75 Jahre Demokratie lebendig

Deutscher Bundestag
Wissenschaftliche Dienste

Sachstand

Herausgabepflichten von Daten und Informationen an US-amerikanische Sicherheitsbehörden

Zu den Auswirkungen auf die Nutzung von Cloud-Diensten durch Behörden

Herausgabepflichten von Daten und Informationen an US-amerikanische Sicherheitsbehörden
Zu den Auswirkungen auf die Nutzung von Cloud-Diensten durch Behörden

Aktenzeichen:	WD 3 - 3000 - 105/23
Abschluss der Arbeit:	19.01.2024 (zugleich letzter Abruf der Internetseiten)
Fachbereich:	WD 3: Verfassung und Verwaltung

Inhaltsverzeichnis

1. Überblick

Der vorliegende Sachstand fasst **erstens** die wesentlichen Vorschriften des US-amerikanischen Rechts zusammen, nach denen **Anbieter von Vermittlungsdiensten** grundsätzlich verpflichtet werden können, **Daten und Informationen** auch von deutschen Kunden oder Vertragspartnern an US-amerikanische Sicherheitsbehörden **herauszugeben** (dazu unter 2.1.).[1] Unter Vermittlungsdiensten werden vorliegend bestimmte **Dienstleistungen der Informationsgesellschaft** im Sinne des Art. 3 Buchstabe g des Digital Services Act (DSA)[2] verstanden, wie Kommunikationsdienste („reine Durchleitung“) oder sog. „Hosting“-Dienste, bei denen von einem Nutzer bereitgestellte Informationen in dessen Auftrag gespeichert werden. So ist etwa auch ein Cloud-Computing-Dienst ein „Hosting“-Dienst und damit ein Vermittlungsdienst im Sinne des Art. 3 Buchstabe g DSA.[3] Des Weiteren wird der Anwendungsbereich **dieser US-amerikanischen Vorschriften** erörtert (dazu 2.2.).

Im Ergebnis zeigt sich, dass aus **US-amerikanischer Perspektive** die **Anwendung** dieser Herausgabeverpflichtungen grundsätzlich davon abhängt, ob die verlangten Daten und Informationen unter der **Kontrolle der jeweils verpflichteten US-amerikanischen Unternehmen** stehen – unabhängig vom Standort der Daten bzw. der Server. Das Ausmaß und die Form der Kontrolle unterliegt der Prüfung im Einzelfall. Aus **europäischer Perspektive** wird eine mögliche extraterritoriale Ausübung der US-amerikanischen Vorschriften zwar problematisiert, allerdings nicht grundsätzlich für unzulässig gehalten. Die Europäische Kommission hat in diesem Zusammenhang deutlich gemacht, dass bei grenzüberschreitenden Verpflichtungen wegen des völkerrechtlichen Territorialitätsprinzips und des Prinzips der gegenseitigen Rücksichtnahme („principles of territoriality and comity under public international law“) jedenfalls die Interessen und Gesetze des jeweils betroffenen Landes berücksichtigt werden müssen.[4]

Zweitens befasst sich der Sachstand mit der **Nutzung von Cloud-Diensten durch deutsche Behörden** unter Berücksichtigung dessen, dass die Anbieter dieser Cloud-Dienste Adressaten einer Herausgabeverpflichtung von US-amerikanischen Sicherheitsbehörden sein können (dazu 3.). Zum einen muss die Verwaltung als staatliche Stelle die Datensicherheit gewährleisten. Dazu gehört die Sicherstellung, dass die im Rahmen der staatlichen Aufgabenwahrnehmung erhobenen und verarbeiteten Daten für die staatlichen Stellen stets zur Verfügung stehen und auf sie zugegriffen werden kann. Zum anderen sind die öffentlichen Stellen in Deutschland bei der Verarbeitung

---

1 Eine vollständige Übersicht aller Vorschriften, die etwaige Herausgabepflichten begründen, ist im vorliegenden Umfang schwierig, vgl. insoweit zu einer unübersichtlichen Menge an gesetzlich verfassten sowie nicht-gesetzlich verfassten Rechtsquellen, Vladeck, Expertenbericht für Facebook im Schrems-Verfahren vor den irischen Gerichten, 02.11.2016, S. 4 Rn. 14; ders., Gutachten zum aktuellen Stand des US-Überwachungsrechts und der Überwachungsbefugnisse, 15.11.2021, S. 11.

2 Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19.10.2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste).

3 Vgl. Erwägungsgrund 29 des DSA.

4 Europäische Kommission, Brief of the European Commission on behalf of the European Union as *Amicus Curiae* in support of neither party, In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Cooperation, S. 6 f.

personenbezogener Daten an die Anforderungen der Datenschutz-Grundverordnung (DSGVO)[5] gebunden. Aufgrund der datenschutzrechtlichen Bedenken öffentlicher Stellen, Dienste US-amerikanischer Anbieter zu nutzen oder von Anbietern, die im Zusammenhang mit solchen stehen können, haben einige Cloud-Diensteanbieter besondere Angebote für die Nutzung von Cloud-Diensten im öffentlichen Sektor entwickelt. Beispielsweise sollen die Daten ausschließlich in der Europäischen Union bzw. Europäischen Freihandelszone gespeichert und verarbeitet werden.[6]

Im Ergebnis zeigt sich, dass die datenschutzrechtliche Rechtmäßigkeit der Nutzung dieser Cloud-Dienste durch Behörden von mehreren Aspekten im Einzelfall abhängt. Die Nutzung von Cloud-Diensten von Anbietern mit Sitz und Servern in der EU erscheint jedenfalls dann datenschutzrechtlich unproblematisch, wenn der Anbieter keine Tochtergesellschaft eines US-amerikanischen Unternehmens ist und im Übrigen die allgemeinen Rechtmäßigkeitsvoraussetzungen erfüllt sind. Aber auch für den Fall, dass der Anbieter eine Tochtergesellschaft eines US-amerikanischen Unternehmens ist, wird mittlerweile vertreten, dass allein eine **Gefahr einer Herausgabeverpflichtung** nach US-amerikanischem Recht nicht zu einer unzulässigen Übermittlung nach Art. 44 ff. DSGVO führen müsse. Diese Gefahr sei nach Art. 28 DSGVO im Rahmen der Prüfung der Zuverlässigkeit des Cloud-Diensteanbieters als Auftragsverarbeiter durch die Behörde als Verantwortlicher im Einzelfall zu berücksichtigen. Außerdem gilt mit Blick auf die Nutzung von **Cloud-Diensten US-amerikanischer Anbieter**, dass personenbezogene Daten wegen des neuen Angemessenheitsbeschlusses der Europäischen Kommission vom 10. Juli 2023 jedenfalls derzeit an zertifizierte Unternehmen rechtssicher übermittelt werden können.

2. Herausgabeverpflichtungen nach US-amerikanischen Recht

2.1. US-amerikanische Rechtsvorschriften

Für die Herausgabe von Daten und Informationen an US-amerikanische Sicherheitsbehörden sind insbesondere der **Electronic Communications Privacy Act (ECPA)**[7] aus dem Jahr 1986 und der **Foreign Intelligence Surveillance Act (FISA)**[8] aus dem Jahr 1978 von Bedeutung. Die relevanten Vorschriften wurden im United States Code (im Folgenden USC)[9] übernommen, der die allgemeinen und dauerhaften Gesetze der USA konsolidiert und kodifiziert.[10] Der ECPA steht in den

---

5 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).

6 Vgl. Amazon Web Services to Launch AWS European Sovereign Cloud, 25.10.2023.

7 Electronic Communications Privacy Act (ECPA) vom 21.10.1986 (Pub. L. 99-508, 100 Stat. 1848), im Wesentlichen zuletzt geändert durch „Consolidated Appropriations Act" vom 23.03.2018 (Pub. L. 115-141).

8 Foreign Intelligence Surveillance Act (FISA) vom 25.10.1978 (Pub. L. 95-511), zuletzt im Wesentlichen geändert durch „FISA Amendments Reauthorization Act of 2017" vom 19.01.2018 (Pub. L. 115-118).

9 United States Code (USC) vom 30.06.1926, zuletzt geändert am 17.11.2023.

10 Siehe zu weiteren Vorschriften der Indienstnahme von Unternehmen, Roßnagel/Geminn/Johannes/Müller, Auswirkungen ausländischer Gesetzgebung auf die deutsche Cybersicherheit, DuD 2022, 156 (158 f.).

§§ 2510 ff. im 18. Titel des USC zum Straf- und Strafprozessrecht („Crimes And Criminal Procedure; and Appendix“). Er umfasst unter anderem den **Stored Communications Act (SCA)**[11] mit den §§ 2701 ff. im 18. Titel des USC (nachfolgend zitiert als 18 USC §§ 2510 ff. bzw. §§ 2701 ff.). Der FISA steht in den §§ 1801 ff. des 50. Titels des USC im 36. Kapitel („Chapter 36—Foreign Intelligence Surveillance“) und umfasst die Befugnisse zur Auslandsaufklärung der US-amerikanischen Nachrichtendienste (nachfolgend zitiert als 50 USC §§ 1801 ff.). Diese Vorschriften wurden mehrfach geändert und angepasst. Die vorliegend relevanteste Änderung folgt aus dem **Clarifying Lawful Overseas Use of Data Act** (**CLOUD Act**)[12] aus dem Jahr 2018. Von Bedeutung sind außerdem die sog. **National Security Letters** sowie die **Executive Order (E.O.) 12333**[13] und die **E.O. 14086**[14].

2.1.1. Im Bereich des Strafverfahrens

Während 18 USC §§ 2501 ff. die Grundsätze der Überwachung **laufender Kommunikationen** regeln, beziehen sich 18 USC §§ 2701 ff. auf die Grundsätze des Zugangs zu **gespeicherten Kommunikationen und Aufzeichnungen** („Stored Wire and Electronic Communications and Transactional Record Access“). So steht es nach 18 USC § 2701(a) unter Strafe, wenn sich jemand Zugang zu gespeicherten Kommunikationen und Daten verschafft, soweit gesetzlich nichts anderes geregelt ist. Entsprechend gilt gemäß 18 USC § 2702(a), dass Anbieter von **elektronischen Kommunikationsdiensten** („electronic communication service“) oder **Remote-Computing-Diensten** („remote computing service“), die Inhalte der dort gespeicherten Kommunikation grundsätzlich nicht absichtlich offenlegen dürfen. Nach 18 USC § 2510(15) ermöglichen **elektronische Kommunikationsdienste** ihren Nutzern, elektronische Kommunikation zu senden oder zu empfangen. Elektronische Kommunikation ist gemäß 18 USC § 2510(12) die vollständige oder teilweise **Übertragung von Zeichen, Signalen, Schriftzeichen, Bildern, Geräuschen, Daten oder Informationen jeglicher Art** durch ein drahtgebundenes, Funk-, elektromagnetisches, fotoelektronisches oder fotooptisches System, das den nationalen oder ausländischen Handel berührt. Ein **Remote-Computing-Dienst** ist nach 18 USC § 2711(2) die Bereitstellung von Computerspeicher- oder -verarbeitungsdiensten für die Öffentlichkeit mittels eines elektronischen Kommunikationssystems. Eine Ausnahme vom Offenlegungsverbot regelt beispielsweise 18 USC § 2702(b)(7). Danach ist die Offenlegung gegenüber Strafverfolgungsbehörden zulässig, wenn der Anbieter der Kommunikationsdienste die Inhalte zufällig erhalten hat und es so scheint, dass diese Inhalte mit einer Straftat im Zusammenhang stehen.

---

11 Vgl. dazu im ECPA vom 21.10.1986 (Pub. L. 99-508, 100 Stat. 1860).

12 Siehe dazu Division V Sec. 101 des Consolidated Appropriations Act vom 23.03.2018 (Pub. L. 115-141).

13 Executive Order No. 12333 „United States Intelligence Activities“ (E.O. 12333) vom 04.12.1981; vgl. auch 50 USC § 3001.

14 Executive Order No. 14086 „Enhancing Safeguards for United States Signals Intelligence Activities“ (E.O.14086) vom 07.10.2022; vgl. auch 50 USC § 3001.

18 USC § 2703 regelt darüber hinaus das Recht bestimmter staatlicher Stellen („governmental entity"),[15] Anbieter von elektronischen Kommunikationsdiensten oder Remote-Computing-Diensten zu verpflichten, bestimmte Informationen offenzulegen („disclose"). Die jeweiligen Voraussetzungen für eine Herausgabeverpflichtung sind sehr komplex und unterscheiden sich sowohl nach Art des adressierten Diensteanbieters als auch nach Art und Aufbewahrungsdauer der Information, die herausgegeben werden soll. Insoweit wird im Wesentlichen zwischen einer einfachen **Vorlageverfügung** („administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena"), einer **gerichtlichen Anordnung** im Sinne des 18 USC § 2703(d) („court order") und einem **gerichtlichen (Durchsuchungs-)Beschlusses** („warrant issued using the procedures described in the Federal Rules of Criminal Procedure […] by a court of competent jurisdiction") unterschieden.[16]

Eine **Vorlageverfügung** ist beispielsweise gegenüber Anbietern von elektronischen Kommunikationsdiensten ausreichend, wenn die staatliche Stelle zum einen die Herausgabe von Kommunikationsinhalten fordert, die in einem elektronischen Kommunikationssystem für mehr als 180 Tage aufbewahrt werden. Zum anderen setzt sie voraus, dass die staatliche Stelle den betroffenen Kunden über die Offenlegung benachrichtigt oder die Benachrichtigung jedenfalls nach den Voraussetzungen des 18 USC § 2705 spätestens nach 90 Tagen erfolgt (18 USC § 2703(a), 18 USC § 2703(b)(1)(B)(i)). Dies gilt entsprechend gegenüber Anbietern von Remote-Computing-Diensten für die Herausgabe von Kommunikationsinhalten unabhängig von der Aufbewahrungsdauer (18 USC § 2703(b)(1)(B)(i)). Eine Vorlageverfügung reicht zudem bei der Herausgabe anderer Basiskundeninformationen („basic subscriber information" im Sinne von 18 USC § 2703(c)(2), wie z.B. Name oder Adresse)[17] aus. In dem Fall ist eine Benachrichtigung des betroffenen Kunden nicht erforderlich (18 USC § 2703(c)(2)).

Eine **gerichtliche Anordnung** im Sinne des 18 USC § 2703(d) ist ebenfalls ausreichend, wenn ein Anbieter von Remote-Computing-Diensten Kommunikationsinhalte herausgeben soll und die staatliche Stelle den Kunden darüber benachrichtigt hat (18 USC § 2703(b)(1)(B)(ii)). Auf der Grundlage einer gerichtlichen Anordnung können nach 18 USC § 2703(c)(1)(B) neben Basiskundeninformationen und Kommunikationsinhalten auch andere Informationen über Kunden herausgefordert werden, ohne den Kunden darüber zu benachrichtigen. Die Besonderheit der gerichtlichen Anordnung nach 18 USC § 2703(d) liegt vor allem darin, dass die fordernde staatliche Stelle konkrete und bestimmbare Tatsachen vortragen muss, aus denen sich berechtigte Gründe ergeben, dass die Informationen für ein laufendes strafrechtliches Verfahren wesentlich sind

15 Nach 18 USC § 2711(4) ist eine „governmental entity" weit zu verstehen als ein Ministerium oder eine Behörde der USA oder eines Bundesstaates der USA oder politische Unterteilung dessen („[…] department or agency of the United States or any State or political subdivision thereof").

16 Vgl. zur Systematik des 18 USC § 2703, Brief for the United States (im Fall von United States of America, Petitioner v. Microsoft Corporation), S. 2 ff.

17 Vgl. dazu Brief for the United States (im Fall von United States of America, Petitioner v. Microsoft Corporation), S. 3, vgl. ferner dazu als „non-content data" oder „so-called metadata", European Data Protection Board, Annex. Initial legal assessment of the impact of the US CLOUD Act on the EU legal framework for the protection of personal data and the negotiations of an EU-US Agreement on cross-border access to electronic evidence, 10.07.2019, S. 2.

(„specific and articulable facts showing that there are reasonable grounds to believe that the […] information sought, are relevant and material to an ongoing criminal investigation.“).

Schließlich kann eine staatliche Stelle gegenüber Anbietern von Kommunikationsdiensten die Herausgabe von Kommunikationsinhalten, die **180 Tage oder weniger** in einem elektronischen Kommunikationssystem aufbewahrt wurden, immer nur auf der Grundlage eines **gerichtlichen (Durchsuchungs-)Beschlusses** fordern (18 USC § 2703(a)). Ein solcher gerichtlicher Beschluss ist außerdem erforderlich, wenn die Inhalte des Anbieters von Kommunikationsdiensten **mehr als 180 Tage aufbewahrt** wurden oder ein Anbieter von Remote-Computing-Diensten die Kommunikationsinhalte herausgeben soll und der betroffenen Kunde über die Herausgabe **nicht benachrichtigt werden soll** (18 USC § 2703(a), 18 USC § 2703(b)(A)).

Durch den **CLOUD Act** wurden die Vorschriften der 18 USC §§ 2703 ff. durch **18 USC § 2703(h)** und **18 USC § 2713** ergänzt. Ausgangspunkt war ein Rechtsstreit zwischen US-amerikanischen Strafverfolgungsbehörden und Microsoft über den Zugang zu Daten, die in Irland gespeichert und aufbewahrt wurden.[18] Um die Rechtsunsicherheit zu beseitigen, wurde der CLOUD Act erlassen.[19] So bestimmt **18 USC § 2713**, dass Anbieter elektronischer Kommunikations- bzw. Vermittlungsdienste oder sog. Remote-Computing-Dienste, die der US-amerikanischen Gerichtsbarkeit unterliegen,[20] auch dann zur Offenlegung von Daten und Informationen nach den 18 USC §§ 2701 ff. verpflichtet werden können, wenn sich die **Daten und Informationen außerhalb der USA** befinden. Voraussetzung ist, dass sich die Daten jedenfalls **im Besitz, Gewahrsam oder unter der Kontrolle des Anbieters** befinden.

Außerdem haben die zur Offenlegung verpflichteten Diensteanbieter nach 18 USC § 2703(h) das Recht, die **Änderung oder Aufhebung des entsprechenden Offenlegungsverfahrens** zu beantragen, auch wenn sie ihren Sitz außerhalb der USA haben („Comity Analysis and Disclosure of Information Regarding Legal Process Seeking Contents of Wire or Electronic Communication“). Dies setzt erstens voraus, dass der jeweilige verpflichtete Anbieter davon überzeugt ist, dass der Kunde oder Teilnehmer seines Dienstes kein US-Bürger ist, seinen Wohnsitz nicht in den USA hat und die geforderte Offenlegung ein erhebliches Risiko begründen würde, dass der Anbieter gegen Rechtsvorschriften eines anderen Staates verstößt. Zweitens muss nach 18 USC § 2703(h)(2)(B) das Gericht, das dieses Verfahren prüft, der staatlichen Stelle, die die Offenlegung der Daten beantragt hat („governmental entity that applied for or issued the legal process“), Möglichkeit zur Stellungnahme gewähren und dem Antrag auf Änderung oder Aufhebung des jeweiligen Verfahrens entsprechen, wenn

---

18 Vgl. ausführlich dazu Rutherford, The CLOUD Act: Creating Executive Branch Monopoly over Cross-Border Data Access, Berkeley Technology Law Journal 2019 (Vol. 34/4), 1177 (1185).

19 Vgl. Rutherford, The CLOUD Act: Creating Executive Branch Monopoly over Cross-Border Data Access, Berkeley Technology Law Journal 2019 (Vol. 34/4), 1177 (1186 f.).

20 Vgl. dazu Divison V—CLOUD Act Sec. 102(2) des Consolidated Appropriations Act vom 23.03.2018 (Pub. L. 115-141): „Such efforts by the United States Government are being impeded by the inability to access data stored outside the United States that is in the custody, control, or possession of communications-service providers that are subject to jurisdiction of the United States“.

– die geforderte Offenlegung zu einer Verletzung von Rechtsvorschriften eines anderen Staates führen würde;

– auf der Grundlage einer Gesamtschau aller Umstände, Gerechtigkeitserwägungen gebieten, dass das Verfahren verändert oder aufgehoben wird; und

– der Kunde oder Teilnehmer des jeweiligen Dienstes kein US-Bürger ist und seinen Wohnsitz nicht in den USA hat.

Für die angeführte Gesamtschau aller Umstände soll das Gericht unter anderem die Interessen der USA, einschließlich der Ermittlungsinteressen der Stelle, die die Offenlegung fordert, sowie Natur und Ausmaß der Bindungen und der Anwesenheit des Diensteanbieters in den USA berücksichtigen.

2.1.2. Im Bereich der Auslandsaufklärung

Die wohl relevanteste Vorschrift aus dem Bereich der Auslandsaufklärung ist **50 USC § 1881a** (zum Teil auch als **Section 702** [des FISA] bezeichnet). Nach **50 USC § 1881a(a)** können der Attorney General und der Director of National Intelligence zur Auslandsaufklärung eine gezielte Überwachung einer oder mehrerer bestimmter Personen genehmigen, die sich wahrscheinlich **außerhalb der USA** aufhalten und selbst **keine US-Personen** sind. Zum Teil wird in der Öffentlichkeit und rechtswissenschaftlichen Literatur in diesem Zusammenhang von einer Rechtsgrundlage für „Massenüberwachungen“ oder „Massenerhebung“ gesprochen.[21] Nach eigenen Angaben des „Office of the Director of National Intelligence” (ODNI) in seinem Transparenzbericht 2022 ermächtigt **50 USC § 1881a bzw. Section 702 des FISA** staatliche Stellen indes nicht zur „bulk collection“.[22] Insoweit ist es nicht ausgeschlossen, dass unterschiedliche Begriffsverständnisse herrschen. Das US-amerikanische Gesetz spricht jedenfalls von „targeting certain persons“, was rein dem Wortlaut nach für eine gezielte Überwachung spricht.[23]

50 USC § 1881a setzt **keine gerichtliche Anordnung bzw. keinen gerichtlichen Beschluss** voraus (anders z.B. elektronische Überwachung nach 50 USC §§ 1804, 1805). Die staatliche Stelle, die die Herausgabe von Daten und Informationen begehrt, muss außerdem keinen wahrscheinlichen Grund („probable cause“) dafür darlegen, dass unter anderem das Überwachungsziel eine ausländische Gewalt bzw. ein Agent derer ist („foreign power or an agent of a foreign power“, vgl. dazu z.B. 50 U.S.C. §§ 1804(a)(3)(A), 1805(a)(2)(A)). Die zwei wesentlichen Voraussetzungen einer Überwachung nach 50 USC § 1881a sind vielmehr eine **Feststellung bzw. Einschätzung** der jeweiligen Umstände, auf Grund derer eine Überwachung erforderlich ist („determination“,

---

21 Siehe Glocker, Der neue Angemessenheitsbeschluss zum EU–U.S. Data Privacy Framework, RDi 2023, 465 (469); vgl. dazu ferner NOYB - Europäisches Zentrum für digitale Rechte, Europäische Kommission gibt EU-US-Datentransfers 3. Runde beim EuGH, 10.07.2023; Holland, heise online, US-Befugnis zur Massenüberwachung: Wichtiger Abgeordneter ausspioniert, 13.03.2023.

22 Office of the Director of National Intelligence, Annual Statistical Transparency Report regarding the Intelligence Community’s Use of National Security Surveillance Authorities, Calendar Year 2022, April 2023, S. 14.

23 „Bulk collection“ ist gemäß Sec. 4(b) der E.O. 14086 definiert als „authorized collection of large quantities of signals intelligence data that, due to technical or operational considerations, is acquired without the use of discriminants (for example, without the use of specific identifiers or selection terms)”.

50 USC § 1881a(c)(2)), und eine **Zertifizierung** der Maßnahme („certification“, 50 USC § 1881a(h)). Insoweit regelt 50 USC § 1881a(h)(2)(A)(vi), dass die Erhebung der relevanten Informationen **durch oder mit der Hilfe eines Anbieters elektronischer Kommunikationsdienste** („electronic communication service provider“) erfolgen soll. Der Begriff der Anbieter elektronischer Kommunikationsdienste ist nach 50 USC § 1881 weit definiert und umfasst sowohl Anbieter elektronischer Kommunikationsdienste im Sinne von 18 USC § 2510 als auch Anbieter von Remote-Computing-Diensten im Sinne von 18 USC § 2711 (zu diesen Begriffen bereits unter 2.1.1.).

Gemäß 50 USC § 1881a(i)(1)(A) werden die jeweiligen Anbieter elektronischer Kommunikationsdienste **schriftlich angewiesen** („[…] may direct, in writing, an electronic communication service provider […]“), der Regierung die erforderlichen Informationen in einer Weise weiterzugeben, die die **Geheimhaltung** der Informationsbeschaffung vor allem auch dem Überwachungssubjekt gegenüber wahrt. Des Weiteren sieht 50 USC § 1881a(i)(2) eine **Kompensation** für die jeweiligen Anbieter elektronischer Kommunikationsdienste und 50 USC § 1881a(i)(3) ihre Haftungsbefreiung vor. Nach 50 USC § 1881a(i)(4) können Anbieter elektronischer Kommunikationsdienste die schriftliche Anweisung vor dem Foreign Intelligence Surveillance Court (FISC) **anfechten** („challenging of directives“). Anders als 18 USC § 2703 unterscheidet 50 USC § 1881a, soweit ersichtlich, nicht zwischen den Arten der Daten und Informationen („content“/„basic subscriber information“). So wird außerdem wohl auch keine Unterscheidung gemacht, ob die Daten noch übermittelt („in transit“) oder bereits aufbewahrt („stored“) werden.[24]

50 USC § 1862(d) regelt zwar eine weitere Rechtsgrundlage zur Verpflichtung von Unternehmen, Aufzeichnungen zur Auslandsaufklärung oder für Ermittlungen im Bereich des internationalen Terrorismus an US-amerikanische Nachrichtendienste **heimlich herauszugeben**. Diese Möglichkeit kann allerdings nur an Unternehmen bestimmter im Gesetz genannter Branchen („common carrier, public accommodation facility, physical storage facility, or vehicle rental facility“) gerichtet werden. Nicht dazu zählen Vermittlungsdienste nach dem vorliegenden Verständnis (zur Definition unter 1.). Zwar regelte 50 USC § 1861 a.F. das Recht, von jedem Unternehmen sämtliche Unterlagen („any tangible things“) zu verlangen.[25] Dazu wurden auch „Daten auf Servern“ gezählt.[26] Diese Vorschrift wurde jedoch im Jahr 2020 nicht verlängert, sodass sie außer Kraft getreten ist somit und nicht mehr angewendet werden kann.[27]

---

24 Vgl. Vladeck, Gutachten zum aktuellen Stand des US-Überwachungsrechts und der Überwachungsbefugnisse, 15.11.2021, S. 2 f.

25 Zum Teil wird die Vorschrift auch „Section 215“ genannt, weil sie durch „Section 215“ des USA Patriot Act eingefügt wurde; vgl. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) (Pub. L. 107-56 [zu Section 215 auf 115 STAT. 287]) vom 26.10.2001.

26 Vgl. dazu Voigt, Weltweiter Datenzugriff durch US-Behörden - Auswirkungen für deutsche Unternehmen bei der Nutzung von Cloud-Diensten, MMR 2014, 158 (159).

27 Zur letzten Verlängerung der Vorschrift bis zum 15.03.2020 („Sunset“), Section 1703 des Gesetzes „Further Continuing Appropriations Act, 2020, and Further Health Extenders Act of 2019“ (Pub. L. 116-69; 133 STAT. 1143) vom 21.11.2019; siehe dazu Vladeck, Gutachten zum aktuellen Stand des US-Überwachungsrechts und der Überwachungsbefugnisse, 15.11.2021, S. 10.

2.1.3. E.O. 12333 und E.O. 14086

Die **E.O. 12333** aus dem Jahr 1981, die zuletzt 2008 geändert wurde, ist die Rechtsgrundlage für nachrichtendienstliche Maßnahmen („United States Intelligence Activities"), die nicht durch andere gesetzliche Vorschriften, wie z.B. die 50 USC 1801 ff., gedeckt sind.[28] Dabei sind die Maßnahmen nicht auf Anbieter von elektronischen Kommunikationsdiensten oder Remote-Computing-Diensten beschränkt.[29] Außerdem sieht die E.O. 12333 für Maßnahmen weder eine ex-ante noch eine ex-post Prüfung durch Gerichte vor.[30] Insgesamt ist der **Wortlaut der E.O. 12333 sehr weit** und lässt Fragen zum Anwendungsbereich offen. So ist unter anderem nicht abschließend geklärt, ob die E.O. als Rechtsgrundlage für Überwachungsmaßnahmen herangezogen werden kann, die „sich auf Daten im Transit durch die USA beziehen".[31] Indes ergibt sich aus dem Wortlaut der E.O. 12333, soweit ersichtlich, **kein ausdrückliches Recht** staatlicher Stellen oder Sicherheitsbehörden, Unternehmen zur Herausgabe von Daten und Informationen zu verpflichten.

Am 7. Oktober 2022 hat der Präsident der USA die **E.O. 14086** „Enhancing Safeguards for United States Signals Intelligence Activities" erlassen. Sie enthält keine über die E.O. 12333 oder sonstiges US-amerikanisches Recht hinausgehenden Rechtsgrundlagen für die Verpflichtung von Unternehmen, Daten und Informationen herauszugeben. Dennoch sind die durch die E.O. 14086 bestimmten Regelungen insoweit relevant, als sie **weitere Schutzmaßnahmen für Überwachungsmaßnahmen der US-amerikanischen Sicherheitsbehörden** festlegen sollen.[32] So sollen Überwachungsmaßnahmen unter anderem nur in einem Ausmaß und einer Weise möglich sein, die verhältnismäßig zum Zweck sind, zu dem sie genehmigt wurden (Sec. 2(a)(ii)(B) E.O. 14086: „ […] proportionate to the validated intelligence priority for which they have been authorized, […]"). Dies wird außerdem deutlich durch Sec. 2(c)(i) E.O. 14086: „[…]the United States […] shall consider the availability, feasibility, and appropriateness of other less intrusive sources and methods for collecting the information necessary to advance a validated intelligence priority, including from diplomatic and public sources, and shall prioritize such available, feasible, and appropriate alternatives to signals intelligence". Ferner wird nach Sec. 2(c)(ii) E.O. 14086 der Vorrang von gezielten Überwachungsmaßnahmen gegenüber einer „bulk collection" bestimmt. Insbesondere sieht Sec. 3 E.O. 14086 einen neuen zweistufigen Rechtsmittelmechanismus vor, der qualifizierte Beschwerden („qualifying complaints") aus einem qualifizierten Staat („qualifying state") betrifft. Ein Staat wird insoweit durch den US-Attorney General qualifiziert, der unter anderem voraussetzt, dass der jeweilige Staat angemessene Garantien für den Schutz personenbezogener Daten

---

28 Dazu ausführlich Seak, Grenzen der Datenübermittlungen aus der EU in Drittstaaten – anhand des Beispiels der USA, 2022, S. 166 m.w.N.

29 Vgl. dazu Seak, Grenzen der Datenübermittlungen aus der EU in Drittstaaten – anhand des Beispiels der USA, 2022, S. 166.

30 Siehe dazu Council of the European Union, Report on the findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection (16987/13), 27.11.2013, S. 12.

31 Seak, Grenzen der Datenübermittlungen aus der EU in Drittstaaten – anhand des Beispiels der USA, 2022, S. 167 mit Hinweis auf die Entscheidung des irischen High Court, der insoweit von einer Anwendung der E.O. 12333 ausgehe.

32 Siehe für eine Übersicht der Regelungen der E.O. 14086, Lejeune, Datentransfer mit den USA auf der Grundlage der Executive Order von Präsident Biden vom 7.10.2022, CR 2022, 775 ff.

von US-Personen vorsieht (vgl. Sec. 3(f)(i)(A) E.O. 14086). Des Weiteren sieht Sec. 3(d) E.O. 14086 die Einrichtung eines „Data Protection Review Court“ vor, an deren Einschätzungen sich die Sicherheitsbehörden der Intelligence Community halten sollen (Sec. 3(d)(ii) E.O. 14086). Vereinzelt werden auch Schutzmechanismen für Nicht-US-Personen in Gleichstellung mit US-Personen geregelt, wie bei der Verbreitung bzw. Weiterübermittlung von personenbezogenen Daten (Sec. 2(iii)(A)(1)(a) E.O. 14086).

Zu berücksichtigen ist dabei, dass die E.O. 14086 eine Reaktion auf die Schrems-II-Entscheidung des EuGH war (dazu näher unter 3.2.5.). Der EuGH erklärte in dieser Entscheidung den bis zu dem Zeitpunkt geltenden Angemessenheitsbeschluss „Privacy Shield“ für unwirksam, der die Zulässigkeit von Datentransfers zwischen den Mitgliedstaaten der EU und den USA regelte. Somit waren infolge der EuGH-Entscheidung diese Datentransfers nicht mehr rechtssicher. Der EuGH begründete seine Entscheidung insbesondere damit, „dass weder Section 702 noch die E.O. 12333 […] den im Unionsrecht nach dem Grundsatz der Verhältnismäßigkeit bestehenden Mindestanforderungen genügen, so dass nicht angenommen werden kann, dass die auf diese Vorschriften gestützten Überwachungsprogramme auf das zwingend erforderliche Maß beschränkt sind“.[33]

2.1.4. National Security Letters

Weitere Verpflichtungen von bestimmten Unternehmen, Daten und Informationen herauszugeben, können im Übrigen auf sogenannte **National Security Letters (NSL)** gestützt werden.[34] In Bezug auf Anbieter von Kommunikationsdiensten ist insoweit 18 USC § 2709 einschlägig, der die Herausgabe unter anderem von Kundeninformationen und Aufzeichnungen der Kommunikationstransaktionen regelt. Weitere Rechtsgrundlagen für NSL ergeben sich aus 12 USC § 3414, 15 USC § 1681u, und 15 USC § 1681v, wobei Vermittlungsdienste nach dem vorliegenden Verständnis jedoch nicht unter die Normadressaten fallen dürften. Allerdings dürfen laut dieser Vorschriften keine Kommunikationsinhalte gefordert und herausgegeben werden.[35]

2.2. Anwendungsbereich der US-amerikanischen Vorschriften

Die genannten Vorschriften begründen Herausgabepflichten zunächst für **Daten und Informationen**, die sich **innerhalb der USA** befinden, gegenüber US-amerikanischen Unternehmen, die auch ihren **Sitz in den USA** haben.[36] In diesem Fall ist die Anwendung des US-amerikanischen Rechts, soweit ersichtlich, unstrittig. Demgegenüber ist die Rechtslage unübersichtlich, wenn es

---

33 EuGH, Urteil vom 16.07.2020 - C-311/18, Rn. 184.

34 Vgl. Congressional Research Service, National Security Letters in Foreign Intelligence Investigations: Legal Background, 30.07.2015; Vladeck, Expertenbericht für Facebook im Schrems-Verfahren vor den irischen Gerichten, 02.11.2016, S. 15 Rn. 52, abrufbar unter: https://iapp.org/media/pdf/resource_center/Schrems-testimony-Vladeck.pdf; vgl. dazu auch Seak, Grenzen der Datenübermittlungen aus der EU in Drittstaaten – anhand des Beispiels der USA, 2022, S. 165 f.

35 Siehe dazu auch Vladeck, Gutachten zum aktuellen Stand des US-Überwachungsrechts und der Überwachungsbefugnisse, 15.11.2021, S. 11.

36 Vgl. zum Adressatenkreis der 18 USC §§ 2703, 2713, Cording/Götzinger, Der CLOUD Act aus europäischer Sicht, CR 2018, 636 (637).

um die **extraterritoriale Anwendung** der Vorschriften geht. Dies ist zum einen der Fall, wenn sich die **Daten und Informationen**, deren Herausgabe US-amerikanische Sicherheitsbehörden von US-amerikanischen Unternehmen begehren, **außerhalb der USA** befinden.[37] Insoweit ist unter anderem nicht abschließend geklärt, ob diese Herausgabeverpflichtungen auch auf außerhalb der USA gespeicherte Daten und Informationen von **Tochtergesellschaften mit Sitz außerhalb der USA** gerichtet sein können. Zum anderen wird wegen der extraterritorialen Rechtsanwendung auch die unmittelbare Verpflichtung von **Unternehmen mit Sitz außerhalb der USA**, wie auch Tochtergesellschaften von US-amerikanischen Unternehmen mit Sitz außerhalb der USA, problematisiert.

2.2.1. Verpflichtung von Unternehmen mit Sitz in den USA

18 USC § 2713 regelt, dass für die Geltendmachung von Herausgabeforderungen **gegenüber US-amerikanischen Unternehmen** der **Speicher- und Aufbewahrungsort der Daten und Informationen irrelevant** ist (zur Vorschrift bereits oben unter 2.1.1.). 18 USC § 2713 ist aus US-amerikanischer Perspektive eine deklaratorische Regelung. Die Verpflichtung eines US-amerikanischen Unternehmens, auch außerhalb der USA aufbewahrte Daten nach 18 USC § 2703 herauszugeben, sei keine unzulässige extraterritoriale Rechtsanwendung.[38] Es komme für eine zulässige Rechtsanwendung maßgeblich auf die **Verfügungsgewalt der US-amerikanischen Unternehmen über die jeweiligen Daten** an und nicht auf den Standort der verlangten Daten und Informationen.[39] Entsprechend ist die mittlerweile einfachgesetzlich festgelegte zentrale Voraussetzung des 18 USC § 2713, dass das jeweilige Unternehmen selbst über die in einem anderen Staat gespeicherten oder aufbewahrten Daten **verfügen** muss, diese sich **in seiner Obhut** oder **unter seiner Kontrolle** befinden („within such provider's possession, custody, or control“). Diese Begriffe werden im Gesetz nicht näher definiert, sondern sind Gegenstand der Auslegung.[40] In der rechtswissenschaftlichen Literatur wird in diesem Zusammenhang unter anderem auf den Begriff der „Kontrolle“ im Sinn der Rule 34 und Rule 45 der Federal Rules of Civil Procedure hingewiesen, der weder Eigentum noch Besitz verlange, sondern es ausreichen lasse, „wenn das Recht, die Befugnis oder

---

37 Vgl. Uecker, Extraterritoriale Regelungshoheit im Datenschutzrecht, 2017, S. 33: „Eine Regelung ist extraterritorial, wenn durch sie Regelungshoheit derart ausgeübt wird, dass ihr auch Personen, Sachen usw. außerhalb des eigenen Staatsgebiets unterworfen werden“.

38 Brief for the United States (im Fall von United States of America, Petitioner v. Microsoft Corporation), S. 13: „Applying Section 2703 to require the disclosure of data stored abroad does not violate the presumption against extraterritoriality“; vgl. dazu ferner Hemmings/Srinivasan/Swire, Defining the Scope of “Possession, Custody, or Control” for Privacy Issues and the CLOUD Act (October 7, 2019), 10 Journal of National Security Law and Policy 631 (2020), S. 631 (637) m.w.N.

39 Brief for the United States (im Fall von United States of America, Petitioner v. Microsoft Corporation), S. 14.

40 Vgl. ebenfalls zum Auslegungsbedürfnis European Data Protection Board, Annex. Initial legal assessment of the impact of the US CLOUD Act on the EU legal framework for the protection of personal data and the negotiations of an EU-US Agreement on cross-border access to electronic evidence, 10.07.2019, S. 2.

die tatsächliche Möglichkeit besteht, die Informationen von einem Dritten zu erlangen“.[41] **Rechtliche Kontrolle** im Sinne dieser Gesetze liege beispielsweise bei Niederlassungen der US-amerikanischen Unternehmen oder hundertprozentigen Tochtergesellschaften von US-amerikanischen Unternehmen außerhalb von USA vor.[42] Unter Verweis auf andere US-amerikanische Gesetze wird sogar argumentiert, dass US-amerikanische Gerichte bereits dann Kontrolle im Sinne des CLOUD Act annehmen könnten, wenn eine Tochtergesellschaft nur zu 25 Prozent im Eigentum eines US-amerikanischen Unternehmens stehe.[43] Als ein Beispiel der **tatsächlichen Kontrolle** wird die Konstellation angeführt, bei der zwischen dem zur Herausgabe verpflichteten US-amerikanischen Unternehmen und einem anderen Unternehmen mit Sitz im Ausland, das über die Daten verfügt, zwar keine rechtliche Bindung besteht, aber der Unternehmensvorstand identisch ist.[44] Im Ergebnis ist davon auszugehen, dass die Kontrolle von mehreren Faktoren abhängt, z.B. der Konzernstruktur oder den tatsächlichen Zugriffsmöglichkeiten im Einzelfall. US-amerikanische Unternehmen sollen demgegenüber **nicht zur Herausgabe gezwungen** werden können, wenn **keine rechtlichen oder tatsächlichen Zugriffsmöglichkeiten** bestehen „und diese bei einer Tochtergesellschaft oder einem unabhängigen Geschäftspartner gespeichert sind, die Kooperationsersuchen ablehnen“.[45]

18 USC § 2713 gilt allerdings nur für die Herausgabeverpflichtung nach den 18 USC §§ 2703 ff. Die Vorschrift gilt nicht für diejenigen **Herausgabeverpflichtungen im Bereich der Auslandsaufklärung** nach 50 USC § 1881a(i)(1)(A) oder auf der Grundlage von NSL oder der E.O. 12333. In diesem Zusammenhang wird angeführt, dass 50 USC § 1881a jedenfalls nicht angewendet werden könne, wenn die Daten und Informationen von einer Nicht-US-Person **ohne jeglichen Bezug zu einem US-amerikanischen Konzern außerhalb der USA** aufbewahrt werden.[46] Eine Überwachung könne dennoch auf der Grundlage der E.O. 12333 erfolgen.[47] In dem Fall, dass ein US-amerikanisches Unternehmen – einschließlich seiner EU-Tochterunternehmen – die Daten außerhalb

41 Determann/Nebel, U.S. CLOUD Act – Wolken über der Datenschutz-Grundverordnung?, CR 2018, 408 (410); vgl. ähnlich zu Rule 16(a)(1)(B, D-F) der Federal Rules of Criminal Procedure auch Hemmings/Srinivasan/Swire, Defining the Scope of “Possession, Custody, or Control” for Privacy Issues and the CLOUD Act (October 7, 2019), 10 Journal of National Security Law and Policy 631 (2020, S. 631 (655).

42 Hemmings/Srinivasan/Swire, Defining the Scope of “Possession, Custody, or Control” for Privacy Issues and the CLOUD Act (October 7, 2019), 10 Journal of National Security Law and Policy 631 (2020), S. 631 (656).

43 Hemmings/Srinivasan/Swire, Defining the Scope of “Possession, Custody, or Control” for Privacy Issues and the CLOUD Act (October 7, 2019), 10 Journal of National Security Law and Policy 631 (2020), S. 631 (657 f.).

44 Hemmings/Srinivasan/Swire, Defining the Scope of “Possession, Custody, or Control” for Privacy Issues and the CLOUD Act (October 7, 2019), 10 Journal of National Security Law and Policy 631 (2020), S. 631 (659 f.).

45 Determann/Nebel, U.S. CLOUD Act – Wolken über der Datenschutz-Grundverordnung?, CR 2018, 408 (410).

46 Vladeck, Gutachten zum aktuellen Stand des US-Überwachungsrechts und der Überwachungsbefugnisse, 15.11.2021, S. 8.

47 Vladeck, Gutachten zum aktuellen Stand des US-Überwachungsrechts und der Überwachungsbefugnisse, 15.11.2021, S. 8.

der USA aufbewahrt, könne 50 U.S.C. § 1881a jedoch aus US-amerikanischer Sicht gleichermaßen anwendbar sein.[48]

2.2.2. Verpflichtung von Unternehmen mit Sitz außerhalb der USA?

Teilweise wird argumentiert, dass 18 USC § 2713 so weit ausgelegt werden könne, dass auch **ausländische Unternehmen** bzw. nicht-US-amerikanische Unternehmen, wie auch Tochterunternehmen mit Sitz außerhalb der USA, **Adressaten einer entsprechenden Herausgabeverpflichtung** sein könnten. Dies solle bereits „[b]ei ausreichenden Anknüpfungspunkten" gelten, die einen hinreichenden Bezug zur US-amerikanischen Gerichtsbarkeit begründen.[49] Für eine Herausgabeverpflichtung könne ausreichen, dass die zur Herausgabe verpflichteten Unternehmen lediglich in den USA „Geschäftsniederlassungen betreiben" oder „aus dem Ausland auf dem US-Markt ausgerichtete Dienstleistungen anbieten".[50]

Dies wäre eine **extraterritoriale Ausübung des US-amerikanischen Rechts** in einem anderen Staat, die die territoriale Souveränität des jeweiligen anderen betroffenen Staates berührt.[51] Die extraterritoriale Ausübung ist völkerrechtlich zwar nicht per se verboten, allerdings muss insoweit zwischen Ausübung, Rechtsanwendung und Rechtsdurchsetzung bzw. Vollstreckung differenziert werden.[52] Vor allem die Vollstreckung einer solchen Herausgabeverpflichtung in einem fremden Hoheitsgebiet ist grundsätzlich ausgeschlossen und könnte nur mithilfe desjenigen Staates erfolgen, dessen Hoheitsgebiet berührt ist.[53]

Die extraterritoriale Ausübung von nationalen Vorschriften setzt einen **sog. „genuine link"** voraus, d.h. eine Verbindung oder einen Bezug zu dem das Gesetz erlassenden Staat.[54] Als Beispiel

---

48 Vladeck, Gutachten zum aktuellen Stand des US-Überwachungsrechts und der Überwachungsbefugnisse, 15.11.2021, S. 8.

49 Vgl Bürgerrechtevereinigung „Electronic Frontier Foundation", The U.S. CLOUD Act and the EU: A Privacy Protection Race to the Bottom, 09.04.2018: „sufficient jurisdictional nexus to send an order", z.B. gegen Telegram mit US-amerikanischen Kunden, vgl. dazu Cording/Götzinger, Der CLOUD Act aus europäischer Sicht, CR 2018, 636 (637); vgl. dazu m.w.N. Wissenschaftliche Dienste des Deutsche Bundestages, DSGVO und Nutzung US-amerikanischer Cloud-Dienste, WD 3 - 3000 - 102/21, 03.06.2021, S. 13.

50 Vgl. dazu Schweizer Bundesamt für Justiz, Bericht zum US CLOUD Act, 17.09.2021, S. 17, mit Hinweis auf den Bericht der französischen Nationalversammlung „Rétablir la souveraineté de la France et de l'Europe et protéger nos entreprises des lois et mesures à portée extraterritoriale» vom 26.06.2019, S. 29 f.

51 Cording/Götzinger, Der CLOUD Act aus europäischer Sicht, CR 2018, 636 (638).

52 Wissenschaftliche Dienste des Deutsche Bundestages, Zur extraterritorialen Ausübung von Hoheitsgewalt, WD 2 - 3000 - 176/18, 03.06.2021, S. 4.

53 Vgl. dazu Klose/Momsen, § 33 Überblick über das Datenschutzsanktionenrecht in den USA, in: Klaas/Momsen/Wybitul, Datenschutzsanktionsrecht, Rn. 56, die die Frage aufwerfen, „inwiefern mit dem Herausgabeverlangen [virtueller Daten] überhaupt in fremde Hoheitsgebiete eingegriffen" werde; vgl. ferner Uecker, Extraterritorialer Anwendungsbereich der DS-GVO, ZD 2019, 67 (68).

54 Wissenschaftliche Dienste des Deutsche Bundestages, Zur extraterritorialen Ausübung von Hoheitsgewalt, WD 2 - 3000 - 176/18, 03.06.2021, S. 4.

für eine solche Verbindung wird im rechtswissenschaftlichen Schrifttum die Betroffenheit personenbezogener Daten von US-Staatsbürgern angeführt.[55] Wenn eine solche Verbindung fehlt, hängt die extraterritoriale Ausübung des nationalen Rechts letztlich ebenfalls von der Mitwirkung des anderen betroffenen Staates ab.[56] Auch die Europäische Kommission führt insoweit aus:

> In the European Union's view, from the perspective of public international law, when a public authority requires a **company established in its own jurisdiction** to produce **electronic data stored on a server in a foreign jurisdiction**, the principles of territoriality and comity under public international law are engaged, and the **interests and laws of that foreign jurisdiction must be taken into account**.
>
> Any domestic law that creates **cross-border obligations –** whether enacted by the United States, the European Union, or another state **–** should be applied and interpreted in a manner that is **mindful of the restrictions of international law and considerations of international comity**. The European Union's foundational treaties and case law enshrine the principles of "mutual regard to the spheres of jurisdiction" of sovereign states and of the need to interpret and apply EU legislation in a manner that is consistent with international law.[57]

Innerhalb der rechtswissenschaftlichen Literatur wird daher insbesondere auf die Bedeutung und Notwendigkeit von Rechtshilfeabkommen („Mutual Legal Assistance Treaties", kurz MLAT) hingewiesen, die die jeweiligen betroffenen Interessen von zwei Staaten und die damit einhergehenden Rechtsunsicherheiten regeln können.[58] Zwar sieht der CLOUD Act mit 18 U.S.C. § 2523 ähnlich vor, dass Durchführungsvereinbarungen für den Zugang zu Daten durch ausländische Regierungen geschlossen werden können („Executive agreements on access to data by foreign governments"). Bisher haben die USA nach eigenen Angaben solche Vereinbarungen jedoch nur mit dem Vereinigten Königreich und Australien geschlossen. Derzeit laufen Verhandlungen mit Kanada und der EU.[59] Eine eigene Vereinbarung zwischen den USA und Deutschland gibt es bisher nicht.

2.3. Zwischenfazit

US-amerikanische Sicherheitsbehörden können US-amerikanische Unternehmen verpflichten, Daten und Informationen, auf die sie rechtlich und tatsächlich zugreifen können, unabhängig von ihrem Standort bzw. dem Standort des Servers, herauszugeben. Darüber hinaus wird zum Teil

---

55 Klose/Momsen, § 33 Überblick über das Datenschutzsanktionenrecht in den USA, in: Klaas/Momsen/Wybitul Datenschutzsanktionsrecht, Rn. 54 f.

56 Wissenschaftliche Dienste des Deutsche Bundestages, Zur extraterritorialen Ausübung von Hoheitsgewalt, WD 2 - 3000 - 176/18, 03.06.2021, S. 4.

57 Europäische Kommission, Brief of the European Commission on behalf of the European Union as *Amicus Curiae* in support of neither party, In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Cooperation, S. 6 f.; Hervorhebungen nicht im Original.

58 Cording/Götzinger, Der CLOUD Act aus europäischer Sicht, CR 2018, 636 (638).

59 Siehe dazu auf der Internetseite des US-amerikanischen Justizministeriums („U.S. Department of Justice"), CLOUD Act Resources, letzter Stand: 24.10.2023.

vertreten, dass hierzu auch Unternehmen verpflichtet werden können, die ihren Sitz nicht in den USA haben. Dies ist jedoch besonders aus völkerrechtlicher Perspektive nicht abschließend geklärt.

3. Nutzung von Cloud-Diensten durch Behörden

Nachfolgend wird erörtert, ob und gegebenenfalls inwieweit es mit deutschem Recht vereinbar ist, wenn **deutsche Behörden Cloud-Dienste nutzen**, die – trotz der genannten völkerrechtlichen Bedenken – auch Adressaten der US-amerikanischen Herausgabeverpflichtungen sein können. Im Folgenden werden nur private Cloud-Diensteanbieter betrachtet und nicht etwa behördeninterne oder staatliche Cloud-Lösungen.[60]

Zur Überprüfung der rechtlichen Zulässigkeit der Nutzung von den oben genannten privaten Cloud-Diensten wird als erstes eine etwaige Verantwortung oder **Gewährleistungspflicht des Staates in Bezug auf personenbezogene Daten** und ihre **Datensicherheit** erörtert, die er im Rahmen der Wahrnehmung staatlicher Aufgaben erhoben hat oder im Rahmen der Aufgabenwahrnehmung verwendet (dazu unter 3.1.). Zweitens werden die relevanten **datenschutzrechtlichen Anforderungen der DSGVO** näher dargestellt (3.2.).

3.1. Gewährleistung der Datensicherheit

Es stellt sich zunächst die Frage, ob und gegebenenfalls in welchem Umfang Daten, die der Staat im Rahmen seiner Aufgabenwahrnehmung und -erfüllung erhebt und nutzt, den öffentlich-rechtlichen Herrschaftsbereich des Staates überhaupt verlassen und an einen privaten Cloud-Anbieter übertragen werden dürfen. Verfassungsrechtlich ist dies nicht ausdrücklich geregelt.[61] In der rechtswissenschaftlichen Literatur wird vereinzelt auf einfachgesetzliche Vorschriften hingewiesen, die die Verantwortlichkeit der Datenverarbeitung im Einzelfall regeln,[62] wie z.B. §§ 17 Abs. 3, 2 Abs. 2 des Finanzverwaltungsgesetzes (FVG)[63], § 126 Abs. 3 der Grundbuchordnung (GBO)[64] oder § 497 der Strafprozessordnung (StPO)[65].

---

60 Zur Einrichtung von Cloud-Diensten durch öffentlich-rechtliche Institutionen, juristische Personen des öffentlichen Rechts oder des Privatrechts, die aber im vollständigen Eigentum des Bundes oder des Landes stehen, Ernst, Der Grundsatz digitaler Souveränität, 2020, S. 16.

61 So auch Ernst, Der Grundsatz digitaler Souveränität, 2020, S. 25.

62 Ernst, Der Grundsatz digitaler Souveränität, 2020, S. 15, 78 ff.

63 Finanzverwaltungsgesetz in der Fassung der Bekanntmachung vom 04.04.2006 (BGBl. I S. 846, 1202), zuletzt geändert am 21.12.2023 (BGBl. 2023 I Nr. 397).

64 Grundbuchordnung in der Fassung der Bekanntmachung vom 26.05.1994 (BGBl. I S. 1114), zuletzt geändert am 19.12.2022 (BGBl. I S. 2606).

65 Strafprozeßordnung in der Fassung der Bekanntmachung vom 07.04.1987 (BGBl. I S. 1074, 1319), zuletzt geändert am 26.07.2023 (BGBl. 2023 I Nr. 203).

Wenn staatliche Stellen oder die Verwaltung IT-Dienstleistungen einsetzen, wie Cloud-Dienste von privaten Anbietern, wird die Verantwortung des Staates unter den Stichworten der Datenhoheit oder auch digitalen Souveränität der Verwaltung diskutiert.[66] Digitale Souveränität wird im Sinne eines Teilaspekts der Souveränität eines Staates definiert als „unabhängige Selbstbestimmung in Bezug auf digitale Systeme und Daten“ und „alleinige Kontrolle über die Speicherung, Weitergabe und Nutzung von Daten oder auch die Fähigkeit, Hardware-Komponenten zu entwickeln, herzustellen und zu kontrollieren“.[67] Die Datenhoheit bzw. die digitale Souveränität der Verwaltung wird unter anderem der Pflicht des Staates, die **Funktionsfähigkeit der Verwaltung** sowie den **Schutz personenbezogener Daten** zu gewährleisten, entnommen. Funktionsfähigkeit der Verwaltung setze danach insbesondere voraus, dass die von der Verwaltung für einen bestimmten Zweck erhobenen und genutzten Daten zur Aufgabenerfüllung verfügbar sein sollten und dies nicht durch die Nutzung von Cloud-Diensten privater Anbieter gefährdet werden dürfe.[68] Dem grundrechtlichen Schutz personenbezogener Daten aus dem Recht auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG wird insoweit außerdem besondere Bedeutung zugemessen, „weil sich der Bürger der rechtsverbindlich angeordneten Datenerhebung und -verarbeitung durch den Staat regelmäßig schwerer entziehen kann“ als der Datenverarbeitung durch Private.[69] Vereinzelt wird in diesem Zusammenhang auch **Art. 33 Abs. 4 GG** angeführt, wonach die **Ausübung hoheitsrechtlicher Befugnisse als ständige Aufgabe in der Regel Angehörigen des öffentlichen Dienstes** zu übertragen ist, die in einem öffentlich-rechtlichen Dienst- und Treueverhältnis stehen. Allerdings gelte dies nur als äußerste Privatisierungsgrenze.[70] Nicht erfasst von der Vorschrift sei daher „[d]ie Wahrnehmung bloßer technischer Hilfsfunktionen, wie bspw. Auftragsverarbeitung in der Cloud i.S.v. Art. 28 DSGVO“.[71]

Im Übrigen wird davon ausgegangen, dass eine „**vollständige Souveränität**“ – d.h. ausschließliche Nutzung von IT-Lösungen und Dienstleistungen aus dem öffentlich-rechtlichen Herrschaftsbereich unabhängig von privaten Anbietern – vor allem aus Kostenaspekten und Praktikabilitäts-

66 Vgl. Kelber/Bortnikov, Digitale Souveränität von Sicherheitsbehörden und Nachrichtendiensten, NJW 2023, 2000.

67 Vgl. Kleine Anfrage u.a. der Fraktion der FDP, BT-Drs. 19/10952, S. 1 (siehe zur Antwort BT-Drs. 19/11445); vgl. ferner Bundesministerium für Wirtschaft und Klimaschutz, Digitale Souveränität und Künstliche Intelligenz – Voraussetzungen, Verantwortlichkeiten und Handlungsempfehlungen, 2018, S. 3; vgl. ferner Übersicht zur Definition, Bundesministerium für Wirtschaft und Klimaschutz, Schwerpunktstudie Digitale Souveränität – Bestandsaufnahme und Handlungsfelder, S. 61 ff.; vgl. zu einfachgesetzlichen Umsetzungen auf Landesebene, Gesetz zur Gewährleistung der digitalen Souveränität der Freien Hansestadt Bremen - Land und Stadtgemeinde - vom 12.06.2022; Hamburgisches IT-Souveränitätsgesetz (HmbITSG) vom 20.12.2022, Kelber/Bortnikov, Digitale Souveränität von Sicherheitsbehörden und Nachrichtendiensten, NJW 2023, 2000.

68 Ausführlich dazu Ernst, Der Grundsatz digitaler Souveränität, 2020, S. 36.

69 Ernst, Der Grundsatz digitaler Souveränität, 2020, S. 57.

70 Vgl. Heckmann/Scheurer in: Heckmann/Paschke, jurisPK-Internetrecht, 7. Aufl. Stand: 04.01.2024, Kap. 9 Rn. 772.

71 Vgl. Heckmann/Scheurer in: Heckmann/Paschke, jurisPK-Internetrecht, 7. Aufl. Stand: 04.01.2024, Kap. 9 Rn. 772.

gründen nur schwer umzusetzen sei. Es müsse vielmehr zwischen Kosten und Nutzen abgewogen werden.[72] So entschied das Bundesverfassungsgericht in Bezug auf die Vorratsdatenspeicherung ähnlich, dass die Beauftragung privater IT-Dienstleister nicht per se ausgeschlossen sei, aber die Vorratsdatenspeicherung einer „gesetzlichen Gewährleistung eines besonders hohen Standards der Datensicherheit" bedürfe:

> Angesichts des Umfangs und der potentiellen Aussagekraft der mit einer solchen Speicherung geschaffenen Datenbestände ist die Datensicherheit für die Verhältnismäßigkeit der angegriffenen Vorschriften von großer Bedeutung. Dieses gilt besonders, weil **die Daten bei privaten Diensteanbietern gespeichert werden**, die **unter den Bedingungen von Wirtschaftlichkeit und Kostendruck handeln** und dabei nur **begrenzte Anreize zur Gewährleistung von Datensicherheit** haben. Sie handeln grundsätzlich privatnützig und sind **nicht durch spezifische Amtspflichten gebunden**. Zugleich ist die Gefahr eines illegalen Zugriffs auf die Daten groß, denn angesichts ihrer vielseitigen Aussagekraft können diese für verschiedenste Akteure attraktiv sein. Geboten ist daher ein besonders hoher Sicherheitsstandard, der über das allgemein verfassungsrechtlich gebotene Maß für die Aufbewahrung von Daten der Telekommunikation hinausgeht. Solche Anforderungen der Datensicherheit gelten dabei sowohl für die Aufbewahrung der Daten als auch für deren Übermittlung; ebenso bedarf es effektiver Sicherungen zur Gewährleistung der Löschung der Daten.[73]

Das Bundesverfassungsgericht macht in dieser Entscheidung ebenfalls deutlich, dass das Grundgesetz selbst keine genauen verfassungsrechtlichen Datensicherheitsvorgaben macht, aber es im Ergebnis auf eine Abwägung im Einzelfall ankommt.[74] Dazu gehören unter anderem Aspekte zur Art betroffenen Daten und zur Art der hoheitlichen Aufgabe, für die die Daten verarbeitet bzw. die IT-Dienstleistung genutzt werden soll.

Übertragen auf die Nutzung von Cloud-Diensten von Anbietern, die gegebenenfalls US-amerikanischen Herausgabeverpflichtungen unterliegen könnten, durch deutsche Behörden, muss mit Blick auf die jeweilige Aufgabe und das Ausmaß der möglichen Datensicherheit im Einzelfall abgewogen werden. So sind im Fall von kritischen Daten entsprechend hohe Anforderungen an die Datensicherheit zu stellen.[75] Bezüglich der Anforderung der jederzeitigen Verfügbarkeit der Daten

---

72 Vgl. Kleine Anfrage u.a. der Fraktion der FDP, BT-Drs. 19/10952, S. 1 (siehe zur Antwort BT-Drs. 19/11445).

73 BVerfGE 125, 260 (325), Hervorhebungen nicht im Original.

74 BVerfGE 125, 260 (326 f.): „Die Verfassung gibt nicht detailgenau vor, welche Sicherheitsmaßgaben im Einzelnen geboten sind. Im Ergebnis muss jedoch ein Standard gewährleistet werden, der unter spezifischer Berücksichtigung der Besonderheiten der durch eine vorsorgliche Telekommunikationsverkehrsdatenspeicherung geschaffenen Datenbestände ein besonders hohes Maß an Sicherheit gewährleistet".

75 Bundesministerium für Wirtschaft und Klimaschutz, Digitale Souveränität und Künstliche Intelligenz – Voraussetzungen, Verantwortlichkeiten und Handlungsempfehlungen, 2018, S. 12: „[…] kritische Daten der Verwaltung [dürfen] nur in Systemen verarbeitet werden, bei denen staatliche Organe nicht nur die Hoheit darüber haben, wer auf diese Daten zugreifen kann, sondern bei denen sie die betreffenden Daten jederzeit auch in andere Systeme übertragen und durchsetzbar im ursprünglichen System löschen können. […] Bei öffentlicher Beschaffung sollten Software- und Cloud-Angebote grundsätzlich bevorzugt werden, bei denen der Quellcode geprüft und geändert werden kann"; vgl. ferner zur Zurückhaltung beim IT-Outsourcing durch deutsche Sicherheitsbehörden und Nachrichtendienste, Kelber/Bortnikov, Digitale Souveränität von Sicherheitsbehörden und Nachrichtendiensten, NJW 2023, 2000 (2006).

erscheinen ferner auch Konstellationen der Nutzung von Cloud-Diensten problematisch, bei denen sich die Server, auf denen die jeweiligen Daten gespeichert werden sollen, außerhalb Deutschlands oder der EU befinden und somit dem Herrschaftsbereich der deutschen Verwaltung noch weiter entzogen sind.[76]

3.2. Datenschutzrechtliche Anforderungen

Nachfolgend werden die datenschutzrechtlichen Anforderungen der DSGVO an die Nutzung von Cloud-Diensten, die Adressaten einer US-amerikanischen Herausgabeverpflichtung sein könnten, durch die Verwaltung näher beleuchtet. Dazu werden zunächst die Anwendbarkeit der DSGVO, Cloud-Dienste als Auftragsverarbeitung sowie die allgemeinen Rechtmäßigkeitsvoraussetzungen für die Nutzung von Cloud-Diensten erörtert. Anschließend wird zwischen der Nutzung von Cloud-Diensteanbietern mit Sitz in der EU[77] und solchen mit Sitz in den USA unterschieden.

3.2.1. Anwendbarkeit der DSGVO

Wenn eine **deutsche Behörde** personenbezogene Daten an einen Cloud-Diensteanbieter weitergibt, ist der sachliche und der räumliche Anwendungsbereich der DSGVO unabhängig vom Sitz des Anbieters des Cloud-Dienstes eröffnet. Der sachliche und der räumliche Anwendungsbereich der DSGVO ist außerdem eröffnet, wenn ein **Unternehmen mit Sitz in Deutschland** die personenbezogenen Daten, die zuvor eine Behörde an diese übermittelt hat, an einen Empfänger in einem Drittland weiterübermittelt.[78]

Der **sachliche Anwendungsbereich** richtet sich nach **Art. 2 Abs. 1 DSGVO** auf die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie auf die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. **Personenbezogene Daten** sind nach **Art. 4 Nr. 1 DSGVO** alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Natürliche Personen sind danach identifizierbar, wenn sie direkt oder indirekt, wie unter anderem mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten oder zu einer Online-Kennung, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden können. Behörden arbeiten mit einer Vielzahl unterschiedlicher Daten, die unter anderem nach der genannten Definition auch die Identifikation einer Person ermöglichen, z.B. Daten zum Namen, Alter oder Herkunft. Insoweit ist der sachliche Anwendungsbereich der DSGVO eröffnet. Soweit demgegenüber **rein sachbezogene Daten und Informationen** verarbeitet werden, die auch eine mittelbare Identifizierbarkeit einer natürlichen Person nicht ermöglichen, ist der

---

76 Vgl. ähnlich zur Relevanz des Orts der Datenaufbewahrung, Heckmann/Scheurer, in: Heckmann/Paschke, jurisPK-Internetrecht, 7. Aufl. Stand: 04.01.2024, Kap. 9 Rn. 773.

77 Im Folgenden wird unter EU der gesamte räumliche Anwendungsbereich der DSGVO einschließlich des Europäischen Wirtschaftsraum (EWR) einschließlich Island, Liechtenstein und Norwegen verstanden, siehe dazu Beschluss des Gemeinsamen EWR-Ausschusses Nr. 154/2018 vom 06.07.2018.

78 Siehe zum sachlichen und räumlichen Anwendungsbereich bei Übermittlungen in ein Drittland, EuGH, Urteil vom 16.07.2020 - C-311/18, Rn. 83; Rn. 89; vgl. ferner Jungkind/Raspé/Schramm, Risikoanalyse und zusätzliche Maßnahmen – Konzerninterner Datentransfer nach „Schrems II“, NZG 2020, 1056: „Das betrifft auch Datenströme innerhalb einer Unternehmensgruppe; die DSGVO kennt kein Konzernprivileg“.

Anwendungsbereich der DSGVO allerdings nicht eröffnet.[79] Die **Verarbeitung** von Daten beschreibt nach **Art. 4 Nr. 2 DSGVO** jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie unter anderem das Erheben, die Organisation, das Ordnen, die Speicherung, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung. Im Fall des Einsatzes eines Cloud-Diensteanbieters durch eine Behörde werden diejenigen Daten, die aufbewahrt bzw. gespeichert werden sollen, **an den Cloud-Diensteanbieter weitergegeben**. Wegen der Natur der Sache des Cloud-Computings ist davon auszugehen, dass dieser Vorgang automatisiert abläuft.[80]

Zudem setzt der **räumliche Anwendungsbereich** gemäß Art. 3 Abs. 1 DSGVO voraus, dass die Verarbeitung von personenbezogenen Daten **im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen** oder **eines Auftragsverarbeiters in der EU** erfolgt, **unabhängig davon, ob die Verarbeitung selbst in der EU** stattfindet. **Verantwortlicher** ist nach Art. 4 Nr. 7 DSGVO unter anderem die Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. **Auftragsverarbeiter** ist nach Art. 4 Nr. 8 DSGVO unter anderem die Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten **im Auftrag des Verantwortlichen** verarbeitet. Das Verhältnis zwischen dem Verantwortlichen und dem Auftragsverarbeiter und Anforderungen an die Auftragsverarbeitung regelt **Art. 28 Abs. 1 DSGVO** (näher zu Art. 28 DSGVO nachfolgend unter 3.2.2.).[81] Wenn somit eine deutsche Behörde einen Cloud-Dienst nutzen möchte und dabei personenbezogene Daten verarbeitet, ist unabhängig vom Sitz des Anbieters des Cloud-Dienstes auch der räumliche Anwendungsbereich der DSGVO eröffnet, weil die datenverarbeitende **Behörde eine Niederlassung innerhalb der EU** hat. Der tatsächliche Ort der Datenverarbeitung ist nach Art. 3 Abs. 1 DSGVO ausdrücklich irrelevant.

3.2.2. Cloud-Dienste als Auftragsverarbeitung

Nach der überwiegenden Auffassung sind Cloud-Dienste ein **typischer Fall der Auftragsverarbeitung im Sinne des Art. 28 DSGVO**, jedenfalls solange der Cloud-Dienstanbieter die personenbezogenen Daten nicht für eigene Zwecke verarbeitet.[82] Dies wird lediglich dann problematisiert und die Nutzung von Cloud-Diensten als Funktionsübertragung qualifiziert, wenn „eigenmoti-

---

79 Vgl. ausführlich dazu Wissenschaftliche Dienste des Deutschen Bundestages, DSGVO und Nutzung US-amerikanischer Cloud-Dienste, WD 3 - 3000 - 102/21, 03.06.2021, S. 5 m.w.N.

80 Wissenschaftliche Dienste des Deutschen Bundestages, DSGVO und Nutzung US-amerikanischer Cloud-Dienste, WD 3 - 3000 - 102/21, 03.06.2021, S. 6.

81 Spoerr, in: Wolff/Brink/v. Ungern-Sternberg, BeckOK Datenschutzrecht, 46. Edition (Stand: 01.05.2022), DSGVO Art. 28 Rn. 24c; vgl. ferner Wissenschaftliche Dienste des Deutsche Bundestages, DSGVO und Nutzung US-amerikanischer Cloud-Dienste, WD 3 - 3000 - 102/21, 03.06.2021, S. 6 m.w.N.

82 Spoerr, in: Wolff/Brink/v. Ungern-Sternberg, BeckOK Datenschutzrecht, 46. Edition (Stand: 01.05.2022), DSGVO Art. 28 Rn. 24c mit Hinweis auf European Data Protection Board (EDPB), Leitlinien 07/2020 zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DSGVO, Version 2.0, 07.07.2021, Rn. 30; Heckmann/Scheurer, in: Heckmann/Paschke, jurisPK-Internetrecht, 7. Aufl. Stand: 04.01.2024, Kap. 9, Rn. 299, 819 m.w.N.; Gabel/Lutz, in: Taeger/Gabel, DSGVO - BDSG - TTDSG, 4. Aufl. 2022, DSGVO Art. 28 Rn. 22.

vierte Verarbeitungen der ihnen überlassenen und der durch die Nutzung ihrer Systeme erlangten Daten“ vorgenommen werden.[83] Davon ausgehend, dass die genutzten Daten nicht für eigene Zwecke verarbeitet werden und dies vertraglich abgesichert ist, ist somit Verantwortlicher diejenige Behörde, die einen Cloud-Dienst nutzen möchte, und Auftragsverarbeiter dasjenige Unternehmen, das den Cloud-Dienst anbietet.

Nach Art. 28 Abs. 1 DSGVO darf der Verantwortliche nur mit Auftragsverarbeitern arbeiten, „die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet“. Den Verantwortlichen trifft insoweit eine Auswahlverantwortung.[84]

3.2.3. Allgemeine Rechtmäßigkeitsvoraussetzungen

Im rechtswissenschaftlichen Schrifttum ist umstritten, an welchen Rechtmäßigkeitsvoraussetzungen die Auftragsverarbeitung zu messen ist.[85] Dies klärte die Datenschutzkonferenz – das Gremium der unabhängigen deutschen Datenschutzaufsichtsbehörden – dahingehend, dass es für „die Weitergabe von personenbezogenen Daten an den Auftragsverarbeiter und die Verarbeitung durch den Auftragsverarbeiter […] regelmäßig **keiner weiteren Rechtsgrundlage im Sinne von Art. 6 bis 10 DSGVO als derjenigen** [bedarf], **auf die der Verantwortliche selbst die Verarbeitung stützt**“.[86] Demnach wäre keine gesonderte Rechtsgrundlage für die Weitergabe an den Auftragsverarbeiter erforderlich. Maßgeblich wäre allein die Rechtsgrundlage für die Datenverarbeitung, auf die die Behörde als Verantwortliche selbst die Verarbeitung stützt. Dies kann nur im Einzelfall der Tätigkeiten der Behörden bewertet werden.

Soweit allerdings davon ausgegangen wird, dass die Weitergabe der personenbezogenen Daten an den Auftragsverarbeiter selbst nach Art. 6 Abs. 1 UAbs. 1 Satz 1 DSGVO rechtmäßig sein muss, kommen in erster Linie Buchstaben e) und f) in Betracht.[87] Nach **Art. 6 Abs. 1 UAbs. 1 Satz 1 Buchstabe e) DSGVO** ist die Verarbeitung rechtmäßig, wenn sie für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. In diesem Zusammenhang gilt nach § 6 Abs. 3

---

83 Siehe dazu Ingold, in: Sydow/Marsch, DSGVO/BDSG, 3. Aufl. 2022, DSGVO Art. 28 Rn. 23.

84 Anstatt vieler Martini, in: Paal/Pauly, DSGVO/BDSG, 3. Aufl. 2021, DSGVO Art. 28 Rn. 1.

85 Vgl. zum Streit Spoerr, in: Wolff/Brink/v. Ungern-Sternberg, BeckOK Datenschutzrecht, 46. Ed. 01.05.2022, DSGVO Art. 28 Rn. 29b ff.; Hartung, in: Kühling/Buchner, 4. Aufl. 2024, DSGVO Art. 28 Rn. 13; siehe zur Ansicht, das Art. 6 DSGVO nicht geprüft werden muss, Martini, in: Paal/Pauly, DSGVO/BDSG, 3. Aufl. 2021, DSGVO Art. 28 Rn. 8a ff., wonach allerdings Art. 44 ff. DSGVO anzuwenden sind.

86 Datenschutzkonferenz, Kurzpapier Nr. 13 Auftragsverarbeitung, Art. 28 DS-GVO, 17.12.2018, S. 2; siehe ferner Bayerischer Landesbeauftragte für den Datenschutz, Auftragsverarbeitung Orientierungshilfe, 2019, S. 7.

87 Vgl. Ingold, in: Sydow/Marsch, DSGVO/BDSG, 3. Aufl. 2022, DSGVO Art. 28 Rn. 29; zur Problematik der Einwilligung nach Art. 6 UAbs. 1 Satz 1 Buchstabe a) DSGVO in Über-/Unterordnungsverhältnissen, Wissenschaftliche Dienste des Deutschen Bundestages, DSGVO und Nutzung US-amerikanischer Cloud-Dienste, WD 3 - 3000 - 102/21, 03.06.2021, S. 7 m.w.N; vgl. dazu auch Schantz, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, DSGVO, Art. 6 Abs. 1 Rn. 13; vgl. ähnlich Bayerischer Landesbeauftragte für den Datenschutz, Auftragsverarbeitung Orientierungshilfe, 2019, S. 7.

UAbs. 1 Satz 1 DSGVO, dass die Rechtsgrundlage für die Verarbeitung durch Unionsrecht oder Recht der Mitgliedstaaten, dem der Verantwortliche unterliegt, festgelegt wird. In Deutschland regelt in diesem Zusammenhang § 3 des Bundesdatenschutzgesetzes (BDSG)[88] als allgemeine Regel, dass die Verarbeitung personenbezogener Daten durch eine öffentliche Stelle zulässig ist, wenn sie zur Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgabe oder in Ausübung öffentlicher Gewalt, die dem Verantwortlichen übertragen wurde, erforderlich ist. In der rechtswissenschaftlichen Kommentarliteratur wird die Vorschrift als Generalklausel verstanden, die nur für „eine Datenverarbeitung mit geringer Eingriffsintensität“ gelten könne und subsidiär zu bereichsspezifischen Vorschriften sei.[89] Nach **Art. 6 Abs. 1 UAbs. 1 Satz 1 Buchstabe f) DSGVO** ist die Verarbeitung ferner rechtmäßig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. So können unter anderem Kostengründe als berechtigtes Interesse in Betracht kommen. In der Abwägung wären insbesondere das Recht auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG und das Recht auf den Schutz personenbezogener Daten nach Art. 8 der Charta der Grundrechte der Europäischen Union (GRCh)[90] zu berücksichtigen.[91]

3.2.4. Nutzung von Cloud-Diensten von Anbietern mit Sitz in der EU

Wenn der beauftragte Cloud-Diensteanbieter einen Sitz in der EU hat, die Daten auf einem Server innerhalb der EU speichert und insbesondere auch nicht in einen US-amerikanischen Konzern eingebunden ist, dürfte eine Herausgabeverpflichtung von US-amerikanischen Sicherheitsbehörden mangels eines hinreichenden Bezugs zur US-amerikanischen Gerichtsbarkeit ausgeschlossen sein. Die Nutzung dieser Cloud-Dienste richtet sich insoweit nach den zuvor erläuterten Rechtmäßigkeitsvoraussetzungen.

In Rechtsprechung und Schrifttum ist allerdings nicht abschließend geklärt, ob es sich bei der Nutzung von Cloud-Diensten eines Anbieters mit Sitz in der EU um eine Übermittlung an ein Drittland im Sinne des Art. 44 DSGVO handelt, wenn der Anbieter selbst Tochtergesellschaft einer US-amerikanischen Muttergesellschaft ist. Für eine Übermittlung an ein Drittland gelten die erhöhten Rechtmäßigkeitsanforderungen nach Art. 44 ff. DSGVO.

---

88 Bundesdatenschutzgesetz vom 30.06.2017 (BGBl. I S. 2097), zuletzt geändert am 22.12.2023 (BGBl. 2023 I Nr. 414).

89 Vgl. Lang, in: Taeger/Gabel, DSGVO - BDSG – TTDSG, 4. Aufl. 2022, BDSG § 3 Rn. 15 m.w.N.; vgl. ferner zu Art. 6 Abs. 1 UAbs. 1 Satz 1 lit. e DSGVO und zu bereichsspezifischen Vorschriften, Reimer, in: Sydow/Marsch, DSGVO/BDSG, 3. Aufl. 2022, DSGVO Art. 6 Rn. 66 f.

90 Charta der Grundrechte der Europäischen Union vom 18.12.2000 (ABl. der Europäischen Gemeinschaften C 364).

91 Vgl. dazu Wissenschaftliche Dienste des Deutschen Bundestages, DSGVO und Nutzung US-amerikanischer Cloud-Dienste, WD 3 - 3000 - 102/21, 03.06.2021, S. 8.

3.2.4.1. Gefahr der Übermittlung in ein Drittland?

In der Literatur wird zum Teil von einem weiten Übermittlungsbegriff ausgegangen. Danach sei es für eine Übermittlung im Sinne des Art. 44 Satz 1 DSGVO ausreichend, dass der Zugriff auf personenbezogene Daten aus einem Drittland überhaupt ermöglicht werde. Irrelevant sei indes, ob ein Zugriff tatsächlich erfolgt sei.[92] Dies wird unter anderem mit dem Sinn und Zweck von Art. 44 Satz 2 DSGVO begründet, weil schon ein „latentes Risiko" eines unzulässigen Datenzugriffs dazu führe, dass das durch die DSGVO gewährleistete Schutzniveau für natürliche Personen untergraben werden könnte.[93] Danach müssten bei einer Übermittlung von personenbezogenen Daten die Voraussetzungen der Art. 44 ff. DSGVO berücksichtigt werden (dazu unter 3.2.5.).

Das in diesem Zusammenhang bestehende weite Begriffsverständnis wurde unter anderem innerhalb der vergaberechtlichen Rechtsprechung und durch das Bundeskartellamt in vergaberechtlichen Fällen mehrfach abgelehnt.[94] Ein bloßes latentes Risiko, in der Zukunft einer etwaigen Herausgabeverpflichtung ausgesetzt zu werden, könne den Tatbestand der Übermittlung im Sinn des Art. 44 Satz 1 DSGVO nicht erfüllen.[95] Entsprechend nahm mittlerweile auch die Datenschutzkonferenz dahingehend Stellung, dass die

> Gefahr allein, dass – etwa über gesellschaftsrechtliche Weisungsrechte – die Drittlands-Muttergesellschaft eines EWR-Unternehmens dieses anweisen könnte, oder dass öffentliche Stellen von Drittländern unmittelbar EWR-Unternehmen anweisen könnten, personenbezogene Daten in ein Drittland zu übermitteln, [nicht] genügt […], um eine Übermittlung in ein Drittland i.S.d. Art. 44 ff. DSGVO anzunehmen.[96]

Jedenfalls würde eine Herausgabeverpflichtung von Daten gegenüber dem Cloud-Diensteanbieter mit Sitz in Deutschland oder der EU gegen Art. 48 DSGVO verstoßen, wonach

> [j]egliches Urteil eines Gerichts eines Drittlands und jegliche Entscheidung einer Verwaltungsbehörde eines Drittlands, mit denen von einem Verantwortlichen oder einem Auftragsverarbeiter die Übermittlung oder Offenlegung personenbezogener Daten verlangt wird, […] unbeschadet anderer Gründe für die Übermittlung gemäß diesem Kapitel jedenfalls nur

---

92 Vgl. dazu Pauly, in: Paal/Pauly, DSGVO/BDSG, 3. Aufl. 2021, DSGVO Art. 44 Rn. 5; Juarez, in: BeckOK Datenschutzrecht, 46. Ed. 01.05.2023, DSGVO Art. 44 Rn. 15: „Zugänglichmachung oder Abrufbarkeit von Daten aus dem Drittland"; siehe ferner VK Baden-Württemberg, Beschluss vom 13.07.2022 - 1 VK 23/22, NZBau 2022, 629 (631 f. Rn. 62).

93 Vgl. Juarez, in: BeckOK Datenschutzrecht, 46. Ed. 01.05.2023, DSGVO Art. 44 Rn. 15; siehe auch VK Baden-Württemberg, Beschluss vom 13.07.2022 - 1 VK 23/22, NZBau 2022, 629 (631 f. Rn. 62)

94 Vgl. OLG Karlsruhe, Beschluss vom 07.09.2022 - 15 Verg 8/22, BeckRS 2022, 22588 (Rn. 42); ähnlich im Zusammenhang mit § 80 Abs. 2 SGB X, BKartA, Beschluss vom 13.02.2023 - VK 2-114/22, ZD 2023, 454 (455); bestätigend BKartA, Beschluss vom 20.06.2023 - VK 2-34/23, ZD 2023, 740 (741 Rn. 74).

95 OLG Karlsruhe, Beschluss vom 07.09.2022 - 15 Verg 8/22, BeckRS 2022, 22588 (Rn. 42).

96 Datenschutzkonferenz, Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 31. Januar 2023, 2023, S. 1.

> dann anerkannt oder vollstreckbar werden [dürfen], wenn sie auf eine in Kraft befindliche internationale Übereinkunft wie etwa ein Rechtshilfeabkommen zwischen dem ersuchenden Drittland und der Union oder einem Mitgliedstaat gestützt sind.

Ohne eine entsprechende internationale Übereinkunft ist folglich eine Herausgabe der Daten durch den Anbieter mit Sitz in Deutschland oder der EU aus datenschutzrechtlichen Gründen nach Art. 48 DSGVO grundsätzlich unzulässig.[97] So geht auch das European Data Protection Board (EDPB) davon aus, dass die Übermittlung infolge einer Herausgabeverpflichtung nur unter Berücksichtigung von Art. 6 DSGVO und Art. 49 DSGVO zulässig sei.[98] Vereinzelt wird darüber hinaus auch argumentiert, dass keine Übermittlung im Sinne des Art. 44 DSGVO vorliege, wenn „die USA als unsicheres Drittland die Offenlegung von in der EU gespeicherten personenbezogenen Daten [erzwingen will] und […] diese Offenlegung ohne Beteiligung des in der EU niedergelassenen Auftragsverarbeiters oder Verantwortlichen“ geschieht.[99] In der rechtswissenschaftlichen Literatur wird indes auch auf das Verhältnis von Art. 48 DSGVO zu Art. 49 Abs. 1 Buchstabe e) DSGVO hingewiesen. So könnten zur Herausgabe verpflichtete Unternehmen mit Art. 48 DSGVO argumentieren, dass die Vorschrift nur „unbeschadet anderer Gründe für die Übermittlung gemäß diesem Kapitel“ gelte und dadurch Übermittlungen „zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen“ nach Art. 49 Abs. 1 lit. e) DSGVO für die Unternehmen weiter möglich seien.[100]

3.2.4.2. Zuverlässigkeit nach Art. 28 DSGVO

Aus Sicht der Datenschutzkonferenz ist vielmehr im Rahmen der **Prüfung der Zuverlässigkeit** die oben genannte **Gefahr bzw. das latente Risiko** zu berücksichtigen, ob der Auftragsverarbeiter selbst oder seine Muttergesellschaft in den USA Adressat von einer Herausgabeverpflichtung sein könnte und er oder sie aufgrund dessen Daten herausgeben müsste:

> […]
>
> 3. Soweit das Risiko besteht, dass eine Norm oder Praxis, die nach EU-Recht unzulässige Verarbeitungen personenbezogener Daten verlangen kann, auch auf EWR-Tochtergesellschaften von Drittlands-Unternehmen anwendbar ist, **genügt die Verarbeitung durch eine EWR-Tochtergesellschaft als Auftragsverarbeiter für sich genommen nicht**, um eine **Zuverlässigkeit im Sinne von Art. 28 Abs. 1 DSGVO** zu erreichen. Soweit eine Norm oder Praxis eines Drittlands

---

97 Weder der neue Angemessenheitsbeschluss vom 10.07.2023 noch das EU-US-„Umbrella Agreement“ sind nach der überwiegenden Auffassung solche internationalen Übereinkünfte, Schröder, in: Kühling/Buchner, DSGVO/BDSG, 4. Aufl. 2024, DSGVO Art. 48 Rn. 16; vgl. ferner European Data Protection Board, Annex. Initial legal assessment of the impact of the US CLOUD Act on the EU legal framework for the protection of personal data and the negotiations of an EU-US Agreement on cross-border access to electronic evidence, 10.07.2019, S. 3.

98 European Data Protection Board, Annex. Initial legal assessment of the impact of the US CLOUD Act on the EU legal framework for the protection of personal data and the negotiations of an EU-US Agreement on cross-border access to electronic evidence, 10.07.2019, S. 3 ff.

99 Vgl. dazu Kremer, Arbeitsteilige Verarbeitungen: Wer übermittelt die Daten ans Drittland?, CR 2021, 719 (723).

100 Rath/Spies, CLOUD Act: Selbst für die Wolken gibt es Grenzen, CCZ 2018, 229 (230).

die abstrakte Gefahr einer nach EU-Recht unzulässigen Übermittlung personenbezogener Daten aus dem EWR in ein Drittland durch eine als Auftragsverarbeiter tätige Stelle in dem EWR – z.B. die EWR-Tochtergesellschaft eines Drittlands-Unternehmens – begründet, sind an die Sorgfalt der **Zuverlässigkeitsprüfung im Sinne von Art. 28 Abs. 1 DSGVO besonders hohe Anforderungen** zu stellen, die dieser Gefahr Rechnung tragen.

4. Dies erfordert zunächst eine **Bewertung sämtlicher Umstände des Einzelfalls**, ob der Auftragsverarbeiter und/oder die von ihm verarbeiteten Daten unter diese drittstaatliche Norm oder Praxis fallen und wenn ja, ob der Auftragsverarbeiter dennoch hinreichend Garantien dafür bietet, dass es nicht zu Verarbeitungen kommt, die nach den Maßstäben der DSGVO bzw. des anwendbaren mitgliedstaatlichen Rechts unzulässig sind.[101]

Zu diesen Umständen des Einzelfalls zählt die Datenschutzkonferenz unter anderem die Prüfung der extraterritorialen Anwendbarkeit des Rechts eines Drittstaats (vgl. dazu oben bereits unter 2.2.2. und den völkerrechtlichen Einwänden) sowie das Risiko, dass die Drittlands-Muttergesellschaft eines EWR-Tochterunternehmens dieses anweisen könnte, personenbezogene Daten in ein Drittland zu übermitteln, oder auch den Ausschluss unzulässiger Übermittlungen durch geeignete technische und organisatorische Maßnahmen. Im Ergebnis müsse jedenfalls der Verantwortliche in der Lage sein, „dass ein Auftragsverarbeiter die Anforderungen aus Art. 28 Abs. 1 und ErwG 81 DSGVO an Fachwissen, Zuverlässigkeit und Ressourcen erfüllt“.[102]

3.2.5. Nutzung von Cloud-Diensten von Anbietern mit Sitz in den USA

Im Fall der Nutzung von Cloud-Diensten eines US-amerikanischen Unternehmens sind über die Rechtmäßigkeitsvoraussetzungen nach Art. 6 DSGVO hinaus auch **die Art. 44 ff. DSGVO** für die Übermittlung von Daten in Drittländer zu berücksichtigen.[103] Zu den Anforderungen des Art. 6 DSGVO wird auf die Ausführungen unter 3.2.3. Bezug genommen. Außerdem haben die Wissenschaftlichen Dienste des Deutschen Bundestages in der Ausarbeitung „DSGVO und Nutzung US-amerikanischer Cloud-Dienste“ die rechtlichen Voraussetzungen in Bezug auf die deutsche Bundesverwaltung sowie die US-amerikanischen Cloud-Anbieter oder Unternehmen mit Sitz in Deutschland, die die Dienste solcher Anbieter verwenden, bereits ausführlich erörtert.[104] Auf

101 Datenschutzkonferenz, Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 31. Januar 2023, 2023, S. 2; Hervorhebungen nicht im Original.

102 Datenschutzkonferenz, Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 31. Januar 2023, 2023, S.4

103 Vgl. Klose/Momsen, § 33 Überblick über das Datenschutzsanktionenrecht in den USA, in: Klaas/Momsen/Wybitul Datenschutzsanktionsrecht, Rn. 62.

104 Wissenschaftliche Dienste des Deutschen Bundestages, DSGVO und Nutzung US-amerikanischer Cloud-Dienste, WD 3 - 3000 - 102/21, 03.06.2021.

diese wird ebenfalls verwiesen. Relevante rechtliche Entwicklungen, wie der sog. Angemessenheitsbeschluss der Europäischen Kommission zum **EU-U.S. Data Privacy Framework** (DPF),[105] werden bei den Ausführungen zusätzlich berücksichtigt.

Nach **Art. 45 Abs. 1 DSGVO** darf eine Übermittlung personenbezogener Daten an ein Drittland vorgenommen werden, wenn die Kommission beschlossen hat, dass das betreffende Drittland, ein Gebiet oder ein oder mehrere spezifische Sektoren in diesem Drittland ein **angemessenes Schutzniveau** bieten. Eine solche **Datenübermittlung bedarf keiner besonderen Genehmigung**. Die Kommission berücksichtigt nach Art. 45 Abs. 2 DSGVO bei der Prüfung der Angemessenheit des gebotenen Schutzniveaus unter anderem die in dem jeweiligen Land geltenden einschlägigen Rechtsvorschriften sowohl allgemeiner als auch sektoraler Art, auch in Bezug auf öffentliche Sicherheit, Verteidigung, nationale Sicherheit und Strafrecht sowie Zugang der Behörden zu personenbezogenen Daten, sowie die Anwendung dieser Rechtsvorschriften.

Für Datenübermittlungen in die USA hat die EU-Kommission am 10. Juli 2023 einen **neuen Angemessenheitsbeschluss, den DPF**, gefasst, nachdem vorherige Angemessenheitsbeschlüsse durch den Europäischen Gerichtshof (EuGH) jeweils für unwirksam erklärt wurden.[106] Da der EuGH entschied, dass in den USA kein angemessenes Schutzniveau für die Übermittlung personenbezogener Daten besteht,[107] erließ der US-amerikanische Präsident Biden am 7. Oktober 2022 die E.O. 14086, die in Reaktion auf die Urteile des EuGH ein hinreichend angemessenes Schutzniveau auch für Datenübermittlungen in die USA begründen sollen. Allerdings wird in der rechtswissenschaftlichen Literatur bezweifelt, dass die durch die E.O. 14086 festgelegten Regelungen einer erneuten Entscheidung des EuGH standhalten könnten.[108] Trotz dieser Zweifel ist dieser Angemessenheitsbeschluss vom 10. Juli 2023 wirksam.

---

105 Angemessenheitsbeschluss, Commission Implementing Decision of 10.07.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework, C(2023) 4745 final.

106 EuGH, Urteil vom 06.10.2015 - Rs. C-362/14 (Schrems I) zur Unwirksamkeit der Entscheidung der Kommission vom 26.07.2000 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 („Safe-Harbor“; ABl. L 215 vom 25.08.2000, S. 7-47); EuGH, Urteil vom 16.07.2020 - C-311/18 (Schrems II) zur Unwirksamkeit des Durchführungsbeschlusses (EU) 2016/1250 der Kommission vom 12.07.2016 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes („Privacy Shield“; ABl. L 207 vom 01.08.2016, S. 1-112).

107 Durchführungsbeschluss (EU) 2023/1795 der Kommission vom 10.07.2023 gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates über die Angemessenheit des Schutzniveaus für personenbezogene Daten nach dem Datenschutzrahmen EU-USA (ABl. L 231/118).

108 Vgl. anstatt vieler zu „Schrems-III“, Roßnagel, Digitale Souveränität im Datenschutzrecht, MMR 2023, 64 (68); vgl. ferner zur Möglichkeit der Nichtigerklärung, Datenschutzkonferenz, Anwendungshinweise zum Angemessenheitsbeschluss der Europäischen Kommission zum Datenschutzrahmen EU-USA (EU-US Data Privacy Framework) vom 10. Juli 2023, 04.09.2023, S. 31.

Ein Rückgriff auf den DPF für Datenübermittlungen im Sinne des Art. 45 DSGVO setzt voraus, dass die **Übermittlung an zertifizierte Stellen** erfolgt.[109] Denn nach 2.1.1. des DPF beruht dieser

> auf einem Zertifizierungssystem, mit dem sich US-Organisationen zu einer Reihe von Datenschutzgrundsätzen verpflichten – die „Grundsätze des Datenschutzrahmens EU-USA", einschließlich der Zusatzgrundsätze (im Folgenden zusammen „Grundsätze") – herausgegeben vom U.S. Department of Commerce (Handelsministerium) und in Anhang I dieses Beschlusses enthalten. […] Um für eine Zertifizierung im Rahmen des Datenschutzrahmens EU-USA infrage zu kommen, muss eine Organisation den Untersuchungs- und Durchsetzungsbefugnissen der Federal Trade Commission (FTC) oder des U.S. Department of Transportation (Verkehrsministerium) […] unterliegen. Die Grundsätze gelten unmittelbar vom Zeitpunkt der Zertifizierung an. […]

Im Fall, dass der US-amerikanische Anbieter von Cloud-Diensten folglich keine Zertifizierung nach dem DPF besitzt, gelten die übrigen geeigneten Garantien bzw. Maßnahmen für eine Übermittlung an ein Drittland, wie unter anderem von Standard-Vertragsklauseln oder Binding Corporate Rules.[110]

Übermittlungen in Drittstaaten können außerdem grundsätzlich aufgrund einer der Bedingungen nach **Art. 49 Abs. 1 UAbs. 1 DSGVO im Einzelfall zulässig** sein. Dabei ist allerdings zum einen zu berücksichtigen, dass die Ausnahmekonstellationen eng auszulegen sind.[111] Zum anderen erscheinen die in Art. 49 DSGVO geregelten Bedingungen weniger auf die vorliegende Konstellation zu passen. Vor allem die Einwilligung (Art. 49 Abs. 1 Buchstabe a) DSGVO) wäre sowohl aus praktischen Gründen als auch wegen des Subordinationsverhältnisses zwischen der Verwaltung und den Betroffenen problematisch.[112] Im Übrigen regelt Art. 49 Abs. 3 DSGVO, dass Art. 49 Abs. 1 UAbs. 1 Buchstabe a) DSGVO mit der Einwilligung nicht für Tätigkeiten gilt, die Behörden in Ausübung ihrer hoheitlichen Befugnisse durchführen. Dies gilt auch für Art. 49 Abs. 1 UAbs. 1 Buchstabe b) und c) DSGVO. Ferner erscheint die Übermittlung aus wichtigen Gründen des öffentlichen Interesses nach Art. 49 Abs. 1 UAbs. 1 Buchstabe d) DSGVO nicht einschlägig zu sein. Denn Erwägungsgrund 112 der DSGVO benennt als Beispiele vielmehr „den internationalen Datenaustausch zwischen Wettbewerbs-, Steuer- oder Zollbehörden, zwischen Finanzaufsichtsbehörden oder zwischen für Angelegenheiten der sozialen Sicherheit oder für die öffentliche Gesundheit zuständigen Diensten, beispielsweise im Falle der Umgebungsuntersuchung bei ansteckenden Krankheiten oder zur Verringerung und/oder Beseitigung des Dopings im Sport". Letztlich dürften die Ausnahmen nach Art. 49 Abs. 1 UAbs. 1 Buchstabe e) bis g) ebenfalls nicht einschlägig ein.

---

109 Vgl. zur Zertifizierung, Glocker, Der neue Angemessenheitsbeschluss zum EU-U.S. Data Privacy Framework, RDi 2023, 465 (467).

110 Ausführlich dazu Wissenschaftliche Dienste des Deutschen Bundestages, DSGVO und Nutzung US-amerikanischer Cloud-Dienste, WD 3 - 3000 - 102/21, 03.06.2021, S. 10 ff.

111 Vgl. Zerdick, in: Ehmann/Selmayr, DSGVO, 2. Aufl. 2018, Art. 49 Rn. 4 m.w.N.

112 Dazu bereits oben unter 3.2.3. Vgl. ferner Wissenschaftliche Dienste des Deutschen Bundestages, DSGVO und Nutzung US-amerikanischer Cloud-Dienste, WD 3 - 3000 - 102/21, 03.06.2021, S. 15.

Bereits aus US-amerikanischer Perspektive ist schließlich der **Speicherort der Daten** durch das US-amerikanische Unternehmen für Herausgabeverpflichtungen irrelevant (vgl. dazu oben zum CLOUD Act 2.1.1.). Auch aus einer datenschutzrechtlichen Perspektive erscheint diese Maßnahme, Daten vor Zugriffen aus den USA zu schützen, indem sie innerhalb der EU auf Servern gespeichert werden, entsprechend fraglich.[113] Denn Herausgabeverpflichtungen von US-amerikanischen Sicherheitsbehörden an US-amerikanische Unternehmen, die der DSGVO unterliegen, sind nach Art. 48 DSGVO unzulässig, wenn kein internationales Abkommen besteht und sich auch im Übrigen keine Rechtsgrundlage aus Art. 6 DSGVO und Art. 49 DSGVO ergibt. Entsprechend gelten auch in diesem Zusammenhang die Ausführungen zur Prüfung der Zuverlässigkeit des Auftragsverarbeiters nach Art. 28 DSGVO.

***

113 So im Ergebnis auch Wissenschaftliche Dienste des Deutschen Bundestages, DSGVO und Nutzung US-amerikanischer Cloud-Dienste, WD 3 - 3000 - 102/21, 03.06.2021, S. 13.