NEWSLETTER | 3. August 2020

ÖSTERREICH

Handlungsbedarf beim Datenverkehr in Drittstaaten – EU-US Privacy Shield vom EuGH für unwirksam erklärt

EuGH erklärt nach vier Jahren EU-US Privacy Shield für unwirksam und macht weitreichende Vorgaben für Datentransfers in Drittstaaten.

Am 16.7.2020 hat der EuGH hat im Verfahren Data Protection Commissioner (Irland) gg. Schrems, Facebook Ireland (Rechtssache C-311/18; „Schrems II“) entschieden, dass:

- das EU-US Datenschutzschild (Privacy Shield) mit sofortiger Wirkung ungültig ist und
- EU-Standardvertragsklauseln (SCC) zwar gültig sind, aber im Einzelfall zusätzlich geprüft werden muss, ob im Drittland tatsächlich angemessene und durchsetzbare Rechte und wirksame Rechtsbehelfe für Betroffene bestehen.

Das EU-US Datenschutzschild ist ein Beschluss der EU Kommission, der auf einer Absprache mit den USA basiert. Wesentliche Bestandteile waren einerseits Zusicherungen der US-Regierung und andererseits Datenschutz-Grundsätze, die von US-Unternehmen einzuhalten sind. US Unternehmen konnten sich unter dem Datenschutzschild registrieren und galten damit hinsichtlich des Datenschutzniveaus als gleichwertig, sodass keine weiteren Maßnahmen erforderlich waren.

Wer ist betroffen?

Direkt betroffen sind alle, die Daten in die USA transferieren. Auch wenn Daten in eine EU-Cloud eines US-Anbieters (z.B. Microsoft oder Amazon) übertragen werden, kommt es idR zum Transfer in die USA, weil US-Mitarbeiter auf die Daten zur Administration, zum Erbringen von Dienstleistungen etc. Zugriff haben. Betroffen sind auch alle, die Daten in sonstige Drittländer transferieren oder Standardvertragsklauseln verwenden.

Welche Voraussetzungen gelten für Datentransfers in Drittstaaten?

Generell ist ein Datentransfer nur zulässig, wenn u.a. im Empfängerland ein angemessenes Datenschutzniveau herrscht. Dies ist innerhalb der EU und des EWR gewährleistet. Für alle anderen Länder (sog. Drittstaaten) muss ein angemessenes Datenschutzniveau gewährleistet sein. Dies erfolgt mit:

- Angemessenheitsbeschluss der EU Kommission (dzt. für die Schweiz, Kanada, Argentinien, Guernsey und die Isle of Man),
- Binding Corporate Rules (BCR), d.s. verbindliche unternehmens- bzw. konzerninterne Datenschutzvorschriften, die von einer Datenschutzbehörde genehmigt wurden, oder
- Standardvertragsklauseln (SCC), d.s. Musterverträge der EU-Kommission, die von Unternehmen mit Datenempfängern in Drittstaaten abgeschlossen werden.

Nach dem EuGH-Urteil genügen aber SCC und BCR alleine nicht mehr. Das Datenschutzniveau im Drittstaat ist ebenfalls zu prüfen und ggfs. mit zusätzlichen Maßnahmen sicherzustellen.

Verfasst von:

Mag. Ingo Braun

✉ ingo.braun@benn-ibler.com
☎ +43 1 531 55 700

Benn-Ibler Rechtsanwälte GmbH
Tuchlauben 8, 1010 Wien

Was machen die Datenschutzbehörden?

Neben den unterschiedlichsten Stellungnahmen von Datenschutzbehörden gibt es auch eine erste Reaktion des Europäischen Datenschutzausschusses (EDSA). Diese ist zwar streng, aber konkret.

- Es gibt keine Übergangsfrist.
- Datenverkehr in die USA aufgrund des Privacy Shields ist einzustellen.
- Vor jedem Datentransfer in die USA aufgrund von SCC oder BCR ist genau zu prüfen, ob unter Berücksichtigung aller Umstände und zusätzlich ergriffener Maßnahmen ein angemessenes Datenschutzniveau sichergestellt werden kann.
- Kann kein angemessenes Datenschutzniveau sichergestellt werden, ist der Datenverkehr einzustellen. Falls dies nicht erfolgt, muss das Unternehmen die zuständige Datenschutzbehörde verständigen.

EDSA hat angekündigt, weitere Information zu den zusätzlich zu ergreifenden Maßnahmen zur Sicherstellung eines angemessenen Datenschutzniveaus zur Verfügung zu stellen.

Was ist zu tun?

Für Unternehmen mit Datenverkehr in die USA besteht der größte Handlungsbedarf. Aber letztlich ist fast jeder Datenverkehr in Drittstaaten betroffen. Die bislang publizierten Vorschläge reichen von Abwarten und Beobachten bis zur vollen Erfüllung der Anforderungen des EDSA.

Während dzt. noch Rechtsunsicherheit herrscht, können folgende Schritte erfolgen:

- Zuerst sollten alle Datentransfers, die jeweils übermittelten Daten und das damit verbundene Risiko überprüft werden.
- Bei Datentransfers in die USA sollten sofort mögliche Lösungen gesucht werden. Bspw. Umstellung auf EU-Clouds (ohne US-Zugriff zur Wartung etc.)
- Das Datenschutzniveau in Drittstaaten sollte analysiert werden. Dazu kann etwa beim Vertragspartner im Drittstaat nach-gefragt werden, ob sie unter die vom EuGH genannten Überwachungsgesetze (d.s. Section 702 FISA und EO 12333) fallen.
- Zusätzliche Maßnahmen sollten erwogen werden. Bspw. könnte eine starke Verschlüsselung der Daten erfolgen. Doch können auch andere rechtliche, technische und organisatorische Maßnahmen passend sein.
- Abzuwarten sind die Reaktionen der zuständigen Datenschutzbehörde und weitere Hinweise der EDSA.
- Datenschutzbeauftragte werden die Geschäftsführung über die Folgen des EuGH-Urteils und die davon im Unternehmen betroffenen Datenverarbeitungen informieren müssen. Letztlich wird jede Umstellung auch zu Kosten führen.

Nachdem eine sofortige Umstellung oder Beendigung von Datentransfers in Drittstaaten für die meisten Unternehmen unmöglich ist, kann so bei Nachfragen der Datenschutzbehörde zumindest ein rasches Handeln dargelegt werden. Auch wenn damit keine Strafen vermieden werden können, wäre dies zumindest zu Gunsten des Unternehmens zu berücksichtigen.

Verfasst von:

Mag. Ingo Braun

✉ ingo.braun@benn-ibler.com
☎ +43 1 531 55 700

Benn-Ibler Rechtsanwälte GmbH
Tuchlauben 8, 1010 Wien