DATENSCHUTZRAHMEN EU-USA

HÄUFIG GESTELLTE FRAGEN (FAQ) FÜR EUROPÄISCHE UNTERNEHMEN[1]

Angenommen am 16. Juli 2024

Translations proofread by EDPB Members.
This language version has not yet been proofread.

[1] In diesem Kontext bezieht sich „europäische Unternehmen“ auf Unternehmen im EWR, die personenbezogene Daten an nach dem Datenschutzrahmen EU-USA zertifizierte Unternehmen in den USA übermitteln oder übermitteln können.

Inhalt

FRAGE 1: WAS IST DER DATENSCHUTZRAHMEN EU-USA?

Beim Datenschutzrahmen EU-USA („Datenschutzrahmen“) handelt es sich um einen Selbstzertifizierungsmechanismus für Unternehmen in den USA. Unternehmen, die sich gemäß dem Datenschutzrahmen selbstzertifiziert haben, müssen Grundsätze, Vorschriften und Pflichten im Zusammenhang mit der Verarbeitung personenbezogener Daten von EWR-Personen einhalten. Weitere Informationen über diese Verpflichtungen finden Sie in den Grundsätzen des Datenschutzrahmens.[2]

Die Europäische Kommission war der Auffassung, dass Übermittlungen personenbezogener Daten aus dem EWR an Unternehmen in den USA, die gemäß dem Datenschutzrahmen zertifiziert sind, ein angemessenes Schutzniveau genießen.[3] Infolgedessen können personenbezogene Daten ungehindert an in den USA zertifizierte Unternehmen übermittelt werden, ohne dass weitere Sicherheitsvorkehrungen getroffen oder eine Genehmigung eingeholt werden müssten. Hier finden Sie einige relevante Links mit weiteren Informationen:

- Europäische Kommission: Fragen und Antworten:Datenschutzrahmen[4]
- Website zum Datenschutzrahmen des US-Handelsministeriums[5]
- Entscheidung der Europäischen Kommission über ein angemessenes Schutzniveau für personenbezogene Daten im Rahmen des Datenschutzrahmens EU-USA[6]

Der Datenschutzrahmen gilt für alle Arten von personenbezogenen Daten, die aus dem EWR in die USA übermittelt werden, einschließlich personenbezogener Daten, die zu kommerziellen oder gesundheitlichen Zwecken verarbeitet werden, und Personaldaten, die im Rahmen eines Beschäftigungsverhältnisses erhoben werden (im Folgenden: „Personaldaten“), solange das Empfängerunternehmen in den USA im Rahmen des Datenschutzrahmens selbstzertifiziert ist, diese Arten von Daten zu verarbeiten.[7]

FRAGE 2: WELCHE US-UNTERNEHMEN KOMMEN FÜR DEN DATENSCHUTZRAHMEN EU-USA INFRAGE?

Um zur Selbstzertifizierung gemäß dem Datenschutzrahmen berechtigt zu sein, muss ein Unternehmen in den USA den Ermittlungs- und Durchsetzungsbefugnissen der US-Handelskommission (Federal Trade Commission, „FTC“) oder des US-Verkehrsministeriums

[2] https://www.dataprivacyframework.gov/program-articles/Participation-Requirements-Data-Privacy-Framework-(DPF)-Principles

[3] Der Angemessenheitsbeschluss für den Datenschutzrahmen EU-USA wurde von der Europäischen Kommission am 10. Juli 2023 angenommen. Er wurde von der Europäischen Kommission und dem US-Handelsministerium als Ersatz für den Beschluss (EU) 2016/1250 zum Datenschutzschild konzipiert, der vom Europäischen Gerichtshof am 16. Juli 2020 in der Rechtssache C-311/18, *Data Protection Commissioner gegen Facebook Ireland Limited und Maximilian Schrems (Schrems II)*, für ungültig erklärt wurde.

[4] https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_3752

[5] https://www.dataprivacyframework.gov/s/

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

[7] Nicht alle Selbstzertifizierungen gemäß dem Datenschutzrahmen decken Personaldaten ab. Daher ist gegebenenfalls zu prüfen, ob dies der Fall ist. Siehe auch Frage 3.

(Department of Transportation, „DoT“) unterliegen. In Zukunft könnten noch weitere US-Behörden einbezogen werden.[8]

Dies bedeutet, dass beispielsweise gemeinnützige Organisationen, Banken, Versicherungsunternehmen und Betreiber öffentlicher Telekommunikationsnetze (in Bezug auf den Betrieb öffentlicher Telekommunikationsnetze), die nicht in die Zuständigkeit der FTC oder des DoT fallen, keine Selbstzertifizierung nach dem Datenschutzrahmen vornehmen können.

FRAGE 3: WELCHE MAßNAHMEN SIND ZU TREFFEN, BEVOR PERSONENBEZOGENE DATEN AN EIN UNTERNEHMEN IN DEN USA ÜBERMITTELT WERDEN, DAS TATSÄCHLICH ODER VORGEBLICH GEMÄß DEM DATENSCHUTZRAHMEN ZERTIFIZIERT IST?

Bevor ein Datenexporteur im EWR personenbezogene Daten an ein Unternehmen in den USA übermittelt, das behauptet, gemäß dem Datenschutzrahmen selbstzertifiziert zu sein, muss er sich vergewissern, dass das Unternehmen in den USA über eine aktive Selbstzertifizierung verfügt (Zertifizierungen müssen jährlich erneuert werden) und dass diese Zertifizierung die fraglichen Daten abdeckt (insbesondere, ob sie Personaldaten bzw. Nicht-Personaldaten abdeckt).[9]

Um zu überprüfen, ob eine gültige Selbstzertifizierung vorliegt, müssen Datenexporteure im EWR nachsehen, ob das betreffende Unternehmen in den USA auf der Liste zum Datenschutzrahmen EU-USA[10] auf der Website des US-Handelsministerium geführt wird. Diese Liste enthält auch ein Verzeichnis der Unternehmen, die aus der Liste gestrichen wurden („*inactive participants*“ – inaktive Teilnehmer), wobei die Gründe für die Streichung angegeben werden. Ein Datenexporteur aus dem EWR kann sich bei der Übermittlung personenbezogener Daten an solche Unternehmen nicht auf den Datenschutzrahmen berufen. Bitte beachten Sie, dass Unternehmen, die aus der Liste zum Datenschutzrahmen gestrichen wurden, weiterhin die Grundsätze des Datenschutzrahmens auf personenbezogene Daten anwenden müssen, die sie erhalten haben, während sie sich am Datenschutzrahmen beteiligten, solange sie diese Daten speichern.

Für die Übermittlung personenbezogener Daten an Unternehmen in den USA, die nicht (oder nicht mehr) nach dem Datenschutzrahmen selbstzertifiziert sind, können andere Übermittlungsgründe gemäß Kapitel V der DSGVO genutzt werden, z. B. verbindliche interne Datenschutzvorschriften oder Standardvertragsklauseln.

Die Tatsache, dass der Empfänger in den USA gemäß dem Datenschutzrahmen selbstzertifiziert ist, ermöglicht es Datenexporteuren im EWR, Kapitel V der DSGVO einzuhalten, aber alle anderen Anforderungen der DSGVO und anderer nationaler Datenschutzvorschriften bleiben anwendbar.

3.1. Übermittlungen an US-Tochtergesellschaften von Unternehmen, die gemäß dem Datenschutzrahmen EU-USA zertifiziert sind

[8] Siehe Anhang I des Angemessenheitsbeschlusses, Grundsätze des Datenschutzrahmens EU-USA, herausgegeben vom US-Handelsministerium, Absatz I.2.
[9] Siehe die Definition von „Personaldaten“ unter Frage 1.
[10] https://www.dataprivacyframework.gov/list

Bei Übertragungen an Unternehmen in den USA, die Tochtergesellschaften einer gemäß dem Datenschutzrahmen zertifizierten Muttergesellschaft sind, müssen die EWR-Datenexporteure prüfen, ob sich die Zertifizierung der Muttergesellschaft auch auf die betreffende Tochtergesellschaft erstreckt.

Weitere Informationen darüber, wie Sie den Umfang der Selbstzertifizierung eines Unternehmens überprüfen können, einschließlich der Frage, ob andere US-Unternehmen oder US-Tochtergesellschaften abgedeckt sind, finden Sie hier.[11]

3.2. Übermittlungen an ein Unternehmen in den USA, das als für die Verarbeitung Verantwortlicher fungiert

Vor der Übermittlung personenbezogener Daten an einen für die Verarbeitung Verantwortlichen in den USA muss ein Datenexporteur aus dem EWR sicherstellen, dass die Übermittlung allen einschlägigen Bestimmungen der DSGVO entspricht. In einem ersten Schritt kann der Datenexporteur personenbezogene Daten nur dann an ein Unternehmen in den USA weitergeben, wenn es eine Rechtsgrundlage für die Verarbeitung gibt (Artikel 6 DSGVO). Darüber hinaus müssen alle anderen Anforderungen der DSGVO erfüllt werden (z. B. Zweckbindung, Verhältnismäßigkeit, Richtigkeit und Informationspflichten gegenüber betroffenen Personen). Zu beachten ist, dass der Datenexporteur aus dem EWR gemäß den Artikeln 13 und 14 der DSGVO bei der Übermittlung von Daten an ein selbstzertifiziertes Unternehmen in den USA die betroffenen Personen über die Identität der Empfänger ihrer Daten und darüber informieren muss, dass die Übermittlung unter den Angemessenheitsbeschluss für den Datenschutzrahmen EU-USA fällt.

3.3. Übermittlungen an ein Unternehmen in den USA, das als Auftragsverarbeiter fungiert

Wenn ein für die Verarbeitung Verantwortlicher aus dem EWR Daten an einen Auftragsverarbeiter in den USA übermittelt, sind der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter verpflichtet, einen Datenverarbeitungsvertrag gemäß Artikel 28 der DSGVO zu schließen (im Folgenden: „Datenverarbeitungsvertrag“). Diese Verpflichtung gilt unabhängig davon, ob der Auftragsverarbeiter gemäß dem Datenschutzrahmen selbstzertifiziert ist.

Weitere Informationen zu den Vertragsanforderungen für Übermittlungen an Auftragsverarbeiter in den USA finden Sie hier.[12]

Der Abschluss eines Datenverarbeitungsvertrags ist notwendig, damit sich der US-Auftragsverarbeiter dazu verpflichtet, dass er

- die personenbezogenen Daten nur auf dokumentierte Weisung des für die Verarbeitung Verantwortlichen – auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation – verarbeitet, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem für die Verarbeitung Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung

[11] https://www.dataprivacyframework.gov/program-articles/How-to-Verify-an-Organization-s-Privacy-Data-Privacy-Framework-(DPF)-Commitments
[12] https://www.dataprivacyframework.gov/program-articles/Contract-Requirements-for-Data-Transfers-to-a-Processor

mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet;

- gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen;
- geeignete technische und organisatorische Maßnahmen ergreift, um ein dem Risiko angemessenes Sicherheitsniveau im Einklang mit den Anforderungen der Datenverarbeitungsvereinbarung (gemäß Artikel 32 DSGVO) und den Abschnitten 4 und 10 des Datenschutzrahmens zu gewährleisten;
- die im Datenverarbeitungsvertrag (gemäß Artikel 28 Absätze 2 und 4 DSGVO) und in Abschnitt II.3.B des Datenschutzrahmens genannten Bedingungen für die Beauftragung eines anderen Auftragsverarbeiters einhält;
- unter Berücksichtigung der Art der Verarbeitung den Verantwortlichen, soweit möglich, mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von dessen Pflicht zur Beantwortung von Anträgen auf Ausübung der in Kapitel III der DSGVO festgelegten Rechte der betroffenen Person unterstützt;
- unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung seiner in den Artikeln 32 bis 36 der DSGVO genannten Pflichten unterstützt;
- nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder löscht oder zurückgibt und die vorhandenen Kopien löscht, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht;
- dem für die Verarbeitung Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in Artikel 28 der DSGVO niedergelegten Pflichten zur Verfügung stellt und Überprüfungen – einschließlich Inspektionen –, die vom für die Verarbeitung Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglicht und dazu beiträgt. In Bezug auf diesen letzten Punkt unterrichtet der Auftragsverarbeiter unverzüglich den Verantwortlichen, wenn seiner Ansicht nach eine Anweisung gegen den Datenschutzrahmen verstößt.

Wenn der US-Auftragsverarbeiter einen anderen Auftragsverarbeiter („Unterauftragsverarbeiter“) damit beauftragt, bestimmte Verarbeitungstätigkeiten im Namen des für die Verarbeitung Verantwortlichen im EWR durchzuführen, muss der Auftragsverarbeiter sicherstellen, dass die Anforderungen des Abschnitts II.3.B des Datenschutzrahmens erfüllt sind. Dazu gehört auch, dass der Unterauftragsverarbeiter das gleiche Schutzniveau für personenbezogene Daten bietet, wie es im Datenschutzrahmen vorgeschrieben ist, und die gleichen Datenschutzverpflichtungen erfüllt, wie sie im Datenverarbeitungsvertrag festgelegt sind. Kommt ein Unterauftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der ursprüngliche US-Auftragsverarbeiter gegenüber dem Verantwortlichen weiterhin in vollem Umfang für die Einhaltung der Pflichten des Unterauftragsverarbeiters.

FRAGE 4: WO FINDE ICH INFORMATIONEN ÜBER DIE ZERTIFIZIERUNG VON US-AMERIKANISCHEN TOCHTERGESELLSCHAFTEN EUROPÄISCHER UNTERNEHMEN?

US-Tochtergesellschaften von EWR-Unternehmen können sich selbst gemäß dem Datenschutzrahmen zertifizieren, wenn sie der Zuständigkeit der FTC oder des DoT unterliegen.

Weitere Informationen zu den Zulassungsvoraussetzungen finden Sie hier[13]. Ein Leitfaden zum Selbstzertifizierungsverfahren kann hier abgerufen werden.[14]

[13] https://www.dataprivacyframework.gov/program-articles/U-S-Subsidiaries-of-European-Businesses-Participation-in-the-Data-Privacy-Framework-(DPF)-Program

[14] https://www.dataprivacyframework.gov/program-articles/How-to-Join-the-Data-Privacy-Framework-(DPF)-Program-(part%E2%80%931)