Luther.

Newsflash | Juli 2023

EU-Kommission erlässt Angemessenheitsbeschluss – Ungehinderter Datentransfer in die USA?

Die Europäische Kommission hat am 10. Juli 2023 ihren Angemessenheitsbeschluss für den Datenschutzrahmen zwischen der Europäischen Union („EU“) und den USA, das „Trans-Atlantic Data Privacy Framework“ („DPF“), angenommen. Danach gewährleisten die Vereinigten Staaten im Verhältnis zur EU ein angemessenes Schutzniveau für personenbezogene Daten, die aus der EU an US-Unternehmen übermittelt werden. Voraussetzung ist, dass die US-Unternehmen an dem DPF teilnehmen. Mit der Annahme des Angemessenheitsbeschlusses können EU-Unternehmen nun grundsätzlich personenbezogene Daten an teilnehmende US-Unternehmen übermitteln, ohne noch weitere zusätzliche Datenschutzgarantien umsetzen zu müssen. Auch wenn der Beschluss mit Freude erwartet wurde und den Austausch von Daten mit US-Unternehmen vereinfacht, stellt dieser leider keinen Freibrief für den Datentransfer in die USA dar.

I. Hintergrund

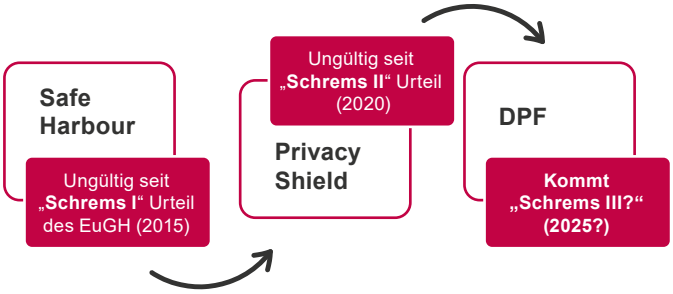
1. Rechtliche Anforderungen an einen Drittlandtransfer

Die Übermittlung von personenbezogenen Daten in Länder außerhalb der EU (sog. Drittländer) ist nach der Datenschutzgrundverordnung („DSGVO“) nur zulässig, wenn sie im Rahmen einer zweistufigen Legitimationsprüfung den Anforderungen beider Stufen genügt. Im Rahmen der ersten Stufe ist sicherzustellen, dass für die Verarbeitung ein gesetzlicher Erlaubnistatbestand gemäß Art. 6 ff. DSGVO existiert und – sofern erforderlich – sonstige Voraussetzungen (etwa der Abschluss einer Auftragsverarbeitungsvertrages gemäß Art. 28 DSGVO) erfüllt sind. Im Rahmen der zweiten Stufe muss nach den Art. 45 ff. DSGVO sichergestellt werden, dass ein **angemessenes Datenschutzniveau** im Empfängerland

selbst oder zumindest beim Empfänger der Daten existiert. Eine Übermittlung personenbezogener Daten in ein Drittland ist nach Art. 45 Abs. 1 DSGVO zulässig, wenn die EU-Kommission einen entsprechenden Angemessenheitsbeschluss zu dem Drittland nach Art. 45 Abs. 3 DSGVO gefasst hat. Aufgrund von Angemessenheitsbeschlüssen können personenbezogene Daten frei und sicher aus dem Europäischen Wirtschaftsraum (EWR), zu dem die 27 EU-Mitgliedstaaten sowie Norwegen, Island und Liechtenstein gehören, in ein Drittland übermittelt werden, ohne dass weitere Bedingungen oder Genehmigungen erforderlich sind.

2. Datentransfer in die USA vor dem Trans-Atlantic Data Privacy Framework

In den letzten drei Jahren gab es für die USA keinen gültigen Angemessenheitsbeschluss. Die Gründe dafür in Kürze:



- Der Europäische Gerichtshof (nachfolgend „EuGH“) erklärte die beiden Vorgängerabkommen Safe Harbour (EuGH, 06.10.2015 – C-362/14 “**Schrems I**”) und den Privacy Shield (EuGH, 16.07.2020 – C-311/18 “**Schrems II**”) nach Klagen des österreichischen Datenschutzaktivisten Max Schrems für unwirksam.
- Die Europäische Kommission und die US-Regierung nahmen daraufhin Gespräche über ein neues Regelwerk auf, um die vom Gerichtshof erhobenen Bedenken auszuräumen und den Weg für einen neuen Angemessenheitsbeschluss zu ebnen.
- Ergebnis war 2022 die Einigung auf ein “Trans-Atlantic Data Privacy Framework” als Nachfolgemodell. Daraufhin unterschrieb US-Präsident Biden im Oktober 2022 eine entsprechende Durchführungsverordnung („**Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities**“), die durch Verordnungen des US-Generalstaatsanwalts Garland ergänzt wurde.
- Die Europäische Kommission veröffentlichte im Dezember 2022 ihren Entwurf für einen Angemessenheitsbeschluss zum DPF, zu dem der Europäische Datenschutzausschuss („EDSA“) im Februar 2023 eine Stellungnahme abgab.
- Der Angemessenheitsbeschluss für das DPF soll nun als ein drittes Regelwerk erst einmal Rechtssicherheit schaffen. Er trat mit seiner Annahme am 10. Juli in Kraft.

Bis zu diesem Zeitpunkt waren Unternehmen verpflichtet, geeignete alternative Maßnahmen für den Datentransfer zwischen der EU und den USA zu ergreifen. Als Mindestvoraussetzung mussten die Standardvertragsklauseln („SCC“) der Europäischen Kommission aus 2021 abgeschlossen werden, die den Schutz des Transfers von personenbezogenen Daten in einen unsicheren Drittstaat sicherstellen sollen. Die SCC brachten zudem eine Pflicht zur Prüfung und zum Nachweis eines in tatsächlicher Sicht hinreichenden Datenschutzniveaus mit sich (sog. “Transfer Impact Assessment”, kurz TIA, auf Deutsch: “Datentransfer-Folgeabschätzung” bezeichnet).

Doch auch dies reichte mitunter nicht aus: Die österreichische und die französische Datenschutzbehörde haben unabhängig voneinander Anfang 2022 aufgrund von Datenschutzbeschwerden entschieden, dass die Einbindung z. B. des Tracking-Tools Google Analytics regelmäßig gegen die DSGVO verstoße. Insbesondere genügten nach ihrer Auffassung die für die Übermittlung in die USA verwendeten SCCs nicht, um auszuschließen, dass die übertragenen Daten der Überwachung durch US-Nachrichtendienste unterliegen könnten. Auch der EDSA empfahl 2020 zusätzliche Schutzmaßnahmen und legte dabei den Fokus auf technische Maßnahmen (z. B. Verschlüsselung oder Pseudonymisierung personenbezogener Daten vor der Datenübermittlung), die dann durch vertragliche und organisatorische Maßnahmen ergänzt werden können. Im Ergebnis verblieb daher bislang stets ein gewisses Restrisiko bei einem Transfer von Daten in die USA.

II. Trans-Atlantic Data Privacy Framework

Der Angemessenheitsbeschluss soll nun die lang ersehnte Rechtssicherheit für den Datentransfer in die USA schaffen. So erklärte die Kommissionspräsidentin Ursula von der Leyen: „*Der neue Datenschutzrahmen EU-USA wird einen sicheren Datenverkehr für die Europäerinnen und Europäer gewährleisten und den Unternehmen auf beiden Seiten des Atlantiks Rechtssicherheit bieten.*“

1. Neue verbindliche Garantien des DPF

Schwerpunkt des US-Rechtsrahmens ist die Verbesserung der Sicherheitsvorkehrungen für nachrichtendienstliche Tätigkeiten der Vereinigten Staaten im Bereich Fernmelde- und

elektronische Aufklärung. Mit der Durchführungsverordnung wurden die von den USA im Rahmen dieser grundsätzlichen Einigung eingegangenen Verpflichtungen in US-amerikanisches Recht umgesetzt und die Pflichten der US-amerikanischen Unternehmen innerhalb des Datenschutzrahmens EU-USA ergänzt.

Der DPF sieht für die von den Datenübermittlungen an teilnehmende Unternehmen in den USA betroffenen EU- Bürger mehrere **neue Rechte** vor. Die US-Regierung hat zudem ein **neues zweistufiges Rechtsbehelfsverfahren** mit unabhängigen und verbindlichen Befugnissen eingerichtet, mit dem Beschwerden von Einzelpersonen, deren Daten aus dem EWR an Unternehmen in den USA übermittelt wurden, bezüglich der Verarbeitung ihrer Daten durch US-Nachrichtendienste beigelegt werden sollen. Die neuen Beschränkungen und Garantien enthalten Regelungen zu:

- **Verhältnismäßigkeit:** Die US-Nachrichten verpflichten sich, den Zugriff auf Daten von EU-Bürgern auf das zum Schutz der nationalen Sicherheit erforderliche und verhältnismäßige Maß zu beschränken.
- **Beschwerdeverfahren:** Auf der ersten Ebene können EU-Bürger eine Beschwerde beim “Civil Liberties Protection Officer”, dem Bürgerrechtsbeauftragten der US-Nachrichtendienste, einreichen. Dazu reicht es aus, dass sie eine Beschwerde bei ihrer nationalen Datenschutzbehörde einreichen. Diese sorgt dafür, dass die Beschwerde ordnungsgemäß in die USA übermittelt wird und der Beschwerdeführer alle weiteren Informationen über das Verfahren sowie das Ergebnis erhält.
- **Überprüfungsverfahren:** Auf der zweiten Ebene können Einzelpersonen die Entscheidung des “Civil Liberties Protection Officer” vor dem neu geschaffenen “Data Protection Review Court” anfechten. Der Review Court ist befugt, Beschwerden von EU-Bürgern zu untersuchen sowie die relevanten Informationen von Nachrichtendiensten anzufordern. Der Review Court kann verbindliche Entscheidungen treffen und beispielsweise die Löschung von Daten anordnen, wenn festgestellt wird, dass gegen die in der Durchführungsverordnung vorgesehenen Schutzmaßnahmen verstoßen wurde.

III. Kommentar: Auswirkungen für Unternehmen

Mit dem Erlass des DPF kann der Datentransfer von personenbezogenen Daten in die USA ohne zusätzliche Sicherheiten erfolgen. Die Vereinbarung von SCCs und die Durchführung von TIAs sind grundsätzlich nicht mehr erforderlich. Abgeschlossene SCCs bleiben gleichwohl in Kraft. Unternehmen sollten zudem folgendes beachten:

1. Zertifizierung der Organisation erforderlich

Dies **gilt jedoch nur**, sofern der jeweilige Datenimporteur, an den personenbezogene Daten übermittelt werden, auch unter dem DPF zertifiziert ist. Dies müssen Unternehmen in der EU vorab prüfen. Dabei müssen auch die **Angaben zur Reichweite der Zertifizierung unter dem DPF** beachtet werden. Das DPF wird vom US-Department of Commerce verwaltet, das Zertifizierungsanträge bearbeitet und überwacht, ob die teilnehmenden Unternehmen weiterhin die Zertifizierungsanforderungen erfüllen.

Dieses veröffentlicht – wie auch seinerzeit für die Vorgängerabkommen Safe Harbour und Privacy Shield – online eine entsprechende Liste, anhand welcher überprüft werden kann, ob die betreffende Organisation zertifiziert ist. Unternehmen, die sich bereits dem Privacy Shield angeschlossen haben, wird wahrscheinlich ein einfacherer Zugang zur Zertifizierung angeboten werden. Es ist davon auszugehen, dass große US-Unternehmen wie Meta, Google und Microsoft die Zertifizierung zeitnah nutzen werden.

Für den Fall, dass der Empfänger über keine Zertifizierung verfügt, bleibt es bei der notwendigen Anwendung der SCCs. Allerdings kann dann aller Voraussicht nach im Rahmen der Durchführung des TIAs auf eine intensive Prüfung des Vorliegens von ausreichenden Zusatzgarantien durch den Verweis auf den Angemessenheitsbeschluss verzichtet werden.

2. Rechts(un)sicherheit

Die Funktionsweise des DPF soll regelmäßig gemeinsam von der Europäischen Kommission und den Vertretern der europäischen Datenschutzbehörden sowie der zuständigen US-Behörden überprüft werden. Die erste Überprüfung soll binnen eines Jahres nach dem Inkrafttreten des DPF erfolgen, um zu ermitteln, ob alle einschlägigen Elemente vollständig umgesetzt wurden und in der Praxis wirksam funktionieren.

Es steht fest: Rechtssicherheit bietet das DPF nur so lange, wie ein „angemessenes Schutzniveau“ in den USA gewährleistet ist und der EuGH das DPF nicht für unwirksam erklärt.

Das DPF ist abhängig von der Durchführungsverordnung der USA. Auch der Europäische Datenschutzausschuss (EDSA) hebt in seiner Stellungnahme zum DPF aus Februar 2023 hervor, dass seine Zustimmung vom tatsächlichen und praktischen Vollzug der von den USA vorgeschlagenen Anpassungen abhänge, etwa im Hinblick auf die Definition von Verhältnismäßigkeit und die Reaktion auf Abhilfeersuche. Es kann jedoch nicht mit Sicherheit angenommen werden, dass die Durchführungsverordnung allen zukünftigen politischen Entwicklungen in den USA standhalten wird.

Zudem sind bereits jetzt **EuGH-Klagen** am Horizont erkennbar. Der NOYB-Vorsitzende Max Schrems, der beide vorherigen Angemessenheitsbeschlüsse vor dem EuGH erfolgreich angegriffen hatte, begrüßt den neuen Angemessenheitsbeschluss mit den Worten: "*Man sagt, die Definition von Wahnsinn ist, dass man immer wieder das Gleiche tut und dennoch ein anderes Ergebnis erwartet.*" Der Datenschutzverein NOYB hält den neuen Angemessenheitsbeschluss für eine „weitgehende Kopie" des Vorgängers, ohne dass die im „Schrems II- Urteil" gerügte Überwachungsproblematik der USA gelöst worden sei. NOYB bereitet sich bereits jetzt für die erneute Anfechtung beim EuGH vor. Sollte der Fall dem EuGH noch dieses Jahr vorgelegt werden, wäre eine endgültige Entscheidung voraussichtlich nicht vor 2025 zu erwarten. Zu berücksichtigen ist dabei, dass der EuGH in der Vergangenheit den Privacy Shield mit sofortiger Wirkung für ungültig erklärt und den Unternehmen keine Frist für den Wechsel zu einem alternativen Übermittlungsmechanismus eingeräumt hat.

Wer in Zukunft nicht gezwungen werden will, ad hoc auf politische Entscheidungen der EU-Kommission, des EuGH oder der US-Regierung zu reagieren, setzt beim Einsatz von US-Anbietern nicht nur auf den Angemessenheitsbeschluss, sondern ergreift vorsichtshalber auch weitere Maßnahmen, wie z. B. den Abschluss der SCC als alternativer Transfermechanismus, oder prüft, ob andere Rechtsgrundlagen den Transfer rechtfertigen können (Art. 49 DSGVO).

Auch eine Überprüfung und Bewertung des eigenen Datentransfers an US-Dienstleister im Rahmen der Durchführung eines TIAs ist weiterhin zu empfehlen. Dieses bleibt ein wertvolles Instrument, um sicherzustellen, dass diese die notwendigen Datenschutzanforderungen vollständig erfüllen.

IV. Praktische Hinweise

- Das DPF trat mit seiner Annahme am 10. Juli 2023 in Kraft.
- Mit seiner Annahme können EU-Unternehmen nun **grundsätzlich** personenbezogene Daten an am DPF teilnehmende US-Unternehmen übermitteln, ohne zusätzliche Datenschutzgarantien abschließen bzw. einführen zu müssen.
- Liegt ein Angemessenheitsbeschluss vor, ist die Übermittlung von Daten in diesen Drittstaat unter denselben Voraussetzungen zulässig, unter denen auch eine Datenübermittlung innerhalb des EWR zulässig wäre. Das bedeutet: **Auch Übermittlungen in Drittstaaten mit angemessenem Datenschutzniveau bedürfen einer Rechtsgrundlage für die Datenverarbeitung nach Art. 6 oder 9 DSGVO** bzw. des BDSG. Das DPF ist zudem **kein Freibrief für jegliche Datenübermittlung** in die USA. Es gibt Sonderregelungen, wie bspw. bei der Verarbeitung von Gesundheitsdaten, oder auch branchenspezifische Vorgaben, wie z. B. in der Finanzbranche, die ggf. ergänzend zu beachten sind. Hier ist Diskussionsbedarf mit US-Unternehmen zu erwarten, da diese aller Voraussicht neben dem DPF keine weiteren Regelungen abschließen wollen.
- Der Angemessenheitsbeschluss macht zudem **den Abschluss von Auftragsverarbeitungsverträgen oder Joint-Controller-Vereinbarungen nicht obsolet.** Verschaffen Sie sich auch einen Überblick über Subunternehmer ihrer US-Vertragspartner, die ggf. nicht nur in den USA, sondern in China oder Indien ihren Sitz haben. Auch mit diesen sind vertragliche Regelungen und ausreichende Garantien zu vereinbaren, die den Transfer von Daten legitimieren.
- **Datenschutzerklärungen aktualisieren**: Der Hinweis auf einen Angemessenheitsbeschluss bei einem Drittlandtransfer ist gemäß Art. 13 Abs. 1 lit. f) DSGVO verpflichtend. Auch bei der Angabe der Empfänger der übermittelten Daten muss darüber informiert werden, ob diese unter das DPF fallen.
- **Verarbeitungsverzeichnisse aktualisieren**: Die Verarbeitungsverzeichnisse im Sinne des Art. 30 DSGVO, die einen US-Datentransfer dokumentieren, müssen durch die Angabe des Angemessenheitsbeschlusses als Rechtsgrundlage für den Datentransfer ergänzt werden.
- **Standardvertragsklauseln** bleiben weiter wirksam und können höhere Anforderungen (Zusatzgarantien) an die Sicherheit der Datenübermittlung in die USA regeln, als das DPF vorsieht. Die Durchführung von **Datentransfer-Folgenabschätzungen (TIAs)** ist weiterhin zu empfehlen. Bestehende SCC sollten zunächst nicht ersetzt werden, da

offen ist, ob und wie lange das DPF in Kraft bleibt. Daneben lassen sich die oben dargestellten Bedenken der Datenschutzaufsichtsbehörden, dass die auf Grundlage der SCCs übertragenen Daten der Überwachung durch US-Nachrichtendienste unterliegen könnten, nicht mehr ohne Weiteres aufrechterhalten. Eine solche lückenlose Überwachung soll gerade durch das DPF verhindert werden und die Prozesse in den USA wurden entsprechend umgesetzt.

Ihre Ansprechpartner:

Dr. Jörg Alshut
Rechtsanwalt, Licencié en Droit (Orléans), Partner
Berlin
T +49 30 52133 21890
joerg.alshut@luther-lawfirm.com

Silvia C. Bauer
Rechtsanwältin, Partnerin
Köln
T +49 221 9937 25789
silvia.c.bauer@luther-lawfirm.com

Dr. Maximilian Dorndorf
Rechtsanwalt, Partner
Essen
T +49 201 9220 24027
maximilian.dorndorf@luther-lawfirm.com

Dr. Stefanie Hellmich, LL.M.
Rechtsanwältin, Partnerin
Frankfurt a.M.
T +49 69 27229 24118
stefanie.hellmich@luther-lawfirm.com

Christian Kuß, LL.M.
Rechtsanwalt, Partner
Köln
T +49 221 9937 25686
christian.kuss@luther-lawfirm.com

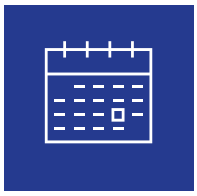
Dr. Kay Oelschlägel
Rechtsanwalt, Fachanwalt für IT-Recht, Partner
Hamburg
T +49 40 18067 12175
kay.oelschlaegel@luther-lawfirm.com

Dr. Michael Rath
Rechtsanwalt, Fachanwalt für IT-Recht, Certified ISO/IEC 27001 Lead Auditor, Partner
Köln
T +49 221 9937 25795
michael.rath@luther-lawfirm.com

Dr. Wulff-Axel Schmidt
Rechtsanwalt, Partner
Frankfurt a.M.
T +49 69 27229 27078
wulff-axel.schmidt@luther-lawfirm.com

Carsten Andreas Senze
Rechtsanwalt, Partner
Stuttgart
T +49 711 9338 25222
carsten.a.senze@luther-lawfirm.com

Veranstaltungen, Veröffentlichungen und Blog



Eine Übersicht mit unseren Veranstaltungen finden Sie hier.

Eine Liste unserer aktuellen Veröffentlichungen finden Sie hier.

Unseren Blog finden Sie hier.

Impressum

Verleger: Luther Rechtsanwaltsgesellschaft mbH
Anna-Schneider-Steig 22, 50678 Köln, Telefon +49 221 9937 0
Telefax +49 221 9937 110, contact@luther-lawfirm.com
V.i.S.d.P.: Silvia C. Bauer
Luther Rechtsanwaltsgesellschaft mbH
Anna-Schneider-Steig 22, 50678 Köln, Telefon +49 221 9937 0
maximilian.dorndorf@luther-lawfirm.com

Bildnachweis: Seite 1: Denis Putilov / Adobe Stock

Haftungsausschluss

Obgleich dieser Newsletter sorgfältig erstellt wurde, wird keine Haftung für Fehler oder Auslassungen übernommen. Die Informationen dieses Newsletters stellen keinen anwaltlichen oder steuerlichen Rechtsrat dar und ersetzen keine auf den Einzelfall bezogene anwaltliche oder steuerliche Beratung. Hierfür stehen unsere Ansprechpartner an den einzelnen Standorten zur Verfügung.

Stand: Juli 2023