EuGH: „Privacy Shield“-Abkommen ist unwirksam

Am 12.7.2016 trat das „Privacy Shield“-Abkommen in Kraft. Dieser Beschluss der Europäischen Kommission sollte ein angemessenes Datenschutzniveau für die Datenübermittlung in die USA gewährleisten und einen sicheren Rechtsrahmen für Unternehmen schaffen. Der EuGH (Urt. v. 16.7.2020 – C-311/18) erklärte ihn heute für ungültig.

Hintergrund

Die DSGVO bestimmt in Art. 45, dass personenbezogene Daten grundsätzlich nur dann in ein Drittland übermittelt werden dürfen, wenn ein angemessenes Datenschutzniveau in dem Zielland gewährleistet werden kann.

> *(1) Eine Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation darf vorgenommen werden, wenn die Kommission beschlossen hat, dass das betreffende Drittland, ein Gebiet oder ein oder mehrere spezifische Sektoren in diesem Drittland oder die betreffende internationale Organisation ein angemessenes Schutzniveau bietet. Eine solche Datenübermittlung bedarf keiner besonderen Genehmigung.*

Hierzu erließ die Europäische Kommission am 12.7.2016 den Durchführungsbeschluss (EU) 2016/1250 über die Angemessenheit des vom EU-US-Datenschutzschild („Privacy Shield“) gebotenen Schutzes. Dieser Beschluss der Kommission folgte auf das SafeHarbor-Abkommen, das der EuGH 2015 (Urt. v. 6.10.2015 – C-362/14) für ungültig erklärte.

Worum ging es in dem Verfahren?

Ausgangspunkt des Verfahrens war die Weiterleitung personenbezogener Daten der Facebook Ireland Ltd. an die Facebook Inc. in den USA. Nachdem der EuGH bereits das SafeHarbor-Abkommen für ungültig erklärt hatte, hat der Kläger seine Beschwerde umformuliert und geltend gemacht, dass die USA keinen ausreichenden Schutz der dorthin übermittelten Daten gewährleisteten. Er beantragte, die von Facebook Ireland nunmehr auf der Grundlage der Standardschutzklauseln im Anhang des Beschlusses 2010/87 vorgenommene Übermittlung seiner personenbezogenen Daten aus der EU in die USA für die Zukunft auszusetzen oder zu verbieten. Die irische Aufsichtsbehörde war der Auffassung, dass die Bearbeitung der Beschwerde des Klägers insbesondere von der Gültigkeit des Beschlusses 2010/87 über Standardvertragsklauseln abhänge, und strengte daher ein Verfahren vor dem High Court an, um dem EuGH die entsprechenden Fragen zur Vorabentscheidung vorlegen zu können. Nachdem dieses Verfahren bereits 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 EuGH nach der Anwendbarkeit der DSGVO auf Übermittlungen personenbezogener Daten, die auf die Standardschutzklauseln im Beschluss 2010/87 gestützt werden, nach dem Schutzniveau, das die DSGVO im Rahmen einer solchen Übermittlung verlangt, und den Pflichten, die den Aufsichtsbehörden in diesem Zusammenhang obliegen. Zudem fragte der High Court nach der Gültigkeit sowohl des Beschlusses 2010/87 über Standarddatenschutzklauseln als auch des Privacy Shield-Beschlusses 2016/1250.

Das Urteil des EuGH

Der EuGH erklärte den Privacy Shield-Beschluss 2016/1250 der Europäischen Kommission für ungültig. Der Beschluss über Standardvertragsklauseln 2010/87 für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern sei jedoch wirksam.

Gleichwertiges Schutzniveau auch im Drittland erforderlich

Der EuGH stellte klar, dass bei einer Übermittlung personenbezogener Daten in ein Drittland ein Schutzniveau erforderlich ist, das mit dem in der Union vergleichbar ist.

> *Folglich ist auf die Fragen 2, 3 und 6 zu antworten, dass Art. 46 Abs. 1 und Art. 46 Abs. 2 Buchst. c der DSGVO dahin auszulegen sind, dass die nach diesen Vorschriften erforderlichen geeigneten Garantien, durchsetzbaren Rechte und wirksamen Rechtsbehelfe gewährleisten müssen, dass die Rechte der Personen, deren personenbezogene Daten auf der Grundlage von Standarddatenschutzklauseln in ein Drittland übermittelt werden, ein Schutzniveau genießen, das dem in der Union durch die DSGVO im Licht der Charta garantierten Niveau der Sache nach gleichwertig ist.*

Für diese Beurteilung seien sowohl die vertraglichen Vereinbarungen zwischen Datenexporteur und -empfänger als auch die Rechtsordnung des entsprechenden Landes zu berücksichtigen.

> *Bei der insoweit im Zusammenhang mit einer solchen Übermittlung erforderlichen Beurteilung sind insbesondere die vertraglichen Regelungen zu berücksichtigen, die zwischen dem in der Union ansässigen Verantwortlichen bzw. seinem dort ansässigen Auftragsverarbeiter und dem im betreffenden Drittland ansässigen Empfänger der Übermittlung vereinbart wurden, sowie, was einen etwaigen Zugriff der Behörden dieses Drittlands auf die übermittelten personenbezogenen Daten betrifft, die maßgeblichen Elemente der Rechtsordnung dieses Landes. In der letztgenannten Hinsicht entsprechen die Elemente, die im Kontext von Art. 46 der DSGVO zu berücksichtigen sind, denen, die in ihrem Art. 45 Abs. 2 in nicht abschließender Weise aufgezählt werden.*

Prüfung durch die Datenschutzbehörden

Eine weitere Vorlagefrage betraf die Verwendung von Standarddatenschutzklauseln, sofern kein gültiger Angemessenheitsbeschluss der Kommission vorliegt. Das vorlegende Gericht wollte wissen, ob die zuständige Datenschutzbehörde dazu verpflichtet sei, die Übermittlung personenbezogener Daten in ein Drittland auszusetzen oder zu verbieten, wenn sie der Auffassung ist, dass die Klauseln in diesem Drittland nicht eingehalten werden oder nicht eingehalten werden können und dass der nach dem Unionsrecht, insbesondere nach den Art. 45 und 46 der DSGVO sowie nach der Charta, erforderliche Schutz der übermittelten Daten nicht gewährleistet werden kann. Der EuGH bestätigte eine entsprechende Pflicht der Datenschutzbehörden.

> *Nach alledem ist auf die achte Frage zu antworten, dass Art. 58 Abs. 2 Buchst. f und j der DSGVO dahin auszulegen ist, dass die zuständige Aufsichtsbehörde, sofern kein gültiger Angemessenheitsbeschluss der Kommission vorliegt, verpflichtet ist, eine auf Standarddatenschutzklauseln, die von der Kommission erarbeitet wurden, gestützte Übermittlung personenbezogener Daten in ein Drittland auszusetzen oder zu verbieten, wenn diese Behörde im Licht aller Umstände dieser Übermittlung der Auffassung ist, dass die Klauseln in diesem Drittland nicht eingehalten werden oder nicht eingehalten werden können und dass der nach dem Unionsrecht, insbesondere nach den Art. 45 und 46 der DSGVO sowie nach der Charta, erforderliche Schutz der übermittelten Daten nicht mit anderen Mitteln gewährleistet werden kann, es sei denn, der in der Union ansässige Verantwortliche bzw. sein dort ansässiger Auftragsverarbeiter hat die Übermittlung selbst ausgesetzt oder beendet.*

Beschluss über Standarddatenschutzklauseln

wirksam

Eine weitere Frage betraf die Wirksamkeit des Beschlusses 2010/87 der Kommission, also der Standarddatenschutzklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern. Hintergrund ist, dass diese Standarddatenschutzklauseln drittstaatliche Behörden nicht binden, ein angemessenes Schutzniveau für die übermittelten Daten zu gewährleisten. Der EuGH kommt zu dem Ergebnis, dass der Beschluss 2010/87 über Standardvertragsklauseln gültig ist. Dass ihr Vertragscharakter die Behörden des Drittlandes nicht binde, sei hierfür nicht entscheidend.

> *Der bloße Umstand, dass Standarddatenschutzklauseln, die wie die im Anhang des SDK-Beschlusses befindlichen in einem gemäß Art. 46 Abs. 2 Buchst. c der DSGVO ergangenen Beschluss der Kommission enthalten sind, die Behörden der Drittländer, in die möglicherweise personenbezogene Daten übermittelt werden, nicht binden, kann folglich die Gültigkeit dieses Beschlusses nicht berühren.*

Erforderlich sei vielmehr das Vorhandensein wirksamer Mechanismen, die die Einhaltung eines entsprechenden Schutzniveaus gewährleisten können.

> *Vielmehr hängt die Gültigkeit eines solchen Beschlusses davon ab, ob er im Einklang mit dem aus Art. 46 Abs. 1 und Art. 46 Abs. 2 Buchst. c der DSGVO im Licht der Art. 7, 8 und 47 der Charta resultierenden Erfordernis 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.*

Dies sei bei den Standarddatenschutzklauseln der Fall, so der EuGH. Sie seien gültig.

Privacy-Shield gewährt US-Recht Vorrang

Die weiteren Fragen betrafen die Wirksamkeit des Privacy Shield-Beschlusses der Kommission. Die Prüfung des Privacy Shields durch den EuGH ergab, dass dieser den Erfordernissen der nationalen Sicherheit, des öffentlichen Interesses und der Einhaltung des amerikanischen Rechts Vorrang einräumt, was Eingriffe in die Grundrechte der Personen ermögliche, deren Daten in die Vereinigten Staaten übermittelt werden.

> *Allerdings wird in Abschnitt I.5 des Anhangs II („Grundsätze des EU-US-Datenschutzschilds[,] vorgelegt vom amerikanischen Handelsministerium“) des DSS-Beschlusses auch ausgeführt, dass die Einhaltung dieser Grundsätze u. a. insoweit begrenzt sein könne, „als Erfordernissen der nationalen Sicherheit, des öffentlichen Interesses oder der Durchführung von Gesetzen Rechnung getragen werden muss“. Somit wird in diesem Beschluss, ebenso wie in der Entscheidung 2000/520, diesen Erfordernissen Vorrang vor den genannten Grundsätzen eingeräumt; aufgrund dieses Vorrangs sind die selbstzertifizierten US-Organisationen, die aus der Union personenbezogene Daten erhalten, ohne jede Einschränkung verpflichtet, diese Grundsätze unangewendet zu lassen, wenn sie in Widerstreit zu den genannten Erfordernissen stehen und sich deshalb als mit ihnen unvereinbar erweisen (vgl. entsprechend, zur Entscheidung 2000/520, Urteil vom 6. Oktober 2015, Schrems, C-362/14, EU:C:2015:650, Rn. 86).*

Keine Möglichkeit der Durchsetzung

Die Ermächtigung von amerikanischen Behörden zur Durchführung von Überwachungsprogrammen lasse keine Einschränkungen auf das zwingend erforderliche Maß erkennen. Zudem werden den betroffenen Personen keine Rechte verliehen, die gegenüber den amerikanischen Behörden gerichtlich durchgesetzt werden können.

Demzufolge lässt Section 702 des FISA in keiner Weise erkennen, dass für die darin enthaltene Ermächtigung zur Durchführung von Überwachungsprogrammen zum Zweck der Auslandsaufklärung Einschränkungen bestehen; genauso wenig ist erkennbar, dass für potenziell von diesen Programmen erfasste Nicht-US-Personen Garantien existieren. […]

Nach den Feststellungen im DSS-Beschluss müssen die auf Section 702 des FISA gestützten Überwachungsprogramme zwar unter Beachtung der aus der PPD-28 folgenden Anforderungen durchgeführt werden. Während die Kommission in den Erwägungsgründen 69 und 77 des DSS-Beschlusses hervorgehoben hat, dass solche Anforderungen für die amerikanischen Nachrichtendienste verbindlich seien, hat die amerikanische Regierung jedoch auf eine Frage des Gerichtshofs eingeräumt, dass die PPD-28 den betroffenen Personen keine Rechte verleihe, die gegenüber den amerikanischen Behörden gerichtlich durchgesetzt werden könnten. Folglich ist die PPD-28 nicht geeignet, ein Schutzniveau zu gewährleisten, das dem aus der Charta resultierenden Niveau der Sache nach gleichwertig wäre; dies steht im Widerspruch zu Art. 45 Abs. 2 Buchst. a der DSGVO, wonach die Feststellung dieses Niveaus u. a. davon abhängt, ob die Personen, deren Daten in das fragliche Drittland übermittelt wurden, über wirksame und durchsetzbare Rechte verfügen.

Privacy Shield ist ungültig

Der EuGH kommt zu dem Ergebnis, dass die USA kein angemessenes Schutzniveau gewährleisten. Er erklärte den Beschluss 2016/1250 für ungültig.

Daher hat die Kommission bei ihrer Feststellung in Art. 1 Abs. 1 des DSS-Beschlusses, dass die Vereinigten Staaten für personenbezogene Daten, die im Rahmen des EU-US-Datenschutzschilds aus der Union an Organisationen in diesem Drittland übermittelt würden, ein angemessenes Schutzniveau gewährleisteten, die Anforderungen verkannt, die sich aus Art. 45 Abs. 1 der DSGVO im Licht der Art. 7, 8 und 47 der Charta ergeben. Daraus folgt, dass Art. 1 des DSS-Beschlusses mit Art. 45 Abs. 1 der DSGVO, ausgelegt im Licht der Art. 7, 8 und 47 der Charta, unvereinbar und somit ungültig ist. Da Art. 1 des DSS-Beschlusses untrennbar mit dessen Art. 2 bis 6 sowie dessen Anhängen verbunden ist, führt seine Ungültigkeit zur Ungültigkeit des gesamten Beschlusses.

Nach alledem ist festzustellen, dass der DSS-Beschluss ungültig ist.

Wirkungen des Privacy Shields sind nicht aufrechtzuerhalten

Zudem stellte der EuGH klar, dass die Wirkungen des Privacy Shield-Beschlusses nicht aufrechtzuerhalten seien. Dies sei zur Vermeidung einer Regelungslücke nicht notwendig, denn Art. 49 DSGVO regle, unter welchen Voraussetzungen personenbezogene Daten in Drittländer übermittelt werden können, falls weder ein Angemessenheitsbeschluss noch geeignete Garantien nach Art. 46 DSGVO vorliegen.

Zu der Frage, ob die Wirkungen dieses Beschlusses aufrechtzuerhalten sind, um die Entstehung eines rechtlichen Vakuums zu vermeiden (vgl. in diesem Sinne Urteil vom 28. April 2016, Borealis Polyolefine u. a., C-191/14, C-192/14, C-295/14, C-389/14 und C-391/14 bis C-393/14, EU:C:2016:311, Rn. 106), ist festzustellen, dass in Anbetracht von Art. 49 der DSGVO durch die Nichtigerklärung eines Angemessenheitsbeschlusses wie des DSS-Beschlusses jedenfalls kein solches rechtliches Vakuum entstehen kann. In dieser Vorschrift ist nämlich klar geregelt, unter welchen Voraussetzungen personenbezogene Daten in Drittländer übermittelt werden können, falls weder ein Angemessenheitsbeschluss nach Art. 45 Abs. 3 der DSGVO vorliegt noch geeignete Garantien im Sinne ihres Art. 46 bestehen.

Fazit

Durch das Urteil des EuGH entsteht eine große Rechtsunsicherheit, wenn eine Übermittlung personenbezogener Daten in die USA stattfindet.

Für eine solche Übermittlung bestehen nun insbesondere folgende Möglichkeiten: Zur Übermittlung von Daten in Drittstaaten können Standarddatenschutzklauseln verwendet verwenden. Der EuGH hat mit seinem Urteil gleichzeitig festgestellt, dass der entsprechende Beschluss 2010/87 der Kommission wirksame Mechanismen vorsieht, die in der Praxis gewährleisten können, dass das vom Unionsrecht verlangte Schutzniveau eingehalten wird. Nach diesem Beschluss müssen der Datenexporteur und der Empfänger der Übermittlung vorab prüfen, ob das erforderliche Schutzniveau im betreffenden Drittland eingehalten wird. Zudem muss der Empfänger dem Datenexporteur gegebenenfalls mitteilen, dass er die Standardschutzklauseln nicht einhalten kann. In diesem Fall muss der Exporteur die Datenübermittlung aussetzen und/oder vom Vertrag mit dem Empfänger zurücktreten.

Eine andere Möglichkeit ist eine Übermittlung unter den Voraussetzungen des Art. 49 DSGVO. Dort ist festgelegt, unter welchen Bedingungen eine Übermittlung personenbezogener Daten an ein Drittland zulässig ist, falls weder ein Angemessenheitsbeschluss vorliegt noch geeignete Garantien bestehen. In Betracht kommt hier insbesondere die Einwilligung der betroffenen Person. Problematisch wird bei dieser Möglichkeit jedoch sein, dass die betroffene Person zuvor über die für sie bestehenden möglichen Risiken einer solchen Datenübermittlung unterrichtet werden muss.

Die Europäische Kommission ist nun gefragt, schnell für Rechtssicherheit zu sorgen.

Marian Weyo/Shutterstock.com