[Nichtamtliche Übersetzung]

DATENSCHUTZRAHMEN EU-USA

[Red. Anm., Englische Bezeichnung: EU-U.S. Data Privacy Framework]

F.A.Q. FÜR EUROPÄISCHE UNTERNEHMEN[1]

Q1. Was ist der EU-US-Datenschutzrahmen?

Q2. Welche US-Unternehmen sind berechtigt, dem EU-U.S. Data Privacy Framework beizutreten?

Q3. Was ist zu tun, bevor Sie personenbezogene Daten an ein Unternehmen in den USA übermitteln, das nach dem EU-U.S. Data Privacy Framework zertifiziert ist oder behauptet, dies zu sein?

Q4. Wo finde ich Hinweise zur Registrierung von US-Tochtergesellschaften europäischer Unternehmen?

Q1. Was ist der EU-US-Datenschutzrahmen?

Der EU-US-Datenschutzrahmen („DPF“) ist ein Selbstzertifizierungsmechanismus für Unternehmen in den USA. Unternehmen, die sich im Rahmen des Datenschutzrahmens selbst zertifizieren lassen, müssen seine Grundsätze, Regeln und Pflichten in Bezug auf die Verarbeitung personenbezogener Daten von EWR-Bürgern einhalten. Weitere Informationen zu diesen Verpflichtungen finden Sie in den Grundsätzen des Datenschutzrahmens.

Die Europäische Kommission ist der Auffassung, dass Übermittlungen personenbezogener Daten aus dem EWR an im Rahmen des Datenschutzrahmens zertifizierte Unternehmen ein angemessenes Schutzniveau genießen.[2] Folglich können personenbezogene Daten uneingeschränkt an US-zertifizierte Unternehmen übermittelt werden, ohne dass weitere Schutzmaßnahmen getroffen oder eine Genehmigung eingeholt werden muss. Hier sind einige relevante Links für weitere Informationen:

- Fragen und Antworten der Europäischen Kommission: Datenschutzrahmen
- die Website des Data Privacy Framework, die vom US-Handelsministerium verwaltet wird
- Beschluss der Europäischen Kommission über ein angemessenes Schutzniveau für

[1] Unter „europäische Unternehmen“ sind in diesem Zusammenhang Unternehmen im EWR zu verstehen, die personenbezogene Daten an nach dem Datenschutzrahmen zertifizierte Unternehmen in den USA übermitteln oder übermitteln können.

[2] Der Beschluss über die Angemessenheit des Datenschutzrahmens EU-USA wurde von der Europäischen Kommission am 10. Juli 2023 angenommen. Es wurde von der Europäischen Kommission und dem US-Handelsministerium entwickelt, um den Datenschutzschild-Beschluss (EU) 2016/1250 zu ersetzen, der vom Europäischen Gerichtshof in Brüssel am 16. Juli 2020 in der Rechtssache C-311/18, Data Protection Commissioner gegen Facebook Ireland Limited und Maximillian Schrems (Schrems II) für ungültig erklärt wurde.

personenbezogene Daten im Rahmen des Datenschutzrahmens EU-USA

Der Datenschutzrahmen gilt für alle Arten von personenbezogenen Daten, die aus dem EWR in die USA übermittelt werden, einschließlich personenbezogener Daten, die für kommerzielle oder gesundheitliche Zwecke verarbeitet werden sowie für Beschäftigtendaten, die im Rahmen eines Beschäftigungsverhältnisses erhoben werden (im Folgenden: „HR Data"), solange das Empfängerunternehmen in den USA im Rahmen des Datenschutzrahmens selbst zertifiziert ist, um diese Arten von Daten zu verarbeiten.[3]

Q2. Welche US-Unternehmen sind berechtigt, dem EU-U.S. Data Privacy Framework beizutreten?

Um für eine Selbstzertifizierung beim DPF in Frage zu kommen, muss ein Unternehmen in den USA den Ermittlungs- und Durchsetzungsbefugnissen der US-amerikanischen Federal Trade Commission (im Folgenden „FTC") oder des US-Verkehrsministeriums (im Folgenden „DoT") unterliegen. Andere gesetzliche US Organe können in Zukunft einbezogen werden.[4]

Dies bedeutet, dass beispielsweise gemeinnützige Organisationen, Banken, Versicherungsgesellschaften und Telekommunikationsdienstleister (in Bezug auf common carrier Tätigkeiten), die nicht der Gerichtsbarkeit der FTC oder des DoT unterliegen, sich nicht im Rahmen des DPF selbst zertifizieren können.

Q3. Was ist zu tun, bevor Sie personenbezogene Daten an ein Unternehmen in den USA übermitteln, das nach dem EU-US-Datenschutzrahmen zertifiziert ist oder behauptet, dies zu sein?

Vor der Übermittlung personenbezogener Daten an ein Unternehmen in den USA, das behauptet, im Rahmen des Datenschutzrahmens selbst zertifiziert zu sein, muss sich ein Datenexporteur im EWR vergewissern, dass das Unternehmen in den USA über eine aktive Selbstzertifizierung verfügt (Zertifizierungen müssen jährlich erneuert werden) und dass diese Zertifizierung die betreffenden Daten abdeckt (insbesondere, wenn sie HR-Data bzw. non-HR-Data abdeckt).[5]

Um zu überprüfen, ob eine Selbstzertifizierung aktiv und anwendbar ist, müssen Datenexporteure im EWR prüfen, ob das Unternehmen in den USA auf der auf der Website des US-Handelsministeriums veröffentlichten Online-Liste des EU-US-Datenschutzrahmens (DPF-Liste) steht. Diese Liste enthält auch ein Verzeichnis der aus der Liste gestrichenen Unternehmen („inactive participants"), wobei die Gründe für ihre Streichung angegeben werden. Ein EWR-Datenexporteur kann sich bei der Übermittlung personenbezogener Daten an solche Unternehmen dann nicht auf das DPF berufen. Bitte beachten Sie, dass Unternehmen, die von der DPF-Liste entfernt wurden, weiterhin die Prinzipien des Datenschutzrahmens (DPF-Principles) auf personenbezogene Daten anwenden müssen, die sie während ihrer Teilnahme am DPF erhalten haben, solange sie diese Daten speichern.

Für die Übermittlung personenbezogener Daten an Unternehmen in den USA, die im Rahmen des Datenschutzrahmens nicht (oder nicht mehr) selbst zertifiziert sind, können andere

[3] Beachten Sie, dass nicht alle DPF-Selbstzertifizierungen HR-Data abdecken. Deshalb ist es wichtig, gegebenenfalls zu prüfen, ob dies der Fall ist. Siehe auch Q3.
[4] Siehe Anhang I des Angemessenheitsbeschlusses, Grundsätze des EU-US-Datenschutzrahmens, herausgegeben vom US-Handelsministerium, Absatz I.2.
[5] Siehe Definition von HR-Data in Q1.

Übermittlungsinstrumente gem. Kapitel V der DSGVO verwendet werden, wie z.B. verbindliche interne Datenschutzvorschriften oder Standarddatenschutzklauseln.

Die Tatsache, dass der Empfänger in den USA im Rahmen des Datenschutzrahmens selbst zertifiziert ist, ermöglicht es Datenexporteuren im EWR, Kapitel V der DSGVO einzuhalten, aber alle anderen Anforderungen der DSGVO und anderer nationaler Datenschutzgesetze bleiben anwendbar.

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

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

Weitere Informationen zur Überprüfung des Umfangs der Selbstzertifizierung einer Organisation, einschließlich der Frage, ob andere US-Unternehmen oder US-Tochtergesellschaften erfasst sind, finden Sie hier.

3.2. Übertragungen an ein Unternehmen in den USA, das als Verantwortlicher fungiert

Vor der Übermittlung personenbezogener Daten an einen für die Verarbeitung Verantwortlichen in den USA muss ein EWR-Datenexporteur 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 eine Rechtsgrundlage für die Verarbeitung besteht (Art. 6 DSGVO). Darüber hinaus müssen alle anderen Anforderungen der DSGVO erfüllt sein (z. B. Zweckbindung, Verhältnismäßigkeit, Richtigkeit und Informationspflichten gegenüber betroffenen Personen). Beachten Sie, dass der EWR-Datenexporteur bei der Übermittlung von Daten an ein selbstzertifiziertes Unternehmen in den USA gemäß den Artikeln 13 und 14 DSGVO die betroffenen Personen über die Identität der Datenempfänger sowie darüber informieren muss, dass die Übermittlung unter den Angemessenheitsbeschluss des EU-US-Datenschutzrahmens fällt.

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

Wenn ein EWR-Verantwortlicher Daten an einen Auftragsverarbeiter in den USA übermittelt, sind der Verantwortliche und der Auftragsverarbeiter verpflichtet, eine Datenverarbeitungsvereinbarung gemäß Artikel 28 DSGVO abzuschließen (im Folgenden: Datenverarbeitungsvereinbarung), unabhängig davon, ob der Auftragsverarbeiter im Rahmen des DPF selbst zertifiziert ist.

Weitere Informationen zu den Vertragsanforderungen für Übermittlungen an einen Auftragsverarbeiter in den USA finden Sie hier.

Der Abschluss einer Datenverarbeitungsvereinbarung ist erforderlich, um sicherzustellen, dass sich der US-Auftragsverarbeiter verpflichtet,

- die personenbezogenen Daten nur auf dokumentierte Weisungen des für die Verarbeitung Verantwortlichen zu verarbeiten, auch in Bezug auf die Übermittlung

personenbezogener Daten an ein Drittland oder eine internationale Organisation, es sei denn, dies ist nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, erforderlich; in einem solchen Fall unterrichtet der Auftragsverarbeiter den für die Verarbeitung Verantwortlichen vor der Verarbeitung über diese rechtliche Verpflichtung, es sei denn, diese Rechtsvorschriften verbieten eine solche Informationen aus wichtigen Gründen des öffentlichen Interesses;

- sicherzustellen, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Verschwiegenheit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen;
- geeignete technische und organisatorische Maßnahmen zu ergreifen, um ein dem Risiko angemessenes Sicherheitsniveau zu gewährleisten, das im Einklang mit den Anforderungen der Datenverarbeitungsvereinbarung (gemäß Artikel 32 der DSGVO) steht und den Abschnitten 4 und 10 des Datenschutzrahmens entspricht;
- die in der Datenverarbeitungsvereinbarung (gem. Artikel 28 Absätze 2 und 4 DSGVO) und Abschnitt II.3.B des DPF genannten Bedingungen für die Beauftragung eines anderen Auftragsverarbeiters einzuhalten;
- unter Berücksichtigung der Art der Verarbeitung, den für die Verarbeitung Verantwortlichen durch geeignete technische und organisatorische Maßnahmen, soweit dies möglich ist, zu unterstützen, damit der für die Verarbeitung Verantwortliche seiner Antwortpflicht im Hinblick auf die nach Kapitel III der DSGVO festgelegten Rechte der betroffenen Person nachkommen kann;
- den für die Verarbeitung Verantwortlichen bei der Einhaltung seiner Verpflichtungen gemäß den Artikeln 32 bis 36 DSGVO unter Berücksichtigung der Art der Verarbeitung und der dem Auftragsverarbeiter zur Verfügung stehenden Informationen zu unterstützen;
- nach Wahl des für die Verarbeitung Verantwortlichen alle personenbezogenen Daten nach Beendigung der Erbringung von Dienstleistungen im Zusammenhang mit der Verarbeitung zu löschen oder an den Verantwortlichen zurückzusenden und vorhandene Kopien löschen, es sei denn, das Unionsrecht oder das Recht der Mitgliedstaaten schreibt die Speicherung der personenbezogenen Daten vor;
- dem für die Verarbeitung Verantwortlichen alle Informationen zur Verfügung zu stellen, die erforderlich sind, um die Einhaltung der in Artikel 28 der DSGVO festgelegten Verpflichtungen nachzuweisen sowie Audits, einschließlich Inspektionen durch den für die Verarbeitung Verantwortlichen oder einem anderen von diesem beauftragten Prüfer zu ermöglichen und dazu beizutragen. In Bezug auf diesen letzten Punkt, unterrichtet der Auftragsverarbeiter den für die Verarbeitung Verantwortlichen unverzüglich, wenn seiner Ansicht nach eine Anweisung gegen das DPF verstößt.

Beauftragt der US-Auftragsverarbeiter einen anderen Auftragsverarbeiter („Unterauftragsverarbeiter“) mit der Durchführung bestimmter Verarbeitungstätigkeiten im Namen des für die Verarbeitung Verantwortlichen im EWR, so muss der Auftragsverarbeiter sicherstellen, dass die Anforderungen gemäß Abschnitt II.3.B DPF erfüllt sind. Dazu gehört auch, sicherzustellen, dass der Unterauftragsverarbeiter das gleiche Schutzniveau für personenbezogene Daten wie im DPF und die gleichen Datenschutzverpflichtungen bietet, die in der Datenverarbeitungsvereinbarung festgelegt sind. Kommt ein Unterauftragsverarbeiter seinen Datenschutzverpflichtungen nicht nach, haftet der ursprüngliche US-Auftragsverarbeiter gegenüber dem Verantwortlichen in vollem Umfang für die Erfüllung der Verpflichtungen dieses Unterauftragsverarbeiters.

Q4. Wo finde ich Anleitungen zur Zertifizierung von US-Tochtergesellschaften europäischer Unternehmen?

US-Tochtergesellschaften von EWR-Unternehmen können sich beim DPF selbst zertifizieren, wenn sie der Zuständigkeit der Federal Trade Commission (FTC) oder des US-Verkehrsministeriums (DoT) unterliegen.

Weitere Informationen zu den Zulassungsvoraussetzungen finden Sie hier und einen Leitfaden zum Selbstzertifizierungsverfahren finden Sie hier.