Anwendungshinweise

der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 4. September 2023[1]

Übermittlung personenbezogener Daten aus Europa an die USA

Anwendungshinweise zum Angemessenheitsbeschluss der Europäischen Kommission zum Datenschutzrahmen EU-USA (EU-US Data Privacy Framework) vom 10. Juli 2023

Mit diesen Anwendungshinweisen sollen die wesentlichen Hintergründe und Inhalte des neuen Angemessenheitsbeschlusses der Europäischen Kommission zum Datenschutzrahmen EU-USA vom 10. Juli 2023[2] (EU-US Data Privacy Framework, abgekürzt: EU-US DPF) erläutert werden. Sie richten sich sowohl an Verantwortliche und Auftragsverarbeiter in Deutschland, die personenbezogene Daten an die USA übermitteln, als auch an betroffene Personen. Die Anwendungshinweise beleuchten insbesondere die Reichweite und den Anwendungsbereich der Neuregelung, den Einsatz alternativer Instrumente für Übermittlungen an die USA sowie Umfang und Durchsetzung von Rechten betroffener Personen gegenüber Stellen in den USA.

---

[1] **Die Anwendungshinweise wurden durch die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder gegen die Stimme des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit verabschiedet.**

[2] Angemessenheitsbeschluss zum EU-US DPF, abrufbar unter: https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en.

Inhaltsverzeichnis

I. Allgemeine Informationen

1. Allgemeines zu Drittlandsübermittlungen

1.1. Übermittlung an Drittländer – Begriffsverständnis

Der Europäische Datenschutzausschuss (EDSA) erläutert in den Leitlinien 05/2021 sein Verständnis des Übermittlungsbegriffs i. S. d. Art. 44 ff. DS-GVO („transfer“).[3] Der Begriff der Übermittlung in diesem Sinne ist nicht auf zielgerichtete und absichtliche Vorgänge beschränkt. Vielmehr kann es sich auch beim Einräumen einer faktischen Zugriffsmöglichkeit aus dem Drittland (beispielsweise für administrative oder Supportzwecke) um eine Übermittlung handeln.[4] Drittländer sind Länder, in denen die DS-GVO nicht gilt. Die DS-GVO gilt zum einen unmittelbar in den Mitgliedstaaten der Europäischen Union, also den Vertragspartnern des EU-Vertrags. Darüber hinaus gilt die DS-GVO durch Beschluss Nr. 154/2018 des Gemeinsamen EWR-Ausschusses vom 06.07.2018 auch in den übrigen EWR-Staaten (Island, Liechtenstein, Norwegen).

1.2. Zweistufige Prüfung der Rechtmäßigkeit der Übermittlung an Drittländer

Eine Datenübermittlung an Drittländer ist nach Art. 44 Abs. 1 S. 1 DS-GVO nur dann zulässig, wenn neben den Bestimmungen des Kapitels V (Übermittlungen personenbezogener Daten an Drittländer oder an internationale Organisationen) auch die übrigen Bestimmungen der DS-GVO eingehalten werden.

Es muss somit zunächst geprüft werden, ob für die Verarbeitung von personenbezogenen Daten eine Rechtsgrundlage gem. Art. 6 Abs. 1 DS-GVO und ggf. Art. 9 Abs. 2 DS-GVO einschlägig ist. Weiterhin muss auch die Einhaltung der weiteren Bestimmungen der DS-GVO, insbesondere die Einhaltung der Grundsätze aus Art. 5 DS-GVO, gewährleistet sein (1. Stufe).

In diesem Sinne im Einklang mit den übrigen Anforderungen der DS-GVO verarbeitete personenbezogene Daten dürfen nur dann an ein Drittland übermittelt werden, wenn die Übermittlung zusätzlich nach einer der Bestimmungen des Kapitels V DS-GVO

---

[3] EDSA: Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR [bisher nur auf Englisch verfügbar], S. 3, abrufbar unter: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052021-interplay-between-application-article-3_en.

[4] Ebd., S. 8, Rn. 16.

legitimiert werden kann (2. Stufe). Die möglichen Übermittlungsinstrumente nach Kapitel V DS-GVO werden im folgenden Abschnitt kurz erläutert.

1.3. Kapitel V – Übersicht zu den Übermittlungsinstrumenten

Ein **Angemessenheitsbeschluss** gem. Art. 45 DS-GVO ermöglicht eine den Anforderungen von Kapitel V DS-GVO entsprechende Datenübermittlung an das jeweilige Drittland. Der Europäischen Kommission kommt hier die zentrale Beurteilungskompetenz zu, im Rahmen von sog. Angemessenheitsbeschlüssen festzustellen, dass in einem Drittland ein mit der EU vergleichbares Datenschutzniveau gewährleistet ist. Dabei muss die Europäische Kommission gemäß Art. 45 Abs. 2 lit. b DS-GVO insbesondere auch prüfen, ob **wirksame verwaltungsrechtliche und gerichtliche Rechtsbehelfe** für betroffene Personen bestehen, deren personenbezogene Daten übermittelt werden. Diese Beurteilung erstreckt sich unter Umständen nicht auf ein Land als Ganzes, sondern kann auch bestimmte Regionen, Branchen oder internationale Organisationen betreffen (Art. 45 Abs. 1 DS-GVO). Bei dem **EU-US Data Privacy Framework (EU-US DPF)** handelt es sich um einen solchen Angemessenheitsbeschluss, hier beschränkt auf zertifizierte Stellen[5] Sofern die Europäische Kommission einen Angemessenheitsbeschluss zu einem Drittland, einem Gebiet oder einem oder mehreren Sektoren veröffentlicht, ist keine weitere Legitimierung für die Drittlandsübermittlung nach Kapitel V DS-GVO erforderlich. Allerdings müssen Verantwortliche regelmäßig die Aktualität des Angemessenheitsbeschlusses prüfen. Eine aktuelle Liste der Angemessenheitsbeschlüsse und weitere Informationen sind auf der Website der Europäischen Kommission verfügbar.[6]

Darüber hinaus kommen **geeignete Garantien** gem. Art. 46 DS-GVO als Übermittlungsinstrumente in Betracht. Hierbei ist aber zu berücksichtigen, dass diese allein möglicherweise noch nicht ausreichen, um ein mit der EU der Sache nach gleichwertiges Datenschutzniveau zu gewährleisten. In den EDSA-Empfehlungen 01/2020 werden daher zusätzliche Maßnahmen aufgezeigt, die ggf. ergriffen werden müssen, um das vom Gesetz geforderte Schutzniveau doch noch zu erreichen.[7]

---

[5] Vgl. Art. 1 des Angemessenheitsbeschlusses zum EU-US DPF.

[6] Europäische Kommission: Adequacy decisions, abrufbar unter: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_de.

[7] EDSA: Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten, abrufbar unter: https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_de.

Garantien i. S. d. Art. 46 DS-GVO sind beispielsweise **Verwaltungsvereinbarungen** oder **andere bindende und durchsetzbare Dokumente** (Art. 46 Abs. 2 lit. a, Abs. 3 lit. b DS-GVO) für Datenübermittlungen zwischen Behörden und sonstigen öffentlichen Stellen.

Als geeignete Garantien häufige Verwendung finden **Standarddatenschutzklauseln** (Standard Data Protection Clauses) gem. Art. 46 Abs. 2 lit. c und d DS-GVO in Form von Standardvertragsklauseln (Standard Contractual Clauses, SCCs). Art. 46 Abs. 2 lit. c DS-GVO betrifft Klauseln, die unmittelbar von der Europäischen Kommission erlassen werden. Die von der Europäischen Kommission im Jahr 2021 erlassenen und veröffentlichten Standardvertragsklauseln sind modular aufgebaut und können ohne weitere Genehmigung verwendet werden.[8] Verantwortliche und Auftragsverarbeiter, die die Klauseln für Drittlandsübermittlungen nutzen wollen, müssen daraus das für ihre jeweilige Situation passende Modul auswählen. Die Standarddatenschutzklauseln sollen ein gleichwertiges Schutzniveau wie in der EU gewährleisten. Ob das für die jeweilige Übermittlung tatsächlich gegeben ist, muss der Verantwortliche aber entsprechend der Empfehlungen 01/2020 eigenständig prüfen, und ggf. muss er hierfür zusätzliche Maßnahmen ergreifen.

Weitere Möglichkeiten, geeignete Garantien sicherzustellen, sind die Anwendung **genehmigter Verhaltensregeln** gem. Art. 40, 46 Abs. 2 lit. e DS-GVO oder eines **genehmigten Zertifizierungsmechanismus** gem. Art. 42, 46 Abs. 2 lit. f DS-GVO, welche jeweils um weitere rechtsverbindliche und durchsetzbare Verpflichtungen des Verantwortlichen oder Auftragsverarbeiters im Drittland ergänzt werden müssen. Zu beiden vorgenannten Übermittlungsinstrumenten hat der EDSA bereits Leitlinien herausgegeben.[9]

Als geeignete Garantien für Drittlandsübermittlungen innerhalb einer Unternehmensgruppe oder von Gruppen von Unternehmen kommen zudem **verbindliche interne**

---

[8] Europäische Kommission: Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (Text with EEA relevance), abrufbar unter: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021D0914&qid=1688729959265.

[9] EDSA: Leitlinien 4/2021 über Verhaltensregeln als Instrument für Übermittlungen, abrufbar unter: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042021-codes-conduct-tools-transfers_de.
EDSA: Leitlinien 7/2022 über die Zertifizierung als Instrument für Übermittlungen, abrufbar unter: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072022-certification-tool-transfers_de.

Datenschutzvorschriften (Binding Corporate Rules, BCR) gem. Art. 46 Abs. 2 lit. b, Art. 47 DS-GVO in Betracht. Der EDSA hat in seinen Empfehlungen 01/2022 weitere Hinweise und ein Formular zur Antragstellung hierfür zur Verfügung gestellt.[10]

Sofern weder ein einschlägiger Angemessenheitsbeschluss besteht noch geeignete Garantien (einschließlich verbindlicher interner Datenschutzvorschriften) verwendet werden, kann die Drittlandsübermittlung in **Ausnahmefällen** gem. Art. 49 DS-GVO zulässig sein. In den entsprechenden EDSA-Leitlinien 2/2018 wird näher erläutert, unter welchen speziellen Bedingungen diese Ausnahmefälle Anwendung finden können.[11]

2. Vor- und Entstehungsgeschichte des EU-US DPF

Der Europäische Gerichtshof (EuGH) erklärte 2015 und 2020 in den sog. „Schrems I"- und „Schrems II"-Urteilen zwei frühere Angemessenheitsbeschlüsse für zertifizierte Stellen in den USA („Safe Harbor" sowie „Privacy Shield") aufgrund unverhältnismäßiger Zugriffsbefugnisse der US-Sicherheitsbehörden und unzureichender Rechtsschutzmöglichkeiten für betroffene Personen für ungültig.

Im Juli 2000 hatte die Europäische Kommission noch auf Grundlage der alten EU-Datenschutzrichtlinie[12] einen Angemessenheitsbeschluss für zertifizierte Stellen in den USA angenommen, um einen ungehinderten transatlantischen Datenaustausch zu ermöglichen (**sog. „Safe Harbor"**).[13] Nachdem jedoch nicht zuletzt durch die Enthüllungen von Edward Snowden offengelegt wurde, dass US-Sicherheitsbehörden systematisch und massenhaft auf an die USA übermittelte personenbezogene Daten von EU-Bürgerinnen und EU-Bürgern zugreifen und damit die „Safe Harbor"-Grundsätze mit großer Wahrscheinlichkeit gravierend verletzt werden, erklärte der EuGH im

---

[10] EDSA: Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR). Derzeit nur in englischer Sprachfassung verfügbar, abrufbar unter: https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-12022-application-approval-and_de.

[11] EDSA: Leitlinien 2/2018 zu den Ausnahmen nach Artikel 49 der Verordnung 2016/679, abrufbar unter: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_de.

[12] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

[13] 2000/520/EG: Entscheidung der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des „sicheren Hafens" und der diesbezüglichen „Häufig gestellten Fragen" (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA.

Oktober 2015 in der **sog. „Schrems I"-Entscheidung**[14] den „Safe Harbor"-Angemessenheitsbeschluss der Europäischen Kommission für ungültig.

Nach Verabschiedung der DS-GVO erließ die Europäische Kommission im Juli 2016 den Angemessenheitsbeschluss zum **sog. „EU-US Privacy Shield"**[15] , funktionell eine Nachfolgeregelung zu „Safe Harbor". Im Juli 2020 erklärte der EuGH in der **sog. „Schrems II"-Entscheidung**[16] auch die entsprechende Kommissionsentscheidung zum „Privacy Shield" für unionsrechtswidrig und ungültig. Der EuGH stützte sein „Schrems II"-Urteil auf zwei zentrale Kritikpunkte an der Rechtslage in den USA: Zum einen stellte er unter Verweis auf die US-Sicherheitsgesetze FISA[17] Section 702 und Executive Order 12333 fest, dass die Befugnisse der US-Sicherheitsbehörden, auf die übermittelten personenbezogenen Daten zuzugreifen, unbestimmt und unverhältnismäßig sind. Zum anderen kritisierte der EuGH, dass für EU-Ausländer in den USA keine ausreichenden Rechtsschutzmöglichkeiten zur Überprüfung solcher Zugriffe bestehen.

Mit der Ungültigerklärung des Angemessenheitsbeschlusses zum „Privacy Shield" konnten Übermittlungen von einem Tag auf den anderen nicht mehr auf diesen gestützt werden. Somit bestand in der Praxis eine Lücke für transatlantische Datenübermittlungen, die nun durch den neuen Angemessenheitsbeschluss zum EU-US DPF, dem mehrjährige Verhandlungen zwischen der EU und den USA vorangingen, geschlossen wurde.

Im März 2022 hatten die Präsidentin der Europäischen Kommission und der Präsident der Vereinigten Staaten von Amerika (US-Präsident) zunächst eine grundsätzliche Einigung über einen neuen transatlantischen Datenschutzrahmen verkündet.[18] Im Oktober 2022 erließ der US-Präsident ein Dekret, die Executive Order 14086, welche zusammen mit den *regulations* des US-Justizministers die o. g. grundsätzliche Einigung in Rechtsvorschriften umsetzte und die Kritikpunkte des EuGH im „Schrems II"-Urteil (Unverhältnismäßigkeit der Zugriffe von US-Sicherheitsbehörden sowie

[14] EuGH, Urt. v. 6. Oktober 2015, Rs. C-362/14 (sog. Schrems I).
[15] 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.
[16] EuGH, Urt. v. 16. Juli 2020, Rs. C-311/18 (sog. Schrems II).
[17] Foreign Intelligence Surveillance Act.
[18] S. PM der Europäischen Kommission, abrufbar unter: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2087.

unzureichender Rechtsschutz betroffener Personen)[19] adressierte. Die Europäische Kommission veröffentlichte daraufhin im Dezember 2022 den Entwurf des Angemessenheitsbeschlusses zum EU-US DPF.[20] Nachdem der Beschlussentwurf von den Mitgliedstaaten im sogenannten Komitologieverfahren bestätigt worden war, nahm die Europäische Kommission den Angemessenheitsbeschluss zum EU-US DPF am 10. Juli 2023 an. Dieser trat am selben Tag in Kraft.[21]

II. Informationen für Daten übermittelnde Stellen (= Datenexporteure)

1. Der Anwendungsbereich des EU-US DPF

1.1. Wer kann sich zertifizieren lassen? Wie wird zertifiziert?

Eine Selbstzertifizierung unter dem EU-US DPF steht US-Organisationen offen, die der Aufsicht der Federal Trade Commission (FTC, eine eigenständige US-Bundesbehörde, die für Wettbewerbskontrolle sowie Verbraucherschutz zuständig ist)[22] oder des US Department of Transportation (DOT, US-Verkehrsministerium)[23] unterliegen. Das EU-US DPF enthält den Hinweis, dass zukünftig gegebenenfalls Zuständigkeiten weiterer US-Behörden hinzukommen können.[24] Bislang steht eine Zertifizierung jedoch nur Unternehmen offen, welche einer der genannten aufsichtsbehördlichen Zuständigkeiten unterliegen.

---

[19] S. PM der Europäischen Kommission, abrufbar unter: https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_6045, Schrems II Urteil des EuGH (C-311/18) v. 16. Juli 2020.

[20] S. zum Entwurf des Angemessenheitsbeschlusses zum EU-US; DPF: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7631. Zu diesem Beschlussentwurf verabschiedete der EDSA eine Stellungnahme, abrufbar unter: https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-52023-european-commission-draft-implementing_en; auch das Europäische Parlament veröffentlichte eine Entschließung zum Entwurf, abrufbar unter: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0204_DE.html.

[21] Angemessenheitsbeschluss zum EU-US DPF, abrufbar unter: https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en; s. PM der Europäischen Kommission, abrufbar unter: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721; Q&A https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_3752.

[22] S. zur Zuständigkeit FTC insb. Annex IV des Angemessenheitsbeschlusses zum EU-US DPF.

[23] S. zur Zuständigkeit DOT insb. Annex V des Angemessenheitsbeschlusses zum EU-US DPF.

[24] S. EWG (9), Annex I, Section I.2 des Angemessenheitsbeschlusses zum EU-US DPF.

Für die Aufnahme der Zertifizierung in die Liste des US-Handelsministeriums (US Department of Commerce, DOC) ist es erforderlich, dass die jeweilige US-Organisation dem DOC unter anderem folgende Informationen[25] übermittelt:

- den Namen der betreffenden US-Organisation (US-Unternehmen oder US-Tochtergesellschaften),
- den Zweck, zu dem die Organisation personenbezogene Daten verarbeiten wird,
- die Kategorie der personenbezogenen Daten, die von der Zertifizierung erfasst werden,
- die gewählte Überprüfungsmethode,
- den einschlägigen unabhängigen Regressmechanismus und
- die für die Durchsetzung der Grundsätze zuständigen gesetzlichen Stelle.

Werden sämtliche Anforderungen nach Prüfung durch das DOC erfüllt, erklären die jeweiligen US-Organisationen öffentlich (z. B. auf ihrer Website), dass sie sich zur Einhaltung der Vorgaben des EU-US DPF verpflichten, ihre Datenschutzrichtlinien zur Verfügung stellen und diese vollständig umsetzen.[26]

Das DOC unterhält und veröffentlicht eine „Data Privacy Framework List“ (DPF-Liste), welche diejenigen US-Organisationen auflistet, die ihre Selbstzertifizierung unter dem EU-US DPF abgeschlossen haben.[27] Nur Übermittlungen an dort aufgelistete US-Organisationen können auf den EU-US DPF gestützt werden.

Im Rahmen eines „Follow-up-Verfahrens“ muss die US-Organisation die Umsetzung ihrer Datenschutzpraxis vor dem Hintergrund der Vorgaben des EU-US DPF überprüfen.[28] Zum Erhalt der Zertifizierung erfolgt eine jährliche „Neu-Zertifizierung“ mit Verpflichtungserklärungen gegenüber dem DOC und einer Prüfung durch das DOC.[29]

[25] S. EWG (48), Annex I, Section III.6.b und Annex III des Angemessenheitsbeschlusses zum EU-US DPF.
[26] S. Annex III des Angemessenheitsbeschlusses zum EU-US DPF.
[27] S. Artikel 1; Annex I, Section I.2, III.6.d des Angemessenheitsbeschlusses zum EU-US DPF.
[28] Annex I, Section III.7.
[29] Annex I, Section III.6.d.

Die FTC, deren Zuständigkeit in 15 U.S.C. § 45 geregelt ist, weist auf Bereiche hin, in welchen sie keine bzw. nur eingeschränkte Zuständigkeiten hat.[30] Sollte der Datenexporteur Übermittlungen in diesen Bereichen – das betrifft insbesondere den **Bankensektor**, das **Versicherungsgewerbe** und die **Betreiber öffentlicher Telekommunikationsnetze** – planen, ist dies ggf. nicht auf Grundlage des Angemessenheitsbeschlusses zum EU-US DPF möglich. Jedenfalls muss der Datenexporteur genau prüfen, ob der Datenimporteur auf der EU-US-DPF-Liste gelistet wurde.

Die Zuständigkeit des DOT besteht gemäß 49 U.S.C. § 41712 gegenüber Luftfahrtunternehmen und Flugscheinvermittlern.[31]

Der Angemessenheitsbeschluss zum EU-US DPF ist sektoral und erfasst nur Datenübermittlungen an teilnehmende US-Organisationen. Dies bedeutet, dass es sich nicht um einen umfassenden Angemessenheitsbeschluss für die gesamten USA handelt. Datenexporteure müssen daher prüfen, ob ihre geplanten Datenübermittlungen in den Anwendungsbereich des Beschlusses fallen und damit auf Grundlage dieses Übermittlungsinstrumentes vorgenommen werden können.

Hinweis für Datenexporteure:

Um bewerten zu können, ob die geplante Übermittlung auf das EU-US DPF gestützt werden kann, muss der Datenexporteur prüfen, ob der Datenimporteur (US-Organisation, an welche die personenbezogenen Daten übermittelt werden), auf der EU-US-DPF-Liste aktuell aufgeführt ist. Diese Liste ist abrufbar unter https://www.dataprivacyframework.gov/s/.

[30] S. EWG (9) und Annex IV FN 2 des Angemessenheitsbeschlusses zum EU-US DPF, hier nur Darstellung im Überblick: Die FTC weist darauf hin, dass sie nicht befugt sei, strafrechtliche Maßnahmen zu erlassen oder in Angelegenheiten der nationalen Sicherheit zu entscheiden, und die meisten anderen hoheitlichen Maßnahmen zudem außerhalb ihrer Zuständigkeit liegen würden. Ausnahmen der Zuständigkeit bestünden zudem im wirtschaftlichen Bereich, die den Bankensektor, den Luftverkehr, das Versicherungsgewerbe und die Betreiber öffentlicher Telekommunikationsnetze betreffen. Außerdem bestehe keine oder nur eine eingeschränkte Zuständigkeit gegenüber „Non profit"-Organisationen. In manchen Fällen überschnitten sich die Kompetenzen der FTC mit denen anderer Strafverfolgungsbehörden.

[31] S. EWG (9) und Annex V, S. 1 ff. des Angemessenheitsbeschlusses zum EU-US DPF.

1.2. Welche Übermittlungen sind erfasst?

Auf Grundlage des EU-US DPF können nahezu alle Übermittlungen personenbezogener Daten aus der EU sowie dem EWR[32] an US-Organisationen, die aufgrund ihrer Zertifizierung zum EU-US DPF in der EU-US-DPF-Liste gelistet sind, erfolgen.[33]

Allerdings sind keine Datenübermittlungen von Stellen außerhalb der EU (EWR), welche der DS-GVO gem. Art. 3 Abs. 2 DS-GVO unterfallen, an Organisationen in den USA, welche in der EU-US-DPF-Liste, aufgelistet sind, vom Angemessenheitsbeschluss umfasst.[34]

Zudem gilt eine „**journalistische Ausnahme**" für Daten im Zusammenhang mit journalistischer Aktivität und Medienarchiven. Diese Daten können daher nicht auf Grundlage des EU-US DPF übermittelt werden.[35]

Bei Beschäftigtendaten („Human resources data" – HR-Daten), welche im Beschäftigungskontext übermittelt werden, muss geprüft werden, ob die Zertifizierung sich tatsächlich auch auf diese Daten bezieht,[36] da die Zertifizierung diese nicht zwingend erfasst.

Hinweis für Datenexporteure:

Beschäftigtendaten sind nur erfasst, wenn der Eintrag des Datenimporteurs in der EU-US-DPF-Liste (https://www.dataprivacyframework.gov/s/participant-search) in der Rubrik „Covered Data" den Eintrag „HR Data" enthält.

[32] S. EWG (7) FN 14 des Angemessenheitsbeschlusses zum EU-US DPF.
[33] S. EWG (10) des Angemessenheitsbeschlusses zum EU-US DPF.
[34] S. FN 5, Information note des EDSA, abrufbar unter: https://edpb.europa.eu/system/files/2023-07/edpb_informationnoteadequacydecisionus_en.pdf.
[35] S. EWG (10) und Annex I, Section III.2. des Angemessenheitsbeschlusses zum EU-US DPF.
[36] S. bspw. EWG (67), Annex I, Section III.6.b.viii, 9.d.ii des Angemessenheitsbeschlusses zum EU-US DPF. Nach dem Verständnis der US-Seite sind davon allerdings nur personenbezogene Daten der Beschäftigten der zertifizierten Organisation erfasst (https://www.dataprivacyframework.gov/s/article/How-to-Join-the-Data-Privacy-Framework-DPF-Program-part-2-dpf).

1.3. Ab welchem Zeitpunkt können die Übermittlungen erfolgen?

Auf Grundlage des EU-US DPF können personenbezogene Daten ab dem Zeitpunkt, zu welchem die Organisation auf der EU-US-DPF-Liste gelistet wird, übermittelt werden.[37]

1.4. Was gilt für noch bestehende Zertifizierungen zum EU-US Privacy Shield?

Mit dem sog. „Schrems II"-Urteil[38] hat der EuGH den Angemessenheitsbeschluss zum „Privacy Shield" für unwirksam erklärt. Ab diesem Zeitpunkt konnten daher keine Datenübermittlungen mehr auf Grundlage dieses Übermittlungsinstrumentes erfolgen.

Für US-Organisationen mit noch bestehenden Selbstzertifizierungen zum „Privacy Shield" besteht ein Aktualisierungserfordernis im Hinblick auf das nunmehr geltende EU-US DPF. Die Aktualisierung muss innerhalb von drei Monaten nach In-Kraft-Treten des Angemessenheitsbeschlusses umgesetzt sein. Die Frist der jährlichen Re-Zertifizierung, welche für bereits unter dem „Privacy Shield" zertifizierte Organisationen unverändert weitergilt, wird hierdurch nicht verlängert.[39]

Um sicherzustellen, dass es sich um eine aktuelle Zertifizierung handelt, muss – wie oben beschrieben – die Auflistung der betreffenden US-Organisation in der EU-US-DPF-Liste überprüft werden.

2. Wesentliche inhaltliche Vorgaben des EU-US DPF

2.1. Die datenschutzrechtlichen Vorgaben des EU-US DPF für zertifizierte Datenimporteure in den USA

Mit der Selbstzertifizierung unter den EU-US DPF unterwerfen sich Datenimporteure in den USA einem datenschutzrechtlichen Regelungsregime, das inhaltliche Nähe zur DS-GVO aufweist und sich nur geringfügig von den entsprechenden Vorgaben in den vorangegangenen Angemessenheitsbeschlüssen für die USA (Privacy Shield Principles und Safe Harbor Principles) unterscheidet. Die sogenannten **EU-US DPF Principles** sind als Annex I dem Angemessenheitsbeschluss der Europäischen Kommission beigefügt.

---

[37] S. EWG (49) und Artikel 1 sowie und Annex I, Section I.3 des Angemessenheitsbeschlusses zum EU-US DPF.

[38] EuGH, Urt. v. 16. Juli 2020, Rs. C-311/18 (sog. Schrems II).

[39] S. Annex I., Section III.6.d und e des Angemessenheitsbeschlusses zum EU-US DPF, s. Website zum Data Privacy Framework, abrufbar unter: https://www.dataprivacyframework.gov/s/article/FAQs-EU-U-S-Data-Privacy-Framework-EU-U-S-DPF-dpf, insb. Q 3.

Dort werden zunächst die Begriffe „personenbezogenes Datum“, „besondere Kategorien personenbezogener Daten“, „Verarbeitung“, „Verantwortlicher“ und „Auftragsverarbeiter“ in einer der DS-GVO entsprechenden Weise definiert.

In Bezug auf den Grundsatz der Rechtmäßigkeit der Verarbeitung (Art. 5 Abs. 1 lit. a DS-GVO) sehen die DPF Principles anstelle des in Art. 6 DS-GVO geregelten Verbots mit Erlaubnisvorbehalt mit enumerativ aufgezählten Rechtsgrundlagen einen sogenannten „N**otice and choice“-Mechanismus** vor. Weiterübermittlungen an Dritte und Zweckänderungen sind danach nur zulässig, wenn der Importeur die betroffenen Personen unter anderem über die Kategorien der erhobenen Daten, die Zwecke für die sie erhoben werden sowie die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten informiert („notice“) und eine Opt-out-Möglichkeit („choice“) anbietet.[40] Der **Transparenzgrundsatz** wird außer durch die Informationspflichten des „Choice“-Mechanismus auch dadurch umgesetzt, dass der Datenimporteur Informationen zur Umsetzung und Implementierung seiner datenschutzrechtlichen Pflichten, z. B. in Form von Datenschutzrichtlinien, sowie zum EU-US DPF veröffentlichen und allen betroffenen Mitarbeitenden zur Verfügung stellen muss.[41]

Der **Grundsatz der Zweckbindung** besagt, dass der Verantwortliche bei der Erhebung einen oder mehrere Zwecke, für den bzw. die die Daten erhoben werden, festlegt und jede weitere Verwendung der Daten nur zulässig ist, wenn sie mit dem ursprünglichen Erhebungszweck nicht unvereinbar ist.[42] Für die Frage der Vereinbarkeit soll es auf die Erwartungen einer vernünftigen Person im Kontext der jeweiligen Datenerhebung ankommen.[43]

Personenbezogene Daten müssen richtig und vollständig verarbeitet werden. Umfang und Dauer der Verarbeitung müssen dem Zweck angemessen, hierfür erheblich sowie auf das für die Zwecke der Verarbeitung erforderliche Maß beschränkt sein (**Grundsätze der Datenminimierung, Speicherbegrenzung, Richtigkeit und Erforderlichkeit**).[44]

---

[40] Annex I, Section II.1 und II.2 des Angemessenheitsbeschlusses zum EU-US DPF.
[41] S. EWG (25) bis (28) des Angemessenheitsbeschlusses zum EU-US DPF.
[42] S. Annex I, Section II.5.a sowie EWG (13) des Angemessenheitsbeschlusses zum EU-US DPF.
[43] S. FN. 6 zu Annex I, Section II.5.a des Angemessenheitsbeschlusses zum EU-US DPF.
[44] S. Annex I, Section II.5.a und b sowie EWG (20), (21) und (22) des Angemessenheitsbeschlusses zum EU-US DPF.

Für die **Verarbeitung besonderer Kategorien personenbezogener Daten** bedarf es einer ausdrücklichen Einwilligung der betroffenen Person („opt-in“), wenn eine Zweckänderung vorliegt oder die Daten an einen Dritten weiterübermittelt werden.[45]

Weiterübermittlungen der personenbezogenen Daten durch den Importeur in den USA an eine dritte Stelle (Verantwortlicher oder Auftragsverarbeiter) in den USA, ein anderes Drittland oder die EU sind nur zulässig, wenn der Importeur durch einen Vertrag mit dem Dritten sicherstellt, dass die personenbezogenen Daten dort denselben Schutz genießen wie beim Importeur.[46]

Zudem muss der Importeur geeignete und angemessene technische und organisatorische Maßnahmen ergreifen, um die personenbezogenen Daten vor Verlust, Missbrauch, unberechtigtem Zugang, Offenlegung, Veränderung oder Löschung zu schützen (**Sicherheitsgrundsatz**).[47]

Ab dem Zeitpunkt der Selbstzertifizierung ist der Importeur dafür verantwortlich, dass seine Datenschutzrichtlinien den Vorgaben des EU-US DPF genügen und auch tatsächlich umgesetzt werden. Dazu sind Schulungen der Mitarbeitenden sowie regelmäßige Audits durch interne oder externe Stellen vorzusehen. Durch eine ausreichende Dokumentation muss der Importeur in der Lage sein, jederzeit die Einhaltung seiner datenschutzrechtlichen Pflicht nachweisen zu können (**Rechenschaftspflicht**).[48]

Die gegenüber Verantwortlichen und Auftragsverarbeitern vorgesehenen **Betroffenenrechte** umfassen ein Recht auf Berichtigung oder Ergänzung unrichtiger oder unvollständiger personenbezogener Daten, ein Recht auf Löschung rechtswidrig verarbeiteter Daten sowie ein Auskunftsrecht. Letzteres steht unter dem Vorbehalt, dass Aufwand und Kosten für seine Erfüllung beim Verantwortlichen oder Auftragsverarbeiter nicht außer Verhältnis zu den im jeweiligen Einzelfall berührten Risiken für die Privatsphäre der betroffenen Person stehen dürfen. Zudem kann die Erteilung der Auskunft stets von der Zahlung einer angemessenen, nicht übermäßig hohen Gebühr abhängig gemacht werden. Die drohende Offenbarung von Betriebs- und Geschäftsgeheimnissen oder entgegenstehende überwiegende öffentliche Interessen oder

[45] S. Annex I, Section II.2.c des Angemessenheitsbeschlusses zum EU-US DPF.
[46] S. EWG (37) bis (43) des Angemessenheitsbeschlusses zum EU-US DPF.
[47] S. Annex I, Section II.4.a sowie EWG (23) und (24) des Angemessenheitsbeschlusses zum EU-US DPF.
[48] S. EWG (44) bis (46) des Angemessenheitsbeschlusses zum EU-US DPF.

berechtigte Interessen Dritter können dazu berechtigen, einen Auskunftsanspruch abzulehnen.[49]

Hinweis für Datenexporteure:

Die im EU-US DPF geregelten Rechte betroffener Personen und Pflichten zertifizierter Stellen in den USA lassen weitergehende Rechte und Pflichten aus einer direkten Anwendbarkeit der DS-GVO auf Stellen in den USA gemäß Art. 3 Abs. 2 DS-GVO (Marktortprinzip) ebenso unberührt wie alle datenschutzrechtlichen Pflichten – einschließlich der Erfüllung von Betroffenenrechten –, denen der in die jeweilige Datenübermittlung an die USA eingebundene Datenexporteur in der EU als Verantwortlicher, gemeinsam Verantwortlicher oder Auftragsverarbeiter nach der DS-GVO unterliegt.

2.2. Vorgaben zum Zugriff auf personenbezogene Daten durch öffentliche Stellen der USA

Im Angemessenheitsbeschluss werden die gesetzlichen Grundlagen, Grenzen und Schutzmechanismen wiedergegeben, die für die **Erhebung und Nutzung personenbezogener Daten** durch öffentliche Stellen der USA **zu Strafverfolgungszwecken** oder **aus Gründen der nationalen Sicherheit** gelten.

In aller Regel erfordern danach Zugriffe **zu Strafverfolgungszwecken** eine gerichtliche Anordnung, die hinreichende Verdachtsgründe im Einzelfall voraussetzt und den Umfang der zu erhebenden personenbezogenen Daten auf das für die Zwecke der Strafverfolgung erforderliche Maß begrenzt.[50]

Die Strafverfolgungsbehörden müssen danach sicherstellen, dass die von ihnen erhobenen und gespeicherten Daten richtig, relevant, aktuell und vollständig sind, und diese durch geeignete technische und organisatorische Maßnahmen vor unberechtigtem Zugriff durch Dritte oder Verlust schützen. Außerdem sind geeignete Löschungsfristen, Datenschutzschulungen und regelmäßige Audits vorzusehen. Eine

[49] S. Annex I, Section II.6.a und Section III.8 sowie EWG (29) bis (36) des Angemessenheitsbeschlusses zum EU-US DPF.

[50] S. EWG (92), (93) und (96) des Angemessenheitsbeschlusses zum EU-US DPF.

Übermittlung der personenbezogenen Daten an andere öffentliche Stellen setzt voraus, dass diese sie für die Erfüllung der ihnen zugewiesenen Aufgaben benötigen, z. B. zum Schutz der Sicherheit oder des Eigentums von Personen, um Straftaten zu verhindern oder aufzuklären oder zum Schutz der nationalen Sicherheit.[51]

Begrenzungen und Schutzmechanismen, die die dafür zuständigen öffentlichen Stellen der USA beim **Zugriff** auf personenbezogene Daten **aus Gründen der nationalen Sicherheit** beachten müssen, sieht ein einschlägiges Dekret, US Executive Order 14086,[52] vor. Die dort geregelten Vorgaben sind für diese öffentlichen Stellen der USA rechtlich bindend und für betroffene Personen aus einem sogenannten qualifizierten Land – wozu nach der am 30.06.2023 erfolgten Anerkennung durch die USA auch alle EU- und EWR-Mitgliedstaaten zählen[53] – unter den in der Executive Order 14086 festgelegten Voraussetzungen einklagbar.[54] Sie gelten sowohl für die Erhebung personenbezogener Daten in den USA – z. B. auf Grundlage von Section 702 des Foreign Intelligence Surveillance Act (FISA) – als auch für den Zugriff auf Daten außerhalb der USA, z. B. für einen Zugriff auf Daten im Transit auf der Grundlage der Executive Order 12333, und ergänzen die nach anderen gesetzlichen Regelungen bestehenden Beschränkungen und Garantien, ohne diese zu verdrängen; zur Anwendung kommt demnach stets die datenschutzfreundlichste Regelung.[55]

Die Executive Order 14086 enthält einen **Katalog erlaubter** (u. a. Schutz der nationalen Sicherheit der USA, ihrer Verbündeten und Partner, Abwehr von Spionage, Sabotage und anderen geheimdienstlichen Aktivitäten fremder Mächte, Schutz freier Wahlen und des politischen Willensbildungsprozesses sowie der Infrastruktur und des öffentlichen Eigentums der USA) **und** einen Katalog **verbotener Ziele und Zwecke** für die Verarbeitung personenbezogener Daten durch **Nachrichtendienste** der USA. Zu den verbotenen Zielen und Zwecken zählen beispielsweise die Unterdrückung der freien

---

[51] S. EWG (101) bis (106) des Angemessenheitsbeschlusses zum EU-US DPF.

[52] Executive Order 14086 vom 7. Oktober 2022: Enhancing Safeguards for United States Signals Intelligence Activities, abrufbar unter: https://www.federalregister.gov/documents/2022/10/14/2022-22531/enhancing-safeguards-for-united-states-signals-intelligence-activities.

[53] S. Executive Order 14086, section 3.(f) sowie Statement from US Secretary of Commerce Gina Raimondo on the European Union-US Data Privacy Framework | US Department of Commerce vom 3. Juli 2023 (abrufbar unter: https://www.commerce.gov/news/press-releases/2023/07/statement-us-secretary-commerce-gina-raimondo-european-union-us-data) wonach die Anerkennung mit der Verabschiedung des Angemessenheitsbeschlusses wirksam geworden ist.

[54] S. Executive Order 14086, section 3.(a) sowie 4.(d) und (k).

[55] S. Executive Order 14086, section 5.(c).

Meinungsäußerung und der Verbreitung unerwünschter politischer Ansichten durch Individuen und die Presse, die Unterdrückung der Verfolgung berechtigter privater Belange sowie die Ausforschung von Betriebs- und Geschäftsgeheimnissen des nicht öffentlichen Sektors von Drittländern zur Stärkung der US-Wirtschaft.[56]

Des Weiteren schreibt das Dekret vor, dass nachrichtendienstliche Aktivitäten den Grundsätzen der **Erforderlichkeit** und der **Verhältnismäßigkeit** genügen müssen. Erforderlich ist eine Datenerhebung nach der Executive Order 14086 dann, wenn sie bei vernünftiger Betrachtung unter Berücksichtigung aller Umstände des Einzelfalls notwendig ist, um ein festgelegtes Aufklärungsinteresse („validated intelligence priority“) zu fördern.[57] Dem Grundsatz der **Verhältnismäßigkeit** entsprechen Aufklärungsaktivitäten der Geheimdienste nach der Executive Order 14086, wenn sie nach Umfang, Art und Dauer verhältnismäßig für das verfolgte Aufklärungsinteresse sind, wobei ein angemessener Ausgleich zwischen dem Aufklärungsinteresse und den Rechten und Freiheiten aller betroffenen Personen, unabhängig von ihrer Nationalität oder ihrem Wohnsitz, gefunden werden soll.[58] Mit weniger Eingriffen in die Privatsphäre verbundene Erhebungen sollen – soweit solche verfügbar sind und dies möglich und angemessen ist – vorrangig eingesetzt werden.[59]

Eine massenhafte Sammlung von Daten (sogenannte „**bulk collection“**) ist grundsätzlich nur zulässig, wenn der verfolgte Zweck im Einzelfall durch gezielte Erhebungen nicht erreicht werden kann. Dabei gesammelte Daten sollen, sobald es möglich ist, auf das für die Erreichung des verfolgten Zwecks (z. B. Terrorabwehr) erforderliche Maß reduziert werden, insbesondere, indem die hierfür nicht relevanten Daten baldmöglichst gelöscht werden.[60] Es bestehen Ausnahmen für Fälle, in denen „bulk collection“ als vorbereitende Maßnahme für gezielte Erhebungen eingesetzt wird.[61]

Das Dekret enthält zudem Vorgaben für die **Weiterübermittlung** personenbezogener Daten an andere Stellen, die **Speicherdauer**, technische und organisatorische Maßnahmen zum Schutz vor Verlust oder unberechtigtem Zugriff durch Dritte, die

[56] S. Executive Order 14086, section 2.(b).
[57] S. Executive Order 14086, section 2.(a).(ii).(A).
[58] S. Executive Order 14086, section 2.(a).(ii).(B).
[59] S. Executive Order 14086, section 2.(c).(i).(A).
[60] S. Executive Order 14086, section 2.(c).(ii).
[61] S. Executive Order 14086, section 2.(c).(ii).(D).

Datenqualität sowie die Anpassung und Veröffentlichung von Richtlinien der jeweiligen verantwortlichen Stelle zum Umgang mit personenbezogenen Daten.[62]

3. Überwachung zertifizierter Stellen in den USA

Die Möglichkeit einer Zertifizierung unter das EU-US DPF besteht nur für Organisationen, die den Ermittlungs- und Durchsetzungsbefugnissen der FTC oder des DOT unterliegen.

3.1. Rechtsrahmen

Der FTC Act (15 U.S.C. § 45) verbietet **„unfaire" oder „irreführende" Handlungen oder Praktiken** mit Bezug auf den Handel. Das Verbraucherschutzmandat des FTC beinhaltet die Durchsetzung von Gesetzen zum Schutz der Privatsphäre und der Sicherheit von Verbraucherinnen und Verbrauchern und deren Daten.

Das im FTC Act enthaltene Verbot unlauterer oder irreführender Handlungen oder Praktiken umfasst auch solche Praktiken, die in den USA einen vernünftigerweise vorhersehbaren Schaden verursachen oder wahrscheinlich verursachen werden oder ein wesentliches Verhalten in den USA beinhalten.[63] Die FTC kann, um ausländische Verbraucherinnen und Verbraucher zu schützen, alle Rechtsmittel einsetzen, die zum Schutz inländischer Verbraucherinnen und Verbraucher zur Verfügung stehen.[64]

Die Befugnis des DOT und dessen Office of Aviation Consumer Protection (OACP – Amt für Verbraucherschutz in der Luftfahrt) aus 49 U.S.C. 41712 richtet sich gegen unlautere oder irreführende Praktiken eines Luftfahrtunternehmens oder eines Flugscheinvermittlers. Abschnitt 41712 ist nach dem Vorbild von Abschnitt 5 des FTC Act (15 U.S.C. 45) gestaltet und wird auch angewandt, wenn Teilnehmer am EU-US DPF dessen Grundsätze nicht einhalten.[65]

Im **Durchsetzungsverfahren** ist ein DOT Administrative Law Judge („ALJ") befugt, Unterlassungsanordnungen und Geldstrafen zu verhängen. Verstöße gegen Abschnitt 41712 können zu Unterlassungsanordnungen und der Verhängung von Geldstrafen in

---

[62] S. Executive Order 14086, section 2.(c).(iii) und (iv). Die überarbeiteten Richtlinien sind abrufbar unter: https://www.intel.gov/ic-on-the-record-database/results/oversight/1278-odni-releases-ic-procedures-implementing-new-safeguards-in-executive-order-14086.

[63] Annex IV, Section I.b. des Angemessenheitsbeschlusses zum EU-US DPF.

[64] Annex IV, Section I.b. des Angemessenheitsbeschlusses zum EU-US DPF.

[65] Annex V, Section 1.A des Angemessenheitsbeschlusses zum EU-US DPF.

Höhe von bis zu 37.377 Dollar für jeden Verstoß gegen Abschnitt 41712 führen.[66] Das DOT ist **nicht befugt, einzelnen Beschwerdeführern Schadenersatz** zu gewähren oder sie finanziell zu entlasten. Das DOT ist jedoch befugt, Vergleiche zu genehmigen, die den Verbraucherinnen und Verbrauchern direkt zugutekommen (z. B. Bargeld, Gutscheine).[67]

Für Weiterleitungen von Beschwerden betroffener Personen durch Datenschutzaufsichtsbehörden der EU-Mitgliedstaaten hat die FTC ein **standardisiertes Verweisungsverfahren** geschaffen und den EU-Mitgliedstaaten Leitlinien zu der Art von Informationen mitgeteilt, die die FTC bei ihrer Untersuchung benötigt. Die FTC hat eine Kontaktstelle für Verweisungen aus den EU-Mitgliedstaaten benannt.[68]

Die FTC kann nach einer Verweisung eine Reihe von **Maßnahmen** ergreifen, um die angesprochenen Probleme zu lösen, zum Beispiel die Datenschutzrichtlinien der Organisation überprüfen, weitere **Informationen** direkt von der Organisation oder von Dritten einholen, bei der verweisenden Stelle Informationen einholen, prüfen, ob es **weitere gleichartige Verstöße** oder eine **erhebliche Anzahl von betroffenen Verbraucherinnen und Verbrauchern** gibt und gegebenenfalls ein **Durchsetzungsverfahren** einleiten.[69]

Die FTC will weiterhin erhebliche Verstöße gegen die EU-US-DPF-Grundsätze auf eigene Initiative untersuchen und dabei eine Reihe von Instrumenten einsetzen.[70]

Hinweis für betroffene Personen:

Um mittelbar eine Untersuchung beim OACP des DOT oder der FTC auszulösen, kann eine entsprechende Beschwerde bei der Datenschutzaufsichtsbehörde in der EU/im EWR eingereicht werden. Das Recht zur unmittelbaren Beschwerde direkt in den USA (siehe III.1) bleibt erhalten und kann im Einzelfall zur Beschleunigung des Verfahrens hilfreich sein.

[66] Annex V, Section II.B des Angemessenheitsbeschlusses zum EU-US DPF.
[67] Annex V, Section II.B des Angemessenheitsbeschlusses zum EU-US DPF.
[68] Annex IV, Section II des Angemessenheitsbeschlusses zum EU-US DPF.
[69] Annex IV, Section II des Angemessenheitsbeschlusses zum EU-US DPF.
[70] Annex IV, Section II des Angemessenheitsbeschlusses zum EU-US DPF.

3.2. Rechtsdurchsetzung und Überwachung

Die FTC kann Vollstreckungsanordnungen erwirken und überwachen, um die Einhaltung der EU-US-DPF-Grundsätze zu gewährleisten. Verstöße gegen die Verwaltungsanordnungen der FTC können Geldstrafen in Höhe von bis zu 50.120 Dollar pro Verstoß bzw. 50.120 Dollar pro Tag bei fortgesetztem Verstoß nach sich ziehen.[71] Das kann im Falle von Praktiken, die viele Verbraucherinnen und Verbraucher betreffen, zu Geldstrafen in Höhe von mehreren Millionen Dollar führen. Die FTC wird diese Anordnungen auf ihrer Website den Unternehmen zugeordnet auflisten.[72]

Das OACP des DOT wird insbesondere, wenn eine Anordnung erlassen wurde, die eine Fluggesellschaft oder einen Flugscheinvermittler anweist, künftige Verstöße gegen die EU-US-DPF-Grundsätze und Section 41712 zu unterlassen, die Einhaltung der Anordnung überwachen. Das DOT wird diese Anordnungen auf ihrer Website verfügbar machen.[73]

Die FTC ist in der Vergangenheit wiederholt zur Durchsetzung der datenschutzrechtlichen Vorgaben der vorangegangenen Angemessenheitsentscheidungen für die USA (EU-US Privacy Shield und Safe Harbor) tätig geworden[74] und hat in diesem Zusammenhang Strafzahlungen in beträchtlicher Höhe verhängt.[75] Viele frühere Fälle der Durchsetzung von Safe Harbor sowie des EU-US Privacy Shields betrafen Probleme mit der Selbstzertifizierung.[76] Das DOC wird den Selbstzertifizierungsprozess verwalten und überwachen, sowie die EU-US-DPF-Liste führen.

3.3. Zusammenarbeit mit Europäischen Datenschutzaufsichtsbehörden

Die FTC und das DOT werden mit den Europäischen Datenschutzaufsichtsbehörden koordiniert zusammenarbeiten. Das beinhaltet Informationen an die Europäischen Datenschutzaufsichtsbehörden über den Stand der Beschwerden und wenn möglich, eine Bewertung der verwiesenen Fälle, einschließlich einer Beschreibung der wichtigsten aufgeworfenen Fragen und etwaiger Maßnahmen zur Behebung von Rechtsverstößen sowie deren Wirksamkeit im Zuständigkeitsbereich der FTC.

---

[71] 15 U.S.C. § 45(m); 16 C.F.R. § 1.98.
[72] Annex IV, Section III des Angemessenheitsbeschlusses zum EU-US DPF.
[73] Annex V, Section II.C des Angemessenheitsbeschlusses zum EU-US DPF.
[74] Appendix A - Privacy Shield and Safe Harbor Enforcement des Angemessenheitsbeschlusses zum EU-US DPF.
[75] Appendix A - Privacy Shield and Safe Harbor Enforcement des Angemessenheitsbeschlusses zum EU-US DPF.
[76] Annex IV, Section I.c des Angemessenheitsbeschlusses zum EU-US DPF.

III. Informationen für betroffene Personen zu Rechtsschutzmöglichkeiten

Die **Schaffung unabhängiger und unparteiischer Rechtsbehelfsmechanismen** zur Überprüfung etwaiger Zugriffe nationaler Sicherheitsbehörden der USA war elementare Voraussetzung für das Zustandekommen eines neuen Angemessenheitsbeschlusses (siehe dazu unter III.3).

1. Rechtsschutz im Rahmen des EU-US DPF gegenüber zertifizierten Organisationen

Zertifizierte Organisationen müssen wirksame und leicht zugängliche unabhängige Rechtsbehelfsmechanismen vorsehen, mit denen die Beschwerden und Streitigkeiten von Personen für diese kostenlos untersucht und zügig gelöst werden können. Die Rechtsbehelfsmechanismen können entweder in den USA oder in der EU bereitgestellt werden, wobei der letztere Fall auch die Möglichkeit umfasst, sich freiwillig zur Zusammenarbeit mit den EU-Datenschutzaufsichtsbehörden zu verpflichten.

Das EU-US DPF hält für betroffene Personen verschiedene Möglichkeiten bereit, wirksamen Rechtsschutz zu erlangen.

Zum einen können betroffene Personen Beschwerde

- direkt bei der betreffenden zertifizierten Organisation,
- bei einer von der zertifizierten Organisation benannten unabhängigen Beschwerdestelle,
- bei den Datenschutzaufsichtsbehörden in der EU,
- beim DOC oder
- bei der FTC

einreichen.

Sofern der Beschwerde nicht durch einen dieser Rechtsbehelfsmechanismen abgeholfen werden konnte, können die betroffenen Personen zum anderen ein verbindliches Schiedsverfahren anstrengen. Die betroffenen Personen können einen oder alle genannten Rechtsbehelfe in Anspruch nehmen; nur das Schiedsverfahren setzt voraus, dass vor der Durchführung bestimmte Rechtsmittel ausgeschöpft sein müssen. Die Rechtsbehelfe stehen dabei in keinem Alternativverhältnis, es muss auch keine bestimmte Reihenfolge eingehalten werden.

Über die zur Verfügung stehenden Rechtsbehelfe informiert die Website des DoC unter https://www.dataprivacyframework.gov/s/participant-search im Eintrag für die jeweilige Organisation unter der Rubrik „Questions or Complaints“.

Im Einzelnen:

a) Beschwerde direkt bei der zertifizierten Organisation

Für die Bearbeitung solcher Beschwerden muss die **zertifizierte Organisation** einen entsprechenden **wirksamen Rechtsbehelfsmechanismus einrichten und über diesen sowie über die benannte unabhängige Beschwerdestelle (vgl. b)) in ihrer Datenschutzrichtlinie informieren**. Eine Beschwerde muss binnen 45 Tagen nach ihrem Eingang gegenüber der betroffenen Person beantwortet werden.

b) Beschwerde bei einer von der zertifizierten Organisation benannten unabhängigen Beschwerdestelle

Die von der zertifizierten Organisation benannte **Beschwerdestelle** kann sich **in der EU/dem EWR oder den USA** befinden und bietet den betroffenen Personen angemessenen und kostenlosen Rechtsschutz. Sie muss auf ihrer Webseite die einschlägigen Informationen zum EU-US DPF sowie zu den von ihr in diesem Zusammenhang angebotenen Diensten zur Verfügung stellen. Sofern die zertifizierte Organisation der Entscheidung der Beschwerdestelle nicht nachkommt, muss die Beschwerdestelle dies melden. Eine solche Weigerung bzw. ein häufiger Verstoß gegen Datenschutzgrundsätze kann letztlich dazu führen, dass die zertifizierte Organisation durch das DOC von der EU-US-DPF-Liste (vgl. II.1.) gestrichen wird.

c) Beschwerde bei einer nationalen Datenschutzaufsichtsbehörde in der EU/im EWR

Betroffene Personen können Beschwerden auch bei einer **nationalen Datenschutzaufsichtsbehörde** in der EU bzw. im EWR einreichen, die von ihren Ermittlungs- und Abhilfebefugnissen gemäß der DS-GVO Gebrauch machen kann. Die zertifizierten Organisationen sind **verpflichtet**, bei der Untersuchung und Lösung einer Beschwerde durch eine Datenschutzaufsichtsbehörde **mitzuwirken**, wenn es sich um die Verarbeitung von Personaldaten handelt, die im Rahmen eines **Beschäftigungsverhältnisses** erhoben werden, oder wenn sich die betreffende Organisation **freiwillig der Aufsicht der Datenschutzaufsichtsbehörden unterworfen** hat. Die Feststellungen und Empfehlungen der Datenschutzaufsichtsbehörden erfolgen durch ein informelles Gremium auf EU-Ebene („DPA Panel“), das unter anderem einen einheitlichen Ansatz

beim Umgang mit Beschwerden gewährleisten soll. Kommt die Organisation den erteilten Empfehlungen nicht zeitnah nach, leitet das DPA Panel den Fall entweder an das DOC weiter, das die Organisation von der EU-US-DPF-Liste streichen kann, oder für Vollstreckungsmaßnahmen etwa an die FTC. Zu diesem Zweck richten das DOC sowie die FTC jeweils eine **Kontaktstelle** für die Zusammenarbeit mit den nationalen Datenschutzaufsichtsbehörden in der EU/im EWR ein.

Falls die Datenschutzaufsichtsbehörde nicht oder nur unzureichend tätig wird, kann die betroffene Person dagegen **vor den nationalen Gerichten** des betreffenden EU-Mitgliedstaats vorgehen.

Betroffene Personen können sich sogar dann an eine nationale Datenschutzaufsichtsbehörde wenden, wenn das DPA Panel nicht von der zertifizierten Organisation als Beschwerdestelle benannt wurde. In diesem Fall wird die nationale Datenschutzaufsichtsbehörde die Beschwerde an das DOC oder die FTC weiterleiten.

d) Beschwerde beim DOC

Das **DOC hat sich verpflichtet, Beschwerden** über die Nichteinhaltung der Grundsätze des EU-US DPF seitens einer zertifizierten Organisation **entgegenzunehmen, zu prüfen und sich nach besten Kräften um eine Lösung zu bemühen**. Dazu nimmt die eingerichtete **Kontaktstelle** (vgl. c)) direkt Kontakt mit der betreffenden Datenschutzaufsichtsbehörde auf und informiert diese spätestens 90 Tage nach Befassung über den Stand der Beschwerde. So wird es betroffenen Personen ermöglicht, Beschwerden direkt an ihre nationale Datenschutzaufsichtsbehörde zu richten und sie an das DOC als der US-Behörde, die das EU-US DPF verwaltet, weiterleiten zu lassen. Das DOC kann die Nichteinhaltung der Datenschutzgrundsätze mit Streichung von der EU-US-DPF-Liste sanktionieren.

e) Beschwerde bei der FTC

Eine zertifizierte Organisation muss der **aufsichtlichen Zuständigkeit der US-Behörden unterliegen**, insbesondere der der FTC, die die erforderlichen Ermittlungs- und Durchsetzungsbefugnisse haben, um die Einhaltung der Grundsätze des EU-US DPF durchzusetzen. Die **FTC prüft in erster Linie Hinweise auf Nichteinhaltung der Grundsätze des EU-US DPF**, die sie von unabhängigen Beschwerdestellen, dem DOC oder Datenschutzaufsichtsbehörden erhalten hat. Die FTC hat sich verpflichtet, ein standardisiertes **Verweisungsverfahren sowie eine Kontaktstelle** für die Weiterleitung von Beschwerden durch Datenschutzaufsichtsbehörden (vgl. c)) zu schaffen und

Informationen über eine Befassung auszutauschen. Zudem nimmt die FTC **auch direkt Beschwerden von betroffenen Personen an** und führt eigeninitiativ Untersuchungen zum EU-US DPF durch.

f) Beschwerde beim EU-US-DPF-Schiedsgericht

Falls keines der vorstehenden Rechtsmittel der Beschwerde für die betroffene Person zufriedenstellend abgeholfen hat, kann diese ein **verbindliches Schiedsverfahren beim EU-US-DPF-Schiedsgericht als letzter Beschwerdestelle** anstrengen. Auf diese Möglichkeit muss die zertifizierte Organisation die betroffene Person hinweisen. Das Schiedsgericht setzt sich aus einem Pool von mindestens zehn Schiedsrichtern zusammen, die vom DOC und der Europäischen Kommission benannt werden. Aus diesem Pool wählen die Parteien ein **Gremium aus einem oder drei Schiedsrichtern** aus. Das Schiedsgericht kann nicht monetäre billigkeitsrechtliche Maßnahmen verhängen, die erforderlich sind, um die Nichteinhaltung der Grundsätze des EU-US DPF zu beheben.

Ein Schiedsverfahren kann nicht in Anspruch genommen werden, wenn eine Datenschutzaufsichtsbehörde die rechtliche Befugnis hat, den Streit bezüglich der zertifizierten Organisation beizulegen, also in den Fällen, in denen die Organisation im Hinblick auf die Verarbeitung von Personaldaten, die im Rahmen eines Beschäftigungsverhältnisses erhoben werden, entweder zur Zusammenarbeit oder zur Befolgung der Ratschläge der Datenschutzaufsichtsbehörden verpflichtet ist oder sich hierzu freiwillig verpflichtet hat. Betroffene Personen können die Schiedsentscheidung vor den US-Gerichten gemäß dem Federal Arbitration Act durchsetzen.

g) Gerichtliche Rechtsbehelfe

Wenn eine zertifizierte Organisation die Grundsätze des EU-US DPF nicht einhält, bestehen **zusätzliche gerichtliche Rechtsbehelfe nach US-Recht**, einschließlich der Geltendmachung von Schadenersatz.[77]

2. Rechtsbehelfe im Rahmen des Zugriffs und der Nutzung personenbezogener Daten zu Strafverfolgungszwecken

Bezüglich des Eingriffs in das Recht auf Schutz der personenbezogenen Daten, die im Rahmen des EU-US DPF zu **Strafverfolgungszwecken** übermittelt werden, bietet das

[77] S. EWG (96) des Angemessenheitsbeschlusses zum EU-US DPF.

US-Recht nach den Feststellungen des Angemessenheitsbeschlusses **Rechtsbehelfsmechanismen,** die den betroffenen Personen die Möglichkeit geben, **vor einem unabhängigen und unparteiischen Gericht rechtliche Schritte einzuleiten**, um Zugang zu ihren personenbezogenen Daten zu erhalten oder die Berichtigung oder Löschung dieser Daten zu erwirken.[78] So können beispielsweise behördliche Vorladungen vor Gericht angefochten werden. Insbesondere der Freedom of Information Act[79] und der Electronic Communications Privacy Act[80] bieten betroffenen Personen, unabhängig von ihrer Nationalität, Rechtsbehelfe gegen eine Behörde oder ihre Beamten, wenn diese Behörden personenbezogene Daten verarbeiten.

3. Rechtsbehelfe im Rahmen des Zugriffs und der Nutzung personenbezogener Daten für Zwecke der nationalen Sicherheit

Auch hier bestehen für die betroffene Person verschiedene Möglichkeiten, rechtliche Schritte einzuleiten. Nach den Feststellungen des Angemessenheitsbeschlusses ermöglichen sie den betroffenen Personen zusammengenommen die Überprüfung der Rechtmäßigkeit des staatlichen Zugriffs sowie, falls ein Verstoß festgestellt wird, die Behebung dieses Verstoßes, einschließlich der Berichtigung oder Löschung ihrer personenbezogenen Daten.

Der neue **Rechtsbehelfsmechanismus gemäß Executive Order 14086** löst das bisherige System der Ombudsperson ab und ersetzt es durch ein zweistufiges Verfahren.

Nach Mitteilung der EU-Kommission gelten alle von der US-Regierung im Bereich der nationalen Sicherheit implementierten Schutzmaßnahmen – einschließlich der Rechtsbehelfe – unabhängig von den verwendeten Übermittlungsinstrumenten für alle Datenübermittlungen im Rahmen der Datenschutz-Grundverordnung an US-Unternehmen.[81]

---

[78] S. EWG (91) ff sowie EWG (114) des Angemessenheitsbeschlusses zum EU-US DPF.
[79] 5 United State Code, § 552.
[80] 18 United State Code, §§ 2701-2712.
[81] Vgl. Q&A der Europäischen Kommission, abrufbar unter https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_3752.

Im Einzelnen:

a) Beschwerde bezüglich US-Signalaufklärung vor dem CLPO

Jede Person in der EU/im EWR hat das Recht, Beschwerde wegen eines mutmaßlichen Verstoßes gegen US-amerikanisches Recht für Signalaufklärungsaktivitäten einzureichen.[82] Die Zulässigkeitsvoraussetzungen hierfür sind insgesamt gering, da beschwerdeführende Personen nicht nachweisen müssen, dass die eigenen Daten tatsächlich von US-Signalaufklärungsaktivitäten betroffen waren. Letztendlich müssen nur bestimmte Anhaltspunkte für eine Überprüfung geliefert werden.[83] Die Beschwerde wird **zunächst bei einer nationalen Datenschutzaufsichtsbehörde in der EU/im EWR eingelegt**, um einen niedrigschwelligen Zugang zum Rechtsbehelfsverfahren zu schaffen. Die **Datenschutzaufsichtsbehörde führt die Beschwerde dann dem Rechtsbehelfsmechanismus zu**. Erste Untersuchungen führt der **Civil Liberties Protection Officer of the Director of National Intelligence (CLPO)** durch. Dieser ist unter anderem dafür verantwortlich, die Einhaltung der geltenden bürgerlichen Freiheiten und Datenschutzanforderungen durch das Office of the Director of National Intelligence zu überwachen. Im Rahmen seiner Überprüfung hat der CLPO **weitreichende Zugriffsrechte auf Informationen** und darf von Nachrichtendiensten nicht bei seiner Arbeit behindert werden. Sofern der CLPO einen Verstoß gegen geltendes US-Recht feststellt, **entscheidet er – bindend für die Nachrichtendienste –** über entsprechende Abhilfe. Die betroffene Person erfährt über die betreffende Datenschutzaufsichtsbehörde in der EU/im EWR von der Entscheidung des CLPO, wonach entweder kein Verstoß festgestellt oder angemessene Abhilfe geleistet wurde. Durch diese standardisierte Mitteilung soll neben der Information der betroffenen Person auch die Vertraulichkeit der Geheimdienstmaßnahmen sichergestellt werden.

b) Berufung vor dem DPRC

Die Entscheidung des CLPO kann sowohl vom Beschwerdeführer als auch von der entsprechenden US-Behörde binnen 60 Tagen nach Erhalt der Entscheidung **vor dem Data Protection Review Court (DPRC) angefochten** werden. Betroffene Personen können diesen **Antrag wiederum über eine nationale Datenschutzaufsichtsbehörde in der EU** stellen. Der DPRC wird im Angemessenheitsbeschluss als **unabhängiges**

[82] Signalaufklärung ist eine Form der nachrichtendienstlichen Erkenntnisgewinnung, die elektronische Kommunikation und Daten aus Informationssystemen sammelt, vgl. EWG (123) des Angemessenheitsbeschlusses zum EU-US DPF.

[83] Vgl. EWG (178) sowie Fußnote 347 zu EWG (176) des Angemessenheitsbeschlusses zum EU-US DPF.

Gericht bezeichnet. Es handelt sich allerdings nicht um ein ordentliches Gericht, sondern um einen durch die Executive Order 14086 neu geschaffenen Spruchkörper bestehend aus mindestens sechs Richtern, die vom Attorney General in Absprache mit dem Privacy and Civil Liberties Oversight Board (PCLOB), dem Handelsminister und dem Director of National Intelligence für eine – verlängerbare – Amtszeit von vier Jahren ernannt werden.[84] Das PCLOB ist ein eigenständiges Gremium innerhalb der Exekutive, das aus einem überparteilichen, fünfköpfigen Vorstand besteht, der vom Präsidenten mit Zustimmung des Senats für eine feste Amtszeit von sechs Jahren ernannt wird. Dessen Aufgabe besteht darin, die Privatsphäre sowie die bürgerlichen Freiheiten im Bereich der Terrorismusbekämpfungspolitik zu schützen.[85] Die Anträge werden beim DPRC von einem **Gremium bestehend aus drei Richtern**, darunter ein Vorsitzender Richter, geprüft, das von einem **Sonderanwalt** unterstützt wird, der Zugang beispielsweise auch zu Verschlusssachen hat und die Interessen des/der Beschwerdeführenden vertritt.

Der DPRC beschließt schriftlich mit Stimmenmehrheit. Die **Entscheidung ist bindend**. Falls bei der Überprüfung ein Verstoß gegen die geltenden Vorschriften festgestellt wird, werden in der Entscheidung **geeignete Abhilfemaßnahmen** festgelegt. Dazu gehören die Löschung rechtswidrig erhobener Daten, die Löschung der Ergebnisse unangemessen durchgeführter Abfragen, die Beschränkung des Zugriffs auf rechtmäßig erhobene Daten auf entsprechend geschultes Personal oder der Rückruf von Geheimdienstberichten, die Daten enthalten, die ohne rechtmäßige Genehmigung erworben oder unrechtmäßig verbreitet wurden. Die betroffene Person erhält wiederum über die nationale Datenschutzaufsichtsbehörde in der EU/im EWR eine standardisierte Mitteilung über den Abschluss des Verfahrens, dass entweder kein Verstoß festgestellt oder eine Entscheidung mit geeigneten Abhilfemaßnahmen getroffen wurde.

c) Überprüfung des Rechtsbehelfsmechanismus

Die **Funktionsweise** des Rechtsbehelfsmechanismus wird **jährlich vom PCLOB überprüft**. So wird beispielsweise kontrolliert, ob CLPO und DPRC Beschwerden zeitnah bearbeitet haben, ob diese vollen Zugang zu den notwendigen Informationen erhalten haben und ob die US Intelligence Community (ein Zusammenschluss von 18 US-Nachrichtendiensten) den Bestimmungen von CLPO und DPRC vollständig

[84] S. EWG (185) des Angemessenheitsbeschlusses zum EU-US DPF.
[85] Vgl. https://www.pclob.gov/About/HistoryMission.

nachgekommen ist. Der **Prüfbericht** wird unter anderem dem Präsidenten sowie den Geheimdienstausschüssen im Kongress vorgelegt und wird auch in die **regelmäßige Überprüfung des Angemessenheitsbeschlusses durch die Europäische Kommission einfließen**. Zudem wird das PCLOB jährlich eine **öffentliche Zertifizierung** vornehmen, ob der Rechtsbehelfsmechanismus Beschwerden im Einklang mit den Anforderungen der Executive Order 14086 bearbeitet.

d) Verfahren vor ordentlichen US-Gerichten

Neben dem speziellen Rechtsbehelfsmechanismus gemäß Executive Order 14086 gibt es auch **Rechtsschutzmöglichkeiten vor den ordentlichen US-Gerichten**.[86] Diese setzen allerdings den Nachweis eines sog. **„Standing"**, also den Nachweis der persönlichen Betroffenheit von einer Maßnahme, voraus. Diese verfahrensrechtliche Voraussetzung erschwert die Einleitung von Gerichtsverfahren gegen heimliche Überwachungsmaßnahmen vor ordentlichen Gerichten erheblich.

Der Angemessenheitsbeschluss führt aus, dass jede Person insbesondere auch gemäß FISA die Möglichkeit habe, zum Beispiel eine **Zivilklage auf Schadenersatz**[87] gegen die USA einzureichen, wenn Informationen über sie rechtswidrig und vorsätzlich verwendet oder offengelegt wurden, oder um die Rechtmäßigkeit der Überwachung anzufechten, falls die US-Regierung beabsichtigt, Informationen, die sie aus der elektronischen Überwachung gewonnen hat, gegen die Person in Gerichts- oder Verwaltungsverfahren in den USA zu verwenden oder offenzulegen.

Schließlich gibt der Angemessenheitsbeschluss an, dass es mehrere spezifische Möglichkeiten gibt, rechtliche Schritte gegen Regierungsbeamte einzuleiten, wenn die Regierung unrechtmäßig auf personenbezogene Daten zugreift oder diese verwendet. Dies würde auch für angebliche Zwecke der nationalen Sicherheit gelten. Der Administrative Procedure Act[88] bietet nach dem Angemessenheitsbeschluss darüber hinaus eine allgemeinere Abhilfemöglichkeit, wonach jede Person, die aufgrund einer behördlichen Maßnahme einen Schaden erleidet oder durch eine behördliche Maßnahme benachteiligt oder geschädigt wird, das Recht hat, eine gerichtliche

[86] S. EWG (195) des Angemessenheitsbeschlusses zum EU-US DPF.
[87] S. EWG (196) des Angemessenheitsbeschlusses zum EU-US DPF.
[88] 5 United State Code, § 702.

Überprüfung zu beantragen. Darunter fallen beispielsweise auch auf FISA gestützte Maßnahmen.

Schließlich hat nach den Ausführungen im Angemessenheitsbeschluss[89] gemäß dem Freedom of Information Act[90] jeder das Recht, **Zugang zu Aufzeichnungen der Bundesbehörden** zu erhalten, einschließlich solcher Aufzeichnungen, die personenbezogene Daten der Person enthalten. Dieser Zugang kann laut Angemessenheitsbeschluss auch die Einleitung eines Verfahrens vor ordentlichen Gerichten erleichtern, z. B. zur Unterstützung der Beweisführung. Der Angemessenheitsbeschluss verweist jedoch u. a. in Bezug auf Datenverarbeitungen zu Zwecken der Strafverfolgung und der nationalen Sicherheit auf mögliche Ausnahmen von diesem Recht.

IV. Übermittlung personenbezogener Daten an die USA auf der Grundlage anderer Übermittlungsinstrumente

1. Übermittlungen an nicht zertifizierte Stellen

Übermittlungen an US-Empfänger, die nicht unter dem EU-US DPF zertifiziert sind, können nicht auf den Angemessenheitsbeschluss der Europäischen Kommission vom 10. Juli 2023 gestützt werden. Stattdessen ist ein anderes Übermittlungsinstrument aus Kapitel V DS-GVO nötig, etwa geeignete Datenschutzgarantien nach Art. 46 DS-GVO, beispielsweise in Form von Standarddatenschutzklauseln, um ein Schutzniveau zu gewährleisten, das dem in der Union garantierten der Sache nach gleichwertig ist (vgl. I.1.3.).

2. Folgen des Angemessenheitsbeschlusses für Übermittlungen auf Grundlage von Standardvertragsklauseln (SCCs) und anderen Garantien nach Art. 46 DS-GVO

Sofern Übermittlungen an die USA auf Grundlage geeigneter Garantien aus Art. 46 DS-GVO – beispielsweise SCCs oder BCR – gestützt werden, erfordert dies nach der Rechtsprechung des EuGH eine Bewertung der Rechtslage und -praxis des Drittlands

[89] S. EWG 199 des Angemessenheitsbeschlusses zum EU-US DPF
[90] 5 United State Code, § 552.

(sog. Transfer Impact Assessment – TIA)[91] und ggf. die Ergreifung geeigneter zusätzlicher Maßnahmen (sog. „supplementary measures“).[92]

Nach Mitteilung der EU-Kommission gelten alle von der US-Regierung im Bereich der nationalen Sicherheit implementierten Schutzmaßnahmen unabhängig von den verwendeten Übermittlungsinstrumenten für alle Datenübermittlungen im Rahmen der Datenschutz-Grundverordnung an US-Unternehmen.[93] Deshalb können Datenexporteure im Rahmen der Datenübermittlung mithilfe geeigneter Garantien (Art. 46 DS-GVO) die von der EU-Kommission im Angemessenheitsbeschluss ausgeführten Bewertungen für ihr Transfer Impact Assessment berücksichtigen.

V. Ausblick

Bei dem Angemessenheitsbeschluss handelt es sich um geltendes EU-Recht, solange er in Kraft ist. Er wird ein Jahr nach Inkrafttreten und danach spätestens alle vier Jahre von der Europäischen Kommission auf seine Wirksamkeit überprüft und kann ggf. angepasst oder aufgehoben werden.[94]

Zudem können Angemessenheitsbeschlüsse nach Art. 45 DS-GVO durch den EuGH gerichtlich überprüft und ggf. für ungültig erklärt werden. Auf diese Möglichkeit müssen Verantwortliche sich einstellen.

Verliert der Angemessenheitsbeschluss seine Gültigkeit, müssten Verantwortliche die entsprechenden Übermittlungen auf ein anderes, wirksames Übermittlungsinstrument aus Kapitel V DS-GVO stützen oder die in Rede stehenden Übermittlungen einstellen.

---

[91] EuGH Urt. v. 16. Juli 2020, C-311/18 („Schrems II“), Rn. 134 zu TIAs für Übermittlungen auf der Grundlage von SCCs.

[92] EuGH Urt. v. 16. Juli 2020, C-311/18 („Schrems II“), Rn. 131 sowie EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.

[93] Vgl. Q&A der Europäischen Kommission unter https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_3752.

[94] Vgl. EWG 211 ff. des Angemessenheitsbeschlusses zum EU-US DPF.

VI. Weitergehende Hinweise

Für weitere Informationen zum Angemessenheitsbeschluss zum EU-US DPF siehe auch:

- „Q&A“ der Europäischen Kommission zum Angemessenheitsbeschluss zum EU-US DPF[95] und
- Informationspapier des EDSA zum Angemessenheitsbeschluss zum EU-US DPF[96].

[95] Europäische Kommission Q&A zum EU-US DPF, abrufbar unter: https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_3752.

[96] Information note des EDSA, abrufbar unter: https://edpb.europa.eu/system/files/2023-07/edpb_informationnoteadequacydecisionus_en.pdf.