

Was ist bei der Übermittlung von Personendaten ins Ausland zu beachten?

Der Gerichtshof der Europäischen Union (EuGH) hat in einem kürzlich publizierten Entscheid die Übermittlung von Personendaten in Drittländer erheblich erschwert. Welche Auswirkungen hat dieser Entscheid auf Unternehmen in der Schweiz?



Daniela Fábíán Masoch

Die geltende EU Datenschutz-Grundverordnung (DSGVO) und das schweizerische Datenschutzgesetz (DSG) verbieten grundsätzlich die Übermittlung von Personendaten aus dem Europäischen Wirtschaftsraum (EWR) und der Schweiz in Länder, die keinen angemessenen Datenschutz gewährleisten (Drittländer).

Eine Übermittlung in Drittländer, einschliesslich Fernzugriff, ist nur erlaubt, wenn mindestens eine der gesetzlich vorgesehenen Schutzmassnahmen getroffen wird, wie beispielsweise die Anwendung von EU-Standardvertragsklauseln (SCC) zwischen Datenexporteuren und Datenempfängern oder die Einführung von verbindlichen internen Unternehmensregeln (BCR) für den internen Datenaustausch. Eine Übermittlung ist auch erlaubt, wenn eine Ausnahmeregelung vorliegt, beispielsweise die ausdrückliche Einwilligung der betroffenen Personen.

Die USA gelten grundsätzlich aus europäischer Sicht als Drittland. Sowohl die EU als auch die Schweiz haben jedoch mit den USA ein Regelwerk erarbeitet, den sogenannten EU-U.S. Privacy Shield und CH-U.S. Privacy Shield. Dieses Regelwerk erlaubt die Übermittlung von Personendaten aus der EU und der Schweiz an US-Unternehmen, die sich dem jeweiligen Privacy Shield unterstellt haben.

Das Urteil des EuGH in Sachen Schrems II erschwert die grenzüberschreitende Datenübermittlung

Am 16. Juli 2020 hob der Gerichtshof der Europäischen Union (EuGH) in der Rechtssache C-311/18 – Data Protection Commissioner v. Facebook Ireland and Maximilian Schrems (Schrems II) den EU-U.S. Privacy Shield mit sofortiger Wirkung auf. Der Grund für diese Entscheidung liegt darin, dass das US-Recht aufgrund der weitgehenden Befugnisse der US Geheimdienste gemäss der Einschätzung des EuGH kein Schutzniveau bietet, das dem in der Europäischen Union im Wesentlichen gleichwertig ist.

Gleichzeitig bestätigte der EuGH die prinzipielle Gültigkeit von SCC. Der EuGH appelliert jedoch an die bereits in den SCC festgeschriebenen Verpflichtungen von Unternehmen, die Personendaten auf der Grundlage von SCC aus der EU in ein Drittland exportieren oder importieren, und betont, dass die reine Unterzeichnung der SCC nicht ausreicht. Die Parteien müssen im Einzelfall prüfen, ob die SCC im Empfängerland eingehalten werden können und die Rechte der betroffenen Personen im Empfängerland ein angemessenes Schutzniveau geniessen, das dem in der Europäischen Union gleichwertig ist.

Ist dies nicht der Fall, muss der Datenexporteur zusätzliche Schutzmassnahmen ergreifen oder die betreffende Datenübermittlung aussetzen. Schutzmassnahmen können technischer Natur sein, wie beispielsweise die Verschlüsselung der Daten. Zusätzliche vertragliche Absicherungen und organisatorische Massnahmen sind ebenfalls denkbar. Der EuGH legt jedoch nicht fest, welche Art von Schutzmassnahmen ergriffen werden sollen, und lässt somit den Unternehmen einen gewissen Spielraum.

Was bedeutet dieses Urteil für Unternehmen in der Schweiz?

Das EuGH-Urteil ist auf die Schweiz nicht direkt anwendbar. Somit bleibt der CH-U.S. Privacy Shield

vorerst gültig. Auch vom Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) anerkannte SCC können weiterhin für Datenübermittlungen aus der Schweiz genutzt werden. Der EDÖB hat das Urteil des EuGH zur Kenntnis genommen, hat sich aber noch nicht zur Gültigkeit des CH-U.S. Privacy Shields geäussert. Es ist jedoch zu erwarten, dass die Behörde dem EuGH-Urteil folgen und auch den CH-U.S. Privacy Shield für ungültig erklären wird (wie sie es auch 2015 nach der Ungültigkeitserklärung des Vorgängerabkommens Safe-Harbor getan hat). Für Unternehmen in der Schweiz, die dem DSG unterliegen, besteht somit aufgrund des EuGH-Urteils vorerst kein dringender Handlungsbedarf. Dennoch sollten die internen und externen Datenflüsse jetzt schon ermittelt und Vorbereitungen für einen kurzfristigen Wechsel von Privacy Shield auf SCC getroffen werden. Auf viele Unternehmen in der Schweiz ist jedoch auch die DSGVO anwendbar. Diese Unternehmen sollten jetzt aktiv werden, um Personendaten weiterhin legitim in Drittländer übermitteln zu können und signifikante Bussgelder zu vermeiden.

Was können Unternehmen tun?

- Unternehmen sollten die Entwicklungen in der EU und in der Schweiz überwachen und insbesondere auf die Herausgabe von Leitlinien und revidieren SCC als auch auf eine allfällige Ungültigkeitserklärung des CH-U.S. Privacy Shields achten.
- Interne und externe grenzüberschreitende Datenübermittlungen sollten ermittelt und dokumentiert werden.
- Für Datenübermittlungen, die auf den EU-U.S. Privacy Shield gestützt sind, sollten SCC mit den Datenempfängern vereinbart werden.
- Für Datenübermittlungen auf der Grundlage von SCC (einschliesslich konzerninterner

Datenübermittlungsvereinbarungen) sollten im Rahmen der Due Diligence mit dem Datenempfänger Analysen im Empfängerland durchgeführt und gegebenenfalls zusätzliche vertragliche, organisatorische und technische Massnahmen getroffen werden.

- Schliesslich sollten Unternehmen ihre Datenübermittlungsstrategie überdenken und gegebenenfalls einen Wechsel auf robustere Mechanismen, wie BCR in Betracht ziehen.

Über die Autorin

Daniela Fábíán Masoch ist Rechtsanwältin und Gründerin von Fabian Privacy Legal, einer Anwaltskanzlei mit Sitz in Basel, die sich auf internationales, europäisches und schweizerisches Datenschutzrecht spezialisiert hat.

Sie berät und unterstützt multinationale Unternehmen mit einem pragmatischen Ansatz bei der Bewertung, Entwicklung, Umsetzung und Überwachung von Datenschutzstrategien, Governance-Modellen und globalen Datenschutzprogrammen sowie Datentransferstrategien, einschliesslich BCR.

Weitere Informationen:
www.privacylegal.ch

