Der EuGH prüft den EU-Standardvertrag und das EU-US-PrivacyShield.
Der EU-Standardvertrag "überlebt"... allerdings bestehen auch hier heftige Restzweifel.
Die Einwilligung gemäß Artikel 49 (1a) DS-GVO wird an Bedeutung gewinnen.

Gerichtshof der Europäischen Union
PRESSEMITTEILUNG Nr. 91/20
Luxemburg, den 16. Juli 2020

Presse und Information

Urteil in der Rechtssache C-311/18
Data Protection Commissioner / Maximillian Schrems und Facebook Ireland

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[1] (DSGVO) bestimmt, dass personenbezogene Daten grundsätzlich 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 Rechtsvorschriften oder seiner internationalen Verpflichtungen ein angemessenes Schutzniveau gewährleistet[2]. 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[3]. 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[4].

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 2000/520[5] (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)[6].

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 Ungültigerklärung der Safe-Harbour-Entscheidung durch den Gerichtshof umzuformulieren. Mit seiner umformulierten Beschwerde macht Herr Schrems geltend,

---

[1] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (ABl. 2016, L 119, S. 1).
[2] Art. 45 der DSGVO.
[3] Art. 46 Abs. 1 und Abs. 2 Buchst. c der DSGVO.
[4] Art. 49 der DSGVO.
[5] Entscheidung der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des „sicheren Hafens“ und der diesbezüglichen „Häufig gestellten Fragen“ (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA (ABl. 2000, L 215, S. 7).
[6] Urteil des Gerichtshofs vom 6. Oktober 2015, Schrems, C-362/14 (vgl. auch Pressemitteilung Nr. 117/15).

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 2010/87[7] 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[8].

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.

Auch die Datenverarbeitung der Geheimdienste muss beurteilt werden!

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.**

Ein EU-Standardvertrag hilft nicht weiter, wenn es sich beim Drittland um einen Überwachungsstaat handelt.
Die Schraube wird weiter angezogen. Dieser Aspekt wird noch große Diskussionen auslösen!

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,**

---

[7] Beschluss der Kommission vom 5. Februar 2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates (ABl. 2010, L 39, S. 5) in der Fassung des Durchführungsbeschlusses (EU) 2016/2297 der Kommission vom 16. Dezember 2016 (ABl. 2016, L 334, S. 100).

[8] Durchführungsbeschluss (EU) 2016/1250 der Kommission vom 12. Juli 2016 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes (ABl. 2016, L 207, S. 1).

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.**

Die irische Aufsichtsbehörde muss also die staatliche Überwachung beurteilen und ggf. die Übermittlung verbieten.

A.) 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.

B.) 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 Privacy-Shield-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. Im Klartext: Die USA sind ein "Überwachungsstaat", der keine Grenzen kennt.

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.**

HINWEIS: Im Wege eines Vorabentscheidungsersuchens können die Gerichte der Mitgliedstaaten in einem bei ihnen anhängigen Rechtsstreit dem Gerichtshof Fragen nach der Auslegung des Unionsrechts oder nach der Gültigkeit einer Handlung der Union vorlegen. Der Gerichtshof entscheidet nicht über den nationalen Rechtsstreit. Es ist Sache des nationalen Gerichts, über die Rechtssache im Einklang mit der Entscheidung des Gerichtshofs zu entscheiden. Diese Entscheidung des Gerichtshofs bindet in gleicher Weise andere nationale Gerichte, die mit einem ähnlichen Problem befasst werden.

Pressekontakt: Hartmut Ost ☎ (+352) 4303 3255

Filmaufnahmen von der Verkündung des Urteils sind verfügbar über „Europe by Satellite“ ☎ (+32) 2 2964106

Das EU-US-PrivacyShield ist nicht EU-rechtskonform, weil es voraussetzt, dass in den USA ein Mindestmaß an Datenschutz gewährleistet ist. Der EuGH stellt aber fest, dass es sich um einen unbegrenzten "Überwachungsstaat" handelt, der den betroffenen Personen keine Garantien oder Rechtsstaatlichkeit gewährt.

Insofern hat die EU-Kommission sowohl bei SafeHarbor, als auch hier beim EU-PrivacyShield eine falsche Einschätzung getroffen. Die EU-Kommission hat die polititsche Wirklichkeit der USA ausgeblendet, und man hat sich von den windelweichen Zusagen der USA (gerne) blenden lassen.

Der EU-Standardvertrag hingegen ist nicht zu bemängeln, weil er u.a. voraussetzt, dass die Vertragspartner die staatlichen Überwachungsprogramme beurteilen und ggf. zu dem Ergebnis kommen müssen, dass der Vertrag letztlich unwirksam wäre.

Logisch zu Ende gedacht (wenn man also 1 und 1 zusammenzählt) bedeutet dies:

Auch die EU-Standardverträge sind mit US-Unternehmen keine Option, weil der EuGH bereits festgestellt hat, dass es sich um einen Überwachungsstaat handelt. Daher dürfen die potentiellen Vertragspartner den Vertrag nicht unterschreiben. Leider geht der EuGH auf diese logische Konsequenz nicht ein. Diese "Bombe" wird also erst später zünden...

Sollte sich die obige Erkenntnis durchsetzen, so gäbe es derzeit wohl kein Mittel mehr, um Daten von EU-Bürgern in die USA zu transferieren.

Die Verantwortlichen müssen aber auch bei allen anderen Drittländern (Indien, Korea etc.) kritisch prüfen, ob die allgemeine staatliche Situation einen EU-Standardvertrag zulässt. Ein "blindes" Ausfüllen dieses EU-Standardvertrages ist nicht rechtskonform.

Der Druck auf einen "Angemessenheitsbeschluss" wird größer. Die Regierungen von Drittländern werden eines Tages vielleicht ihre Gesetzgebung ändern, um als "angemessen" eingeschätzt zu werden und personenbezogene Daten aus der EU erhalten zu dürfen.

... oder die EU wird vom WWW abgeschnitten und die IT-Globalisierung wird gestoppt.

Der Artikel 49 (1) DS-GVO wird wohl an Bedeutung gewinnen, denn dort wird die Zulässigkeit unter den Aspekten EINWILLIGUNG, VERTRAGSERFÜLLUNG etc. thematisiert.