerichtshof darüber hinaus eine rechtsverbindliche Verpflichtung verlangt, „zu prüfen und festzustellen, ob der ausländische Empfänger von Erkenntnissen ein annehmbares Mindestmaß an Garantien bietet“[162], die der EDSA in den Bestimmungen der EO über die Verbreitung an ausländische Empfänger nicht in ausdrücklicher Form feststellen kann. Der EDSA fordert die Kommission daher auf, dieses Element weiter zu prüfen.

154. Der EDSA stellt ferner fest, dass die Europäische Kommission bei ihrer Angemessenheitsprüfung nicht berücksichtigt hat, ob mit Drittländern oder internationalen Organisationen geschlossene internationale Abkommen bestehen, die möglicherweise spezifische Bestimmungen für die internationale Übermittlung personenbezogener Daten durch Nachrichtendienste an Drittländer enthalten. Nach Auffassung des EDSA dürfte sich der Abschluss bilateraler oder multilateraler Abkommen mit Drittländern für die Zwecke der nachrichtendienstlichen Zusammenarbeit wahrscheinlich auf den bewerteten Rechtsrahmen für den Datenschutz auswirken.

155. Der EDSA fordert die Europäische Kommission daher auf, abzuklären, ob solche Abkommen bestehen, unter welchen Bedingungen sie geschlossen werden können, und zu prüfen, ob die Bestimmungen internationaler Abkommen das Schutzniveau beeinträchtigen könnten, das personenbezogene Daten, die aus dem EWR übermittelt werden, durch den Rechtsrahmen und die Praxis in Bezug auf Weiterübermittlungen zu Zwecken der nationalen Sicherheit genießen.

[159] Siehe insbesondere EO 14086, Section 2 c iii A 1 d.
[160] Siehe beispielsweise die Stellungnahme 14/2021 des EDSA zum Entwurf eines Durchführungsbeschlusses der Europäischen Kommission gemäß der Verordnung (EU) 2016/679 über die Angemessenheit des Schutzes personenbezogener Daten im Vereinigten Königreich. Angenommen am 13. April 2021, Abschnitte 4.3.2.1 und 4.3.2.2.
[161] Siehe EO 14086, Section 2 c iii A 1 d.
[162] Siehe EGMR (Große Kammer), Verfahren Centrum För Rättvisa gegen Schweden, 25. Mai 2021, Rn. 326.

5) <u>Vorübergehende Sammelerhebung zur Unterstützung der ersten technischen Phase der gezielten Erhebung</u>

156. Der EDSA weist darauf hin, dass sich die Beratungen im Zuge der letzten gemeinsamen Überprüfung des Datenschutzschilds hauptsächlich auf die Auslegung und Anwendung des zusätzlichen Grundes (Situation/Szenarium) für Sammelerhebungen konzentrierten, der im ersten Satz der Fußnote 5 in Section 2 PPD-28 enthalten ist, in dem es heißt: „Die in dieser Section enthaltenen Beschränkungen gelten nicht für Signalaufklärungsdaten, die vorübergehend erhoben werden, um eine gezielte Erhebung zu erleichtern." Die US-Behörden erläuterten damals die Bedeutung von „Signalaufklärungsdaten, die vorübergehend erhoben werden, um eine gezielte Erhebung zu erleichtern". Der EDSA entnimmt diesen Diskussionen, dass diese Fußnote bedeutet, dass Daten in großen Mengen – und unabhängig von den sechs vorgesehenen Zwecken – erhoben werden können, wenn sie vorübergehend erhoben werden, um einen Identifikator für ein festgelegtes Ziel zu ermitteln. Dies wäre somit ein zusätzlicher Grund für die Sammelerhebung von Daten, und in diesem Fall wären nur die allgemeinen Grundsätze von Section 1 der PPD-28 weiterhin anwendbar gewesen. Wie bereits erwähnt, vertrat der EuGH in seinem Urteil in der Rechtssache Schrems II die Auffassung, dass mit EO 12333 und PPD-28 zusammen in Bezug auf Sammelerhebungen „keine hinreichend klare und präzise Einschränkung des Umfangs einer solchen Sammelerhebung personenbezogener Daten besteht"[163].

157. Der EDSA stellt fest, dass es in der EO 14086 nach wie vor eine Ausnahmeregelung gibt, die eine solche Art der Sammelerhebung erlaubt;[164] der EDSA begrüßt jedoch, dass diese Ausnahmeregelung im Vergleich zur PPD-28 eingeschränkt wurde und in der EO 14086 zusätzliche Garantien vorgesehen sind.

158. Der EDSA geht davon aus, dass die neue EO 14086 Garantien vorsieht, die im Zusammenhang mit dieser Art der vorübergehenden technischen Sammelerhebung weiterhin gelten, insbesondere die allgemeinen Grundsätze der Erforderlichkeit und Verhältnismäßigkeit in Bezug auf die validierte nachrichtendienstliche Priorität, wenn Daten vor der gezielten Erhebung ohne Diskriminanten erhoben werden (Section 2 a bis b, Section 2 c i EO 14086). Der EDSA ist überdies der Auffassung, dass eine solche Sammelerhebung, die eine anschließende gezielte Signalaufklärung unterstützt, auch den zusätzlichen Garantien gemäß Section 2 c iii ff. unterliegt.[165]

159. Der EDSA weist jedoch auch darauf hin – siehe Nr. 117 –, dass die Definition des Begriffs „validierte nachrichtendienstliche Priorität" ein Ausnahmeverfahren vorsieht, an dem das CLPO des Office of the Director of National Intelligence nicht beteiligt wäre.

160. Der EDSA stellt jedoch nach wie vor fest, dass die Garantien der Subsection zur Sammelerhebung nicht für die vorübergehende Sammelerhebung gelten, die zur Unterstützung der ersten technischen Phase der gezielten Signalaufklärungstätigkeit gemäß Section 2 c ii D der EO 14086 eingesetzt wird, was insbesondere bedeutet, dass in diesem Zusammenhang gesammelte Daten für andere als die in Section 2 c ii aufgeführten Zwecke verwendet werden können. Der EDSA würde im Beschlussentwurf Klarstellungen zu den Zwecken begrüßen, für die in diesem Zusammenhang in Sammelerhebungen erhobene Daten verwendet werden können, sowie zur Anwendung der in Subsection 2 c i festgelegten Beschränkungen für die Signalaufklärung im Allgemeinen (d. h. nur für die dort aufgeführten legitimen Ziele) im Zusammenhang mit der vorübergehenden Sammelerhebung im Rahmen des Beschlussentwurfs.

[163] EuGH, Urteil Schrems II, Rn. 183.
[164] Siehe EO 14086, Section 2 c ii D, und Beschlussentwurf, Fußnote 226.
[165] Weitere Einzelheiten zu diesen Bestimmungen finden sich in den vorangegangenen Sections.

161. Abschließend betont der EDSA auch, dass diese Ausnahmeregelung für die vorübergehende Sammelerhebung im Hinblick auf die gezielte Sammlung und die ansonsten anzuwendenden Garantien nach wie vor unklar ist, insbesondere in Bezug auf die Frage, für welche Phase die Garantien der EO 14086 gelten würden (Sammelerhebung, weitere gezielte Sammlung), und fordert die Kommission auf, diese Elemente weiter zu bewerten und diese Aspekte auch in der Praxis bei künftigen gemeinsamen Überprüfungen zu bewerten.

162. Darüber hinaus bedauert der EDSA, dass, obgleich der Begriff „vorübergehend" in der EO etwas näher ausgeführt wird als in der PPD-28, dies nach dem Verständnis des EDSA weiterhin zu bedeuten scheint, dass die Sammelerhebung fortgesetzt werden könnte, solange das Ziel nicht ermittelt wurde. In diesem Zusammenhang erinnert der EDSA daran, dass es klarer und präziser Vorschriften bedarf, und betont in diesem Zusammenhang ebenfalls, dass diese Vorschriften für betroffene Personen eine wichtige Garantie darstellen.

163. Abschließend ist festzustellen, dass der EDSA in Bezug auf die für die Sammelerhebung geltenden Garantien nach wie vor Bedenken hegt, dass trotz der in der EO 14086 vorgesehenen zusätzlichen Garantien nach wie vor die Möglichkeit besteht, Daten in großen Mengen, d. h. ohne Diskriminanten, zu erheben, ohne wichtige Garantien wie die vorherige Genehmigung zur Erhebung dieser Daten – auch in der Ausnahmesituation der vorübergehenden technischen Sammelerhebung –, auch unter Berücksichtigung der Notwendigkeit weiterer Klarstellungen und der geäußerten Bedenken in Bezug auf eine strikte Zweckbindung für den späteren Datenzugang, auf klare und strenge Vorschriften für die Vorratsdatenspeicherung und strengere Garantien für die Verbreitung von Daten, die im Zuge von Sammelerhebungen erhoben wurden, einschließlich im Zusammenhang mit Weiterübermittlungen.

164. Generell betont der EDSA, dass die oben genannte Entscheidung des EGMR erneut zeigt, wie wichtig eine umfassende Aufsicht durch unabhängige Aufsichtsbehörden ist. Der EDSA betont, dass eine unabhängige Aufsicht in allen Phasen des staatlichen Zugriffs zu Zwecken der nationalen Sicherheit eine wichtige Garantie gegen willkürliche Überwachungsmaßnahmen und somit für die Bewertung eines angemessenen Datenschutzniveaus ist. Die Garantie der Unabhängigkeit der Aufsichtsbehörden im Sinne von Artikel 8 Absatz 3 der Charta soll eine wirksame und zuverlässige Überwachung der Einhaltung der Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten gewährleisten. Dies gilt insbesondere dann, wenn die Person aufgrund des Wesens der geheimen Überwachung daran gehindert ist, eine Überprüfung zu beantragen oder sich vor oder während der Durchführung der Überwachungsmaßnahme unmittelbar an einem Überprüfungsverfahren zu beteiligen.

165. Der EDSA erinnert daran, dass seiner Auffassung nach die Bewertung der Angemessenheit von allen Umständen des Falles abhängt, insbesondere von der Wirksamkeit der Ex-post-Aufsicht und der im Rechtsrahmen vorgesehenen Rechtsbehelfe.

3.2.2.4 Rechtsrahmen für die Organisation spezifischer Erhebungen für Zwecke der nationalen Sicherheit durch die Elemente der Intelligence Community innerhalb und außerhalb des Hoheitsgebiets der USA

166. In seinem Schrems-II-Urteil betonte der EuGH, Section 702 FISA lasse „in keiner Weise erkennen, dass für die darin enthaltene Ermächtigung zur Durchführung von Überwachungsprogrammen zum Zweck der Auslandsaufklärung Einschränkungen bestehen. Genauso wenig ist erkennbar, dass für potenziell von diesen Programmen erfasste Nicht-US-Personen Garantien existieren."[166] Daraufhin befand der

[166] Siehe EuGH, Urteil Schrems II, Rn. 180.

Gerichtshof: „Unter diesen Umständen ist diese Vorschrift … nicht geeignet, ein Schutzniveau zu gewährleisten, das dem durch die Charta …, wonach eine gesetzliche Grundlage für Eingriffe in Grundrechte, um dem Grundsatz der Verhältnismäßigkeit zu genügen, den Umfang, in dem die Ausübung des betreffenden Rechts eingeschränkt wird, selbst festlegen sowie klare und präzise Regeln für die Tragweite und die Anwendung der betreffenden Maßnahme vorsehen und Mindesterfordernisse aufstellen muss – garantierten Niveau der Sache nach gleichwertig ist". [167]

167. Bezüglich der EO 12333 stellt der Gerichtshof fest, dass „auch dieses Dekret keine Rechte verleiht, die gegenüber den amerikanischen Behörden gerichtlich durchgesetzt werden können" [168], und er befand ferner: „Hinsichtlich dieser im Rahmen der auf die E.O. 12333 gestützten Überwachungsprogramme bestehenden Möglichkeit, auf Daten während ihrer Übermittlung in die Vereinigten Staaten zuzugreifen, ohne dass dieser Zugriff irgendeiner gerichtlichen Kontrolle unterläge, besteht jedenfalls keine hinreichend klare und präzise Eingrenzung des Umfangs einer solchen Sammelerhebung personenbezogener Daten" [169], nachdem er die Bedingungen geprüft hatte, unter denen Sammelerhebungen im Rahmen dieser EO zusammen mit der PPD-28 stattfinden dürfen.

168. Für diese spezifischen Datenerhebungsregelungen sieht die EO 14086 nunmehr neue Vorschriften vor.

3.2.2.4.1 Erhebung von Daten für Zwecke der nationalen Sicherheit gemäß Section 702

169. Der EDSA erinnert daran, dass die Feststellungen zu Section 702 FISA [170], wonach „in der Praxis ‚Nicht-US-Bürger' ebenfalls die Zugangs- und Speicherbeschränkungen genießen, die die Verfahren der verschiedenen Behörden zur Minimierung und/oder zielgenauen Erhebung verlangen, da es kostspielig und schwierig ist, Daten von US-Bürgern in einem großen Datensatz zu identifizieren und daraus zu entfernen, was bedeutet, dass meist der gesamte Datensatz im Einklang mit den höheren US-Datenstandards behandelt wird", im letzten PCLOB-Bericht begrüßt wurden.

170. Nach diesen Feststellungen „funktioniert das Programm nicht durch Erheben von Kommunikation in großen Mengen". Die vom ODNI herausgegebenen Statistical Transparency Reports 2014 und 2021 bestätigten diese Feststellung. Darüber hinaus werden laut PCLOB-Bericht „vorgegebene Selektoren" wie eine E-Mail-Adresse oder eine Telefonnummer verwendet, um die Überwachung gezielt zu machen.

171. Der EDSA weist jedoch auch darauf hin, dass gleichzeitig im Zusammenhang mit Section 702 bei der letzten Überprüfung des Datenschutzschilds klargestellt wurde, dass sich eine als Ziel zu ermittelnde „Person" auf mehrere Personen beziehen könnte, die dieselbe Kennung verwenden, sofern es sich bei allen diesen Personen um Nicht-US-Bürger handelt und die geltenden Kriterien für eine gezielte Maßnahme erfüllt sind Der EDSA erinnert ferner daran, dass bei der dritten jährlichen gemeinsamen Überprüfung des Datenschutzschilds im Jahr 2019 weitere Klarstellungen im Zusammenhang mit dem UPSTREAM-Programm gefordert wurden, um auszuschließen, dass ein massiver und unterschiedsloser Zugriff auf personenbezogene Daten von Nicht-US-Bürgern stattfindet. [171]

172. Darüber hinaus weist der EDSA darauf hin, dass aufgrund der Tatsache, dass die Erhebung nach Section 702 FISA dadurch gerechtfertigt ist, dass „ein wesentlicher Zweck der Beschaffung darin besteht, Auslandsaufklärungsdaten zu erhalten", nach wie vor eine gewisse Unsicherheit hinsichtlich

[167] Siehe EuGH, Urteil Schrems II, Rn. 180.
[168] Siehe EuGH, Urteil Schrems II, Rn. 182.
[169] Siehe EuGH, Urteil Schrems II, Rn. 183.
[170] Siehe PCLOB Report on the Surveillance program operated pursuant of Section 702 FISA, S. 100.
[171] Siehe Dritter gemeinsamer Überprüfungsbericht, S. 17, Nr. 83.

der Zweckbindung und der Erforderlichkeit besteht. Der EDSA stellt jedoch fest, dass gemäß EO 14086 Section 2 a A und B die Signalaufklärung nur dann durchgeführt werden darf, wenn festgestellt wurde, dass die Tätigkeiten erforderlich sind, um eine validierte Priorität voranzubringen, und nur in dem Umfang und in einer Weise, die in einem angemessenen Verhältnis zu dieser Priorität steht, und dass sie so exakt zugeschnitten wie möglich sein muss, um die validierte Priorität voranzubringen, wobei relevante Faktoren wie das Eindringen in die Privatsphäre durch die Erhebung, die Sensibilität der Daten und das Ausbleiben unverhältnismäßiger Auswirkungen auf die Privatsphäre und die bürgerlichen Freiheiten gebührend zu berücksichtigen sind. Der EDSA erwartet jedoch weitere Klarstellungen darüber, wie dies konkret umgesetzt und operationalisiert werden soll, auch im Zusammenhang mit der Anwendung von Section 702 FISA.

173. In diesem Zusammenhang forderte der EDSA in Ermangelung eines direkten Zugangs zu diesen Informationen an sich eine unabhängige Bewertung der Erforderlichkeit und Verhältnismäßigkeit der Definition von „Zielen“ und des Begriffs „Auslandsaufklärung“ in Section 702 FISA (auch im Zusammenhang mit dem UPSTREAM-Programm) nach dessen Verlängerung. Nach Auffassung des EDSA kommt seiner früheren Forderung nach einer weiteren unabhängigen Bewertung des Verfahrens zur Anwendung von Selektoren in bestimmten Fällen („Vorgabe von Selektoren“) sowie nach weiteren Klarstellungen im Zusammenhang mit dem UPSTREAM-Programm maßgebliche Bedeutung zu. Daher fordert der EDSA unter Berücksichtigung der neuen EO 14086 zusätzliche Informationen an, um auch bewerten und überwachen zu können, wie und in welchem Umfang die neu eingeführten Grundsätze der Erforderlichkeit und Verhältnismäßigkeit in diesem Zusammenhang in der Praxis angewandt werden, und erwartet, dass dies auch im Rahmen künftiger gemeinsamer Überprüfungen bewertet wird.

174. Der EDSA begrüßt, dass das voll funktionsfähige Aufsichtsgremium für Privatsphäre und bürgerliche Freiheiten (PCLOB) als unabhängiges Aufsichtsgremium beschlossen hat, „ein Aufsichtsprojekt durchzuführen, um das Überwachungsprogramm, das die Executive Branch gemäß Section 702 des Gesetzes über die Überwachung ausländischer Nachrichtendienste (FISA) betreibt, im Vorgriff auf den Ablauftermin für Section 702 im Dezember 2023 und die bevorstehende Beratung über seine erneuten Genehmigung in der Öffentlichkeit im Kongress zu prüfen“.[172] Der EDSA begrüßt ferner, dass sich die „Überprüfung auf ausgewählte Schwerpunktbereiche für Untersuchungen erstreckt, darunter u. a. Anfragen von US-Bürgern zu Informationen, die gemäß Section 702 erhoben wurden, und die „Upstream“-Erhebung gemäß Section 702“[173] und dass sie „ferner eine Überprüfung des bisherigen und des prognostizierten Wertes und der Wirksamkeit des Programms sowie der Angemessenheit der bestehenden Garantien zum Schutz der Privatsphäre und der bürgerlichen Freiheiten umfasst“[174]. Der EDSA betont daher, dass ein Zugang zu den Feststellungen des PCLOB in diesem Bericht zu Section 702 erforderlich wäre, um die im Rahmen dieses Überwachungsprogramms bereitgestellten und angewandten Datenschutzgarantien angemessen und umfassend zu bewerten.

175. Unter Berücksichtigung der neuen EO 14086 fordert der EDSA darüber hinaus zusätzliche Informationen an, um auch bewerten und überwachen zu können, wie und in welchem Umfang die neu eingeführten Grundsätze der Erforderlichkeit und Verhältnismäßigkeit sowie die anderen in diesem Text vorgesehenen Garantien in diesem Zusammenhang in der Praxis angewandt werden.

[172] Siehe die NOTICE OF THE PCLOB OVERSIGHT PROJECT EXAMINING SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA)
[173] Siehe oben.
[174] Siehe oben.

3.2.2.4.2 Erhebung von Daten für Zwecke der nationalen Sicherheit gemäß Executive Order 12333

176. Wie der EuGH in seinem Urteil in der Rechtssache Schrems II anerkannt hat, sollte sich die Analyse der Rechtsvorschriften des Drittlandes, für das die Angemessenheit der Rechtsvorschriften geprüft wird, nicht auf die Gesetze und Praktiken beschränken, die eine Überwachung innerhalb der physischen Grenzen dieses Landes ermöglichen, sondern auch eine Analyse der rechtlichen Gründe im Recht dieses Drittlands umfassen, die es diesem ermöglichen, eine Überwachung außerhalb seines Hoheitsgebiets in Bezug auf EU-Daten durchzuführen. Die notwendigen Beschränkungen des staatlichen Zugangs zu Daten sollten sich auch auf personenbezogene Daten „während der Übermittlung" in das Land erstrecken, für das die Angemessenheit anerkannt wird.

177. Der EDSA begrüßt den allgemeinen öffentlichen Bericht des PCLOB über die Executive Order 12333, der im April 2021 veröffentlicht wurde, hält jedoch fest, dass dieser Bericht nach wie vor allgemein gehalten ist, da die meisten Feststellungen als Verschlusssache eingestuft sind.

178. In diesem Zusammenhang betont der EDSA angesichts der Unsicherheit und der mangelnden Klarheit darüber, wie die EO 12333 angewendet wurde, und angesichts der Bedeutung einer Klarstellung, wie sie im Lichte der neuen EO 14086 angewandt werden soll, erneut die Bedeutung der erwarteten Berichte des PCLOB zu diesem Text[175]. Er geht jedoch davon aus, dass der Großteil seines Inhalts wahrscheinlich weiterhin als Verschlusssache eingestuft wird, sodass weder der Öffentlichkeit noch dem EDSA weitere Informationen über die konkrete Funktionsweise der EO 12333 sowie über deren Erforderlichkeit und Verhältnismäßigkeit zur Verfügung gestellt würden.

179. Der EDSA würde es daher insbesondere begrüßen, wenn der Bericht des PCLOB über die Anwendung der EO 14086 nicht als Verschlusssache eingestuft wird, sondern nach seiner Fertigstellung uneingeschränkt zugänglich ist, einschließlich der Teile, in denen bewertet wird, wie die Garantien der EO 14086 auf die Datenerhebung nach der EO 12333 angewandt werden. Der EDSA fordert die Kommission ferner auf, diesem Punkt im Rahmen der künftigen gemeinsamen Überprüfungen besondere Aufmerksamkeit zu schenken.

180. Was die verschiedenen Rechtsinstrumente betrifft, die die Möglichkeit vorsehen, Daten für US-Nachrichtendienste im US-Rechtsrahmen zu erheben, weiter abzurufen und weiter zu verarbeiten, würde der EDSA Klarstellungen bezüglich ihres Zusammenspiels mit der neuen EO 14086 begrüßen und erwartet er Zusicherungen, dass die bereits in den früheren Stellungnahmen des EDSA geäußerten Bedenken durch die Annahme dieser neuen Garantien ausgeräumt würden.

181. Der EDSA fordert die Kommission ferner auf, diesen Aspekten im Rahmen künftiger gemeinsamer Überprüfungen besondere Aufmerksamkeit zu schenken.

3.2.2.4.3 PCLOB-Bericht

182. Der EDSA begrüßt, dass die EO 14086 auch die Verpflichtung für den PCLOB vorsieht, einen Bericht über die Umsetzung der EO zu erstellen. Der EDSA betont, dass dieser Bericht eine Bewertung dieser besonderen Möglichkeit der EO enthalten sollte, Daten zu den für die gezielte Erhebung aufgeführten Zwecken sowie in großen Mengen zu erheben, auch aus technischen Gründen, um die Schlüsselbegriffe der EO 14086 und ihr Verständnis in der Praxis und ihre Anwendung in den

[175] Der allgemeine Bericht über die EO 12333 wurde größtenteils als Verschlusssache eingestuft – es wurde lediglich eine kurze, öffentlich zugängliche Fassung veröffentlicht; ebenso wurden der Bericht und die Empfehlungen zu CIA-Tätigkeiten zur Terrorismusbekämpfung gemäß EO 12333 nur teilweise freigegeben.

verschiedenen Überwachungsprogrammen besser zu verstehen. Dieser Bericht wäre auch erforderlich, um zu bewerten, wie die EO in den internen Verfahren und Strategien der Elemente der Intelligence Community umgesetzt wird.

3.2.3 Garantie C – Aufsicht

3.2.3.1 Einleitung

183. Die nachrichtendienstlichen Tätigkeiten der USA unterliegen einem mehrschichtigen Aufsichtsverfahren. Die Struktur der Aufsicht in den USA lässt sich in eine interne und eine externe Aufsicht unterteilen. Alle Elemente der Intelligence Community verfügen über Aufsichts- und Compliance-Beauftragte, die regelmäßig die Signalaufklärungstätigkeiten überwachen, sowie über Beauftragter für Privatsphäre und bürgerliche Freiheiten und Inspectors General. Darüber hinaus gibt es externe Aufsichtsgremien wie das Privacy and Civil Liberties Oversight Board (PCLOB) und das Intelligence Oversight Board.

184. Der EDSA erinnert daran, dass ein Eingriff zum Zeitpunkt der Datenerhebung, aber auch zu dem Zeitpunkt erfolgt, zu dem eine Behörde zur Weiterverarbeitung auf die Daten zugreifen kann. Der EGMR hat mehrfach bestimmt, dass jeder Eingriff in das Recht auf Privatsphäre und Datenschutz einem wirksamen, unabhängigen und unparteiischen Aufsichtssystem unterliegen sollte, das entweder von einem Richter oder von einer anderen unabhängigen Stelle[176] (z. B. einer Verwaltungsbehörde oder einem parlamentarischen Gremium) bereitgestellt werden muss.

185. Der EGMR hat zwar zum Ausdruck gebracht, dass grundsätzlich wünschenswert ist, einen Richter mit der nachprüfenden Kontrolle zu betrauen, er hat jedoch nicht ausgeschlossen, dass auch eine andere Stelle zuständig sein kann, „sofern die Behörde von der Exekutive“[177] und „von den Behörden, welche die Überwachung durchführen, hinreichend unabhängig ist, und mit ausreichenden Machtbefugnissen und Kompetenzen ausgestattet ist, um eine wirksame und ständige Kontrolle ausüben zu können“[178].

186. Der EGMR fügte hinzu, dass „die Art der Ernennung und der Rechtsstatus der Mitglieder des Aufsichtsorgans“[179] bei der Beurteilung der Unabhängigkeit zu berücksichtigen sind.

187. Der EGMR wies ferner darauf hin, es sei zu prüfen, ob die Tätigkeiten der Überwachungsstelle einer Kontrolle durch die Öffentlichkeit zugänglich seien. Erreichen ließe sich dies beispielsweise, wenn die jährlichen Überwachungsberichte an die Regierung bzw. die öffentlichen Berichte dem Parlament vorgelegt und vom Parlament erörtert würden.[180]

188. Die unabhängige Aufsicht über die Umsetzung von Überwachungsmaßnahmen wurde vom EuGH in seinem Urteil in der Rechtssache Schrems II ebenfalls berücksichtigt, in dem es heißt: „zielt die vom FISC ausgeübte Kontrolle darauf ab, zu prüfen, ob diese Überwachungsprogramme dem Ziel entsprechen, Auslandsaufklärungsdaten zu erlangen, betrifft aber nicht die Frage, ‚ob die Personen

[176] EGMR, Verfahren Klass u. a./Deutschland, 6. September 1978 (im Folgenden „EGMR, Urteil Klass“), Rn. 17 und 51.
[177] EGMR, Urteil Zakharov, Rn. 258; EGMR, Iordachi u. a./Moldau, 10. Februar 2009, Rn. 40 und 51; EGMR, Dumitru Popescu/Rumänien, 26. April 2007, Rn. 70–73.
[178] EGMR, Urteil Klass, Rn. 56.
[179] EGMR, Urteil Zakharov, Rn. 278.
[180] EGMR, Urteil Zakharov, Rn. 283; EGMR, L./Norwegen, 9. Juni 1990; EGMR, Kennedy/Vereinigtes Königreich, 18. Mai 2010, Rn. 166.

vorschriftsgemäß als Zielpersonen für die Beschaffung von Auslandsaufklärungsdaten ausgewählt wurden'."[181]

3.2.3.2 Interne Aufsicht

3.2.3.2.1 Inspectors General

189. Der EDSA erkennt an, dass die Inspectors General über eine große Bandbreite von Befugnissen verfügen, die für die Überwachung nachrichtendienstlicher Tätigkeiten erforderlich sind. So haben Inspectors General insbesondere Zugang zu allen Informationen, die erforderlich sind, um die allgemeine Übereinstimmung der Arbeit der Behörden mit den Rechtsvorschriften einschließlich, aber nicht nur, der Gesetze über den Schutz der Privatsphäre und den Datenschutz zu prüfen, und sie können Vorladungen aussprechen und von jeder Person im Zusammenhang mit Ermittlungen der Inspectors General einen Eid leisten lassen.

190. Auf der Grundlage der vorstehenden Ausführungen ist der EDSA der Auffassung, dass Inspectors General im Allgemeinen über umfangreiche Ermittlungsbefugnisse verfügen. Sie haben jedoch keine verbindlichen Abhilfebefugnisse und geben nur unverbindliche Empfehlungen ab.[182]

191. Der EDSA erkennt an, dass Inspectors General grundsätzlich nicht daran gehindert werden dürfen und ihnen nicht untersagt werden darf, ein Audit oder eine Untersuchung einzuleiten, durchzuführen oder abzuschließen, oder im Verlauf eines Audits oder einer Untersuchung eine Vorladung auszusprechen.[183] In diesem Zusammenhang stellt der EDSA jedoch fest, dass die Inspectors General unter der Aufsicht, Leitung und Kontrolle des jeweiligen Ministers/Behördenleiters stehen, der ihnen den Zugang zu Informationen, die Durchführung einer Untersuchung und unter anderem die Anordnung von Vorladungen untersagen kann, wenn der Minister/Behördenleiter feststellt, dass ein solches Verbot zur Wahrung nationaler Interessen erforderlich ist. Der Minister/Behördenleiter muss jedoch die zuständigen Ausschüsse des US-Kongresses über die Ausübung dieser Befugnis in Kenntnis setzen.[184]

192. Der EDSA hält fest, dass Inspectors General nur vom US-Präsidenten entlassen werden können, der den Kongress über die Gründe einer solchen Entlassung informieren muss.

193. Der EDSA stellt fest, dass es seit den Stellungnahmen der Artikel-29-Datenschutzgruppe und dann des EDSA keine wesentlichen Änderungen am internen Aufsichtsmechanismus gegeben hat. Daher zieht der EDSA im Einklang mit der Stellungnahme 01/2016 der Artikel-29-Datenschutzgruppe[185] den Schluss, dass im Allgemeinen ausreichende interne Aufsichtsmechanismen vorhanden sind.

3.2.3.3 Externe Aufsicht

194. Der EDSA stellt fest, dass neben den nachstehend genannten Gremien auch verschiedene andere Stellen innerhalb der US-Regierung die Tätigkeiten der US-Nachrichtendienste beaufsichtigen, wie etwa das Intelligence Oversight Board (IOB) oder die Kongressausschüsse. Letztere können eigene Untersuchungen durchführen und Berichte abfassen.

---

[181] EuGH, Urteil Schrems II, Rn. 179.
[182] Beschlussentwurf, Erwägungsgrund 105.
[183] Inspector General Act von 1978, § 3 a.
[184] Siehe z. B. Inspector General Act von 1978, § 8 (für das Verteidigungsministerium); § 8E (für das DOJ), § 8G d 2 A und B (für die NSA); 50. U.S.C. § 403q b (für die CIA); Intelligence Authorisation Act for Fiscal Year 2010, Section 405 f (für die Intelligence Community).
[185] Stellungnahme 01/2016 der Artikel-29-Datenschutzgruppe.

3.2.3.3.1 Privacy and Civil Liberties Oversight Board (PCLOB)

195. Der EDSA erkennt die umfassende Aufsichtsfunktion des PCLOB in Bezug auf das neue Rechtsbehelfsverfahren und die Umsetzung der EO 14086 an.

196. Erstens umfassen seine neuen Aufgaben die Konsultation des Generalstaatsanwalts zur Ernennung der Richter des DPRC und der Sonderanwälte. Zweitens wird der PCLOB das Rechtsbehelfsverfahren jährlich überprüfen, d. h. die Bearbeitung zulässiger Beschwerden im Rechtsbehelfsverfahren. Dazu gehört auch, ob das CLPO und der Data Protection Review Court zulässige Beschwerden zeitnah bearbeitet haben, uneingeschränkten Zugang zu den erforderlichen Informationen erhalten und im Einklang mit der EO 14086 handeln, und ob sich die Intelligence Community an die Feststellungen des CLPO und des DPRC hält.

197. Darüber hinaus muss der PCLOB konsultiert werden, wenn Nachrichtendienste ihre internen Strategien und Verfahren zur Umsetzung der EO 14086 aktualisieren. Darüber hinaus wird der PCLOB eine Überprüfung der aktualisierten Strategien und Verfahren vornehmen und deren Übereinstimmung mit der EO 14086 bewerten.[186] Auch wenn die Feststellungen des PCLOB im engeren Sinne nicht verbindlich sind, ist der Leiter jedes Elements der Intelligence Community nach geltendem Recht verpflichtet, alle in einer solchen Überprüfung enthaltenen Empfehlungen sorgfältig zu prüfen und umzusetzen oder anderweitig darauf zu reagieren.[187] Der EDSA fordert die Kommission auf, falls der Beschlussentwurf angenommen wird, bei künftigen Überprüfungen besonders darauf zu achten, ob und wie die Empfehlungen des PCLOB auf Ebene der Behörden umgesetzt wurden.

198. Der EDSA erinnert daran, dass der PCLOB als unabhängige Stelle „aufgefordert", aber nicht verpflichtet ist, zu prüfen, ob die in der EO 14086 vorgesehenen Garantien ordnungsgemäß berücksichtigt werden und ob die Intelligence Community die Anforderungen des Rechtsbehelfsverfahrens in vollem Umfang erfüllt. Nach dem Verständnis des EDSA hat der PCLOB jedoch in seiner zusätzlichen Erklärung gegenüber dem EDSA sowie öffentlich erklärt[188], dass er die in der EO 14086 vorgesehene Rolle übernehmen wird.

199. Darüber hinaus begrüßt der EDSA, dass die Ergebnisse der PCLOB-Berichte der Öffentlichkeit zugänglich gemacht werden sollen. In Anbetracht dessen, dass die verschiedenen Stellen innerhalb des Rechtsbehelfsverfahrens und die Stellen der Intelligence Community grundsätzlich die Empfehlungen in den Berichten des PCLOB umsetzen oder auf andere Weise darauf eingehen müssen, erkennt der EDSA an, dass diese Empfehlungen bei den Garantien für den Schutz der Privatsphäre eine wichtige Rolle spielen.

200. Der EDSA stellt fest, dass der Zugang des PCLOB zu Informationen eingeschränkt ist, wenn der US-Präsident „verdeckte Operationen"[189] von Ministerien, Behörden oder anderen Stellen der US-Regierung genehmigt.[190]

---

[186] EO 14086, Section 2 c iv und Section 2 c v.
[187] EO 14086, Section 2 c v B.
[188] https://documents.pclob.gov/prod/Documents/EventsAndPress/4db0a50d-cc62-4197-af2e-2687b14ed9b9/Trans-Atlantic%20Data%20Privacy%20Framework%20EO%20press%20release%20(FINAL).pdf
[189] Gemäß 50 U.S.C. § 3093 e 1 bezeichnet der Ausdruck „verdeckte Operation" eine oder mehrere Tätigkeit(en) der Regierung der Vereinigten Staaten zur Beeinflussung politischer, wirtschaftlicher oder militärischer Gegebenheiten im Ausland, bei denen beabsichtigt ist, dass die Rolle der Regierung der Vereinigten Staaten nicht öffentlich erkennbar oder anerkannt wird, jedoch nicht 1) Tätigkeiten, deren Hauptzweck darin besteht, nachrichtendienstliche Erkenntnisse zu erlangen, traditionelle Tätigkeiten im Bereich der Spionageabwehr.
[190] 42 U.S.C. § 2000ee g 5; 50 U.S. Code § 3093 a.

201. Anknüpfend an seine früheren Stellungnahmen betrachtet der EDSA den PCLOB als ein unabhängiges Gremium, dessen Empfehlungen einen wichtigen Beitrag zu Reformen in den USA geleistet haben und dessen Berichte eine besonders hilfreiche Quelle für das Verständnis der Funktionsweise der verschiedenen Überwachungsprogramme waren, also als ein wesentliches Element der Aufsichtsstruktur.

202. Allerdings bedauerte der EDSA in seinem Dritten jährlichen Überwachungsbericht für den früheren EU-US-Datenschutzschild, dass der PCLOB dem EDSA lediglich die gleichen Informationen zur Verfügung stellte wie der breiten Öffentlichkeit. Darüber hinaus war es bedauerlich, dass der PCLOB im Anschluss an seinen ersten Bericht keine weiteren Berichte über die PPD-28 herausgegeben hat, um zusätzliche Informationen darüber vorzulegen, wie die Garantien der PPD-28 angewandt werden, und auch keinen allgemeinen aktualisierten Bericht zu Section 702 FISA.

203. Daher begrüßt der EDSA die Ankündigung des PCLOB gegenüber dem EDSA, dass in naher Zukunft die Veröffentlichung eines Folgeberichts zu Section 702 FISA zu erwarten ist. Des Weiteren ist der EDSA erfreut ob der Zusage des PCLOB, seine Berichte über die EO 14086 öffentlich zu machen. Der EDSA erinnert jedoch daran, dass die Freigabe nicht als Verschlusssache eingestufter Berichte im US-Recht geregelt ist und mit den Behörden der Intelligence Community abgestimmt werden muss und nicht vom PCLOB von sich aus beschlossen werden kann.

204. Sollte also der Beschlussentwurf angenommen werden, weist der EDSA darauf hin, dass bei künftigen Überprüfungen des Datenschutzrahmens EU-USA die sicherheitsüberprüften Sachverständigen des EDSA in der Lage sein sollten, zusätzliche Dokumente zu überprüfen und gegebenenfalls zusätzliche als Verschlusssache eingestufte Elemente zu erörtern, um sicherzustellen, dass die in den Berichten enthaltenen Informationen angemessen bewertet werden können, wobei die einschlägigen nationalen Sicherheitsinteressen und die geltenden Datenschutzbestimmungen zu berücksichtigen sind.

205. Der EDSA begrüßt die Unabhängigkeit des PCLOB und seine Aufsicht über die nationale Intelligence Community, die den Empfehlungen des PCLOB nachkommen oder auf andere Weise darauf eingehen muss, wie es im Bericht des PCLOB an den US-Kongress heißt.

206. Unter Berücksichtigung der Anforderungen des EGMR an die öffentliche Kontrolle[191], wonach die Berichte eines Aufsichtsorgans dem Parlament vorgelegt und vom Parlament erörtert werden müssen, hält es der EDSA für ausreichend, dass der PCLOB seine Berichte mindestens halbjährlich dem US-Präsidenten und insbesondere den Kongressausschüssen des Senats und des Repräsentantenhauses[192], bei denen es sich um die parlamentarischen Organe der USA handelt, vorlegt.

3.2.3.3.2 Foreign Intelligence Surveillance Court (Gericht für die Überwachung ausländischer Nachrichtendienste) (FISC)

207. Der Foreign Intelligence Surveillance Court ist gemäß Section 702 FISA für die Überwachung der Erhebung personenbezogener Daten zuständig[193], und die Entscheidungen des FISC können vor dem Foreign Intelligence Surveillance Court of Review (FISCR) angefochten werden.

[191] EGMR, Urteil Zakharov, Rn. 283, EGMR, L./Norwegen, 9. Juni 1990; EGMR, Kennedy/Vereinigtes Königreich, 18. Mai 2010, Rn. 166.
[192] 42 U.S.C. § 2000ee e.
[193] 50 U.S.C. 1881 a.

208. Der FISC überwacht das Zertifizierungsverfahren für die Erhebung von Auslandsaufklärungsdaten nach Section 702 FISA und genehmigt elektronische Überwachung, physische Durchsuchung und andere Ermittlungsmaßnahmen zu Zwecken der Auslandsaufklärung.[194] Der FISC genehmigt ferner die Verfahren für das Targeting, die Minimierung und die Abfrage der Zertifikate, die für die US-Nachrichtendienste rechtsverbindlich sind.[195] Stellt der FISC fest, dass die Anforderungen nicht erfüllt sind, kann er die Zertifizierung ganz oder teilweise verweigern und eine Änderung der Verfahren verlangen.

209. Werden Verstöße gegen Targeting-Verfahren festgestellt, kann der FISC den entsprechenden Nachrichtendienst anweisen, Abhilfemaßnahmen zu ergreifen.[196] Diese Abhilfemaßnahmen reichen von individuellen bis zu strukturellen Maßnahmen, z. B. von der Beendigung der Datenerlangung und der Löschung unrechtmäßig erlangter Daten bis hin zu einer Änderung der Erhebungspraxis, und betreffen auch Anleitung und Schulung des Personals.

210. Der EDSA erkennt an, dass gemäß der EO 14086 das CLPO und der DPRC Verstöße dem Assistant Attorney General for National Security melden müssen, der diese Verstöße wiederum dem FISC meldet.[197]

211. Wie der EuGH in seiner Schrems-II-Entscheidung festgestellt hat, genehmigt der FISC keine individuellen Überwachungsmaßnahmen; vielmehr werden Überwachungsprogramme genehmigt.[198] Daher hegt der EDSA nach wie vor Bedenken, dass der FISC keine wirksame gerichtliche Aufsicht über das Targeting von Nicht-US-Bürgern bietet, ein Problem, das durch die neue EO 14086 offenbar nicht gelöst wird.

212. Bezüglich der vorherigen unabhängigen Genehmigung[199] von Überwachung gemäß Section 702 FISA bedauert der EDSA, dass, wie der EDSA dem Beschlussentwurf[200] und Erläuterungen der US-Regierung entnimmt, der FISC bei der Zertifizierung der Programme, mit denen ein Targeting von Nicht-US-Bürgern genehmigt wird, wohl nicht an die zusätzlichen Garantien nach der EO 14086 gebunden ist. Nach Auffassung des EDSA sollten die in dieser Durchführungsverordnung enthaltenen zusätzlichen Garantien in diesem Zusammenhang dennoch berücksichtigt werden. Der EDSA erinnert daran, dass Berichte des PCLOB besonders nützlich wären, um zu bewerten, wie die Garantien der EO 14086 umgesetzt werden und wie diese Garantien angewandt werden, wenn Daten gemäß Section 702 FISA erhoben werden.

3.2.4 Garantie D – Den betroffenen Personen müssen wirksame Rechtsbehelfe zur Verfügung stehen

213. Der EDSA erinnert daran, dass wirksame und durchsetzbare Rechte der natürlichen Person für die Feststellung eines angemessenen Datenschutzniveaus in einem Drittland von grundlegender Bedeutung sind. Betroffene Personen müssen über einen wirksamen Rechtsbehelf verfügen, um ihre

[194] www.fisc.uscourts.gov/about-foreign-intelligence-surveillance-court
[195] 50 U.S.C.1881a (i).
[196] 50 U.S.C. § 1803 h.
[197] EO 14086, Section 3 c i D; EO 14086, Section 3 d i F.
[198] EuGH, Urteil Schrems II, Rn. 179.
[199] Für die Erhebung von Daten in großen Mengen gemäß EO 12333 in Fällen, in denen der FISC nicht zuständig ist, ist der EDSA besorgt, dass es kein vorheriges Genehmigungsverfahren für die Sammelerhebung von Daten gibt (siehe auch Garantie B).
[200] Beschlussentwurf, Erwägungsgrund 165.

Rechte wahrnehmen zu können, wenn sie der Auffassung sind, dass diese nicht geachtet werden oder wurden. Wie der EuGH in seinen Entscheidungen Schrems I und Schrems II erklärte, „verletzt eine Regelung, die keine Möglichkeit für den Bürger vorsieht, mittels eines Rechtsbehelfs Zugang zu den ihn betreffenden personenbezogenen Daten zu erlangen oder ihre Berichtigung oder Löschung zu erwirken, den Wesensgehalt des in Art. 47 der Charta verankerten Grundrechts auf wirksamen gerichtlichen Rechtsschutz“.[201]

214. Das US-amerikanische System für Rechtsbehelfe enthält eine wichtige Einschränkung, die die Einleitung von Gerichtsverfahren gegen Überwachungsmaßnahmen der US-Regierung vor ordentlichen Gerichten sehr erschwert. Nach der US-Verfassung muss eine Einzelperson ihre Klagebefugnis nachweisen, d. h. eine „konkrete, genau spezifizierte und tatsächliche oder unmittelbar bevorstehende Schädigung“ nachweisen.[202] In Überwachungsfällen scheint dieses Erfordernis dadurch zunichte gemacht zu werden, dass die der Überwachung unterliegenden Personen auch nach Beendigung dieser Maßnahmen nicht benachrichtigt werden.

215. In diesem Zusammenhang begrüßt der EDSA, dass mit der EO 14086 ein spezifisches Rechtsbehelfsverfahren für die Bearbeitung und Beilegung von Beschwerden von Nicht-US-Bürgern in Bezug auf US-Signalaufklärungstätigkeiten eingerichtet wurde. In diesem neuen Verfahren gilt das Erfordernis der Klagebefugnis nicht mehr: Gemäß Section 4 k ii der EO 14086 muss der Antragsteller nicht nachweisen, dass seine Daten tatsächlich der US-Signalaufklärung unterlagen. Betroffene Personen können sich somit auf die in der EO 14086 vorgesehenen Garantien berufen, einschließlich der Garantien, die in anderen einschlägigen Gesetzen und Bestimmungen gemäß Section 4 d iii der EO 14086 vorgesehen sind.[203] In diesem Zusammenhang wird mit dem neuen Mechanismus eine Rechtsbehelfsmöglichkeit geschaffen, die andernfalls nicht existieren würde.

216. Das neue Verfahren umfasst zwei Ebenen: Auf der ersten Ebene können natürliche Personen beim Civil Liberties Protection Officer of the Office of the Director of National Intelligence (Bürgerrechtsschutzbeauftragten des Büros des Direktors für nationale Nachrichtendienste) (CLPO) Beschwerde einlegen. Auf der zweiten Ebene haben natürliche Personen die Möglichkeit, die Entscheidung des CLPO vor einer neu geschaffenen Stelle, dem sogenannten Data Protection Review Court (Datenschutzüberprüfungsgericht) (DPRC), anzufechten. Die folgenden Abschnitte befassen sich in erster Linie mit der zweiten Ebene des Rechtsbehelfsverfahrens. Der EDSA ist der Auffassung, dass das CLPO als Amtsträger nicht über ein ausreichendes Maß an Unabhängigkeit von der Exekutive verfügt und somit als solcher die Anforderungen aus Artikel 47 der Charta nicht angemessen erfüllen kann Diese Einschätzung wurde von der Kommission mehrfach bestätigt.

3.2.4.1 Kann die Einrichtung des DPRC auf der Grundlage einer Executive Order an sich ausreichen?

217. Der DPRC ist kein ordentliches Gericht, das vom Kongress nach Artikel III der US-Verfassung eingerichtet wurde, sondern beruht auf einer Executive Order, die vom US-Präsidenten erlassen wurde. Zwar ist sich der EDSA der zugrunde liegenden Erwägung bewusst und begrüßt diese generell, nämlich die Vermeidung des Nachweises der Klagebefugnis (siehe auch Ziffer 215), doch wirft dies eine grundlegende Frage auf: Kann ein solcher Rechtsbehelf (überhaupt) den Anforderungen des Artikels 47 der Charta genügen? Danach hat jede Person, deren durch das Recht der Union garantierte

[201] EuGH, Urteil Schrems I, Rn. 95; EuGH, Urteil Schrems II, Rn. 187.
[202] Clapper/Amnesty International USA, 568 U.S. 398 (2013) II. S. 10.
[203] EO 14086 Section 5 h begründet ausdrücklich das Recht betroffener Personen, Beschwerden im Einklang mit dem Rechtsbehelfsverfahren einzureichen.

Rechte oder Freiheiten verletzt worden sind, das Recht, bei einem zuvor durch Gesetz errichteten Gericht einen wirksamen Rechtsbehelf einzulegen.

218. Während im englischen Wortlaut von Artikel 47 der Charta von einem „tribunal" die Rede ist, werden in anderen Sprachfassungen eher Bezeichnungen verwendet, die dem englischen Wort „court" (Gericht) entsprechen.[204] In der Rechtssache Schrems II hat der EuGH bekräftigt, dass „Einzelne über die Möglichkeit verfügen müssen, Rechtsbehelfe vor einem unabhängigen und unparteiischen Gericht einzulegen, um Zugang zu den sie betreffenden personenbezogenen Daten zu erlangen oder die Berichtigung oder Löschung solcher Daten zu erwirken".[205] Im gleichen Kontext der Beurteilung der Angemessenheit des Datenschutzniveaus ist der EuGH jedoch der Auffassung, dass ein wirksamer gerichtlicher Schutz vor solchen Eingriffen nicht nur von einem Gericht, sondern auch von einem Organ gewährleistet werden kann, das Garantien bietet, die im Wesentlichen den in Artikel 47 der Charta vorgeschriebenen gleichwertig sind.[206] Desgleichen heißt es in der EMRK: „Jede Person, die in ihren Rechten oder Freiheiten verletzt worden ist, hat das Recht, vor einer innerstaatlichen Instanz eine wirksame Beschwerde einzulegen"[207], die nach ständiger Rechtsprechung des EGMR nicht unbedingt eine Justizbehörde sein muss.[208] Vielmehr sind die Befugnisse und Verfahrensgarantien, über die eine Behörde verfügt, insbesondere ihre Unabhängigkeit von der Exekutive und die Gewährleistung eines fairen Verfahrens, für die Beurteilung der Wirksamkeit des Rechtsbehelfs vor dieser Behörde von Bedeutung.[209] Es scheint, dass beide Gerichtshöfe ihre Beurteilung nicht auf rein formale Kriterien stützen, sondern die materiellen Garantien als entscheidend ansehen.

219. In der Rechtssache Schrems II hat der EuGH besonderes Augenmerk auf wirksame Rechtsbehelfe im Bereich des Zugriffs auf personenbezogene Daten im Bereich der nationalen Sicherheit gelegt. Der EDSA nimmt zur Kenntnis, dass der EuGH dabei das Element „zuvor durch Gesetz errichtet" des Artikels 47 der Charta nicht erörtert hat, obwohl der Mechanismus der Ombudsperson des Datenschutzschilds ebenfalls nicht auf dem US-Gesetzesrecht beruhte. Anstatt sich mit diesem Problem zu befassen, bewertete der EuGH verschiedene Aspekte für seine Angemessenheitsprüfung, wie z. B. das Fehlen von Abhilfebefugnissen. Das Schrems-II-Urteil enthält daher keine Orientierungshilfe für die Beurteilung des Begriffs „zuvor durch Gesetz errichtet" gemäß Artikel 47 der Charta. Es gibt jedoch andere Urteile, in denen sich der EuGH zu dieser Frage geäußert hat. In Anlehnung an die ständige Rechtsprechung des EGMR in diesem Zusammenhang erinnerte der EuGH in seinen Rechtssachen C-487/19 und C-132/20 daran, dass der Grund für die Einführung des Ausdrucks „zuvor durch Gesetz errichtet" darin besteht, sicherzustellen, dass die Organisation des Justizsystems in einer demokratischen Gesellschaft nicht vom Ermessen der Exekutive abhängt, sondern durch Gesetz geregelt wird, das vom Gesetzgeber unter Beachtung der Vorschriften über seine Zuständigkeit erlassen wird.[210] Wie sich aus dieser Erklärung ergibt, steht das Recht auf ein zuvor durch Gesetz errichtetes Gericht in engem Zusammenhang mit der Gewährleistung der Unabhängigkeit.

220. Vor diesem Hintergrund kommt der EDSA zu dem Schluss, dass im Zusammenhang mit der Bewertung der Angemessenheit des Schutzniveaus das im Rahmen der EO 14086 geschaffene spezifische

[204] Beispielsweise „Gericht" in der deutschen Sprachfassung.
[205] EuGH, Urteil Schrems II, Rn. 194.
[206] Siehe EuGH, Urteil Schrems II, Rn. 197.
[207] Artikel 13 EMRK.
[208] EGMR, Urteil Klass, Rn. 67; EGMR, Urteil Big Brother Watch, Rn. 359.
[209] EGMR, Urteil Klass, Rn. 67; EGMR, Urteil Big Brother Watch, Rn. 359.
[210] Siehe EuGH, C-487/19, Urteil vom 6. Oktober 2021, W.Ż, C-487/19, ECLI:EU:C:2021:798 und C-132/20, Urteil vom 29. März 2022, Getin Noble Bank S.A., ECLI:EU:C:2022:235, Rn. 129 und 121.

Rechtsbehelfsverfahren im Gegensatz zu Rechtsbehelfen in Gerichten nach Artikel III nicht per se unzureichend ist. Die Analyse des Schutzniveaus in dieser Hinsicht hängt davon ab, ob die in der EO 14086 vorgesehenen und durch die AG-Verordnung ergänzten Garantien die Unabhängigkeit des DPRC gegenüber den anderen Organen hinreichend gewährleisten.

221. Die Kommission sollte kontinuierlich überwachen, ob die in der EO 14086 enthaltenen Vorschriften und ihre ergänzenden Bestimmungen, insbesondere diejenigen zur Förderung der Unabhängigkeit des DPRC, vollständig umgesetzt werden und in der Praxis wirksam funktionieren. Darüber hinaus sollten etwaige Änderungen des Rahmens sorgfältig im Hinblick auf die Auswirkungen auf die Bewertung durch die Kommission gemäß dem Beschlussentwurf überprüft werden. In diesem Zusammenhang stellt der EDSA fest, dass Änderungen der EO 14086 und der AG-Verordnung den Erlass sofort geltender Durchführungsrechtsakte zur Aussetzung, Aufhebung oder Änderung des Angemessenheitsbeschlusses nach sich ziehen können.[211]

3.2.4.2 Ausreichende Unabhängigkeit von der Exekutive

222. In seinem Urteil in der Rechtssache Schrems II betonte der EuGH, dass die Unabhängigkeit des Gerichts oder der Einrichtung, insbesondere von der Exekutive, mit allen erforderlichen Garantien, auch in Bezug auf die Bedingungen für die Abberufung oder den Widerruf der Ernennung, gewährleistet werden muss. Konkret kritisierte der EuGH, dass die Ombudsperson vom Secretary of State ernannt wurde und diesem unmittelbar unterstand. Die Ombudsperson galt als integraler Bestandteil des US-Außenministeriums. Der EuGH stellte ferner fest, dass es keine besonderen Garantien für die Abberufung oder den Widerruf der Ernennung der Ombudsperson gab, wodurch die Unabhängigkeit der Ombudsperson von der Exekutive untergraben würde.

223. Der EDSA räumt ein, dass die Bestimmungen der EO 14086 und der ergänzenden AG-Verordnung keine Berichtspflicht für den DPRC gegenüber dem Generalstaatsanwalt vorsehen, wie sie in einer Vorgesetztenbeziehung bestünde. Der DPRC unterliegt auch nicht der „alltäglichen Aufsicht" des Generalstaatsanwalts[212]. Diese Garantien stellen eine erhebliche Verbesserung gegenüber dem Datenschutzschild dar. Der DPRC ist jedoch bei der Exekutive, d. h. im Justizministerium, angesiedelt. Insbesondere aus diesem Grund werden die Umsetzung und das wirksame Funktionieren der Garantien in der Praxis von entscheidender Bedeutung für die Beantwortung der Frage sein, ob der DPRC, obwohl er nicht integraler Bestandteil des Justizministeriums ist, als eine Einrichtung, die dennoch innerhalb der Exekutive angesiedelt ist, in der Praxis als hinreichend unabhängig angesehen werden kann. Der EDSA fordert die Kommission auf, sorgfältig zu überwachen, ob diese Garantien in der Praxis in vollem Umfang berücksichtigt werden. Darüber hinaus schlägt der EDSA vor, den Begriff „alltägliche Aufsicht" dahin gehend zu präzisieren, dass die „Richter" des DPRC keiner Aufsicht unterliegen. Die Kommission hat bestätigt, dass „alltägliche Aufsicht" in diesem Sinne zu verstehen ist.

224. Zusätzlich zu den oben genannten Garantien sieht der DSR EU-USA bestimmte Garantien für die Ernennung und Entlassung der „Richter" des DPRC vor. Zwar werden sie vom Attorney General ernannt, doch beruht ihre Ernennung auf den Kriterien für die Bewertung von Bewerbern um das Amt eines Bundesrichters und erfordert eine Konsultation des PCLOB. Die Abberufung von „Richtern" vor Ablauf ihrer Amtszeit oder aus einem laufenden Verfahren ist nur unter eng definierten Umständen möglich, die sich, wie es der EDSA versteht, an den für Bundesrichter geltenden Bestimmungen ausrichten.[213] Die Anwendung dieser Vorschriften ist ein weiterer Schritt zur Stärkung der

[211] Beschlussentwurf, Erwägungsgrund 212.
[212] AG-Verordnung, § 201.7 d.
[213] EO 14086, Section 3 d iv; AG-Verordnung § 201.7.

Unabhängigkeit des DPRC, für die wiederum die praktische Umsetzung von entscheidender Bedeutung sein wird. Aus dem Beschlussentwurf geht jedoch nicht eindeutig hervor, ob und wie diese Anforderungen in den Vereinigten Staaten eingehalten werden. Auf der Grundlage zusätzlicher Erläuterungen der Kommission und der US-Regierung geht der EDSA davon aus, dass der PCLOB bei seiner jährlichen Überprüfung des Rechtsbehelfsverfahrens auf die oben genannten Bestimmungen eingehen kann und dass die Verantwortung für die Überwachung und Gewährleistung der Einhaltung aller rechtlichen Anforderungen des Inspectors General im Justizministerium die Anforderungen der EO 14086 und der Verordnungen zur Einrichtung des DPRC umfasst. Der EDSA ersucht die Kommission, diesen Aspekt im Beschlussentwurf zu klären. Allerdings sollte die Kommission diese Garantien berücksichtigen, wenn sie die tatsächliche Praxis der Verarbeitung personenbezogener Daten, wie sie im Beschlussentwurf bewertet wird, überwacht.

225. Im Beschlussentwurf wird nicht auf die Frage eingegangen, ob und unter welchen Bedingungen gegebenenfalls der US-Präsident befugt ist, „Richter" des DPRC zu entlassen oder aus dem Amt zu entfernen. Der EDSA ist der Auffassung, dass eine solche Befugnis nicht bestehen würde, wie von der Europäischen Kommission erläutert und von Vertretern der US-Regierung bestätigt wurde. Der EDSA schlägt vor, diesen Aspekt im Angemessenheitsbeschluss zu klären.

226. Die „Richter" des DPRC werden für vier Jahre ernannt; ihre Amtszeit kann einmal verlängert werden, und sie dürfen zum Zeitpunkt ihrer ersten Ernennung in den beiden vorangegangenen Jahren nicht in der Exekutive beschäftigt gewesen sein.[214] Während ihrer Amtszeit als „Richter" im DPRC dürfen sie keine anderen offiziellen Aufgaben oder Tätigkeiten innerhalb der US-Regierung ausüben.[215] Im Gegensatz zu US-Bundesrichtern können sie jedoch außergerichtlichen Tätigkeiten, einschließlich Geschäftstätigkeiten, Finanztätigkeiten, gemeinnützigen Tätigkeiten zur Mittelbeschaffung, treuhänderischen Tätigkeiten und der Rechtspraxis, nachgehen, sofern diese Tätigkeiten nicht die unparteiische Wahrnehmung ihrer Aufgaben oder die Wirksamkeit oder Unabhängigkeit des DPRC beeinträchtigen.[216] Richterliche Unabhängigkeit ergibt sich nicht nur aus Weisungsfreiheit, sondern auch aus persönlicher Unabhängigkeit. In diesem Zusammenhang sind Faktoren wie die Amtszeit, die Möglichkeit einer Wiederernennung und das Potenzial für Interessenkonflikte von Bedeutung. Die in der EO 14086 bzw. in der AG-Verordnung vorgesehene Amtszeit von vier Jahren, die beispielsweise kürzer ist als die Amtszeit der Richter des EuGH (sechs Jahre mit der Möglichkeit einer Wiederernennung) und des EGMR (neun Jahre ohne Möglichkeit einer Wiederernennung), gibt als solche jedoch keinen Anlass zu ernsten Bedenken. Dem EDSA ist keine einschlägige Rechtsprechung bekannt, die eine Mindestdauer der Amtszeit vorschreibt.[217] Der EDSA erkennt ferner an, dass die Möglichkeit, außergerichtliche Tätigkeiten auszuüben, an die Bedingung geknüpft ist, dass sie, einfach ausgedrückt, nicht zu Interessenkonflikten führen, die die Pflichten des DPRC beeinträchtigen. Der EDSA entnimmt den zusätzlichen Erläuterungen der US-Regierung, dass diese Anforderungen ebenfalls der Überprüfung und Überwachung durch den PCLOB und den Inspector General des Justizministeriums unterliegen (siehe Nr. 226). Wie diese Anforderung in der Praxis angewandt und nachgewiesen wird, sollte ebenfalls im Rahmen der gemeinsamen Überprüfungen behandelt werden.

227. Gemäß Section 3 d i B EO 14086 müssen sich alle „Richter" des DPRC einer Sicherheitsüberprüfung unterziehen, um Zugang zu Verschlusssachen zu erhalten, um also ihre Aufgabe, über Fälle der

[214] AG-Verordnung § 201.3 a.
[215] AG-Verordnung § 201.3 c.
[216] AG-Verordnung § 201.7 c.
[217] Vgl. entsprechend auch EGMR (Große Kammer), Verfahren Centrum För Rättvisa/Schweden, 25. Mai 2021, Rn. 346.

nationalen Sicherheit zu entscheiden, erfüllen zu können.[218] Nach einigen europäischen Gesetzen und Vorschriften über die Sicherheitsüberprüfung hingegen sind Richter von der Verpflichtung zur Sicherheitsüberprüfung befreit, soweit sie richterliche Aufgaben wahrnehmen, da eine solche eingehende Prüfung möglicherweise im Widerspruch zur richterlichen Unabhängigkeit steht.[219] Nach den Erläuterungen der US-Regierung muss ein Bewerber um ein Richteramt an einem US-Gericht einer gründlichen Überprüfung unterzogen werden, wenn er zuvor zum Richter an einem US-Bundesgericht ernannt worden war, denn ein Bundesrichter ist nicht verpflichtet, sich für den Zugang zu für den Fall relevanten Verschlusssachen einer Sicherheitsprüfung zu unterziehen.

228. Nach Auffassung des EDSA lassen die oben dargelegten Umstände teilweise Unterschiede zwischen der Stellung und dem Status eines amerikanischen Bundesrichters und eines „Richters" am DPRC erkennen. Die vorgesehenen Garantien geben jedoch keinen Anlass zu Zweifeln an der Unabhängigkeit des DPRC. Der EDSA fordert die Kommission nachdrücklich auf, im Falle der Annahme des Beschlussentwurfs die oben genannten Garantien bei der ersten gemeinsamen Überprüfung des DSR EU-USA vorrangig zu behandeln. Des Weiteren erwartet der EDSA von der Kommission, dass sie ihrer Zusage, den Angemessenheitsbeschluss aus Dringlichkeitsgründen auszusetzen, aufzuheben oder zu ändern, nachkommen wird, insbesondere wenn die US-Exekutive beschließen würde, die in der EO enthaltenen Garantien einzuschränken[220].

3.2.4.3 Befugnisse des DPRC

3.2.4.3.1 Zugang zu Informationen

229. Ein wirksamer Rechtsschutz setzt voraus, dass das Gericht über ausreichende Ermittlungsbefugnisse verfügt, um die angefochtene Maßnahme überprüfen zu können. In der Rechtssache Kadi II entschied der EuGH in Bezug auf Artikel 47 der Charta, dass die Gerichte der Europäischen Union sich vergewissern müssen, dass eine Entscheidung auf einer hinreichend gesicherten tatsächlichen Grundlage beruht.[221] Wie der EuGH feststellt, „hat der Unionsrichter bei dieser Prüfung gegebenenfalls von der zuständigen Unionsbehörde – vertrauliche oder nicht vertrauliche – Informationen oder Beweise anzufordern, die für eine solche Prüfung relevant sind"[222], wobei „die Geheimhaltungsbedürftigkeit oder Vertraulichkeit … dieser Informationen oder Beweise nicht entgegengehalten werden kann"[223].

230. Gemäß Erwägungsgrund 181 des Beschlussentwurfs überprüft der DPRC die Feststellungen des CLPO mindestens auf der Grundlage des Untersuchungsprotokolls des CLPO sowie aller Informationen und Stellungnahmen des Beschwerdeführers, des Sonderanwalts oder eines Nachrichtendienstes. Im Beschlussentwurf heißt es ferner, dass der DPRC Zugang zu allen erforderlichen Informationen hat, die er über das CLPO erhalten kann. Grundlage hierfür ist die Bestimmung des § 201.9 b AG-Verordnung, wonach der DPRC befugt ist, zu „verlangen, dass das ODNI CLPO das Protokoll durch spezifische erläuternde oder klarstellende Informationen ergänzt und dass das ODNI CLPO erforderlichenfalls zusätzliche Tatsachenfeststellungen trifft, damit das DPRC-Gremium seine Überprüfung durchführen kann". Nach dem Verständnis des EDSA beschränkt sich die vom DPRC vorgenommene Bewertung somit in keiner Weise auf die Feststellungen, die das CLPO auf der ersten Ebene des neuen

[218] Siehe auch AG-Verordnung § 201.11 b und Beschlussentwurf, Erwägungsgrund 177.
[219] Siehe z. B. § 2 Absatz 3 Sicherheitsüberprüfungsgesetz des Bundes (Deutschland).
[220] Beschlussentwurf, Erwägungsgrund 212.
[221] EuGH, verbundene Rechtssachen C-584/10 P, C-593/10 P und C-595/10 P, Europäische Kommission u. a./Yassin Abdullah Kadi, Urteil vom 18. Juli 2013 (im Folgenden „EuGH, Urteil Kadi II"), Rn. 119.
[222] EuGH, Urteil Kadi II, Rn. 120.
[223] EuGH, Urteil Kadi II, Rn. 125.

Rechtsbehelfsverfahrens getroffen hat. Vielmehr kann der DPRC sowohl zusätzliche rechtliche Informationen als auch, was wichtig ist, weitere tatsächliche Umstände für seine Analyse der Frage einholen, ob ein erfasster Verstoß vorliegt. Gleichzeitig stellt der EDSA fest, dass sich diese generell umfangreichen Untersuchungsbefugnisse nicht auf den direkten Zugang zu den über die Person gespeicherten Daten erstrecken. Der Kommission zufolge wird das CLPO immer als Vermittler fungieren, wenn der DPRC weitere Informationen benötigt. Daher stützt sich der Zugang des DPRC zu Informationen, die für die unabhängige Entscheidung über einen Überprüfungsantrag erforderlich sind, in gewissem Umfang darauf, dass das CLPO die erforderlichen Informationen zur Verfügung stellt. Der EDSA erkennt an, dass das CLPO verpflichtet ist, dem DPRC „jede erforderliche Unterstützung" zu gewähren, und dass die Nachrichtendienste verpflichtet sind, dem CLPO Zugang zu Informationen zu gewähren, die für die Durchführung der Überprüfung durch den DPRC erforderlich sind [224]. Der EDSA stellt jedoch auch fest, dass das CLPO selbst nicht unabhängig ist und die erste Untersuchung einer Beschwerde in der ersten Phase des Rechtsbehelfsverfahrens durchführt. Daher begrüßt der EDSA, dass der PCLOB bei seinen jährlichen Überprüfungen des Rechtsbehelfsverfahrens prüfen wird, ob der DPRC uneingeschränkten Zugang zu allen erforderlichen Informationen erhalten hat [225]. Darüber hinaus ersucht der EDSA die Kommission, diesen Aspekt in die gemeinsamen Überprüfungen einzubeziehen, falls der Beschlussentwurf angenommen wird, um die Auswirkungen dieses Systems in der Praxis zu prüfen.

3.2.4.3.2 Abhilfebefugnisse

231. Einer der zentralen Mängel des Datenschutzschilds, die dazu führten, dass der Datenschutzschild vom EuGH in der Rechtssache Schrems II für ungültig erklärt wurde, war das Fehlen verbindlicher Abhilfebefugnisse für die Ombudsperson. Der EuGH stellte fest: „enthält er … keinen Hinweis darauf, dass die Ombudsperson ermächtigt wäre, gegenüber den Nachrichtendiensten verbindliche Entscheidungen zu treffen". [226] Die bloße (politische) Zusage der US-Regierung, dass die Nachrichtendienste jeden von der Ombudsperson festgestellten Verstoß gegen die geltenden Vorschriften korrigieren würden, reichte nicht aus, um ein Schutzniveau zu gewährleisten, das dem in Artikel 47 der Charta garantierten Schutzniveau der Sache nach gleichwertig ist.

232. Im Rahmen des neuen Rechtsbehelfsverfahrens hingegen sind die Entscheidungen von CLPO und DPRC verbindlich. [227] Der EDSA erkennt einerseits an, dass diese Befugnis nicht auf spezifische Maßnahmen beschränkt ist, sondern „geeignete Abhilfemaßnahmen" ermöglicht, um einen festgestellten Verstoß „vollständig abzustellen". Insbesondere wird in Section 4 a der EO 14086 ausdrücklich die Löschung unrechtmäßig erhobener Daten erwähnt. Andererseits stellt der EDSA fest, dass der Wortlaut von Section 4 a EO 14086 eine gewisse Unsicherheit hinsichtlich des Verfahrens zur Bestimmung einer solchen „geeigneten Abhilfemaßnahme" schafft. Eine Maßnahme sollte zwar so konzipiert sein, dass ein Verstoß in vollem Umfang behoben wird, es sollte aber auch geprüft werden, „wie ein Verstoß der festgestellten Art bisher üblicherweise behoben wurde". [228] Bedeutung und Wirkung einer solchen Anforderung sind unklar. Daher fordert der EDSA die Kommission auf, die in der Praxis ergriffenen Abhilfemaßnahmen genau zu überwachen.

[224] EO 14086, Section 3 c i H und Section 3 d iii.
[225] EO 14086, Section 3 e i.
[226] EuGH, Urteil Schrems II, Rn. 196.
[227] EO 14086, Section 3 c ii bzw. Section 3 d ii.
[228] EO 14086, Section 4 a.

3.2.4.4 Einreichung einer Beschwerde im Rahmen des neuen Rechtsbehelfsverfahrens

233. Das im Rahmen der EO 14086 geschaffene Rechtsbehelfsverfahren gilt nur für zugelassene Beschwerden, die von der zuständigen Behörde in einem zugelassenen Staat über US-amerikanische Signalaufklärungstätigkeiten im Zusammenhang mit einem erfassten Verstoß übermittelt werden.[229] Damit dieser Rechtsschutz in Anspruch genommen werden kann, müssen daher mehrere Bedingungen erfüllt sein.

3.2.4.4.1 Benennung als zugelassener Staat

234. Zunächst muss das Land oder die Organisation der regionalen Wirtschaftsintegration, von dem/der aus die Daten in die Vereinigten Staaten übermittelt wurden, vor der Datenübermittlung, die dem Antrag zugrunde liegt, als zugelassener Staat benannt worden sein.[230] Es ist offensichtlich von wesentlicher Bedeutung, dass der vorgesehene Rechtsbehelf zum Zeitpunkt des Inkrafttretens des Angemessenheitsbeschlusses zur Verfügung steht. Dementsprechend sieht Erwägungsgrund 196 des Beschlussentwurfs vor, dass das Inkrafttreten des Beschlusses unter anderem davon abhängig ist, dass die Union für die Zwecke des Rechtsbehelfsverfahrens als zugelassene Einrichtung benannt wird. Tatsächlich scheint die Kommission davon auszugehen, dass die Benennung vor der Annahme des Beschlusses erfolgen wird, da der Entwurf bereits einen Platzhalter für die Benennung der EU durch den Generalstaatsanwalt enthält[231] (im Gegensatz zur Aufnahme der Benennung als aufschiebende Bedingung in den verfügenden Teil des Beschlussentwurfs).

3.2.4.4.2 Beeinträchtigung der Privatsphäre und der bürgerlichen Freiheiten und „Klagebefugnis"

235. Eine „zugelassene Beschwerde" muss sich auf einen mutmaßlichen „erfassten Verstoß" stützen, was wiederum einen Verstoß voraussetzt, der die Privatsphäre und die bürgerlichen Freiheiten des Beschwerdeführers beeinträchtigt.[232] Der EDSA geht auf der Grundlage zusätzlicher Erläuterungen der Kommission davon aus, dass mit einer „Beeinträchtigung" keine Einschränkung der Zulässigkeit einer Beschwerde verbunden sein kann. Vielmehr würde sich, wie die Kommission ausgeführt hat, eine solche Beeinträchtigung auf jede Beschwerde über die Verarbeitung personenbezogener Daten für Signalaufklärungstätigkeiten beziehen, die gegen die in Section 4 d iii genannten Bestimmungen, z. B. die Garantien der EO 14086, verstoßen. Der EDSA bedauert, dass dies im Wortlaut des Beschlussentwurfs nicht näher ausgeführt wird, und fordert die Kommission auf, den Begriff „Beeinträchtigung" weiter zu präzisieren, um sicherzustellen, dass jede Verletzung der Rechte der betroffenen Personen bewertet und behoben wird und dass keine „Schwere" nachgewiesen werden muss, um Zugang zu Rechtsbehelfen und angemessenen Abhilfemaßnahmen zu erhalten.

236. Wie bereits erwähnt, setzt eine Beschwerde unter EO 14086 nicht voraus, dass der Kläger seine Klagebefugnis nachweist (siehe Nr. 215)[233]. Der EDSA begrüßt die Klarstellung in Abschnitt 4 k EO 14086, dass ein „Vertrauenstest" angewandt wird und dass nicht nachgewiesen werden muss, dass auf die Daten des Beschwerdeführers im Zuge von Signalaufklärungstätigkeiten tatsächlich zugegriffen wurde. Die Einrichtung des Rechtsbehelfsverfahrens ist ein wichtiger Schritt, da das Erfordernis der

[229] EO 14086, Section 3 a.
[230] EO 14086, Section 4 d i, Section 4 k i.
[231] Beschlussentwurf, Fußnote 320.
[232] EO 14086, Section 4 k i und Section 4 d ii.
[233] Clapper/Amnesty International USA, 568 U.S. 398 (2013) II. S. 10.

Klagebefugnis es sehr schwierig macht, Überwachungsmaßnahmen vor ordentlichen Gerichten in den Vereinigten Staaten anzufechten.

237. Auf der Grundlage der vorstehenden Ausführungen vertritt der EDSA die Ansicht, dass das Anrufen ordentlicher Gerichte, auf das im Beschlussentwurf ebenfalls Bezug genommen wird[234], kein angemessenes Schutzniveau bietet[235]. In diesem Zusammenhang erinnert der EDSA an seine bereits mehrfach geäußerten Bedenken in Bezug auf das Erfordernis der Klagebefugnis vor ordentlichen Gerichten.[236] Darüber hinaus geht der EDSA auf der Grundlage zusätzlicher Erklärungen der US-Regierung davon aus, dass die EO 14086 zwar die Anrufung der Gerichte mit allgemeiner Zuständigkeit nicht ausschließt, es aber fraglich ist, wie ein solches Gericht diese Durchführungsverordnung anwenden würde. Diese Frage könnte bei künftigen Überprüfungen eingehender geprüft werden, falls der Beschlussentwurf angenommen wird.

3.2.4.4.3 Der Gang des Beschwerdeverfahrens

238. Der EDSA befürwortet grundsätzlich das Verfahren zur Weiterleitung einer Beschwerde über die Aufsichtsbehörden der Mitgliedstaaten und ist nach wie vor der Ansicht, dass die Identifizierung des Beschwerdeführers im Hoheitsgebiet der EU erfolgen sollte. Wie schon bei dem Ombudsmechanismus des Datenschutzschilds sieht der Beschlussentwurf jedoch vor, dass eine betroffene Person, die eine solche Beschwerde einreichen möchte, dies bei einer Aufsichtsbehörde in einem EU-Mitgliedstaat tun muss, die für die Aufsicht über nationale Sicherheitsdienste und/oder die Verarbeitung personenbezogener Daten durch Behörden zuständig ist.[237] In diesem Zusammenhang erinnert der EDSA an seine bereits in der Stellungnahme der Artikel-29-Datenschutzgruppe zum Datenschutzschild geäußerten Bedenken, z. B. mögliche Schwierigkeiten für natürliche Personen bei der Ermittlung der zuständigen Behörde angesichts der Vielfalt von Aufsichtsmechanismen über nationale Sicherheitsdienste in den Mitgliedstaaten.[238] Unter Berücksichtigung der Einbeziehung der nationalen Datenschutzbehörden in die Anwendung des DSR EU-USA und die Aufsicht darüber ist es wohl angemessener, Beschwerden über sie einzureichen.

3.2.4.5 Die Entscheidung des DPRC

239. Nach Abschluss der Prüfung des Antrags des Beschwerdeführers darf der DPRC nicht offenlegen, ob der Beschwerdeführer Gegenstand von US-Signalaufklärungstätigkeiten war oder nicht. Stattdessen wird dem Beschwerdeführer mitgeteilt, dass „bei der Überprüfung entweder keine erfassten Verstöße festgestellt wurden oder das Gericht für die Überprüfung des Datenschutzes eine Entscheidung getroffen hat, die eine angemessene Abhilfemaßnahme verlangt“[239]. Diese Standardantwort dient dem allgemein legitimen Zweck des Schutzes sensibler Informationen über nachrichtendienstliche Tätigkeiten der USA. Der EDSA befürchtet jedoch, dass die EO 14086 keine Ausnahmen von der Standardantwort des DPRC vorsieht.

240. In der Rechtssache Kadi II musste sich der EuGH mit den kollidierenden Interessen des Staatsgeheimnisses einerseits und eines fairen und soweit wie möglich kontradiktorischen Verfahrens andererseits befassen. Der EuGH entschied, dass es in Fällen, in denen zwingende Erwägungen der

[234] Beschlussentwurf, Erwägungsgründe 187ff.
[235] Siehe auch EuGH, Urteil Schrems II, Rn. 191 und 192.
[236] Siehe Stellungnahme 01/2016 der Artikel-29-Datenschutzgruppe, S. 50.
[237] Beschlussentwurf, Erwägungsgrund 169.
[238] Stellungnahme 01/2016 der Artikel-29-Datenschutzgruppe, S. 57f.
[239] EO 14086, Section 3 d i H. Section EO 14086 sieht diese Antwort auch für das CLPO vor.

nationalen Sicherheit der Mitteilung von Informationen oder Beweisen an die betroffene Person entgegenstehen, der Unionsrichter dessen ungeachtet im Rahmen der von ihm ausgeübten richterlichen Kontrolle Techniken anwenden muss, die es ermöglichen, die legitimen Sicherheitsinteressen in Bezug auf die Art und Quelle der Informationen sowie das Erfordernis, dem Einzelnen die Wahrung seiner Verfahrensrechte wie des Rechts, gehört zu werden, und des Grundsatzes des kontradiktorischen Verfahrens hinreichend zu garantieren.[240] Weiter führte der EuGH aus: „Weiter hat der Unionsrichter alle von der zuständigen Unionsbehörde beigebrachten rechtlichen und tatsächlichen Umstände sowie die Stichhaltigkeit der Gründe zu prüfen, die diese Behörde angeführt hat, um eine derartige Mitteilung abzulehnen."[241] Zeigt sich, dass die von der zuständigen Unionsbehörde angeführten Gründe der Mitteilung von Informationen oder Beweisen an die betroffene Person tatsächlich entgegenstehen, ist es noch immer erforderlich, die Erfordernisse, die mit dem Recht auf effektiven gerichtlichen Rechtsschutz verbunden sind, und diejenigen, die sich aus der nationalen Sicherheit ergeben, in angemessener Weise zum Ausgleich zu bringen.[242] Bei diesem Ausgleich kann auf Möglichkeiten wie die Übermittlung einer Zusammenfassung des Inhalts der fraglichen Informationen oder Beweise zurückgegriffen werden.[243] Die Feststellungen des Gerichts geben zwar keine Anforderungen an die von einem Gericht erlassene Entscheidung vor, sondern beziehen sich auf die Entscheidung der zuständigen Behörde und die Durchführung von Gerichtsverfahren, doch liefern sie Anhaltspunkte für die Abwägung der oben genannten Interessen im Zusammenhang mit dem Recht auf effektiven Rechtsschutz. Für weitere Hinweise kann auch auf die Rechtssache Big Brother Watch verwiesen werden, in der der EGMR unter Hinweis auf die Fairness des Verfahrens und insbesondere auf den Grundsatz des kontradiktorischen Verfahrens entschieden hat, dass die Entscheidungen einer gerichtlichen oder anderweitig unabhängigen Stelle begründet werden sollten.[244]

241. Der EDSA erkennt an, dass die Entscheidungen des DPRC in der Tat begründet werden. Der DPRC ist ausdrücklich verpflichtet, eine schriftliche Entscheidung zu erlassen, in der seine Feststellungen und etwaige angemessene Abhilfemaßnahmen dargelegt werden.[245] Darüber hinaus stellt der EDSA fest, dass die betroffene Person benachrichtigt wird, wenn Informationen im Zusammenhang mit einer Überprüfung durch den DPRC freigegeben wurden.[246] Der EDSA erkennt auch die Rolle der im neuen Rechtsbehelfsverfahren vorgesehenen Sonderanwälte an, zu deren Aufgaben auch gehört, sich für die Interessen des Beschwerdeführers in der Sache einsetzen.[247] Angesichts der oben dargelegten Implikationen der Rechtsprechung des EuGH und des EGMR und unter Berücksichtigung der Tatsache, dass die Entscheidung des DPRC nicht angefochten werden kann, sondern rechtskräftig ist[248], hat der EDSA Bedenken hinsichtlich der generellen Anwendung der Standardantwort des DPRC. Der EDSA erinnert daran, dass der PCLOB die Funktionsweise des neuen Rechtsbehelfsverfahrens unabhängig überprüfen wird, und fordert die Kommission auf, dieser Frage, einschließlich einer etwaigen Bewertung dieses Aspekts durch den PCLOB, bei künftigen Überprüfungen des Beschlusses, falls er angenommen wird, besondere Aufmerksamkeit zu widmen.

[240] EuGH, Urteil Kadi II, Rn. 125.
[241] EuGH, Urteil Kadi II, Rn. 126.
[242] EuGH, Urteil Kadi II, Rn. 128.
[243] EuGH, Urteil Kadi II, Rn. 129.
[244] EGMR, Urteil Big Brother Watch, Rn. 359.
[245] AG-Verordnung, § 201.9 g.
[246] EO 14086, Section 3 d v.
[247] AG-Verordnung, § 201.8 g.
[248] AG-Verordnung, § 201.9 g.

4 UMSETZUNG UND ÜBERWACHUNG DES BESCHLUSSENTWURFS

242. In Bezug auf die Überwachung und Überprüfung des Beschlussentwurfs stellt der EDSA fest, dass es nach der Rechtsprechung des EuGH „in Anbetracht der Tatsache, dass das durch ein Drittland gewährleistete Schutzniveau Veränderungen unterworfen sein kann, der Kommission obliegt, im Anschluss an den Erlass eines Angemessenheitsbeschlusses gemäß [Artikel 45 DSGVO] in regelmäßigen Abständen zu prüfen, ob die Feststellung der Angemessenheit des vom fraglichen Drittland gewährleisteten Schutzniveaus in sachlicher und rechtlicher Hinsicht nach wie vor gerechtfertigt ist. Eine solche Prüfung ist jedenfalls dann geboten, wenn Anhaltspunkte vorliegen, die Zweifel daran wecken."[249]

243. Darüber hinaus stellt der EDSA fest, dass in dem Schreiben des DoC vorgesehen ist, dass das DoC und gegebenenfalls andere US-Behörden regelmäßig Sitzungen mit der Kommission, interessierten Datenschutzbehörden in der EU und geeigneten Vertretern des EDSA abhalten werden.[250]

244. Der EDSA ist der Auffassung, dass der Schutz durch bundesstaatliche Gesetze in Bezug auf den Zugriff durch Strafverfolgungsbehörden, die Ausnahmeregelung für die vorübergehende Sammelerhebung im Hinblick auf die gezielte Erhebung durch die nationalen Sicherheitsbehörden der USA, die Anwendung der neu eingeführten Grundsätze der Erforderlichkeit und Verhältnismäßigkeit in der Praxis, auch im Zusammenhang mit dem UPSTREAM-Programm, das Zusammenspiel zwischen der EO 14086 und den verschiedenen Rechtsinstrumenten der USA, die es US-Geheimdiensten ermöglichen, personenbezogene Daten zu erheben und weiterzuverarbeiten, die Umsetzung interner Strategien und Verfahren, die Art und Weise, wie diese Garantien auch im Rahmen der vom FISC geleiteten Aufsicht berücksichtigt werden und die Frage, wie das Rechtsbehelfsverfahren wirksam funktionieren wird, sowie die Themen Weiterübermittlung,, automatisierte Entscheidungen, inhaltliche und wirksame Aufsicht und Durchsetzung der DSR-Grundsätze sowie ein wirksamer Rechtsbehelf im Laufe der nächsten regelmäßigen Überprüfungen besondere Aufmerksamkeit verdienen.

245. Der EDSA stellt fest, dass die Überprüfung des Angemessenheitsbeschlusses ein Jahr nach dem Datum der Übermittlung des Angemessenheitsbeschlusses an die Mitgliedstaaten und danach mindestens alle vier Jahre erfolgen wird.[251] Um die kontinuierliche Überwachung des Angemessenheitsbeschlusses weiter zu verstärken, fordert der EDSA die Kommission auf, die Folgeüberprüfungen mindestens alle drei Jahre vorzunehmen.

246. In Bezug auf die praktische Einbeziehung des EDSA und seiner Vertreter in die Vorbereitung und Durchführung der künftigen regelmäßigen Überprüfungen bekräftigt der EDSA, dass alle einschlägigen Unterlagen einschließlich des Schriftverkehrs rechtzeitig vor den Überprüfungen dem EDSA schriftlich übermittelt werden sollten. Wie bei den im Rahmen des Datenschutzschilds durchgeführten Überprüfungen empfiehlt der EDSA, dass die Modalitäten der Überprüfung spätestens drei Monate vor der Überprüfung zwischen der Kommission, der US-Regierung und dem EDSA vereinbart werden.

247. Darüber hinaus nimmt der EDSA zur Kenntnis und begrüßt, dass Erwägungsgrund 212 des Beschlussentwurfs Beispiele für Änderungen enthält, die das Schutzniveau untergraben und die Einleitung eines „Verfahrens zur Aufhebung im Notfall" rechtfertigen können, das sich auf Änderungen

[249] EuGH, Urteil Schrems I, Rn. 76. Siehe auch Beschlussentwurf, Artikel 3 Absatz 4.
[250] Beschlussentwurf, Anhang III.
[251] Beschlussentwurf, Artikel 3 Absatz 4.

konzentriert, die im Zusammenhang mit der Executive Order 14086 und der damit verbundenen AG-Verordnung vorgenommen werden könnten.

Für den Europäischen Datenschutzausschuss

Vorsitzende

(Andrea Jelinek)