Privacy Shield vom EuGH gekippt

Ein Kommentar von Jürgen Hüneborn, Fachanwalt für IT-Recht, Münster

aus den Rechtsgebieten IT-Recht, Datenschutz | Privacy Shield | safe harbour

16.07.2020

Der österreichische Jurist und Aktivist Max Schrems hat heute einen erneuten Sieg vor dem EUGH davongetragen: Nachdem bereits das vorherige Datenschutzabkommen "Safe Harbour" 2015 für unwirksam erklärt worden war, hat nun die Nachfolgeregelung "Privacy Shield" dasselbe Schicksal ereilt.

Alle Übermittlungen von **personenbezogenen Daten** in die USA, die (nur) auf diesem Abkommen beruhen, müssen nun überdacht und überarbeitet werden. Es gibt nach wie vor eine Möglichkeit, personenbezogene Daten legal in die USA zu übermitteln:

Sog. "*Standartvertragsklauseln*" ermöglichen in Einzelfällen die Datenübertragung. Allerdings werden jetzt wohl über kurz oder lang sämtliche Datenschutzerklärungen geändert werden müssen, in denen eine Datenübermittlung nur aufgrund des "privacy shields" geregelt wird.

Schrems hatte bereits die Entscheidung von 2015 in Bezug auf Facebook erwirkt; er hatte von der irischen Datenschutzbehörde verlangt, zu unterbinden, daß Facebook Ireland seine Daten an den Mutterkonzern in den USA übermitteln darf. Dort würden diese Daten nicht angemessen gegen US-Überwachungsmaßnahmen gesichert, wie bereits die allseits bekannten Enthüllungen von Edward Snowden gezeigt hätten. Facebook USA sei verpfichtet, der NSA oder auch dem FBI Zugang zu sämtlichen Daten zu gewähren, ohne daß Betroffenen hiergegen eine wirksame Rechtsschutzmöglichkeit zur Verfügung stünde.

Dieses Manko hatte "Privacy Shield" eigentlich korrigieren wollen, indem der Mechanismus einer "Ombudsperson" in den Vorgang eingebaut wurde. Dem hat der EUGH nun aber eine Absage erteilt. In der Presseerklärung heißt es dazu:

> *In Bezug auf das Erfordernis des gerichtlichen Rechtsschutzes befindet der Gerichtshof, dass der im Privacy-Shield-Beschluss 2016/1250 angeführte Ombudsmechanismus entgegen den darin von der Kommission getroffenen Feststellungen* ***den betroffenen Personen keinen Rechtsweg zu einem Organ eröffnet, das Garantien böte, die den nach dem Unionsrecht erforderlichen Garantien der Sache nach gleichwertig wären, d.h. Garantien, die sowohl die Unabhängigkeit der durch diesen Mechanismus vorgesehenen Ombudsperson als auch das Bestehen von Normen gewährleisten, die die Ombudsperson dazu ermächtigen, gegenüber den amerikanischen Nachrichtendiensten verbindliche Entscheidungen zu erlassen. Aus all diesen Gründen erklärt der Gerichtshof den Beschluss 2016/1250 für ungültig.***

Gleichzeitig hat der EuGH jedoch eine Tür in die USA offen gelassen: Durch sog. „Standartvertragsklauseln“ dürfen weiterhin personenbezogene Daten in die USA übermittelt

werden – wenn denn diese bestimmten Anforderungen genügen. Es muß gewissermaßen ein äquivalentes Schutzniveau zu dem von der DSGVO regulierten Raum gewährleistet werden. Im einzelnen heißt es:

> *In Bezug auf das im Rahmen einer solchen Übermittlung erforderliche Schutzniveau entscheidet der Gerichtshof, dass die insoweit in der DSGVO vorgesehenen Anforderungen, die sich auf geeignete Garantien, durchsetzbare Rechte und wirksame Rechtsbehelfe beziehen, dahin auszulegen sind, dass die Personen, deren personenbezogene Daten auf der Grundlage von Standarddatenschutzklauseln in ein Drittland übermittelt werden, ein* ***Schutzniveau*** *genießen müssen,* ***das dem in der Union durch die DSGVO im Licht der Charta garantierten Niveau der Sache nach gleichwertig ist. Bei der Beurteilung dieses Schutzniveaus sind sowohl die vertraglichen Regelungen zu berücksichtigen, die zwischen dem in der Union ansässigen Datenexporteur und dem im betreffenden Drittland ansässigen Empfänger der Übermittlung vereinbart wurden, als auch, was einen etwaigen Zugriff der Behörden dieses Drittlands auf die übermittelten Daten betrifft, die maßgeblichen Aspekte der Rechtsordnung dieses Landes.***

Fraglich ist allerdings, ob man nach diesen Anforderungen überhaupt Standartvertragsklauseln für die Übermittlung in die USA konstruieren kann, die ein solches Schutzniveau gewährleisten. Sicherlich werden die großen amerikanischen Anbieter fieberhaft nach Lösungen für dieses Dilemma suchen.

Auf der Google-Webseite fand sich jedenfalls heute noch kein Hinweis auf eine Lösung, im Gegenteil wurden europäische Nutzer von Diensten wie analytics auf Pivacy Shield verwiesen.

Jedenfalls scheint „Abwarten und Teetrinken“ keine Lösung zu sein. Die Aufsichtsbehörden werden vom EuGH aufgefordert, eine Datenübermittlung zu unterbinden, wenn sie der Auffassung sind, daß das Datenschutzniveau trotz der Vertragsklauseln nicht eingehalten wird:

> *Hinsichtlich der Pflichten, die den Aufsichtsbehörden im Zusammenhang mit einer solchen Übermittlung obliegen, befindet der Gerichtshof, dass diese Behörden, sofern kein gültiger Angemessenheitsbeschluss der Kommission vorliegt, insbesondere* ***verpflichtet*** *sind,* ***eine Übermittlung personenbezogener Daten in ein Drittland auszusetzen oder zu verbieten, wenn sie*** *im Licht der Umstände dieser Übermittlung* ***der Auffassung sind,*** *dass die Standarddatenschutzklauseln in diesem Land nicht eingehalten werden oder nicht eingehalten werden können und* ***dass der nach dem Unionsrecht erforderliche Schutz der übermittelten Daten nicht mit anderen Mitteln gewährleistet werden kann, es sei denn, der in der Union ansässige Datenexporteur hat die Übermittlung selbst ausgesetzt oder beendet.***

Was heißt das nun für Sie?

In jedem Fall sollten Sie Ihre Datenschutzerklärungen und Datenverarbeitungsvorgänge dahingehend überprüfen, ob eine Datenübermittlung in die USA ausschließlich aufgrund des Privacy Shields stattfindet. Das wäre künftig unzulässig. Hierfür müßten zukünftig Alternativen gefunden werden. Typischerweise kann dies bei Übermittlungen im Rahmen von Analyse-Tools beim Web-Marketing, Custom-Audiences-Werbung, social-media-Integration und ähnlichen

Vorgängen stattfinden. Hier werden zukünftig nur Standartvertragsklauseln helfen (wenn sie o.g. Schutzniveau garantieren) – oder die Pseudonymisierung der fraglichen Daten, so daß sie im Ergebnis nicht als personenbezogen gelten. In Ausnahmefällen hilft möglicherweise Art. 49 DSGVO weiter, der einige Ausnahmetatbestände auflistet. Eine konkrete Einwilligungserklärung jedes Nutzers mit einer ausführlichen Risikoaufklärung möchten allerdings wohl die wenigsten Unternehmen für alle Nutzer durchführen.

Noch besser wäre es natürlich, direkt einen Anbieter mit Sitz in der EU zu finden – was zugegebenermaßen je nach Aufgabenstellung schwierig ist. Oder einmal technisch zu prüfen, ob es für den Nutzungszweck wirklich **personen**bezogene Daten sein müssen, die da übermittelt werden. Für viele Zwecke des big data und des BI (business intelligence, Geschäftsanalytik) reichen oft auch klug gesammelte pseudonymisierte Daten oder Daten von Benutzergruppen. Die Übermittlung solcher Daten ist in der Regel ohne weitere Vorkehrungen möglich.

In allen IT-rechtlichen und datenschutzrechtlichen Fragestellungen berät Sie gern:

Port7 Rechtsanwälte
Jürgen Hüneborn, Rechtsanwalt
Fachanwalt für IT-Recht
hueneborn@port7.de
0251-203 188 00 | 0163 – 6839657
Am Mittelhafen 16, 48155 Münster
www.port7.de

Quelle Presseerklärung des EuGH:

https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091de.pdf