- Nicht-amtliche Arbeitsübersetzung -

WP245

Das EU-US DATENSCHUTZSCHILD

F.A.Q. FÜR EUROPÄISCHE UNTERNEHMEN

Verabschiedet am 13. Dezember 2016

Q1. Was ist das EU-US Datenschutzschild?

Das EU-US Datenschutzschild[1] ist ein Selbstzertifizierungsmechanismus für in den USA ansässige Unternehmen, der durch die Europäische Kommission als Garant für ein angemessenes Schutzniveau bei der Übermittlung personenbezogener Daten von Stellen in der EU an in den USA ansässige, selbstzertifizierte Unternehmen und damit als ein Element für die rechtlichen Garantien solcher Datenübermittlungen anerkannt wurde.

Hier sind einige Links für weitere Informationen:

- Die im Amtsblatt der EU veröffentlichte Angemessenheitsentscheidung
- Der von der Europäischen Kommission erarbeitete Leitfaden zu dem EU-US Datenschutzschild
- Die vom Handelsministerium der USA verwaltete Website zum Programm des Datenschutzschilds.

[1] Die Angemessenheitsentscheidung des EU-US-Datenschutzschilds („Datenschutzschild“) oder („Rechtsrahmen“) wurde von der Europäischen Kommission am 12. Juli 2016 angenommen. Es wurde von der Europäischen Kommission und dem US-Handelsministerium als Ersatz für die Safe-Harbor-Entscheidung 2000/520/EG erarbeitet, die vom Gerichtshof der Europäischen Union am 6. Oktober 2015 für ungültig erklärt wurde.

Q2. Welche US-Unternehmen kommen für eine Teilnahme am EU-US Datenschutzschild in Frage?

Für eine Berechtigung zur Selbstzertifizierung unter dem Datenschutzschild muss ein in den USA ansässiges Unternehmen den Ermittlungs- und Durchsetzungsbefugnissen der Federal Trade Commission („FTC“) oder des Verkehrsministeriums („Department of Transportation („DoT“) unterliegen. Andere staatliche Körperschaften der USA könnten in Zukunft mit einbezogen werden.

Das bedeutet, dass beispielsweise gemeinnützige Organisationen, Banken, Versicherungsgesellschaften und Anbieter von Telekommunikationsdiensten (in Bezug auf Tätigkeiten als Netzbetreiber) nicht unter die Zuständigkeit der FTC oder des DoT fallen und sich daher nicht unter dem Datenschutzschild selbstzertifizieren können.

Das Datenschutzschild gilt für jede Art personenbezogener Daten, die von einer Stelle in der EU in die USA übermittelt werden, einschließlich Geschäftsdaten, Gesundheitsdaten oder Beschäftigtendaten, solange das empfangende US-Unternehmen sich unter dem Rechtsrahmen selbst zertifiziert hat.

Weitere Informationen finden Sie unter: https://www.privacyshield.gov/.

Q3. Was ist vor einer Übermittlung personenbezogener Daten an ein in den USA ansässiges Unternehmen, das für das Datenschutzschild zertifiziert ist oder dies behauptet, zu tun?

Vor der Übermittlung personenbezogener Daten an ein in den USA ansässiges Unternehmen, das von sich behauptet, unter dem Datenschutzschild zertifiziert zu sein, müssen sich europäische Unternehmen auch vergewissern, ob das in den USA ansässige Unternehmen im Besitz einer gültigen Zertifizierung ist (die Zertifizierungen müssen jährlich erneuert werden), und dass die Zertifizierung für die betreffenden Daten gilt (insbesondere: Beschäftigtendaten bzw. Nicht-Beschäftigtendaten).

Zur Prüfung, ob eine Zertifizierung gültig ist oder nicht, müssen europäische Unternehmen die auf der Website des US-Handelsministeriums veröffentliche Datenschutzschild-Liste einsehen (https://www.privacyshield.gov/list).

Alle in den USA ansässigen Unternehmen werden nach erfolgreichem Abschluss des Selbstzertifizierungsverfahrens in der Liste aufgeführt. Die Datenschutzschild-Liste enthält auch Informationen über die Arten von personenbezogenen Daten, für die sich ein in den USA ansässiges Unternehmen zertifiziert hat (Beschäftigtendaten oder Nicht-Beschäftigtendaten) sowie ausführliche Informationen über die von ihm angebotenen Dienstleistungen.

Das US-Handelsministerium führt auch das Verzeichnis der Unternehmen, die nicht mehr Mitglieder des Datenschutzschilds sind. Diese Unternehmen dürfen nach Beendigung ihrer Teilnahme keine personenbezogenen Daten von EU-Bürgern im Rahmen des Datenschutzschilds erhalten, aber sie müssen weiterhin die Grundsätze des Datenschutzschilds auf diejenigen Daten anwenden, die während ihrer aktiven Mitgliedschaft übermittelt wurden.

Für die Übermittlung personenbezogener Daten an Unternehmen, die nicht oder nicht mehr Mitglieder des Datenschutzschilds sind, können andere von der EU zugelassene Instrumente für die Übermittlung personenbezogener Daten von Einzelpersonen aus der EU an in den USA ansässige Unternehmen genutzt werden, wie beispielsweise verbindliche Unternehmensregelungen [Binding Corporate Rules – BCR] oder Standardvertragsklauseln.

Die Tatsache, dass der Empfänger in den USA Mitglied des EU-US Datenschutzschilds ist, ermöglicht es den europäischen Unternehmen, im Einklang mit dem nationalen Recht zur Umsetzung von Artikel 25 der EG-Richtlinie 95/46 zu handeln; alle anderen im nationalen Datenschutzgesetz festgelegten Anforderungen bleiben gleichwohl anwendbar;

- Zur Übermittlung an in den USA ansässige Unternehmen, die als verantwortliche Stelle handeln:

Vor der Übermittlung personenbezogener Daten müssen die europäischen Unternehmen in ihrer Eigenschaft als verantwortliche Stellen gewährleisten, dass die Übermittlung im Einklang mit dem geltenden Datenschutzrecht erfolgt. Im ersten Schritt können europäische Unternehmen mit in den USA ansässigen Unternehmen nur dann personenbezogene Daten austauschen, wenn es für die Übermittlung eine rechtliche Grundlage gibt (d. h., wenn sie im Einklang mit den nationalen Rechtsvorschriften zur Umsetzung der Artikel 7 und 8 der EU-Richtlinie 95/46/EU erfolgt). Darüber hinaus müssen auch alle anderen, allgemeinen Anforderungen des EU-Datenschutzrechts hinsichtlich der Datenübermittlung(en) eingehalten werden (z. B. Zweckbindung, Verhältnismäßigkeit, [Daten-]Qualität, Informationspflichten gegenüber den Betroffenen). Wenn Daten an ein in den USA ansässiges, zertifiziertes Unternehmen übermittelt werden, dann muss auch das übermittelnde europäische Unternehmen die Betroffenen über die Identität der Empfänger ihrer Daten und auch über den Umstand informieren, dass die Daten den Schutz des Datenschutzschilds genießen.

Europäische Unternehmen sollten zur Kenntnis nehmen, dass geschäftliche Vertragsklauseln (z. B. mit ihren Geschäftspartnern) sie in ihren Möglichkeiten einschränken könnten, personenbezogene Daten an andere Unternehmen außerhalb der EU oder des EWR [Europäischer Wirtschaftsraum] zu übermitteln.

- Zur Übermittlung an in den USA ansässige Unternehmen, die als Auftragsdatenverarbeiter handeln:

Wenn ein in Europa ansässiges Unternehmen in der Rolle als verantwortliche Stelle Daten an einen in den USA ansässigen Auftragsdatenverarbeiter übermittelt, der in seinem Auftrag nur zu Verarbeitungszwecken handelt (Speicherung, IT-Wartung, Helpdesk usw.), sind die beiden Unternehmen gemäß Art. 17 der EG-Richtlinie 95/46/EG verpflichtet, einen Vertrag zur Auftragsdatenverarbeitung zu schließen, unabhängig davon, ob der Auftragsdatenverarbeiter ein Mitglied des Datenschutzschilds ist oder nicht.

Der Abschluss eines Vertrags ist erforderlich, um zu gewährleisten, dass sich der US-Auftragsdatenverarbeiter zu Folgendem verpflichtet:

- Er handelt ausschließlich auf Weisung der verantwortlichen Stelle;

- Er stellt geeignete technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten gegen unbeabsichtigte oder unrechtmäßige Vernichtung oder gegen unbeabsichtigten Verlust, Änderung, die unberechtigte Weitergabe oder Zugang bereit, und er muss wissen, ob eine (weitere) Datenübermittlung erlaubt ist.[2] Unter Berücksichtigung des Standes der Technik und der Kosten für ihre Einführung sollen solche Sicherheitsmaßnahmen ein Schutzniveau gewährleisten, das angesichts der von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden Daten angemessen ist; und

- Unter Berücksichtigung der Art der Verarbeitung soll er die verantwortliche Stelle bei der Wahrnehmung ihrer Verpflichtungen gegenüber Einzelpersonen, die ihr Recht auf Zugang zu ihren personenbezogenen Daten ausüben, unterstützen.

Bitte beachten Sie, dass gemäß der EU-Datenschutzrichtlinie durch nationales Datenschutzrecht zusätzliche Anforderungen auferlegt sein können, beispielsweise könnte von Unternehmen in der EU die Aufnahme zusätzlicher Inhalte in die Auftragsdatenverarbeitungsverträge verlangt werden. Ihre nationale Datenschutzbehörde kann Ihnen weitere Hinweise geben.

Es ist zum Beispiel ratsam, dass das EU-Unternehmen angibt, ob des damit einverstanden ist oder nicht, dass ein US-Auftragsdatenverarbeiter dritte [Unter-] Auftragnehmer zur Datenverarbeitung beauftragen darf, und die dafür geltenden Bedingungen (im Hinblick auf Transparenz, Haftung). Außerdem könnte es für das Unternehmen in der EU auch nützlich sein, Garantien hinsichtlich der Benachrichtigungen über Sicherheitslücken und Verpflichtungen zur Löschung der Daten nach Beendigung des Dienstleistungsvertrages zu erhalten.

Q4. Wo finde ich eine Anleitung bezüglich der Registrierung von US-amerikanischen Tochtergesellschaften europäischer Unternehmen?

Für Informationen über die Registrierung US-amerikanischer Tochtergesellschaften europäischer Unternehmen für die Aufnahme in die Liste des EU-US Datenschutzschildes, gehen Sie bitte auf die entsprechenden Website des US-Handelsministeriums: (https://www.privacyshield.gov/article?id=U-S-Subsidiaries-of-European-Businesses-Participation-in-Privacy-Shield).

Registrierungsmöglichkeiten für die Aufnahme in die Liste des Datenschutzschilds sind auf der Webseite des US-Handelsministeriums verfügbar (https://www.privacyshield.gov/welcome).

[2]Für ergänzende Informationen über die Weiterübermittlung von Daten durch in den USA ansässigen Auftragsdatenverarbeiter lesen Sie bitte die Rubrik „obligatorische Verträge für die Weiterübermittlung“ des Datenschutzschilds und siehe dort Frage 4.

Dort finden Sie auch eine Anleitung für das Selbstzertifizierungsverfahren: (https://www.privacyshield.gov/article?id=How-to-Join-Privacy-Shield-part-1).

Das selbstzertifizierte US-Unternehmen wird auf jeden Fall die unter dem Datenschutzschild geltenden datenschutzrechtlichen Grundsätze befolgen müssen.