

FAQ

zum Angemessenheitsbeschluss für das neue EU-US-Datenschutzabkommen

Inhalt

I.	Allgemein.....	3
Q:	Was ist unter einem Angemessenheitsbeschluss zu verstehen?	3
Q:	Was ist der Vorteil eines Angemessenheitsbeschlusses?	3
Q:	Nach welchen Kriterien wird die Angemessenheit beurteilt?	3
II.	Neues EU-US-Datenschutzabkommen für Datenübermittlungen in die USA	4
Q:	Was regelt das neue TADPF?	4
Q:	Was ist mit dem Vorgänger des TADPF passiert?	4
Q:	Was unterscheidet das neue Datenschutzabkommen vom EU-US-Privacy Shield?	4
Q:	Wie wahrscheinlich ist es, dass auch das neue Datenschutzabkommen für unwirksam erklärt wird?	5
Q:	Bedeutet das neue Datenschutzabkommen, dass nun für die gesamte USA ein angemessenes Datenschutzniveau besteht?	5
Q:	Auf wen findet das neue Datenschutzabkommen keine Anwendung?	6
Q:	Worauf sollten Unternehmen zwingend achten, bevor sie sich auf das neue Datenschutzabkommen berufen?	6
Q:	Was passiert mit den bisherigen Rechtsgrundlagen für Datenübermittlungen in die USA?	6
Q:	Welche Maßnahmen sollten Unternehmen nun umsetzen, um künftig Datenübermittlungen in die USA auf das neue Datenschutzabkommen zu stützen?	6
Q:	Sind die bisherigen EU-Standardvertragsklauseln nun mit dem neuen Datenschutzabkommen überflüssig geworden?	7
Q:	Sollte neben dem neuen Datenschutzabkommen weiterhin ein TIA abgeschlossen werden?	7
Q:	Welche Auswirkungen hat die Entscheidung auf andere Transfermechanismen (wie etwa EU-Standardvertragsklauseln), die für den Datentransfer in die USA herangezogen werden?	7
Q:	Wie lange ist das neue Datenschutzabkommen gültig?	8
Q:	Was sollten Unternehmen tun, wenn sie dauerhafte Rechtssicherheit wollen?	8
Q:	Was passiert, wenn auch das neue Datenschutzabkommen für unwirksam erklärt wird?	8
Q:	Müssen Unternehmen in der EU mit Bußgeldern rechnen?	8

Die Europäische Kommission hat am 10. Juli 2023 ihren Angemessenheitsbeschluss für das neue Datenschutzabkommen zwischen der Europäischen Union (nachfolgend „EU“ genannt) und den USA, das sog. „Trans-Atlantic Data Privacy Framework“ (nachfolgend „TADPF“ genannt), angenommen¹. Mit dem neuen Angemessenheitsbeschluss kommen auf Unternehmen nunmehr bei der Übermittlung von personenbezogenen Daten in die USA einige Erleichterungen zu. Welche Konsequenzen der Angemessenheitsbeschluss konkret hat und worauf Unternehmen künftig achten sollten, soll mit dem vorliegenden FAQ-Dokument näher beleuchtet werden.

I. Allgemein

Q: Was ist unter einem Angemessenheitsbeschluss zu verstehen?

A: Ein Angemessenheitsbeschluss ist ein in der Datenschutz-Grundverordnung (nachfolgend „DS-GVO“ genannt) verankertes Instrument, welches als Rechtsgrundlage für die Übermittlung für personenbezogene Daten in Drittländer (= Länder außerhalb der EU/EWR) herangezogen werden kann. Ein solcher Beschluss wird stets von der Europäischen Kommission erlassen und legt fest, dass das jeweilige Drittland ein angemessenes Datenschutzniveau gewährleistet, welches mit dem Datenschutzniveau in der EU vergleichbar ist².

Q: Was ist der Vorteil eines Angemessenheitsbeschlusses?

A: Mithilfe eines Angemessenheitsbeschlusses wird Unternehmen und Organisationen (nachfolgend „Unternehmen“ genannt) die sichere Übermittlung von personenbezogenen Daten aus der EU in das jeweilige Drittland ermöglicht, ohne dass zusätzliche Genehmigungen oder Mechanismen erforderlich sind. Dadurch gestaltet sich der Datentransfer insgesamt einfacher. Alternative Rechtsgrundlagen, wie etwa EU-Standardvertragsklauseln oder interne Unternehmensrichtlinien (sog. Binding Corporate Rules), sind in der Regel mit mehr Zeitaufwand und zusätzlichen Kosten verbunden, wobei in diesen Fällen auch stets ein gewisses Restrisiko im Hinblick auf die Wirksamkeit der Datenübermittlung verbleibt.

Q: Nach welchen Kriterien wird die Angemessenheit beurteilt?

A: Die Angemessenheit wird von der Europäischen Kommission nach diversen Kriterien beurteilt. Ziel hierbei ist immer, dass das Datenschutzniveau in dem jeweiligen Drittland dem hohen Schutzniveau in der EU entspricht. Welche Kriterien hierfür konkret herangezogen werden, können aus der Orientierungshilfe der europäischen Datenschutzbehörde entnommen werden³.

¹ https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721

² https://ec.europa.eu/commission/presscorner/detail/de/qanda_21_6916

³ <https://ec.europa.eu/newsroom/article29/items/614108/en>

II. Neues EU-US-Datenschutzabkommen für Datenübermittlungen in die USA

Q: Was regelt das neue TADPF?

A: Mit dem neuen Datenschutzabkommen TADPF ist die Europäische Kommission zu dem Entschluss gekommen, dass die USA ein angemessenes Schutzniveau für personenbezogene Daten gewährleistet und auf dieser Grundlage nunmehr personenbezogene Daten aus der EU sicher in die USA transferiert werden können⁴. Damit werden neue verbindliche Garantien eingeführt, um allen vom Europäischen Gerichtshof geäußerten Bedenken Rechnung zu tragen. In diesem Zusammenhang haben die Europäische Kommission und das US-Handelsministerium vereinbart, dass die USA ihr Datenschutzniveau verbessert und die europäische Kommission dafür im Gegenzug die Übermittlung von personenbezogenen Daten aus der EU in die USA als angemessen erachtet.

Q: Was ist mit dem Vorgänger des TADPF passiert?

A: Der Europäische Gerichtshof hat die beiden Vorgängerregelungen des TADPF, das Safe-Harbor-Abkommen sowie das EU-US-Privacy Shield, jeweils mit seinen Schrems I⁵- und Schrems II⁶-Urteilen für unwirksam erklärt. Nach dessen Aufhebung mussten Unternehmen die Datenübermittlungen in die USA sodann auf alternative Rechtsgrundlagen stützen, wie etwa auf EU-Standardvertragsklauseln oder interne Unternehmensrichtlinien (sog. Binding Corporate Rules).

Q: Was unterscheidet das neue Datenschutzabkommen vom EU-US-Privacy Shield?

A: Ein wesentlicher Unterschied des neuen Datenschutzabkommens zum EU-US-Privacy Shield liegt in der von US-Präsident Biden am 7. Oktober 2022 unterzeichneten Durchführungsverordnung, die sog. Executive Order „on Enhancing Safeguards for United States Signals Intelligence Activities“⁷, welche insbesondere die vom Europäischen Gerichtshof im Schrems-II-Urteil getroffenen Vorgaben umsetzen soll. In dieser Vereinbarung werden insoweit erstmals verbindliche Garantien zugesagt, welche die Aktivitäten der US-Geheimdienste auf ein bestimmtes Maß beschränken. Hiernach soll ein Zugriff auf die personenbezogenen Daten der EU-Bürger insbesondere nur dann möglich sein, soweit dies zur nationalen Sicherheit notwendig und die Beeinträchtigung verhältnismäßig ist. Darüber hinaus sollen verpflichtende Verfahren für US-Geheimdienste eingerichtet werden, welche eine wirksame Überwachung der neuen Standards für den Schutz der Privatsphäre von EU-Bürgern gewährleisten.

⁴ https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en

⁵ EuGH, Urteil v. 6.10.2015, C-362/14

⁶ EuGH, Urteil vom 16.7.2020 – C-311/18.

⁷ https://ec.europa.eu/commission/presscorner/detail/en/QANDA_22_6045

Q: Wie wahrscheinlich ist es, dass auch das neue Datenschutzabkommen für unwirksam erklärt wird?

A: Es ist nicht unwahrscheinlich, dass das neue Datenschutzabkommen eine Rechtssicherheit auf Zeit darstellt. Wie bereits das Schrems II-Urteil vor dem Europäischen Gerichtshof gezeigt hat, könnte auch das neue Datenschutzabkommen vom Europäischen Gerichtshof gekippt werden⁸. So hat zumindest Max Schrems angekündigt, auch gegen das neue Datenschutzabkommen rechtlich vorzugehen und hierzu eine entsprechende Stellungnahme veröffentlicht (<https://noyb.eu/de/european-commission-gives-eu-us-data-transfers-third-round-cjeu>). Vor diesem Hintergrund geht Schrems davon aus, dass die Angelegenheit bereits Anfang 2024 erneut vor dem EuGH landen werde, wobei er in diesem Zusammenhang eine vorläufige Aussetzung des EU-US-Datenschutzabkommens für möglich hält. Bis es allerdings zu einem solchen Urteil kommt, kann das neue Datenschutzabkommen als Rechtsgrundlage für den Datentransfer in die USA - sofern die jeweiligen Voraussetzungen erfüllt sind (s. u.) - herangezogen werden.

Q: Bedeutet das neue Datenschutzabkommen, dass nun für die gesamte USA ein angemessenes Datenschutzniveau besteht?

A: Nein. Der Angemessenheitsbeschluss bedeutet nur, dass lediglich im Hinblick auf bestimmte Unternehmen ein angemessenes Datenschutzniveau besteht. Bevor sich also Unternehmen bei der Datenübermittlung aus der EU in die USA überhaupt auf das neue Datenschutzabkommen berufen können, müssen US-Unternehmen zunächst noch ein Selbstzertifizierungsverfahren in den USA durchlaufen. Um eine solche Zertifizierung zu erlangen, müssen US-Unternehmen bestimmte Voraussetzungen erfüllen und sich bspw. dazu verpflichten, im Vorfeld festgelegte Datenschutzbestimmungen einzuhalten, wie etwa die Löschung von personenbezogenen Daten zu veranlassen, soweit diese für den Zweck, für den sie erhoben wurden, nicht mehr erforderlich sind. Die Zertifizierung ist hierbei über die vom US-Handelsministerium betriebene Website www.dataprivacyframework.gov vorzunehmen. Auf dieser Website ist auch künftig eine aktualisierte Liste der zertifizierten und der ehemals zertifizierten Unternehmen veröffentlicht⁹. In diesem Zusammenhang sollten Unternehmen in der EU auch stets auf die Angaben im Hinblick auf die Reichweite der Zertifizierung achten. So kann es bspw. vorkommen, dass sich die Zertifizierung bei einigen US-Unternehmen lediglich auf NON-HR Daten beschränkt, wohingegen bei anderen US-Unternehmen neben HR Daten auch NON-HR Daten von der Zertifizierung umfasst sind. Für alle anderen US-Unternehmen bedeutet das also, dass für den Datentransfer weiterhin alternative Rechtsgrundlagen herangezogen werden müssen, wie etwa der Weg über die EU-Standardvertragsklauseln und des Transfer Impact Assessments (nachfolgend „TIA“ genannt).

⁸ <https://stiftungdatenschutz.org/veroeffentlichungen/datenschutzwoche/detailansicht/datenschutzwoche-vom-17-07-2023-409>

⁹ <https://www.dataprivacyframework.gov/s/participant-search>

Q: Auf wen findet das neue Datenschutzabkommen keine Anwendung?

A: In Bezug auf Datenübermittlungen an bspw. Banken, Fluggesellschaften und Versicherungsgesellschaften in den USA können sich Unternehmen nicht auf den neuen Angemessenheitsbeschluss berufen. Insoweit sieht Anhang I, Abschnitt I. 2 des Beschlusses vor, dass diese US-Unternehmen nicht den Ermittlungs- und Durchsetzungsbefugnissen der Federal Trade Commission unterliegen, was jedoch zwingende Voraussetzung für die Anwendbarkeit des Angemessenheitsbeschlusses ist¹⁰. Der Datentransfer an diese Unternehmen ist daher auf alternative Rechtsgrundlagen aus der DS-GVO zu stützen.

Q: Worauf sollten Unternehmen zwingend achten, bevor sie sich auf das neue Datenschutzabkommen berufen?

A: Unternehmen sollten vor dem Datentransfer dringend überprüfen, ob Subunternehmer in anderen Drittländern eingesetzt werden. In diesen Fällen ist nämlich der Angemessenheitsbeschluss allein nicht mehr ausreichend. Zudem sollte auch darauf geachtet werden, dass sich die in den USA ansässigen Subunternehmer auch zertifizieren lassen. Andernfalls reicht auch hier der Angemessenheitsbeschluss allein nicht mehr aus.

Q: Was passiert mit den bisherigen Rechtsgrundlagen für Datenübermittlungen in die USA?

A: Alle bisherigen Rechtsgrundlagen, welche für die Datenübermittlungen in die USA herangezogen worden sind, wie beispielsweise EU-Standardvertragsklauseln, bleiben weiterhin wirksam und bis zur Zertifizierung des die Daten empfangenden US-Unternehmens auch erforderlich.

Q: Welche Maßnahmen sollten Unternehmen nun umsetzen, um künftig Datenübermittlungen in die USA auf das neue Datenschutzabkommen zu stützen?

A: Unternehmen sollten die folgenden Maßnahmen umsetzen:

- Die Zertifizierung des jeweiligen US-Unternehmens unter dem neuen EU-US-Datenschutzabkommen prüfen und verifizieren lassen;
- prüfen, ob Subunternehmer in anderen Drittländern eingesetzt werden;
- Anpassung der Datenschutz-Folgenabschätzungen, insbesondere im Hinblick auf die Risikobewertung im Zusammenhang mit dem Drittlandtransfer;
- Anpassung der Datenschutzverträge und Datenschutzhinweise. Letztere sollten im Hinblick auf Art. 13 Abs. 1 lit. e) und f) DS-GVO einen Hinweis zum Angemessenheitsbeschluss enthalten und angeben, dass das jeweilige US-Unternehmen als Datenempfänger in den Anwendungsbereich des Angemessenheitsbeschlusses fällt.

¹⁰

https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf

- Aktualisierung des Verzeichnisses von Verarbeitungstätigkeiten insbesondere im Hinblick auf die Rechtsgrundlage für den Drittlandtransfer.

Q: Sind die bisherigen EU-Standardvertragsklauseln nun mit dem neuen Datenschutzabkommen überflüssig geworden?

A: Nein. Die EU-Standardvertragsklauseln bleiben weiterhin bestehen. Spätestens, wenn der Europäische Gerichtshof den neuen Angemessenheitsbeschluss für unwirksam erklärt, könnten die EU-Standardvertragsklauseln wiederaufleben und somit als Rechtsgrundlage für den Datentransfer in die USA herangezogen werden. Gleichwohl sei angemerkt, dass keine Pflicht zum Wechsel des Transfermechanismus besteht und Unternehmen insofern weiterhin die Möglichkeit haben, sich auf diese alternativen Transfermechanismen zu berufen.

Q: Sollte neben dem neuen Datenschutzabkommen weiterhin ein TIA abgeschlossen werden?

A: Streng genommen ist mit dem Inkrafttreten des Angemessenheitsbeschlusses der Abschluss von EU-Standardvertragsklauseln und TIAs nicht mehr erforderlich. Angesichts der Tatsache, dass bereits die beiden Vorgängerregelungen des neuen Datenschutzabkommens vom Europäischen Gerichtshof gekippt wurden, ist zumindest nicht auszuschließen, dass auch das neue Datenschutzabkommen vom Europäischen Gerichtshof künftig für unwirksam erklärt wird (s. o.). Daher sollten gerade bei einer längeren Zusammenarbeit mit US-Unternehmen vertragliche Vorkehrungen getroffen werden. Diese könnten bspw. wie folgt aussehen:

- Unternehmen könnten für diesen Fall den Abschluss der EU-Standardvertragsklauseln sowie die Mithilfe des US-Unternehmens bei der Erstellung eines TIAs verbindlich in den Vertrag aufnehmen.
- Für den Fall, dass nach Ablauf der Selbstzertifizierung keine Re-Zertifizierung erfolgt, endet die Privilegierung durch den Angemessenheitsbeschluss. Auch für diesen Fall sollte der vorstehend genannte Mechanismus gewählt werden. Zudem sollte der US-Partner seine Absicht, die Zertifizierung nicht zu verlängern, frühzeitig mitteilen müssen.

Q: Welche Auswirkungen hat die Entscheidung auf andere Transfermechanismen (wie etwa EU-Standardvertragsklauseln), die für den Datentransfer in die USA herangezogen werden?

A: Da die USA im Zuge des TADPF weitreichende Schutzmaßnahmen zur Steigerung der nationalen Sicherheit und des damit verbundenen Datenschutzniveaus ergriffen haben, hat sich die Sach- und Rechtslage auch im Hinblick auf alternative Transfermechanismen, wie etwa auf die Standardvertragsklauseln, positiv verändert. Insofern gelten diese Schutzmaßnahmen für sämtliche Datenübermittlungen im Rahmen der DS-GVO an US-Unternehmen und unabhängig von den konkret herangezogenen Übertragungsmechanismen. Das heißt, diese Schutzmechanismen können auch positive Auswirkungen auf die Risikobewertung im Rahmen eines TIAs entfalten.

Q: Wie lange ist das neue Datenschutzabkommen gültig?

A: Der Angemessenheitsbeschluss ist nicht befristet. Die Europäische Kommission behält sich jedoch vor, die relevanten Entwicklungen in den USA fortlaufend zu beobachten und den Angemessenheitsbeschluss regelmäßig zu überprüfen. Hierfür ist bereits geplant, dass ein Jahr nach dem Inkrafttreten des Angemessenheitsbeschlusses ermittelt werden soll, ob die wichtigsten Elemente des Datenschutzabkommens in der Praxis im US-Rechtsrahmen auch tatsächlich wirksam umgesetzt wurden.

Q: Was sollten Unternehmen tun, wenn sie dauerhafte Rechtssicherheit wollen?

A: Da nicht auszuschließen ist, dass auch das neue Datenschutzabkommen vom Europäischen Gerichtshof aufgrund eines unzureichenden Schutzniveaus für unwirksam erklärt wird, ist das TADPF mit gewissen Risiken behaftet. In diesem Fall würde für Unternehmen wieder große Unsicherheit herrschen, ob und wie US-Dienstleister eingesetzt oder sonst Daten in die USA transferiert werden dürfen. Wollen Unternehmen ein solches Risiko nicht eingehen, dann sollten Unternehmen nur solche US-Dienstleister einsetzen, die ihre Daten in der EU speichern und nicht gegenüber den US-Geheimdiensten zur Gewährung eines Datenzugangs verpflichtet sind.

Q: Was passiert, wenn auch das neue Datenschutzabkommen für unwirksam erklärt wird?

A: Sollte tatsächlich der Fall eintreten, dass das neue Datenschutzabkommen vom Europäischen Gerichtshof für unwirksam erklärt wird, so müssten Unternehmen erneut alternative Mechanismen für den Datentransfer in die USA heranziehen und bspw. auf die EU-Standardvertragsklauseln zurückgreifen sowie ein TIA durchführen.

Q: Müssen Unternehmen in der EU mit Bußgeldern rechnen?

A: Solange der Angemessenheitsbeschluss nicht für unwirksam erklärt wurde, stellt es eine DS-GVO-konforme Grundlage für die Übermittlung von Daten in die USA dar. Unternehmen müssen daher keine Bußgelder oder Untersagungen durch den Einsatz von US-Unternehmen befürchten, sofern diese dem Data Privacy Framework unterfallen. Sollte jedoch künftig das neue Datenschutzabkommen vom Europäischen Gerichtshof für unwirksam erklärt werden, muss die Nutzung von US-Diensten neu bewertet werden. Bspw. könnte dann zum Problem werden, dass das europäische Unternehmen eng mit US-Unternehmen verzahnt ist und die sich in ihrer Verantwortung befindlichen personenbezogenen Daten auf Servern in den USA befinden. Abhängig von der zu diesem Zeitpunkt herrschenden Sach- und Rechtslage könnten Sie ggf. gegen die DS-GVO verstoßen.