



Internationaler Datentransfer nach USA: Adieu „Privacy Shield“

Autoren: Arbeitskreis Datenschutz | Stand: Juli 2020

Der Europäische Gerichtshof (EuGH) hat mit Urteil vom 16. Juli 2020 (Az. C-311/18) den Beschluss der Europäischen Kommission zum sog. „Privacy Shield“ gekippt. Damit entfällt ein wichtiger Pfeiler datenschutzkonformer Übermittlung personenbezogener Daten aus der EU in die Vereinigten Staaten von Amerika. Unternehmen, die auf Basis des „Privacy Shield“ für eigene Datenübermittlungen das erforderliche angemessene Datenschutzniveau gewährleisten, müssen jetzt dringend die Vereinbarkeit der Datenverarbeitung mit geltendem Recht prüfen und ggf. Verträge, Prozesse und Dokumentation anpassen.

Rechtlicher Hintergrund

Personenbezogene Daten dürfen nach den maßgeblichen Vorschriften der Datenschutz-Grundverordnung („DSGVO“) grundsätzlich nur dann in ein Drittland übermittelt werden, wenn das betreffende Land für die Daten ein angemessenes Schutzniveau bietet (Art. 44 ff. DSGVO). Die Europäische Kommission kann in einem Angemessenheitsbeschluss unter Berücksichtigung verschiedener Prüfkriterien feststellen, dass ein Drittland ein angemessenes Datenschutzniveau gewährleistet. Zu diesen Prüfkriterien gehören unter anderem die innerstaatlichen Vorgaben zu Rechtsstaatlichkeit, zur Achtung der Menschenrechte und Grundfreiheiten sowie zur Anwendung von (Datenschutz-)Vorschriften, zur Existenz und zur Wirksamkeit unabhängiger Aufsichtsbehörden. Liegt kein Angemessenheitsbeschluss vor, darf eine Übermittlung personenbezogener Daten – zusätzlich zu den sonstigen Voraussetzungen der DSGVO – nur dann erfolgen, wenn der in der Europäischen Union ansässige Exporteur der personenbezogenen Daten geeignete Garantien vorsieht.

Neben anderen Möglichkeiten, für ein angemessenes Datenschutzniveau Sorge zu tragen, hatte die Europäische Kommission in der Vergangenheit bereits die sog. „Safe-Harbor-Entscheidung“ (Entscheidung des Europäischen Parlaments und des Rates über die Angemessenheit der Grundsätze des „sicheren Hafens“, 2000/520/EG), den Beschluss zu sog. „Standardvertragsklauseln“ (2010/87/EG) und den Durchführungsbeschluss (EU) 2016/1250 über die Angemessenheit des EU-US-Datenschutzschild („Privacy Shield“) getroffen.

Was bisher geschah...

Bereits vor Jahren hatte ein in Österreich wohnhafter, österreichischer Staatsangehöriger und Nutzer von Facebook, Max Schrems, mit seiner Klage gegen die Datenübermittlung auf Basis der Safe-Harbor-Entscheidung durch Facebook in die USA Aufsehen erregt. In einem Urteil vom 6. Oktober 2015 war der EuGH der Argumentation von Schrems gefolgt, das Recht und die Praxis der Vereinigten Staaten böten keinen ausreichenden Schutz vor dem Zugriff der Behörden auf die dorthin aus der Europäischen Union übermittelten Daten („Schrems I“). Die Datenübermittlung auf Basis von „Safe Harbor“ war mithin unzulässig.

In der Folgezeit stützte Facebook die Angemessenheit des Schutzes in den USA auf EU-Standardvertragsklauseln (2010/87/EG); später wurde zusätzlich die Vereinbarung über den sog. „Privacy Shield“ herangezogen. In den vom Irischen High Court auf erneute Klage von Schrems vorgelegten Vorabentscheidungs-gesuch hatte dieser im Verfahren „Schrems II“ gegenüber dem EuGH die Frage der Gültigkeit sowohl der Standardvertragsklauseln als auch des Privacy Shield aufgeworfen.

Die Entscheidung des EuGH vom 16.7.2020

Während die Standardvertragsklauseln 2010/87 grundsätzlich als ausreichend erachtet wurden, teilt der EuGH in seiner am 16. Juli 2020 veröffentlichten Entscheidung die bereits von Schrems und auch von verschiedenen Datenschutzaufsichtsbehörden kommunizierte Auffassung, dass der Privacy Shield den Anforderungen an den Schutz personenbezogener Daten nicht genüge.

Die Charta der Grundrechte der Europäischen Union verbürge, so der EuGH, die Achtung des Privat- und Familienlebens, den Schutz personenbezogener Daten und das Recht auf effektiven gerichtlichen Rechtsschutz. Explizit in Analogie zu seiner Entscheidung in Sachen „Safe-Harbor“ stellte der EuGH fest, dass der durch den Privacy Shield insoweit eingeräumte Schutz den europäischen Maßstäben nicht hinreichend Rechnung trägt. Dies nicht zuletzt deshalb, weil den Erfordernissen der nationalen Sicherheit, des öffentlichen Interesses und der Einhaltung des US-amerikanischen Rechts Vorrang eingeräumt werde. US-Behörden könnten hiernach auf personenbezogene Daten aus der EU zugreifen und diese – ohne ersichtlich den EU-Vorgaben entsprechende Verhältnismäßigkeitserwägungen oder sonstige Beschränkungen einhalten zu müssen – verwenden. Garantien zum Schutz der Persönlichkeitsrechte von Nicht-US-Bürgern seien ebenso wenig gewährleistet, wie adäquater Rechtsschutz (vgl. Pressemitteilung Nr. 91/20 des Gerichtshofs der Europäischen Union vom 16. Juli 2020 sowie Urteil zu C-311/18).

Auswirkungen für die Praxis

Wie schon die damalige Entscheidung in Sachen Safe Harbor hat auch das jüngste Urteil des EuGH zum Privacy Shield erhebliche Auswirkungen für den transatlantischen Datenaustausch. Die Übermittlung von personenbezogenen Daten aus der Europäischen Union in die USA unter Berufung auf den sog. Privacy Shield ist für sich betrachtet unzulässig. Für Unternehmen entstehen erhebliche Unsicherheiten. Viel wird davon abhängen, wie die Aufsichtsbehörden sich im Lichte des Urteils verhalten und ob/inwieweit die EU und die Vereinigten Staaten schnell eine Alternative zur Verfügung stellen können. Ob andere geeig-

nete Garantien im jeweiligen Einzelfall bestehen, muss von denjenigen Verantwortlichen, die sich bei Ihren Übermittlungen auf die Privacy-Shield-Zertifizierung des US-Unternehmens gestützt haben, zeitnah überprüft werden; derzeit sind 5384 Unternehmen unter dem Privacy Shield Regime gemeldet (Stand: 17.7.2020, 12:43h).

Handlungsbedarf besteht nun – über das sonst schon übliche Maß hinaus – insbesondere im Bereich der Prüfung unternehmensinterner Prozesse, der personenbezogenen Datenübermittlungen zugrundeliegenden Vertragswerke sowie der zugehörigen unternehmensinternen Dokumentation. Wo werden personenbezogene Daten in die USA übermittelt? Welche Garantiemechanismen sind etabliert? In allen Bereichen unternehmerischen Handelns spielt die Gewährleistung eines angemessenen Schutzniveaus bei Datentransfers eine maßgebliche Rolle, sei es bei Cloud-Diensten, den in COVID-19-Zeiten boomenden Videokonferenz-Lösungen, im Bereich von Webseiten und bei Daten-Analytics-Dienstleistungen. Seit 2016 sind in einer Reihe von Bereichen auch die Entscheidung zum Privacy Shield bei der Gestaltung von Unternehmensabläufen referenziert und Prozesse hieraus aufgebaut worden.

Nicht zuletzt bleibt die verpflichtende Information an Betroffene über die Verarbeitung ihrer Daten nach Art. 13 f DSGVO zu prüfen und ggf. anzupassen. Auch dies gilt mit Blick auf die Webseiten von Unternehmen, auf denen häufig entsprechende Hinweise auf den Privacy Shield im Zusammenhang mit Dienstleistungen Dritter, häufig im Bereich Social Media tätiger Datenverarbeiter zu finden sind. Unternehmen sollten unbedingt prüfen, inwieweit Datenverarbeitungen, für die die Übermittlung personenbezogener Daten nach USA zwingend erforderlich sind, bis zur Etablierung anderer geeigneter Garantien eines angemessenen Schutzniveaus, auszusetzen sind.

Bei Verstößen gegen die Regelungen zur Übermittlung personenbezogener Daten an einen Empfänger in einem Drittland nach den Artikeln 44 ff. DSGVO drohen gemäß Art. 83 Abs. 5 lit c) DSGVO empfindliche Geldbußen von bis zu 20.000.000,00 EUR oder – im Fall eines Unternehmens – von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs, je nachdem, welcher der Beträge höher ist. Die in jüngster Vergangenheit von Aufsichtsbehörden in der gesamten EU eingeleiteten Verfahren und verhängten, teils drastischen Geldbußen zeigen die Praxisrelevanz und sollten Anlass genug sein, auch in dieser Hinsicht die eigene datenschutzrechtliche Compliance auf den Prüfstand zu stellen.