von Rechtsanwalt **Jan Lennart Müller**

EuGH: EU-US Privacy-Shield entspricht nicht den Vorgaben der DSGVO und ist ungültig - die sog. Standardvertragsklauseln sind gültig

Ein Paukenschlag aus Luxemburg! Der EuGH hat mit Urteil vom 16.07.2020 das EU-US-Datenschutzschild (Privacy-Shield) für ungültig erklärt! Datentransfers in die USA, welche auf Basis dieses Privacy-Shields erfolgen sollen, sind damit unzulässig. Hingegen erklärte der EuGH den Beschluss 2010/87 der Kommission über die sog. Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländer (also auch in die USA) für gültig. In unserem Beitrag kommentieren wir die Entscheidung des EuGH zunächst und teilen mit, welche Konsequenzen aus dieser Entscheidung zu ziehen sind. Anschließend geben wir die Pressemitteilung des EuGH zum Thema wieder.

A. Kommentar der IT-Recht Kanzlei

I. Die Geschichte wiederholt sich - die Safe-Harbor-Entscheidung aus 2015

Mit seiner Entscheidung vom 06.10.2015 (Az.C-362/14) hatte der Europäische Gerichtshof (EuGH) das sog. Safe Harbor-Abkommen zwischen den USA und der EU als Grundlage für den Transfers von personenbezogenen Daten in die USA für unwirksam erklärt. Bereits damals wurde dem Datentransfer quasi über Nacht der rechtssichere Boden entzogen.

Als Reaktion auf die Entscheidung des EuGH wurde im zeitlichen Nachgang zwischen der EU und den USA das Privacy-Shield ausgehandelt. Das Privacy-Shield sollte als (rechtskonformer) Nachfolger zu Safe-Harbor die Grundlage für eine datenschutzkonforme Übertragung von personenbezogenen Daten in die USA dienen.

II. Welche Datentransfers in die USA sind betroffen?

Von der neuen EuGH-Rechtsprechung sind letztlich alle Arten von Transfers personenbezogener Daten an US-Unternehmen oder auf Server in den USA betroffen, die bislang aufgrund des Privacy-Shield-Abkommens vorgenommen wurden.

Insbesondere sind hiervon etwa Hostingleistungen, Paymenentdienstleistungen, Websanalyse- und Trackingsdienste, Social Network-Dienstleistungen, etc. betroffen.

Auch mit US-Servern verbundene Plugins- oder Website-Analysetools, die personenbezogene Daten abfragen, übertragen und speichern, sind davon erfasst.

III. Wie sollen sich Online-Händler nun verhalten?

Nachdem nun Transfers personenbezogener Daten aus Deutschland in die USA auf Grundlage des Privacy-Shields-Beschlusses nicht mehr möglich ist, stellt sich die Frage, wie Online-Händler von nun an personenbezogene Daten in rechtmäßiger Weise an US-Unternehmen und auf Server in den USA übertragen können.

Aufgrund der Aktualität der Ereignisse wissen selbst die obersten Datenschützer Deutschlands noch keine Antwort.

Denkbar wäre das Folgende:

- Eine Möglichkeit ist und bleibt natürlich die informierte Einwilligung desjenigen, dessen personenbezogene Daten betroffen sind (gemäß Art. 49 Abs. S. 1 a) DSGVO - die sog. Ausnahme im Einzelfall). Die Übermittlung kann auf Basis einer ausdrücklichen und informierten Einwilligung des Betroffenen erfolgen. Der Haken an der Sache: Grundvoraussetzung für eine wirksame Einwilligung ist eine umfassende ordnungsgemäße Vorabinformation des Betroffenen. Hierbei muss der Betroffene über das konkrete Risiko der Datenübermittlung in ein Drittland ohne adäquates Schutzniveau aufgeklärt werden. Diese Information sollte Angaben darüber enthalten, auf welche personenbezogenen Daten und auf **welche Verarbeitungsvorgänge und -zwecke** sich die Zustimmung bezieht. Ferner bedarf es der Angabe des Empfängers und des Zielortes und eines Hinweises auf die dortigen Verarbeitungsvoraussetzungen. Nur wenn der Betroffene aufgrund einer breiten und umfassenden Informationsgrundlage bewusst in den Transfer seiner personenbezogenen Daten eingewilligt hat, legitimiert seine Einwilligung die entsprechenden Datentransfers. Ein versteckter Hinweis in AGB genügt hierfür nicht.
- Eine weitere Möglichkeit besteht nach Art. 49 Abs. 1 S.1 b) DSGVO dann, wenn die Datenübermittlung

zur Vertragsabwicklung erforderlich ist. Diese Rechtfertigung ist dann gegeben, wenn die vertragliche Leistung die Datenübermittlung in die USA bedingt und setzt voraus, dass der Betroffene Vertragspartei ist. Auch Datenübermittlungen im Rahmen des internationalen Zahlungsverkehrs und per Versand abgewickelte Kaufverträge werden hierbei als typische Beispiele für diesen Rechtfertigungsgrund genannt.

- Zudem sind **sog. "Binding Corporate Rules"** (kurz: BCR bzw. sog. verbindliche interne Datenschutzvorschriften) eine mögliche Rechtsgrundlage für die Datenübermittlung (Art. 47 Abs. 1 DSGVO). Dabei handelt es sich um aufwendige, unternehmensinterne Grundsätze zum unternehmensinternen Umgang mit personenbezogenen Daten, etwa von Kunden und Mitarbeitern, die zusammen mit Datenschutzbehörden erarbeitet werden und letztlich auch deren Kontrolle unterliegen. Für insbesondere kleinere und mittelgroße Online-Händler stellen BCR allerdings keine wirkliche Alternative dar, da sie nur unter größerem - auch finanziellem - Aufwand erarbeitet werden können und nicht akut in Kürze auf die Beine zu stellen sind. Diese Ausnahme dürfte aber wohl für kaum einen Online-Händler relevant sein.
- Schließlich können deutsche Online-Händler in ihre vertraglichen Beziehungen mit US-Unternehmen die datenschutzbezogenen sog. EU-Standardvertragsklauseln einbauen. Diese wurden vom EuGH ausdrücklich als zulässig erachtet! Diese Klauseln hat die EU entwickelt, um einen bestimmten Mindeststandard des Datenschutzes für personenbezogene Daten zu formulieren. Hierbei wären Online-Händler allerdings auf die Bereitstellung derartiger Standardvertragsklauseln durch die us-amerikanischen Diensteanbieter angewiesen. Eine kurzfristige Bereitstellung dürfte hier nicht möglich sein.

IV. Beschränkte Reaktionsmöglichkeiten, ein Grund zur Sorge?

Wirklich praxistaugliche Lösungen gibt es für das gegenwärtige Datenschutzproblem somit nicht. Streng genommen dürfte ein weit überwiegender Großteil der täglichen Transfers von personenbezogenen Daten aus Deutschland an US-Unternehmen bzw. US-Server wegen Verstoßes gegen die DSGVO rechtswidrig sein. Abmahnungen durch Konkurrenten oder Verbraucherschutzverbände wären daher grundsätzlich genauso denkbar und möglich wie Sanktionen durch Datenschutzbehörden.

Aufgrund der Erfahrungen zur Entscheidung von Safe-Harbor gehen wir davon aus, dass zumindest in nächster Zeit aller Wahrscheinlichkeit nach kaum Bußgelder oder Abmahnungen drohen. Gleichwohl kann man die zukünftige Entwicklung nicht vorhersehen. Wer den sichersten Weg beschreiten möchte, sollte bis zur Klärung eines zulässigen Datentransfers von der Verwendung US-amerikanischer Diensteanbieter absehen (sofern für den Betrieb personenbezogene Daten der Kunden in die USA übermittelt werden).

Wir gehen davon aus, dass sich die EU und die USA zeitnah zusammensetzen werden, um über ein

Nachfolgeabkommen zum Privacy-Shield zu verhandeln. Zwar ist noch unklar, wann und mit welchem genauen Inhalt das Nachfolgeabkommen in Kraft treten wird. Bis dahin halten wir allerdings ein Einschreiten durch die Datenschutzbehörden für nicht sehr wahrscheinlich.

V. Fazit

Das Privacy-Shield-Urteil des EuGH verunsichert viele Online-Händler. Unklar ist, auf welcher Rechtsgrundlage nun der Transfer von personenbezogenen Daten an US-Unternehmen bzw. auf US-Server im Rahmen von Cloud-Diensten, Social Networks oder sonstigen webbasierten Diensten stattfinden darf. Zwar ist streng genommen nun Vieles, was alltäglich an Datentransfers stattfindet, rechtswidrig, doch dürften die Datenschutzbehörden nach derzeitigem Stand weit davon entfernt sein, die von der Politik verschuldete Rechtsunsicherheit auf dem Rücken kleinerer und mittlerer Unternehmen auszutragen.

Dafür spricht auch das recht moderate Vorgehen der Datenschutzbehörden in der Vergangenheit, als das Safe-Harbor-Abkommen durch den EuGH für unzulässig erklärt worden ist.

Wer allerdings den sichersten Weg beschreiten möchte, sollte auf den Datentransfer in die USA verzichten und entsprechend verwendete Dienste vorerst deaktivieren.

B. Die Pressemitteilung des EuGH:

Der Gerichtshof erklärt den Beschluss 2016/1250 über die Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes für ungültig

Der Beschluss 2010/87 der Kommission über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern ist hingegen gültig

Die Datenschutz-Grundverordnung (DSGVO) bestimmt, dass personenbezogene Datengrundsätzlich nur dann in ein Drittland übermittelt werden dürfen, wenn das betreffende Land für die Daten ein angemessenes Schutzniveau gewährleistet. Nach dieser Verordnung kann die Kommission feststellen, dass ein Drittland aufgrund seiner innerstaatlichen Rechtsvorschriftenoder seiner internationalen Verpflichtungen ein angemessenes Schutzniveau gewährleistet. Liegt kein derartiger Angemessenheitsbeschluss vor, darf eine solche Übermittlung nur erfolgen, wenn der in der Union ansässige Exporteur der personenbezogenen Daten geeignete Garantien vorsieht, die sich u. a. aus von der Kommission erarbeiteten Standarddatenschutzklauseln ergeben können, und wenn die betroffenen Personen über durchsetzbare Rechte und wirksame Rechtsbehelfe verfügen. Ferner ist in der DSGVO genau geregelt, unter welchen Voraussetzungen eine solche Übermittlung vorgenommen werden darf,

falls weder ein Angemessenheitsbeschluss vorliegt noch geeignete Garantien bestehen.

Herr Schrems, ein in Österreich wohnhafter österreichischer Staatsangehöriger, ist seit 2008 Nutzer von Facebook. Wie bei allen anderen im Unionsgebiet wohnhaften Nutzern werden seine personenbezogenen Daten ganz oder teilweise von Facebook Ireland an Server der Facebook Inc., die sich in den Vereinigten Staaten befinden, übermittelt und dort verarbeitet. Herr Schrems legte bei der irischen Aufsichtsbehörde eine Beschwerde ein, die im Wesentlichen darauf abzielte, diese Übermittlungen verbieten zu lassen. Er machte geltend, das Recht und die Praxis der Vereinigten Staaten böten keinen ausreichenden Schutz vor dem Zugriff der Behörden auf die dorthin übermittelten Daten. Seine Beschwerde wurde u. a. mit der Begründung zurückgewiesen, die Kommission habe in ihrer Entscheidung 2000/5205 (sogenannte "Safe-Harbour Entscheidung") festgestellt, dass die Vereinigten Staaten ein angemessenes Schutzniveau gewährleisteten. Mit Urteil vom 6. Oktober 2015 erklärte der Gerichtshof auf ein Vorabentscheidungsersuchen des irischen High Court hin diese Entscheidung für ungültig (im Folgenden: Urteil Schrems I).

Nachdem das Urteil Schrems I ergangen war und der irische High Court daraufhin die Entscheidung, mit der die Beschwerde von Herrn Schrems zurückgewiesen worden war, aufgehoben hatte, forderte die irische Aufsichtsbehörde Herrn Schrems auf, seine Beschwerde unter Berücksichtigung der Ungültigkeitserklärung der Safe-Harbour-Entscheidung durch den Gerichtshof umzuformulieren. Mit seiner umformulierten Beschwerde macht Herr Schrems geltend, dass die Vereinigten Staaten keinen ausreichenden Schutz der dorthin übermittelten Daten gewährleisteten. Er beantragt, die von Facebook Ireland nunmehr auf der Grundlage der Standardschutzklauseln im Anhang des Beschlusses 2010/877 vorgenommene Übermittlung seiner personenbezogenen Daten aus der Union in die Vereinigten Staaten für die Zukunft auszusetzen oder zu verbieten. Die irische Aufsichtsbehörde war der Auffassung, dass die Bearbeitung der Beschwerde von Herrn Schrems insbesondere von der Gültigkeit des Beschlusses 2010/87 über Standardvertragsklauseln abhänge, und strengte daher ein Verfahren vor dem High Court an, damit er den Gerichtshof mit einem Vorabentscheidungsersuchen befassen möge. Nachdem dieses Verfahren eingeleitet worden war, erließ die Kommission den Beschluss (EU) 2016/1250 über die Angemessenheit des vom EU-US-Datenschutzschild ("Privacy Shield") gebotenen Schutzes.

Mit seinem Vorabentscheidungsersuchen fragt der irische High Court den Gerichtshof nach der Anwendbarkeit der DSGVO auf Übermittlungen personenbezogener Daten, die auf die Standardschutzklauseln im Beschluss 2010/87 gestützt werden, sowie nach dem Schutzniveau, das diese Verordnung im Rahmen einer solchen Übermittlung verlangt, und den Pflichten, die den Aufsichtsbehörden in diesem Zusammenhang obliegen. Des Weiteren wirft der High Court die Frage der Gültigkeit sowohl des Beschlusses 2010/87 über Standardvertragsklauseln als auch des Privacy Shield-Beschlusses 2016/1250 auf.

Mit seinem heute verkündeten Urteil stellt der Gerichtshof fest, dass die Prüfung des Beschlusses 2010/87 über Standardvertragsklauseln anhand der Charta der Grundrechte der Europäischen Union nichts

ergeben hat, was seine Gültigkeit berühren könnte. Den Privacy Shield-Beschluss 2016/1250 erklärt er hingegen für ungültig. Der Gerichtshof führt zunächst aus, dass das Unionsrecht, insbesondere die DSGVO, auf eine zu gewerblichen Zwecken erfolgende Übermittlung personenbezogener Daten durch einen in einem Mitgliedstaat ansässigen Wirtschaftsteilnehmer an einen anderen, in einem Drittland ansässigen Wirtschaftsteilnehmer Anwendung findet, auch wenn die Daten bei ihrer Übermittlung oder im Anschluss daran von den Behörden des betreffenden Drittlands für Zwecke der öffentlichen Sicherheit, der Landesverteidigung und der Sicherheit des Staates verarbeitet werden können.

Eine derartige Datenverarbeitung durch die Behörden eines Drittlands kann nicht dazu führen, dass eine solche Übermittlung vom Anwendungsbereich der DSGVO ausgenommen wäre. 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.

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. Sodann prüft der Gerichtshof die Gültigkeit des Beschlusses 2010/87 über Standardvertragsklauseln. Er sieht sie nicht schon dadurch in Frage gestellt, dass die in diesem Beschluss enthaltenen Standarddatenschutzklauseln aufgrund ihres Vertragscharakters die Behörden des Drittlands, in das möglicherweise Daten übermittelt werden, nicht binden. Vielmehr hängt sie davon ab, ob der Beschluss wirksame Mechanismen enthält, die in der Praxis gewährleisten können, dass das vom Unionsrecht verlangte Schutzniveau eingehalten wird und dass auf solche Klauseln gestützte Übermittlungen personenbezogener Daten ausgesetzt oder verboten werden, wenn gegen diese Klauseln verstoßen wird oder ihre Einhaltung unmöglich ist. Der Gerichtshof stellt fest, dass der Beschluss 2010/87 derartige Mechanismen vorsieht. Insoweit hebt er insbesondere hervor, dass gemäß diesem Beschluss der Datenexporteur und der Empfänger der Übermittlung vorab prüfen müssen, ob das erforderliche Schutzniveau im betreffenden Drittland eingehalten wird, und dass der Empfänger dem Datenexporteur gegebenenfalls mitteilen muss, dass er

die Standardschutzklauseln nicht einhalten kann, woraufhin der Exporteur die Datenübermittlung aussetzen und/oder vom Vertrag mit dem Empfänger zurücktreten muss.

Schließlich prüft der Gerichtshof die Gültigkeit des Privacy-Shield-Beschlusses 2016/1250 anhand der Anforderungen der DSGVO im Licht der Bestimmungen der Charta, die die Achtung des Privat- und Familienlebens, den Schutz personenbezogener Daten und das Recht auf effektiven gerichtlichen Rechtsschutz verbürgen. Insoweit stellt er fest, dass in diesem Beschluss, ebenso wie in der Safe-Harbour-Entscheidung 2000/520, den Erfordernissen der nationalen Sicherheit, des öffentlichen Interesses und der Einhaltung des amerikanischen Rechts Vorrang eingeräumt wird, was Eingriffe in die Grundrechte der Personen ermöglicht, deren Daten in die Vereinigten Staaten übermittelt werden. Er kommt zu dem Ergebnis, dass die von der Kommission im PrivacyShield-Beschluss 2016/1250 bewerteten Einschränkungen des Schutzes personenbezogener Daten, die sich daraus ergeben, dass die amerikanischen Behörden nach dem Recht der Vereinigten Staaten auf solche Daten, die aus der Union in dieses Drittland übermittelt werden, zugreifen und sie verwenden dürfen, nicht dergestalt geregelt sind, dass damit Anforderungen erfüllt würden, die den im Unionsrecht nach dem Grundsatz der Verhältnismäßigkeit bestehenden Anforderungen der Sache nach gleichwertig wären, da die auf die amerikanischen Rechtsvorschriften gestützten Überwachungsprogramme nicht auf das zwingend erforderliche Maß beschränkt sind.

Gestützt auf die Feststellungen in diesem Beschluss weist der Gerichtshof darauf hin, dass die betreffenden Vorschriften hinsichtlich bestimmter Überwachungsprogramme in keiner Weise erkennen lassen, dass für die darin enthaltene Ermächtigung zur Durchführung dieser Programme Einschränkungen bestehen; genauso wenig ist ersichtlich, dass für die potenziell von diesen Programmen erfassten Personen, die keine amerikanischen Staatsbürger sind, Garantien existieren. Der Gerichtshof fügt hinzu, dass diese Vorschriften zwar Anforderungen vorsehen, die von den amerikanischen Behörden bei der Durchführung der betreffenden Überwachungsprogramme einzuhalten sind, aber den betroffenen Personen keine Rechte verleihen, die gegenüber den amerikanischen Behörden gerichtlich durchgesetzt werden können.

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.

Den Volltext der Entscheidung können Sie **hier** nachlesen.

Quelle: Pressmitteilung Nr. 91/20 des EuGH vom 16.07.2020

Autor:
RA Jan Lennart Müller
Rechtsanwalt