PRIVACY SHIELD ABKOMMEN FÜR UNGÜLTIG ERKLÄRT

Der Europäische Gerichtshof hat mit der Entscheidung vom 16. Juli 2020 das Privacy Shield Abkommen für ungültig erklärt. Die Entscheidung hat weitreichende Auswirkungen auf den Transfer personenbezogener Daten in die USA.

Hintergrund des Verfahrens
Eine besondere Rolle spielen in diesem Zusammenhang der österreichische Datenschutzaktivist Max Schrems und Facebook. Schrems, seit Jahren Nutzer von Facebook, legte initial bei der Aufsichtsbehörde in Irland eine Beschwerde ein, da bei der Nutzung von Facebook Daten an Server in die USA übermittelt werden. Schrems machte geltend, dass die aktuelle Gesetzeslage und das behördliche Vorgehen in den USA keinen adäquaten Schutz der Daten gewährleisten könnten. 2015 erklärte der Europäische Gerichtshof (EuGH) das ursprüngliche „Safe Harbor Abkommen", den Vorgänger des Privacy Shield, für ungültig („Schrems I").

Trotz des Urteils unterließ Facebook die Übermittlung der Daten nicht, sondern stützte sich größtenteils auf die EU-Standardvertragsklauseln. Als Ergebnis, änderte Max Schrems seine Beschwerde dahingehend, dass die Übermittlung basierend auf den Standardvertragsklauseln unzulässig sei. Der EuGH befasste sich dementsprechend in „Schrems II" mit beiden Aspekten, dem neuen Privacy Shield Abkommen und den Standardvertragsklauseln.

Der EuGH kam zum Ergebnis, dass die Standardvertragsklauseln weiterhin gültig sind, da sich diese mit der Charta der Grundrechte der EU vereinbaren lassen. Den Privacy Shield-Beschluss 2016/1250 erklärte es aber für ungültig.

Privacy Shield für den Transfer personenbezogener Daten
Bisher war für die Übermittlung von personenbezogenen Daten in Drittländer außerhalb der EU essentiell, dass in dem Drittland ein vergleichbares Schutzniveau wie in der EU gewährleistet wird. Für Unternehmen gab es zwei Optionen den Datentransfer zu legitimieren. Eine der wichtigsten in diesem Zusammenhang sind die Angemessenheitsbeschlüsse der EU-Kommission. Per Beschluss kann die Kommission feststellen, dass in einem Drittland, Gebiet oder Sektor personenbezogene Daten einen vergleichbaren Schutz wie in der EU genießen; dies gilt z. B. für Länder wie Neuseeland oder Japan. Ein Transfer von Daten in ein Drittland, für das ein Angemessenheitsbeschluss vorliegt, kann dann ohne eine weitere Genehmigung erfolgen. Das vereinfachte das Verfahren für Unternehmen erheblich. Das Privacy Shield Abkommen war in diesem Kontext eine sektorspezifische Angemessenheitsentscheidung der Kommission. Amerikanische Unternehmen trugen sich in die Privacy Shield Liste ein, die vom US-Handelsministerium geführt wurde, und verpflichteten sich somit die Prinzipien des Privacy Shield zu beachten.

Für Länder, für die kein Angemessenheitsbeschluss vorliegt, konnten Unternehmen alternativ die Standardvertragsklauseln der EU nutzen um ein angemessenes Schutzniveau vertraglich zu forcieren. Die Standardvertragsklauseln sind Musterverträge der EU-Kommission, welche Garantien für Persönlichkeitsrechte gewährleisten. Von den drei Musterverträgen, ist ein Vertrag für die Übermittlung an Auftragsverarbeiter im Drittland vorgesehen, die anderen beiden können für die Datenübermittlung zwischen zwei selbstständig verantwortlichen Stellen genutzt werden. Wichtig ist, dass die Musterverträge unverändert genutzt werden. Ähnlich zu den Standardvertragsklauseln, aber speziell für Datentransfers innerhalb multinationaler Unternehmensgruppen, können die Binding Corporate Rules (verbindliche interne Datenschutzvorschriften) verwendet werden.

Auswirkungen auf die Praxis
Mit dem Urteil zum Privacy Shield, kann mit sofortiger Wirkung dieses nicht mehr als Legitimation für einen Datentransfer genutzt werden. Unternehmen müssen entsprechende Datentransfers unterlassen oder z.B. auf Standardvertragsklauseln umstellen, wobei auch dies keine alleinige Rechtssicherheit bietet. Die Standardvertragsklauseln reichen alleine nicht aus, da der EuGH die Rechtslage in den USA insgesamt kritisch sieht. D. h. neben den Standardvertragsklauseln müssen weitere Schutzmaßnahmen getroffen werden. Die Richter sehen den Datenimporteur und -exporteur in der Pflicht, bestehende Maßnahmen zu prüfen und zu bewerten. In diesem Zusammenhang ist auch eine gewisse Eile geboten. Die Veröffentlichung des Europäischen Datenschutzausschusses[1] zeigt, dass Unternehmen keine besonderen Übergangsfristen gewährt werden.

Is there any grace period during which I can keep on transferring data to the U.S. without assessing my legal basis for the transfer?

No, the Court has invalidated the Privacy Shield Decision without maintaining its effects, because the U.S. law assessed by the Court does not provide an essentially equivalent level of protection to the EU. This assessment has to be taken into account for any transfer to the U.S.

[1] Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, European Data Protection Board, 2020

Welche Maßnahmen sind zu treffen

Im Rahmen von Maßnahmen sollte grundsätzlich immer das Kapitel V der DSGVO berücksichtigt werden, da dieses aufzeigt wie europarechtskonforme Datentransfers in Drittländer umgesetzt werden können. Im Rahmen eines generellen Vorgehens muss geprüft werden, dass alle Anforderungen der DSGVO eingehalten werden und im Folgeschritt sollten dann erst die spezifischen Aspekte der Art. 45 ff. DSGVO an die Übermittlung in Drittländer beachtet werden.

Ein spezifisches Vorgehen zur aktuellen Situation zum Privacy Shield kann dann wie folgt aussehen:

a) Bestandsaufnahme und Analyse

Im ersten Schritt sollten Unternehmen kritisch Ihre Verfahrensverzeichnisse überprüfen und besonders die Datenübermittlungen außerhalb der EU (z. B. in die USA) identifizieren und analysieren. Im Rahmen der Analyse sollten die Datenflüsse kategorisiert werden (z. B. nach Art, Zweck, Umfang und Empfänger).

b) Technisch-organisatorische Maßnahmen

Im Folgeschritt sind noch einmal die technisch-organisatorischen Maßnahmen zu betrachten. Gerade die technischen Maßnahmen sollten dabei hinsichtlich der Verschlüsselung und Pseudonymisierung von Daten genau analysiert werden. Aber auch die Angemessenheit des Schutzniveaus beim Empfänger ist genau zu betrachten. Es sollte dediziert untersucht werden, welche Gesetze den Standardvertragsklauseln entgegenstehen und wie diesen mit Maßnahmen begegnet werden kann.

c) Vertragliche Maßnahmen

Im Rahmen der rechtlichen Analyse sollten nochmal vertragliche Maßnahmen forciert werden, um z.B. behördlichen Datenzugriffen entgegenzuwirken und die Verpflichtung, bei Kenntnis von behördlichen Eingriffen mit Widerspruch oder gerichtlichen Maßnahmen zu reagieren.

Fazit

Das Urteil zum Privacy Shield ist kein Grund in Panik zu verfallen. Maßnahmen sollten aber dennoch nicht zu lange aufgeschoben werden. Es ist essentiell die Datenflüsse umfangreich zu analysieren und dann mit entsprechenden technischen, organisatorischen und rechtlichen Maßnahmen zu reagieren.

Ansprechpartner

RSM Competence Team „Risk Advisory Services"
Dr. Oliver Bungartz – Leiter RAS
Gregor Strobl – Stellvertretender Leiter RAS
Jonathan Schlaeger – Manager Cyber Security

Kontakt über:
+49 40 35006-225
RAS@rsm.de