EDV-Unternehmensberatung
Floß GmbH

Informationsblatt zum neuen EU-US Angemessenheitsbeschluss (Trans-Atlantic Data Protection Framework, TADPF)

Stand des Dokuments: 17.07.2023

Inhaltsverzeichnis

1. Hintergrund: Was hat es mit dem Angemessenheitsbeschluss auf sich?

Seitdem der Europäische Gerichtshof (EuGH) das Datenschutzniveau in den USA im Jahr 2020 als unzureichend deklariert hatte, herrscht bei europäischen Unternehmen sowie öffentlichen Stellen (Behörden) eine große Rechtsunsicherheit im Hinblick auf eventuelle Datenübermittlungen in die USA. Praxisrelevant ist dieses Thema vor allem bei Unternehmen und Behörden, welche Dienstleister mit US-Bezug als Auftragsverarbeiter einsetzen. Dies betrifft Dienste wie zum Beispiel Microsoft Office, Amazon Web Service, Atlassian sowie Google- oder Meta- (vormals Facebook) Anwendungen.

Hintergrund dieser Entscheidung des EuGH sind die sogenannten Edward Snowden Enthüllungen aus dem Jahr 2013. Dieser deckte auf, dass die US-Regierung amerikanische Technologiekonzerne und Spionage-Programme wie "PRISM" oder "Upstream" im Rahmen amerikanischer Überwachungsgesetze (FISA 702 und EO 12.333) nutzte. Es wurden geheimdienstliche Aktivitäten gegenüber Personen und Unternehmen ohne hinreichenden Verdacht oder richterliche Genehmigungen durchgeführt. Insoweit ist die Hauptkritik des EuGH der Verstoß gegen die Grundrechte der Betroffenen auf Privatsphäre, Datenschutz, Verhältnismäßigkeit und wirksamen Rechtsschutz.

Die Europäische Datenschutzgrundverordnung (DSGVO) hat infolge des sogenannten „Marktortprinzips“ (Art. 3 Abs. 2 lit. a) einen Anwendungsbereich, der weit über die Union hinaus geht und den Anspruch hat, personenbezogene Daten, die aus Europa ausgeleitet werden, gleichermaßen wie in der EU zu schützen. Nach der DSGVO ist die grenzüberschreitende Datenübermittlung in ein Drittland außerhalb der EU nur unter bestimmten Voraussetzungen erlaubt, damit das europäische Datenschutzniveau nicht untergraben werden kann (Art. 44 S. 2 DSGVO).

In diesem Zusammenhang sind die in den Art. 44 ff. DSGVO niedergelegten Datenschutzgarantien von Bedeutung. Für die USA lag kein Angemessenheitsbeschluss im Sinne des Art. 45 DSGVO vor, welcher anerkennen würde, dass in den USA ein der EU entsprechendes Datenschutzniveau herrscht. Daher ist für die Datenübermittlung in die Vereinigten Staaten eine häufig genutzte Rechtsgrundlage die von der Europäischen Kommission vorgegebenen EU-Standardvertragsklauseln (Art. 46 Abs. 2 lit. c DSGVO).

Zudem stützten sich US-Technologiekonzerne zunächst auf eine Entscheidung der Europäischen Kommission mit der Bezeichnung "Safe Harbor", mit welcher der Datenschutz bei im Sinne dieses Abkommens zertifizierten US-Unternehmen "im Wesentlichen als gleichwertig" erklärt wurde. Der EuGH hat die Entscheidung der Kommission in der Rechtssache C-362/14 ("Schrems I") im Jahr 2015 angesichts der vagen US-Überwachungsgesetze für nichtig erklärt. In einem neuen Anlauf hat die

Europäische Kommission im Jahr 2016 de facto eine nahezu gleiche – und somit vielkritisierte - Entscheidung über Datenübermittlungen zwischen der EU und den USA unter dem neuen Namen "Privacy Shield" erneut erlassen. Dieses Abkommen wurde dann vom EuGH in der Rechtssache C-311/18 ("Schrems II") im Jahr 2020 mit nahezu derselben Begründung wie im ersten Verfahren für ungültig erklärt.

Somit sind Unternehmen und Behörden, welche infolge z. B. des Einsatzes von Dienstleistern mit US-Bezug Drittstaatenübermittlungen auslösen, ständig dem Risiko von Bußgeldern seitens Datenschutzaufsichtsbehörden oder Klagen durch Betroffene ausgesetzt. Um wieder rechtssichere Drittstaatenübermittlungen in die USA zu ermöglichen, kündigte die Europäische Kommission daher nach der letzten EuGH-Entscheidung von 2020 an, dass ein neues "Rahmenabkommen" mit der US-Regierung ausgearbeitet werden solle.

Am 10.07.2023 hat die Europäische Kommission einen **neuen Angemessenheitsbeschluss (Trans-Atlantic Data Privacy Framework, kurz „TADPF“)** für einen sicheren und vertrauenswürdigen Datenverkehr zwischen der EU und den USA angenommen.[1] Auf der Grundlage des neuen Angemessenheitsbeschlusses können personenbezogene Daten aus der EU an US-Unternehmen, welche im Sinne des TADPF zertifiziert sind, **momentan rechtssicher** übermittelt werden, ohne dass zusätzliche Datenschutzvorkehrungen getroffen werden müssen. Die einzige Voraussetzung ist, dass sich der US-Datenempfänger nach dem TADPF selbst zertifiziert und dem EU-Exporteur gegenüber vertraglich zur Einhaltung desselben verpflichtet. Mit dem TADPF hat die EU-Kommission sich bemüht, neue verbindliche Garantien einzuführen, um allen vom Europäischen Gerichtshof geäußerten Bedenken Rechnung zu tragen.

Die wesentlichen Veränderungen für betroffene EU-Bürger bestehen aus einer Einführung einer **Verhältnismäßigkeitsprüfung bei Datenzugriffen** durch US-Geheimdienste sowie der **Einrichtung eines mehrstufigen Beschwerdeverfahrens.** Diese Änderungen wurden durch US-Präsident Joe Biden in einer Executive Order vom 7. Oktober 2022 eingeführt. Auf der ersten Ebene eines Beschwerdeverfahrens können EU-Bürger eine Beschwerde beim “Civil Liberties Protection Officer” (CLPO) der US-Geheimdienste einreichen. Dieser CLPO trägt die Verantwortung dafür, dass die US-Geheimdienste die Privatsphäre und Grundrechte wahren. Auf der zweiten Ebene haben Einzelpersonen die Möglichkeit, die Entscheidung des Civil Liberties Protection Officer vor dem neu geschaffenen “Data Protection Review Court” (DPRC) anzufechten. Dieser Überprüfungsgerichtshof soll sich aus unabhängigen Mitgliedern zusammensetzen, die aufgrund spezieller Qualifikationen ernannt und nur aus schwerwiegenden Gründen entlassen werden können, wie beispielsweise einer strafrechtlichen Verurteilung. Der Review Court soll berechtigt sein, Beschwerden von

[1] Text zunächst in englischer Sprache hier verfügbar: https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en

EU-Bürgern zu untersuchen, einschließlich der Anforderung relevanter Informationen von Geheimdiensten, und er kann verbindliche Entscheidungen treffen.

2. Kritik am TADPF, Ausblick auf zukünftige Entwicklungen

Ob es der EU-Kommission gelungen ist, die Bedenken des EuGHs auszuräumen, steht noch in den Sternen. Die Kritik an diesem Abkommen ist groß und verweist im Wesentlichen darauf, dass die neu eingeführten Garantien, welche für einen verbesserten Grundrechtsschutz von Betroffenen sorgen sollen, bei weitem nicht ausreichen. Während diese Neuheiten grundsätzlich begrüßenswert sind, erfahren diese jedoch auch im Detail grundlegende Kritik.

Zunächst hat die US-Regierung versäumt, ihre bisherigen Überwachungsgesetze (insbesondere FISA 702) zu ändern. Zudem wird befürchtet, dass die USA im Rahmen der Prüfung der Verhältnismäßigkeit von Datenzugriffen ein grundlegend anders Verständnis von „Verhältnismäßigkeit“ hat als der europäische Gerichtshof. Im Rahmen der Verhandlungen der US-Regierung mit der EU-Kommission wurde versäumt, ein gemeinsames Verständnis hiervon zu entwickeln.

Ferner werden die neu eingerichteten mehrstufigen Rechtsbehelfe im Hinblick auf Zugänglichkeit und Effizienz für EU-Bürger kritisiert. So wird der einzelne EU-Bürger, der sich beschweren möchte, keine direkte Interaktion mit den Beschwerdeinstitutionen selbst haben. Vielmehr muss der betreffende EU-Bürger eine Beschwerde an eine EU-Datenschutzbehörde schicken und diese leitet sie weiter. Ferner wird kein konkretes Ergebnis des Überprüfungsverfahrens mitgeteilt. Vielmehr erhält der betreffende EU-Bürger lediglich eine generische Nachricht darüber ob Verstöße festgestellt wurden. Dies ohne eine konkrete Information darüber, ob er/sie Ziel geheimdienstlicher Aktivitäten ist oder war. Weiterhin könnte eine Abhilfemaßnahme die Löschung von Daten sein, aber andere Betroffenenrechte werden gar nicht adressiert (Auskunft, Berichtigung…). In Bezug auf den neu einzurichtenden “Data Protection Review Court” ist ein Kritikpunkt, dass es sich nicht um ein echtes Gericht im Sinne der US-Verfassung, sondern um eine neu geschaffene Institution in Bereich der Exekutive handelt. Dies ist relevant, da der EuGH in seinem Schrems II Urteil festgestellt hatte, dass ein Rechtsbehelf im Sinne von Art. 47 EU-Grundrechtecharta erforderlich ist (vgl. Rn. 168). In der Executive Order gibt es aber keine Vorgabe, dass die Argumente bzw. das Vorbringen der Betroffenen überhaupt angehört werden müssen. Daher ist es fraglich, ob der EuGH die Einrichtung der neuen Überprüfungsinstanzen als tatsächlich wirksame Rechtsbehelfe für Betroffene sehen wird.

Aufgrund dieser Kritikpunkte hat die österreichische Nichtregierungsorganisation NOYB – Europäisches Zentrum für digitale Rechte (von englisch none of your business, übersetzt: „geht dich nichts an“) bereits angekündigt, gegen den

Angemessenheitsbeschluss der EU-Kommission klagen zu wollen.[2] NOYB rechnet mit einer EuGH-Vorlage gegen Ende 2023 oder Anfang 2024, mit einer Entscheidung desselben irgendwann im Jahre 2024 oder 2025. Für die Dauer des Verfahrens könnte der EuGH das TADPF aussetzen, mit der Folge, dass Übermittlungen auf dieser Basis sodann nicht mehr stattfinden dürfen.

Insoweit bleibt abzuwarten, ob dieses Abkommen ebenfalls dem EuGH zur Prüfung vorgelegt wird und ob es im Gegensatz zu seinen Vorgängern Bestand behält. Dies ist ein verbleibendes Risiko für EU-Unternehmen, welche US-Dienste einsetzen möchten.

3. Was Sie jetzt tun sollten

Unternehmen sollten nun im Hinblick auf das TADPF eine Reihe von Maßnahmen in Angriff nehmen. Diese sind:

1. Prüfung, welche der eigenen, eingesetzten US-Dienstleister nach dem Data Privacy Framework zertifiziert sind. Die Liste der nach dem TADPF selbstzertifizierten Unternehmen wird voraussichtlich auf der Webseite des US Department of Commerce hier verfügbar sein:
   https://www.dataprivacyframework.gov/s/

   - Entscheidung der Geschäftsführung, ob zur rechtlichen Absicherung trotz des Vorliegens von TADPF-Zertifizierungen eingesetzter Dienstleister dennoch die EU-Standardvertragsklauseln abgeschlossen werden sollen.

   - Entscheidung der Geschäftsführung, ob zur rechtlichen Absicherung trotz des Vorliegens von TADPF-Zertifizierungen eingesetzter Dienstleister dennoch Transferfolgenabschätzungen durchgeführt werden sollen.

2. Eine Vereinbarung über eine Auftragsverarbeitung inkl. der Anlage technische und organisatorische Maßnahmen (TOMs) im Sinne des Art. 28 DSGVO ist nach wie vor zwingend erforderlich. Zuvor muss die übliche Prüfung eines zukünftigen Auftragsverarbeiters in nachweisbarer Form erfolgen.

3. Prüfung, ob - unabhängig von der Drittstaatenthematik - je nach Verfahren eine Datenschutzfolgenabschätzung durchzuführen ist.

[2] Siehe öffentliche Stellungnahme von NOYB vom 10.07.2023, https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu

4. Anpassung aller relevanten Datenschutzhinweise (für Webseiten, für Beschäftigte und Kunden…).

   - Der Hinweis auf einen Angemessenheitsbeschluss bei Datentransfers in Drittländer ist eine Pflichtangabe in Datenschutzhinweisen (siehe Art. 13 Abs. 1 lit. e) DSGVO).

5. Anpassung aller relevanten Verzeichnisse für Verarbeitungstätigkeiten nach Art. 30 DSGVO (Verfahrensverzeichnisse).

Kontaktieren Sie uns, wenn wir Sie Fragen haben oder Beratung bei der Umsetzung benötigen. Wir helfen Ihnen gerne und mit Sachverstand weiter.

Ihr Floß Team