Der Bayerische Landesbeauftragte
für den Datenschutz

Erste Hilfe zum Angemessenheitsbeschluss für das EU-U.S. Data Privacy Framework

Aktuelle Kurz-Information 51

Stichwörter: Angemessenheitsbeschluss, Art. 45 DSGVO – Data Privacy Framework List – Datenschutzrahmen EU-USA – EU-U.S. Data Privacy Framework – Rechenschaftspflicht, Art. 5 Abs. 2 DSGVO – Zertifizierung – Zwei-Stufen-Prüfung | **Stand:** 1. August 2023

Was sind die Kernaussagen dieser Aktuellen Kurz-Information?

- Der Angemessenheitsbeschluss für das EU-U.S. Data Privacy Framework bestätigt, dass die USA ein angemessenes Schutzniveau für personenbezogene Daten gewährleisten, die aus der EU an die am EU-U.S. Data Privacy Framework teilnehmenden Unternehmen übermittelt werden.
- Am EU-U.S. Data Privacy Framework nehmen US-Unternehmen teil, die hierfür zertifiziert sind und deshalb auf der „Data Privacy Framework List" stehen.
- Der Angemessenheitsbeschluss vermittelt nicht allein eine Rechtsgrundlage für eine Drittlandübermittlung; Art. 5 ff. DSGVO sind kumulativ zu beachten.

Am 10. Juli 2023 hat die Europäische Kommission einen **Angemessenheitsbeschluss für das EU-U.S. Data Privacy Framework** (deutsch: Datenschutzrahmen EU-USA, im Folgenden: Angemessenheitsbeschluss) erlassen.[1] Damit attestiert sie den Vereinigten Staaten von Amerika (USA) ein **angemessenes Schutzniveau** für personenbezogene Daten, die innerhalb dieses Rahmens aus der Europäischen Union (EU) an US-Unternehmen als Datenimporteure übermittelt werden. Der Angemessenheitsbeschluss ist ein Durchführungsrechtsakt (Art. 291 Abs. 2 Vertrag über die Arbeitsweise der Europäischen Union – AEUV) in der Form eines an die Mitgliedstaaten gerichteten Beschlusses (Art. 288 Abs. 4 AEUV); ihm ist ein besonders geregeltes Verfahren vorangegangen.[2] 1

Der Erlass des Angemessenheitsbeschlusses beendet eine lange Wartezeit für Verantwortliche in der EU, hatte doch der Europäische Gerichtshof mit seinem „Schrems II"-Urteil[3] den Vorgänger des EU-U.S. Data Privacy Framework, das „EU-U.S. Privacy Shield", beanstandet und so Datenübermittlungen in die USA auf den in der Praxis eher „steinigen" Weg der geeigneten Garantien gemäß Art. 46 Datenschutz-Grundverordnung (DSGVO) verwiesen. 2

Zu internationalen Datentransfers hat der Bayerische Landesbeauftragte für Datenschutz erst kürzlich eine umfassende Orientierungshilfe[4] veröffentlicht. Dieser Beitrag konzentriert sich daher auf die Erläuterung der Eckpunkte des Angemessenheitsbeschlusses und auf die Darstellung der Folgen für den bayerischen öffentlichen Sektor. 3

1. Was ist die Ausgangslage?

Vor dem neuen Angemessenheitsbeschluss wurde die Übermittlung personenbezogener Daten in die USA in erster Linie auf **geeignete Garantien gemäß Art. 46 Abs. 1 DSGVO** 4

Der Bayerische Landesbeauftragte für den Datenschutz
80538 München | Wagmüllerstraße 18 | Telefon: +49 89 21 26 72-0
poststelle@datenschutz-bayern.de | https://www.datenschutz-bayern.de

gestützt, die der Datenexporteur (der Verantwortliche oder der Auftragsverarbeiter) vorzusehen hat, wobei den betroffenen Personen zugleich durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen müssen.

5 Diese Garantien können nach Art. 46 Abs. 2 Buchst. c DSGVO insbesondere in sogenannten **Standarddatenschutzklauseln**[5] bestehen, vorausgesetzt, dass die vereinbarten Klauseln tatsächlich auch wirksam sind, ihre Wirksamkeit also nicht durch Rechtsvorschriften oder behördliche Praktiken in den USA beeinträchtigt wird. Eine solche Beeinträchtigung hatte der Europäische Gerichtshof vor allem für Datenübermittlungen angenommen, die etwa in den Anwendungsbereich von Section 702 Foreign Intelligence Surveillance Act of 1978 („FISA")[6] oder von Executive Order 12.333[7] fallen.[8]

6 Daher mussten Datenexporteure speziell in solchen Fällen **zusätzliche Maßnahmen („supplementary measures")** auswählen, um für die übermittelten Daten ein Schutzniveau zu erreichen, das dem unionsrechtlichen Standard gleichwertig war. In der Regel wurden zusätzliche technische Maßnahmen – wie eine Verschlüsselung oder Pseudonymisierung – benötigt, deren Implementierung für Datenexporteure mit erheblichem Aufwand verbunden war. Schließlich mussten Datenexporteure den Nachweis erbringen, dass eine Aufhebung der Verschlüsselung und/oder Pseudonymisierung durch US-Behörden bei dem jeweiligen US-Vertragspartner ausgeschlossen werden konnte. Sofern im Einzelfall keine effektiven zusätzlichen Maßnahmen implementiert werden konnten, durfte die Übermittlung nicht auf Art. 46 DSGVO gestützt werden.

2. Wie schafft der Angemessenheitsbeschluss Erleichterung?

7 Soweit die EU-Kommission durch ihren Angemessenheitsbeschluss bereits festgestellt hat, dass die USA ein angemessenes Schutzniveau für personenbezogene Daten bieten, entfallen für einen Datenexporteur die oben dargestellten (Prüf-)Schritte. Vorausgesetzt ist dabei, dass er die personenbezogenen Daten an ein für das EU-U.S. Data Privacy Framework zertifiziertes US-Unternehmen übermittelt. Der Angemessenheitsbeschluss gilt folglich – wie bereits der vorangegangene Angemessenheitsbeschluss für das EU-U.S. Privacy Shield – **nur partiell** und nicht für alle in den USA ansässigen Datenimporteure. Seine Geltung ist gemäß Art. 45 Abs. 1 Satz 1 DSGVO sachlich auf „spezifische Sektoren" beschränkt (auch sog. sektoraler Angemessenheitsbeschluss). Ist das US-Unternehmen für das EU-U.S. Data Privacy Framework zertifiziert, entfaltet der Angemessenheitsbeschluss dann **unmittelbare Wirkung**; die Datenübermittlung bedarf weder **einer aufsichtsbehördlichen Genehmigung** (vgl. Art. 45 Abs. 1 Satz 2 DSGVO) **noch besonderer Schutzmaßnahmen**.

8 Da ein Angemessenheitsbeschluss seine Wirksamkeit verlieren kann (vgl. Rn. 26 f.), sollte ein Datenexporteur stets zunächst die **aktuelle Liste der Angemessenheitsbeschlüsse** der EU-Kommission konsultieren.[9] Sofern der Datenexporteur das Fortbestehen des Angemessenheitsbeschlusses für das EU-U.S. Data Privacy Framework positiv festgestellt hat, können die Daten dann ohne weitere Prüfung bezüglich Kapitel V DSGVO übermittelt werden.

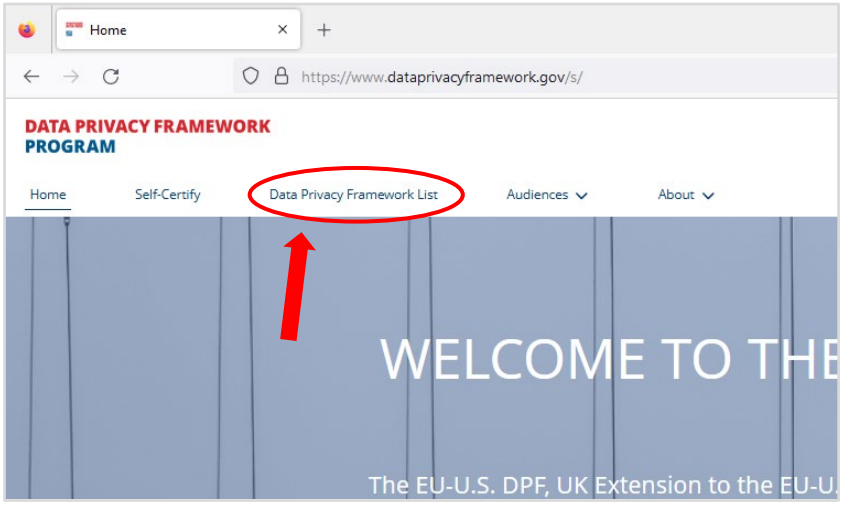
3. Welche Datenübermittlungen betrifft dies?

9 Vom EU-U.S. Data Privacy Framework erfasst werden nahezu alle Übermittlungen personenbezogener Daten an US-Unternehmen, die sich im Rahmen eines **Zertifizierungsmechanismus** zur Einhaltung von bestimmten Datenschutzgrundsätzen verpflichtet haben. Voraussetzung für eine Zertifizierung ist, dass das betreffende US-Unternehmen **der Aufsicht der U.S. Federal Trade Commission**[10] **oder des U.S. Department of Transportation**[11] unterliegt; bei Unternehmen mit mehreren Sparten ist daher denkbar, dass nicht alle Unternehmensbereiche erfasst sind.

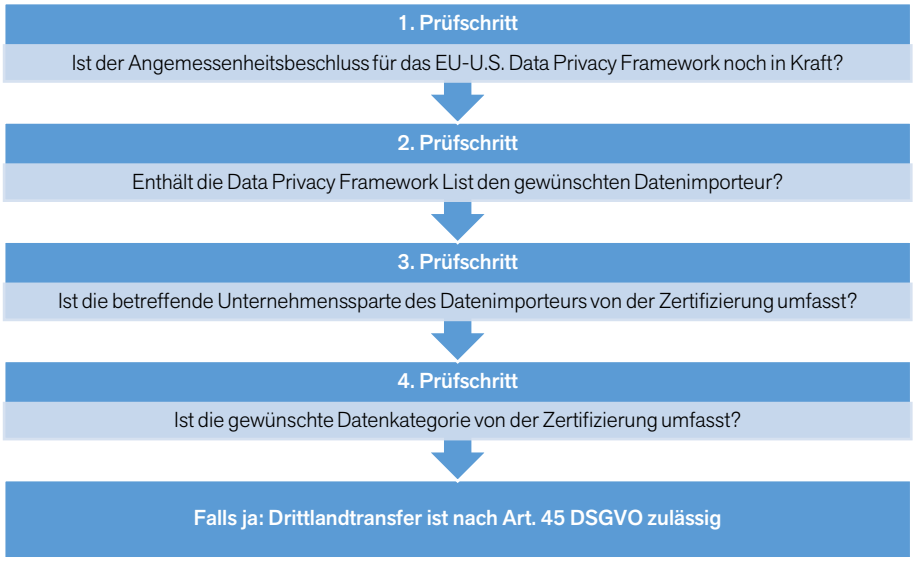
10 **Ausgenommen** vom Anwendungsbereich des EU-U.S. Data Privacy Framework sind **personenbezogene Daten**, die **im Rahmen journalistischer Aktivitäten** zu Zwecken der öffentlichen Kommunikation gesammelt werden, sowie Informationen aus früher veröffentlichtem Material, das aus Medienarchiven stammt. Solche Daten können somit nicht auf der Grundlage des Angemessenheitsbeschlusses übermittelt werden.

11 Auch die Übermittlung von **Personaldaten („HR Data“)**, die im Rahmen eines Beschäftigungsverhältnisses erhoben werden, ist **nicht automatisch** vom EU-U.S. Data Privacy Framework erfasst; vielmehr muss das US-Unternehmen bei seiner Zertifizierung explizit angeben, dass sich diese auch auf die Übermittlung von Personaldaten beziehen soll. Damit geht insbesondere die Verpflichtung einher, mit den nationalen EU-Datenschutz-Aufsichtsbehörden zusammenzuarbeiten.

12 Datenexporteure müssen daher prüfen, ob ihre geplanten Datenübermittlungen in den Anwendungsbereich des Angemessenheitsbeschlusses fallen. Aus Gründen der Rechtssicherheit unterhält und pflegt das U.S. Department of Commerce eine Liste, die die US-Unternehmen enthält, die sich gemäß dem EU-U.S. Data Privacy Framework zertifiziert haben (**„Data Privacy Framework List“**). Dieser Liste kann auch entnommen werden, welche Gesellschaften einer Unternehmensgruppe zertifiziert sind („covered entities“) sowie welche Kategorien personenbezogener Daten („covered data“) bzw. welche Wirtschaftszweige („industries“) umfasst werden. Die Liste sowie weitere Informationen von US-Seite zum EU-U.S. Data Privacy Framework stehen seit dem 17. Juli 2023 auf der Website https://www.dataprivacyframework.gov zur Verfügung:



13 Zusammengefasst ergeben sich daraus für Datenexporteure des bayerischen öffentlichen Sektors folgende Prüfschritte:



14 Datenübermittlungen an US-Unternehmen, die **nicht oder nicht für die gewünschte Übermittlung zertifiziert** sind, müssen (weiterhin) auf **eines der anderen in Art. 44 ff. DSGVO vorgesehenen Übermittlungsinstrumente** gestützt werden.

15 Dabei gelten allerdings nach Mitteilung der EU-Kommission 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. Deshalb können Datenexporteure im Rahmen der Datenübermittlung mithilfe geeigneter Garantien (Art. 46 DSGVO) die von der EU-Kommission im Angemessenheitsbeschluss ausgeführten Bewertungen bei der Prüfung der Wirksamkeit des gewählten Übermittlungsinstruments („Transfer Impact Assessment") berücksichtigen.[12]

4. Ab welchem Zeitpunkt können Daten mit Hilfe des EU-U.S. Data Privacy Framework in die USA übermittelt werden?

16 Personenbezogene Daten können auf Grundlage des EU-U.S. Data Privacy Framework an zertifizierte Unternehmen **von dem Zeitpunkt an** übermittelt werden, zu dem diese vom U.S. Department of Commerce **auf die Data Privacy Framework List** (vgl. Rn. 12) **gesetzt** wurden. Um weiterhin am EU-U.S. Data Privacy Framework teilnehmen zu können, müssen die Unternehmen ihre **Zertifizierung jährlich erneuern**. Sofern ein Unternehmen – aus welchem Grund auch immer – aus dem EU-U.S. Data Privacy Framework ausscheidet, muss es alle Angaben entfernen, die darauf hindeuten, dass es weiterhin am EU-U.S. Data Privacy Framework teilnimmt. Eine regelmäßige Überprüfung der Data Privacy Framework List, die das U.S. Department of Commerce aktuell halten wird, ist Verantwortlichen dringend zu empfehlen, da ohne (fort-)bestehende Zertifizierung die Übermittlung nicht weiter auf den Angemessenheitsbeschluss gestützt werden kann.

Das U.S. Department of Commerce wird außerdem ein Verzeichnis der Unternehmen führen, die von der Data Privacy Framework List gestrichen wurden, und der Öffentlichkeit zugänglich machen, wobei auch der Grund für die Streichung angegeben wird. 17

5. Was ist dennoch zu tun?

Die Rechtmäßigkeit der Übermittlung personenbezogener Daten in Drittländer bemisst sich nicht allein nach den Art. 44 ff. DSGVO. Stets zu beachten sind auch die **allgemeinen Grundsätze für die Verarbeitung personenbezogener Daten nach Art. 5 ff. DSGVO. Dazu zählt insbesondere das Erfordernis einer Rechtsgrundlage.** Vor diesem Hintergrund befreit der Angemessenheitsbeschluss die bayerischen öffentlichen Stellen nicht von allen Sorgen – insbesondere bleibt etwa die Prüfung notwendig, ob Verarbeitungsbefugnisse im Fachrecht oder im allgemeinen Datenschutzrecht eine Übermittlung zulassen und erforderlichenfalls die Voraussetzungen für eine Zweckänderung vorliegen. Ist die Übermittlung auf eine Einwilligung gestützt, muss diese auch wirksam sein. Gefordert ist also immer eine „Zwei-Stufen-Prüfung“:[13] zur Rechtsgrundlage (und allen weiteren Anforderungen der Datenschutz-Grundverordnung an die Rechtmäßigkeit) einer Verarbeitung personenbezogener Daten als erster Stufe tritt das Übermittlungsinstrument – im Fall von Art. 45 DSGVO der Angemessenheitsbeschluss – als zweite Stufe. 18

Vor einer solchen Prüfung sollten bayerische öffentliche Stellen wie bisher auf Grundlage eines Datenschutz-Sicherheitskonzepts die potentiellen Drittlandübermittlungen präzise erfassen (**„know your transfers“**).[14] Dabei ist vor allem auch auf **Weiterübermittlungen** zu achten, wenn zum Beispiel die für den Datenexporteur tätigen US-Auftragsverarbeiter die personenbezogenen Daten an einen Unterauftragsverarbeiter in einem anderen Drittland übermitteln. Schließlich gilt der Angemessenheitsbeschluss für das EU-U.S. Data Privacy Framework für solche Weiterübermittlungen nicht. 19

Um die **Rechenschaftspflicht** gemäß Art. 5 Abs. 2 DSGVO zu erfüllen, müssen bayerische öffentliche Stellen die Zwei-Stufen-Prüfung **dokumentieren**. Aus diesem Grund empfiehlt es sich, gegebenenfalls die Wahl des Übermittlungsinstruments im Verarbeitungsverzeichnis zu aktualisieren bzw. erstmalig zu dokumentieren. Dies geht zwar über die in Art. 30 Abs. 1 Satz 2 Buchst. e DSGVO geforderten Mindestangaben hinaus; die Angabe dient jedoch dem Nachweis, dass die Frage geprüft wurde. 20

Außerdem müssen bayerische öffentliche Stellen ihre **Datenschutzhinweise** aktualisieren, sofern Datenübermittlungen in die USA nun auf das EU-U.S. Data Privacy Framework gestützt werden sollen, da der Hinweis auf einen Angemessenheitsbeschluss bei Drittlandübermittlungen zu den Pflichtangaben in einer Datenschutzerklärung gehört (vgl. Art. 13 Abs. 1 Buchst. f DSGVO). 21

6. Facebook, Microsoft, Google – ab jetzt kein Problem, oder?

Der Erlass des Angemessenheitsbeschlusses für das EU-U.S. Data Privacy Framework bringt auch für bayerische öffentliche Stellen manche Erleichterung mit sich. Allerdings erfassen die Art. 44 ff. DSGVO nur einen Teilaspekt grenzüberschreitender Datenverarbeitungen. 22

23 So sind beispielsweise die sich aus dem Urteil des Europäischen Gerichtshofs zum Betrieb einer **Facebook-Fanpage** ergebenden Konsequenzen zu beachten, wonach in der Regel eine **gemeinsame Verantwortlichkeit** des Fanpage-Betreibers zusammen mit Facebook vorliegen wird.[15] Sofern Facebook dem mitverantwortlichen Seitenbetreiber aber nicht die notwendigen Informationen zur Verfügung stellt, kann dieser seine datenschutzrechtlichen Pflichten, beispielsweise hinsichtlich der Transparenz und der Rechtmäßigkeit der Datenverarbeitung, aber auch die Informationspflichten gemäß Art. 13 DSGVO nicht erfüllen; seiner Rechenschaftspflicht gemäß Art. 5 Abs. 2 DSGVO kann er ebenfalls nicht nachkommen. Daran ändert der neue Angemessenheitsbeschluss nichts.

24 Ferner ist zu berücksichtigen, dass viele Social Media-Anbieter **Daten auch für eigene Zwecke** erheben, um damit umfangreiche Nutzerprofile zu erstellen und diese kommerziell zu nutzen, insbesondere zur Vermarktung zielgruppenorientierter Werbung. Welche personenbezogenen Daten in welcher Art und Weise konkret verarbeitet werden, bleibt allerdings weitgehend unklar. Der **Vorwurf mangelnder Transparenz** im Hinblick auf die Verarbeitung personenbezogener Daten zu eigenen Zwecken gilt gleichermaßen für Microsoft 365. Bayerische öffentliche Stellen erwarten hier zumindest erhebliche Schwierigkeiten, jederzeit den Rechenschaftspflichten nach Art. 5 Abs. 2 DSGVO nachkommen zu können, da Microsoft beispielsweise nicht vollumfänglich offenlegt, welche Verarbeitungen im Einzelnen stattfinden.[16] Auch insofern bietet der neue Angemessenheitsbeschluss keinen problemlösenden „Generalschlüssel".

25 Bayerischen öffentlichen Stellen ist folglich weiterhin zu empfehlen, solche Aspekte bei der Wahl ihrer Betriebsmittel zu berücksichtigen.

7. Ausblick

26 Ein Jahr nach Bekanntgabe des Angemessenheitsbeschlusses an die Mitgliedstaaten wird die EU-Kommission eine **erste Überprüfung** vornehmen, ob die neuen Mechanismen im US-Recht, die Voraussetzung für den Erlass des Angemessenheitsbeschlusses waren, vollständig umgesetzt wurden und in der Praxis wirksam funktionieren. Je nach Ausgang dieser Überprüfung wird die EU-Kommission insbesondere in enger Abstimmung mit dem Europäischen Datenschutzausschuss über die Häufigkeit künftiger Überprüfungen entscheiden. Gemäß Art. 45 Abs. 3 DSGVO müssen diese **mindestens alle vier Jahre** stattfinden.

27 Falls die EU-Kommission feststellen sollte, dass für personenbezogene Daten, die auf Grundlage von Angemessenheitsbeschlüssen an Drittländer übermittelt werden, kein angemessenes Schutzniveau mehr besteht, kann sie den betreffenden Angemessenheitsbeschluss widerrufen, abändern oder aussetzen (vgl. Art. 45 Abs. 5 DSGVO). Daneben können Angemessenheitsbeschlüsse vom Europäischen Gerichtshof überprüft und gegebenenfalls für ungültig erklärt werden.

[1] Commission Implementing Decision of 10. Juli 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, Internet: https://commission.europa.eu/document/download/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en?filename=Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf.

[2] Einzelheiten dazu bei Ehmann, Der Weg zum Angemessenheitsbeschluss für das Transatlantic Data Privacy Framework (TDPF), Stand 5/2023, Internet: https://www.rehm-verlag.de/verwaltung/aktuelle-beitraege-datenschutz/datentransfer-in-die-usa-bedeutsam-auch-fuer-die-verwaltung/.

[3] Europäischer Gerichtshof, Urteil vom 16. Juli 2020, C-311/18.

[4] Vgl. Bayerischer Landesbeauftragter für den Datenschutz, Internationale Datentransfers, Stand 5/2023, Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018 – Orientierungs- und Praxishilfen – Internationaler Datenverkehr".

[5] Vgl. insbesondere Durchführungsbeschluss (EU) 2021/914 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates, C/2021/3972 (ABl. L 199 vom 7. Juni 2021, S. 31).

[6] Zugleich 50 United States Code §§ 1881, 1881a; eingeführt durch FISA Amendments Act of 2008 vom 10. Juli 2008, H.R. 6304, Publ. L. No. 110–261, 122 Stat. 2437; Internet: https://www.govinfo.gov/content/pkg/STATUTE-122/pdf/STATUTE-122-Pg2436.pdf. Zuletzt verlängert bis 31. Dezember 2023 durch FISA Amendments Reauthorization Act of 2017 vom 18. Januar 2018, Publ. L. No. 115–118, 132 Stat. 3; Internet: https://www.congress.gov/115/plaws/publ118/PLAW-115publ118.pdf.

[7] Internet: https://www.archives.gov/federal-register/codification/executive-order/12333.html.

[8] Europäischer Gerichtshof, Urteil vom 16. Juli 2020, C-311/18, Rn. 171 ff.

[9] Internet: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_de.

[10] Vgl. zur Zuständigkeit insbesondere Annex IV des Angemessenheitsbeschlusses (Endnote 1).

[11] Vgl. zur Zuständigkeit insbesondere Annex V des Angemessenheitsbeschlusses (Endnote 1).

[12] Vgl. EU-Kommission, Fragen und Antworten: Datenschutzrahmen EU-USA, 10. Juli 2023, Internet: https://ec.europa.eu/commission/presscorner/api/files/document/print/de/qanda_23_3752/QANDA_23_3752_DE.pdf; zum Transfer Impact Assessment vgl. Bayerischer Landesbeauftragter für den Datenschutz, Internationale Datentransfers, Rn. 62 ff. (Endnote 4).

[13] Zur Zwei-Stufen-Prüfung näher Bayerischer Landesbeauftragter für den Datenschutz, Internationale Datentransfers, Rn. 10 ff. (Endnote 4).

[14] Vgl. Europäischen Datenschutzausschuss, Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten, Version 2.0, Stand 6/2021, Rn. 8 ff., Internet: https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_de.

[15] Europäischer Gerichtshof, Urteil vom 5. Juni 2018, Az. C-210/16.

[16] Vgl. Zusammenfassung des Berichts der Arbeitsgruppe DSK „Microsoft-Onlinedienste" und Abschlussbericht der Arbeitsgruppe DSK „Microsoft-Onlinedienste", Internet: https://www.datenschutz-bayern.de/inhalte/dsk_ent_t.htm.