

Privacy Shield ungültig – Was nun? – Fortsetzung

Von Carmen Lupsan, Rechtsanwältin

Wie bereits in einem vorherigen Beitrag beschrieben, hat der Europäische Gerichtshof (EuGH) am 16. Juli 2020 in dem sog. **Schrems II Urteil** den Privacy Shield für ungültig erklärt. Diese Absprache betreffend den Datenschutz beim Datenaustausch zwischen Europa und den USA war auf das zuvor ebenfalls für ungültig erklärte Safe Harbor- Programm gefolgt.

Am 11. November 2020 hat der Europäische Datenschutzausschuss die folgenden zwei Entwürfe erlassen, die sich auf den Transfer von personenbezogenen Daten aus der Europäischen Union in Drittländer beziehen:

- die Empfehlung 01/2020 über Maßnahmen, die die Transferinstrumente ergänzen, um die Einhaltung des EU-Schutzniveaus für persönliche Daten zu gewährleisten („**Empfehlung 01**“) und
- die Empfehlung 02/2020 über die Europäischen grundlegenden Garantien zu Überwachungsmaßnahmen („**Empfehlung 02**“).

Ausgangslage

Verantwortliche, die sich bei der Datenübermittlung in Drittländer auf Standarddatenschutzklauseln berufen, müssen im Einzelfall zusammen mit dem Empfänger prüfen, ob das Schutzniveau der personenbezogenen Daten im entsprechenden Drittland wesentlich gleichwertig mit dem des Europäischen Wirtschaftsraums ist. Der EuGH hat Datenexporteuren gestattet, zusätzliche Maßnahmen zu den Standarddatenschutzklauseln zu ergreifen, um ein geeignetes Schutzniveau zu gewährleisten, wo die Standarddatenschutzklauseln nicht ausreichend sind.

Gerade um diesen Vorgang zu erleichtern, will der Europäische Datenschutzausschuss zur Hilfe kommen und hat die oben genannten Empfehlungen erlassen. Diese sind noch nicht final.

Empfehlung 01

Die Empfehlung 01 gibt Datenexporteuren sechs Schritte zur Hand, die diese befolgen müssen, wenn Sie personenbezogene Daten in Drittländer übermitteln:

1. Know your transfer

Der Datenexporteur muss eine Bestandsaufnahme aller Datenübermittlungen in Drittländer vornehmen, d.h. er muss diese identifizieren und dokumentieren.

2. Rechtsgrundlage für die Übermittlung ins Drittland

Sollte ein Angemessenheitsbeschluss der EU-Kommission für das Drittland vorliegen, so bedarf es keiner weiteren Prüfungen. Anderenfalls muss der Datenexporteur sicherstellen, dass geeignete Garantien gemäß Art. 46 DSGVO wie verbindliche interne Datenschutzvorschriften (Art. 47 DSGVO), Standarddatenschutzklauseln etc. vorliegen. In

Ausnahmefällen greifen die Bedingungen gemäß Art. 49 DSGVO wie die Einwilligung oder die Erfüllung eines Vertrages mit der betroffenen Person.

3. Bewertung der Rechtsgrundlage

Der Datenexporteur muss prüfen, ob die Rechtsgrundlage unter Punkt 2 ein angemessenes Datenschutzniveau gewährleistet. Näheres hierzu finden Sie unten in der Zusammenfassung der Empfehlung 02.

4. Ergreifen zusätzlicher Maßnahmen

Sollte gemäß Punkt 3 festgestellt werden, dass kein angemessenes Schutzniveau gewährleistet ist, so müssen zusätzliche Maßnahmen ergriffen werden. Eine Liste solcher Maßnahmen hat der Europäische Datenschutzausschuss in der Anlage 2 zur Empfehlung 01 zur Verfügung gestellt.

5. Verfahren für die Umsetzung der zusätzlichen Maßnahmen

Abhängig von den zu ergreifenden Maßnahmen gemäß Punkt 4 sind genaue Verfahrensschritte für deren Umsetzung festzulegen und zu dokumentieren, damit diese intern von den beteiligten Parteien eingehalten werden können.

6. Regelmäßige Wiederholung der Prüfungen

Eine regelmäßige Prüfung der Datenschutzniveaus im Drittland ist erforderlich, um etwaige eingetretene Änderungen diesbezüglich feststellen und entsprechende Maßnahmen ergreifen zu können.

Empfehlung 02

Der Datenexporteur muss eine Rechtmäßigkeitsprüfung vornehmen, um sicherzustellen, dass im Einzelfall die anwendbaren Rechtsvorschriften des Drittlandes ein angemessenes Schutzniveau der zu übermittelnden Daten gewährleisten. Hierfür müssen folgende grundlegende Garantien geprüft werden:

1. Die Verarbeitung der Daten muss auf klaren, genauen und zugänglichen Regeln beruhen;
2. Die Notwendigkeit und Verhältnismäßigkeit des legitimen Zwecks der Verarbeitung muss nachgewiesen werden;
3. Es muss ein unabhängiger Überwachungsmechanismus im Drittland (z.B. Gericht) bestehen;
4. Der betroffenen Person müssen wirksame Rechtsbehelfe zur Verfügung stehen.

Fazit

Die zwei Empfehlungen bieten teilweise Lösungen zur Lücke, die durch das Schrems II Urteil entstanden ist. Gleichzeitig wird es eine Herausforderung für Unternehmen darstellen, die oben dargestellten Prüfungen anzustrengen – diese müssen entsprechend dokumentiert werden, um im Falle einer Kontrolle der Datenschutzaufsichtsbehörde die entsprechenden Nachweise der Erfüllung der Rechenschaftspflicht vorlegen zu können.

Da es sich hierbei noch um Entwürfe handelt, sind die endgültigen Fassungen noch abzuwarten. Zur Empfehlung 01 kann bis zum 21. Dezember Feedback auf der Webseite des Europäischen Datenschutzausschusses eingereicht werden. Die Entwicklungen erwarten wir mit Spannung.

Kontakt und weitere Informationen:



STALFORT Legal. Tax. Audit.
Bukarest – Bistrița – Sibiu

Büro Bukarest:

.: +40 – 21 – 301 03 53

F: +40 – 21 – 315 78 36

M: bukarest@stalfort.ro

www.stalfort.ro