Europäischer Datenschutzausschuss zu Schrems II

Übersetzung bearbeitet von Rechtsanwalt David Seiler: www.ds-law.eu
https://edpb.europa.eu

FAQ - Häufig gestellte Fragen zum Urteil des Gerichtshofs der Europäischen Union in der Rechtssache C-311/18 - Datenschutzbeauftragter gegen Facebook Ireland Ltd und Maximillian Schrems

Angenommen am 23. Juli 2020
https://edpb.europa.eu/sites/edpb/files/files/file1/20200724_edpb_faqoncjeuc31118.pdf

Dieses Dokument zielt darauf ab, Antworten auf einige häufig gestellte Fragen zu geben, die bei den Aufsichtsbehörden ("Aufsichtsbehörden") eingegangen sind, und wird zusammen mit weiteren Analysen weiterentwickelt und ergänzt werden, während das EDPB weiterhin das Urteil des Gerichtshofs der Europäischen Union ("Gerichtshof") prüft und bewertet.

Das Urteil C-311/18 finden Sie hier, und die Pressemitteilung des Gerichtshofs finden Sie hier.

1) Wie hat der Gerichtshof in seinem Urteil entschieden?

In seinem Urteil prüfte der Gerichtshof die Gültigkeit der Entscheidung 2010/87/EG der Europäischen Kommission über **Standardvertragsklauseln ("SCC")** und hielt sie für gültig. In der Tat wird die Gültigkeit dieser Entscheidung nicht durch die bloße Tatsache in Frage gestellt, dass die Standarddatenschutzklauseln in dieser Entscheidung die Behörden des Drittlandes, in das Daten übermittelt werden können, nicht binden, da sie vertraglicher Natur sind.

Diese Gültigkeit hänge jedoch davon ab, ob der Beschluss 2010/87/EG wirksame Mechanismen enthalte, die es in der Praxis ermöglichten, die Einhaltung eines Schutzniveaus zu gewährleisten, das dem in der EU durch das DSGVO garantierten Schutzniveau im Wesentlichen gleichwertig sei, und dass die Übermittlung personenbezogener Daten aufgrund dieser Klauseln ausgesetzt oder verboten werde, wenn diese Klauseln verletzt würden oder nicht eingehalten werden könnten.

In diesem Zusammenhang weist der Gerichtshof insbesondere darauf hin, dass der Beschluss 2010/87/EG dem Datenexporteur und dem Empfänger der Daten (dem "Datenimporteur") die Verpflichtung auferlegt, vor jeder Übermittlung und unter Berücksichtigung der Umstände der Übermittlung zu prüfen, ob dieses Schutzniveau in dem betreffenden Drittland eingehalten wird, und dass der Beschluss 2010/87/EG **den Datenimporteur verpflichtet, den Datenexporteur über die Unfähigkeit zu informieren, die Standarddatenschutzklauseln und erforderlichenfalls zusätzliche Maßnahmen zu den durch diese Klauseln gebotenen zu erfüllen,** wobei **der Datenexporteur dann seinerseits verpflichtet ist, die Datenübermittlung auszusetzen und/oder den Vertrag mit dem Datenimporteur zu kündigen.**[1]
Der Gerichtshof prüfte auch die Gültigkeit der Entscheidung über den Privacy Shield (Beschluss 2016/1250 über die Angemessenheit des Schutzes durch den Privacy Shield der EU und der USA), da die Transfers, um die es im Rahmen des nationalen Rechtsstreits ging, der zum Vorabentscheidungsersuchen führte, zwischen der EU und den Vereinigten Staaten ("USA") stattfanden.
Der Gerichtshof vertrat die Auffassung, dass die Anforderungen des innerstaatlichen Rechts der Vereinigten Staaten und insbesondere bestimmte Programme, die den Zugriff von US-Behörden auf personenbezogene Daten ermöglichen, die aus der EU in die Vereinigten Staaten für Zwecke der

nationalen Sicherheit übermittelt werden, zu Einschränkungen des Schutzes personenbezogener Daten führen, die nicht in einer Weise abgegrenzt sind, die Anforderungen erfüllt, die im Wesentlichen denen des EU-Rechts gleichwertig sind[1], und dass diese Rechtsvorschriften den betroffenen Personen keine vor den Gerichten gegen die US-Behörden einklagbaren Rechte einräumen.

Als Folge eines solchen Grades der Beeinträchtigung der Grundrechte von Personen, deren Daten in dieses Drittland übermittelt werden, erklärte das Gericht die Entscheidung über die Angemessenheit des Datenschutzschildes für ungültig.

2) Hat das Urteil des Gerichts Auswirkungen auf andere Übertragungsinstrumente als den Datenschutzschild?

Im Allgemeinen gilt der vom Gerichtshof festgelegte Schwellenwert für Drittländer auch für alle geeigneten Schutzmaßnahmen nach Artikel 46 DSGVO, die für die Übermittlung von Daten aus dem EWR in ein Drittland verwendet werden. **Das US-Recht, auf das sich der Gerichtshof bezieht** (d.h. Abschnitt 702 FISA und EO 12333), **gilt für jede Übertragung in die USA auf elektronischem Wege,** die in den Anwendungsbereich dieser Gesetzgebung fällt, unabhängig von dem für die Übertragung verwendeten Übertragungsinstrument[2].

3) Gibt es eine Karenzzeit, während der ich weiterhin Daten in die USA übermitteln kann, ohne meine rechtliche Grundlage für die Übermittlung zu prüfen?

Nein, der Gerichtshof hat die Entscheidung über den Schutz der Privatsphäre für ungültig erklärt, ohne ihre Wirkungen aufrechtzuerhalten, weil das vom Gerichtshof beurteilte US-Recht kein im Wesentlichen gleichwertiges Schutzniveau wie die EU bietet. Diese Beurteilung muss bei jeder Übertragung in die USA berücksichtigt werden.

4) Ich habe Daten an einen US-Datenimporteur übermittelt, der sich an den Privacy Shield-Entscheid hält, was soll ich jetzt tun?

Übermittlungen auf der Grundlage dieses Rechtsrahmens sind illegal. Sollten Sie weiterhin Daten in die USA übermitteln wollen, müssten Sie prüfen, ob Sie dies unter den unten aufgeführten Bedingungen tun können.

5) Ich verwende Standardvertragsklauseln (SCCs) mit einem Datenimporteur in den USA, was soll ich tun?

Das Gericht stellte fest, dass das US-Recht (d.h. Abschnitt 702 FISA und EO 12333) kein im Wesentlichen gleichwertiges Schutzniveau gewährleistet.

Ob Sie personenbezogene Daten auf der Grundlage von SCCs übermitteln können, hängt vom Ergebnis Ihrer Beurteilung ab, wobei die Umstände der Übermittlung und zusätzliche Maßnahmen, die Sie ergreifen könnten, zu berücksichtigen sind. Die ergänzenden Massnahmen zusammen mit den SCCs müssten nach einer Einzelfallanalyse der Umstände der Übermittlung sicherstellen, dass das US-Recht das angemessene Schutzniveau, das sie garantieren, nicht beeinträchtigt.

Wenn Sie zu dem Schluss kommen, dass unter Berücksichtigung der Umstände der Übermittlung und möglicher ergänzender Maßnahmen keine angemessenen Schutzmaßnahmen gewährleistet wären, **sind Sie verpflichtet, die Übermittlung personenbezogener Daten auszusetzen oder zu beenden.**

Beabsichtigen Sie jedoch trotz dieser Schlussfolgerung weiterhin Daten zu übermitteln, müssen Sie Ihre zuständige Aufsichtsbehörde[3] benachrichtigen.

6) Ich verwende Verbindliche Unternehmensregeln – Binding Corporate Rules ("BCR") mit einem Unternehmen in den USA, was soll ich tun?

In Anbetracht des Urteils des Gerichtshofs, das den Privacy Shield wegen des Grades an Eingriff des US-Rechts in die Grundrechte von Personen, deren Daten in dieses Drittland übermittelt werden, für ungültig erklärte, und der Tatsache, dass der Privacy Shield auch Garantien für Daten bieten sollte, die mit anderen Instrumenten wie den BCR übermittelt werden, **gilt die Beurteilung des Gerichtshofs auch im Zusammenhang mit den BCR**, da das US-Recht auch diesem Instrument gegenüber Vorrang haben wird.

Ob Sie personenbezogene Daten auf der Grundlage der BCR übermitteln können oder nicht, hängt vom Ergebnis Ihrer Beurteilung ab, wobei die Umstände der Datenübermittlung und zusätzliche Maßnahmen, die Sie ergreifen könnten, zu berücksichtigen sind. Diese ergänzenden Maßnahmen müssten zusammen mit den BCR nach einer Einzelfallanalyse der Umstände der Übermittlung sicherstellen, dass das US-Recht das angemessene Schutzniveau, das sie garantieren, nicht beeinträchtigt.

Wenn Sie zu dem Schluss kommen, dass unter Berücksichtigung der Umstände der Übermittlung und möglicher ergänzender Maßnahmen keine angemessenen Schutzmaßnahmen gewährleistet wären, sind Sie verpflichtet, die Übermittlung personenbezogener Daten auszusetzen oder zu beenden. Beabsichtigen Sie jedoch trotz dieser Schlussfolgerung weiterhin Daten zu übermitteln, müssen Sie Ihre zuständige Aufsichtsbehörde[4] benachrichtigen.

7) Wie steht es mit anderen Übermittlungsinstrumenten nach Artikel 46 DSGVO?

Das **EDPB (European Data Protection Bord = Europäischer Datenschutzausschuss)** wird die Auswirkungen des Urteils auf andere Übermittlungsinstrumente als SCC und BCR beurteilen. Das Urteil stellt klar, dass der Maßstab für angemessene Schutzvorkehrungen in Artikel 46 DSGVO der der "wesentlichen Gleichwertigkeit" ist.

Wie der Gerichtshof betont, ist darauf hinzuweisen, dass Artikel 46 in Kapitel V DSGVO erscheint und dementsprechend im Lichte von Artikel 44 DSGVO zu lesen ist, der festlegt, dass "alle Bestimmungen dieses Kapitels anzuwenden sind, um sicherzustellen, dass das durch diese Verordnung garantierte Schutzniveau für natürliche Personen nicht untergraben wird".

8) Kann ich mich auf eine der Ausnahmeregelungen von Artikel 49 DSGVO berufen, um Daten in die USA zu übermitteln?

Es ist immer noch möglich, Daten aus dem EWR in die USA auf der Grundlage der in Artikel 49 DSGVO vorgesehenen Ausnahmeregelungen zu übertragen, sofern die in diesem Artikel festgelegten Bedingungen zutreffen. Das EDPB verweist auf seine Leitlinien zu dieser Bestimmung[5].
Insbesondere sollte daran erinnert werden, dass, wenn Übertragungen auf der Zustimmung der betroffenen Person beruhen, folgende Merkmale erfüllt sein sollte:

- ausdrückliche Einwilligung,

- spezifisch für die bestimmte Datenübermittlung oder eine Reihe von Übermittlungen (was bedeutet, dass der Datenexporteur sicherstellen muss, dass er eine spezifische Zustimmung einholt, bevor die Übermittlung durchgeführt wird, auch wenn dies nach der Erfassung der Daten geschieht), und
- **informiert, insbesondere über die möglichen Risiken der Übermittlung** (d.h. die betroffene Person sollte auch über die spezifischen Risiken informiert werden, die sich aus der Tatsache ergeben, dass ihre Daten in ein Land übermittelt werden, das keinen angemessenen Schutz bietet, und dass keine angemessenen Garantien zum Schutz der Daten umgesetzt werden).

In Bezug auf Übermittlungen, die für die **Erfüllung eines Vertrags** zwischen der betroffenen Person und dem für die Verarbeitung Verantwortlichen erforderlich sind, ist zu bedenken, dass personenbezogene Daten nur dann übermittelt werden dürfen, wenn die Übermittlung nur gelegentlich erfolgt. Es müsste von Fall zu Fall festgelegt werden, ob Datenübermittlungen als "gelegentlich" oder "nicht gelegentlich" bestimmt werden. In jedem Fall kann diese Ausnahmeregelung nur dann geltend gemacht werden, wenn die Übermittlung objektiv für die Vertragserfüllung erforderlich ist.

In Bezug auf Datenübermittlungen, die **aus wichtigen Gründen des öffentlichen Interesses** erforderlich sind (die im Recht der EU oder der Mitgliedstaaten anerkannt werden müssen[6]), erinnert der EDPB daran, dass die wesentliche Voraussetzung für die Anwendbarkeit dieser Ausnahmeregelung die Feststellung eines wichtigen öffentlichen Interesses und nicht die Art der Organisation ist, und dass diese Ausnahmeregelung zwar nicht auf "gelegentliche" Datenübermittlungen beschränkt ist, dies jedoch nicht bedeutet, dass Datenübermittlungen aufgrund der wichtigen Ausnahmeregelung des öffentlichen Interesses in großem Umfang und systematisch erfolgen können. Vielmehr muss der allgemeine Grundsatz beachtet werden, wonach die Ausnahmeregelungen nach Artikel 49 DSGVO der Praxis nicht zur "Regel" werden dürfen, sondern auf bestimmte Situationen beschränkt werden müssen, und jeder Datenexporteur muss sicherstellen, dass die Übermittlung der strengen Notwendigkeitsprüfung entspricht.

9) Kann ich weiterhin SCCs oder BCRs verwenden, um Daten in ein anderes Drittland als die USA zu übermitteln?

Der Gerichtshof hat darauf hingewiesen, dass die SCC in der Regel weiterhin für die Übermittlung von Daten in ein Drittland verwendet werden können, wobei jedoch der vom Gerichtshof für die Übermittlung in die USA festgelegte Schwellenwert für jedes Drittland gilt. Dasselbe gilt für die BCR.

Das Gericht betonte, dass es dem Datenexporteur und dem Datenimporteur obliegt, zu beurteilen, ob das vom EU-Recht geforderte Schutzniveau in dem betreffenden Drittland eingehalten wird, um festzustellen, ob die von den SCC oder den BCR gebotenen Garantien in der Praxis eingehalten werden können. Ist dies nicht der Fall, sollten Sie prüfen, ob Sie zusätzliche Maßnahmen ergreifen können, um ein im Wesentlichen gleichwertiges Schutzniveau wie im EWR (EWR = Europäischer Wirtschaftsraum = EU + Island, Lichtenstein und Norwegen) zu gewährleisten, und ob das Recht des Drittlandes diese zusätzlichen Maßnahmen nicht beeinträchtigt, um ihre Wirksamkeit zu verhindern.

Sie können sich mit Ihrem Datenimporteur in Verbindung setzen, um die Gesetzgebung seines Landes zu überprüfen und bei der Beurteilung mitzuwirken. Sollten Sie oder der Datenimporteur im Drittland feststellen, dass die Daten, die gemäß den SCC oder den BCR übermittelt werden, nicht über ein Schutzniveau verfügen, das im Wesentlichen dem innerhalb des EWR garantierten Schutzniveau entspricht, sollten Sie die Übermittlungen unverzüglich aussetzen. Falls Sie dies nicht tun, müssen Sie Ihre zuständige Datenschutzaufsichtsbehörde benachrichtigen.

Obwohl es, wie der Gerichtshof betont, in erster Linie Aufgabe der Datenexporteure und Datenimporteure ist, selbst zu beurteilen, ob die Rechtsvorschriften des Bestimmungsdrittlands es dem Datenimporteur ermöglichen, die Standarddatenschutzklauseln oder die BCR einzuhalten, kommt den internationalen Kontroll- und Überwachungsgesellschaften vor der Übermittlung personenbezogener Daten in dieses Drittland auch eine Schlüsselrolle bei der Durchsetzung der DSGVO und beim Erlass weiterer Entscheidungen über Übermittlungen in Drittländer zu.

Um abweichende Entscheidungen zu vermeiden, werden sie daher, wie vom Gerichtshof gefordert, innerhalb des EDPB weiterarbeiten, um die Kohärenz zu gewährleisten, insbesondere wenn Übermittlungen in Drittländer verboten werden müssen.

10) Welche Art von zusätzlichen Maßnahmen kann ich einführen, wenn ich SCC oder BCR zur Übermittlung von Daten in Drittländer verwende?

Die ergänzenden Maßnahmen, die Sie sich gegebenenfalls vorstellen könnten, müssten von Fall zu Fall unter Berücksichtigung aller Umstände der Übermittlung und nach Beurteilung des Rechts des Drittlandes vorgesehen werden, um zu prüfen, ob es ein angemessenes Schutzniveau gewährleistet.

Der Gerichtshof hob hervor, dass es in erster Linie in der Verantwortung des Datenexporteurs und des Datenimporteurs liegt, diese Beurteilung vorzunehmen und die erforderlichen ergänzenden Maßnahmen zu treffen.

Der EDPB analysiert derzeit das Urteil des Gerichtshofs, um festzustellen, welche Art von ergänzenden Maßnahmen zusätzlich zu den SCC oder BCR vorgesehen werden könnten, seien es rechtliche, technische oder organisatorische Maßnahmen, um Daten in Drittländer zu übermitteln, in denen die SCC oder BCR allein nicht das ausreichende Maß an Garantien bieten.

Das EDPB untersucht weiter, worin diese ergänzenden Maßnahmen bestehen könnten, und wird weitere Hinweise geben.

11) Ich benutze einen Auftragsverarbeiter, der Daten verarbeitet, für die ich als für die Verarbeitung Verantwortlicher verantwortlich bin; wie kann ich wissen, ob dieser Auftragsverarbeiter Daten in die USA oder in ein anderes Drittland überträgt?

In dem Vertrag, den Sie mit Ihrem Auftragsverarbeiter gemäss Artikel 28 Abs. 3 DSGVO abgeschlossen haben, muss angegeben werden, ob Übermittlungen zulässig sind oder nicht (es ist zu bedenken, dass auch die Gewährung des Zugriffs auf Daten aus einem Drittland, z.B. für Verwaltungszwecke, einer Übermittlung gleichkommt).

Auch für Auftragsverarbeiter, die Unterauftragsverarbeiter mit der Übermittlung von Daten in Drittländer beauftragen, muss eine Genehmigung erteilt werden. Sie sollten aufpassen und vorsichtig sein, denn eine Vielzahl von EDV-Lösungen kann die Übertragung von personenbezogenen Daten in ein Drittland implizieren (z.B. zu Speicher- oder Wartungszwecken).

12) Was kann ich tun, um die Dienste meines Auftragsverarbeiters weiterhin in Anspruch zu nehmen, wenn aus dem gemäß Artikel 28 Abs. 3 DSGVO unterzeichneten Vertrag hervorgeht, dass Daten in die USA oder in ein anderes Drittland übermittelt werden können?

Wenn Ihre Daten in die USA übertragen werden dürfen und weder zusätzliche Maßnahmen vorgesehen werden können, um sicherzustellen, dass das US-Recht nicht das im Wesentlichen gleichwertige Schutzniveau, wie es im EWR durch die Übertragungsinstrumente geboten wird, beeinträchtigt, noch Ausnahmeregelungen nach Artikel 49 DSGVO gelten, besteht die einzige Lösung darin, eine Änderungs- oder Ergänzungsklausel zu Ihrem Vertrag auszuhandeln, um Übertragungen in die USA zu verbieten.

Wenn Ihre Daten möglicherweise in ein anderes Drittland übertragen werden, sollten Sie auch die Gesetzgebung dieses Drittlandes überprüfen, um zu prüfen, ob sie mit den Anforderungen des Europäischen Gerichtshofs und mit dem erwarteten Schutzniveau für personenbezogene Daten in Einklang steht. Wenn kein geeigneter Grund für eine Übertragung in ein Drittland gefunden werden kann, sollten personenbezogene Daten nicht außerhalb des EWR-Gebiets übertragen werden, und alle Verarbeitungsaktivitäten sollten im EWR-Gebitet stattfinden.

Für den Europäischen Datenschutzausschuss
Die Vorsitzende
Andrea Jelinek

Endnoten

1 Der Gerichtshof betont, dass bestimmte Überwachungsprogramme, die den Zugang von US-Behörden zu personenbezogenen Daten ermöglichen, die aus der EU in die USA zu Zwecken der nationalen Sicherheit übermittelt werden, keine Beschränkungen der den US-Behörden übertragenen Befugnisse oder Garantien für potenziell betroffene Nicht-US-Personen vorsehen.

2 Abschnitt 702FISA gilt für alle "Anbieter von elektronischen Kommunikationsdiensten" (siehe die Definition unter 50USC§ 1881(b)(4)), während EO 12 333 die elektronische Überwachung organisiert, die definiert ist als "Erwerb einer nicht öffentlichen Kommunikation mit elektronischen Mitteln ohne die Zustimmung einer Person, die Partei einer elektronischen Kommunikation ist oder, im Falle einer nicht-elektronischen Kommunikation ohne die Zustimmung einer Person, die am Ort der Kommunikation sichtbar anwesend ist, jedoch ohne die Verwendung von Funkpeilgeräten, die nur dazu dienen, den Standort eines Senders zu bestimmen" (3. 4; b)).

3 Siehe insbesondere Erwägungsgrund 145 des Urteils des Gerichtshofs und Paragraf 4(g) des Beschlusses 2010/87/EU der Kommission sowie Paragraph 5(a) des Beschlusses 2001/497/EG der Kommission und Anhang Satz II(c) des Beschlusses 2004/915/EG der Kommission.

4 Siehe insbesondere Erwägungsgrund 145 des Urteils des Gerichtshofs und Paragraf 4 Buchstabe g des Beschlusses 2010/87/EU der Kommission. Siehe auch Abschnitt 6.3 WP256 rev.01 (Artikel-29-Datenschutzgruppe, Arbeitsdokument zur Erstellung einer Tabelle mit den Elementen und Grundsätzen der BCR, gebilligt vom EDPB, http://ec.europa.eu/newsroom/article29/item- detail.cfm?item_id=614109) und Abschnitt 6.3 WP257 rev.01 (Artikel-29-Datenschutzgruppe, Arbeitsdokument zur Erstellung einer Tabelle mit den Elementen und Grundsätzen der BCR für Verarbeiter, gebilligt vom EDPB, http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614110).

5 Siehe EDPB-Leitlinien 2/2018 zu Ausnahmeregelungen zu Artikel 49 gemäß Verordnung 2016/679, angenommen am 25. Mai 2018, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf S.3.

6 Bezugnahmen auf "Mitgliedstaaten" sind als Bezugnahmen auf "EWR-Mitgliedstaaten" zu verstehen.

7 Siehe insbesondere Randnummer 145 des Urteils des Gerichtshofs. In Bezug auf SCCs siehe Paragraph 4(g) des Beschlusses 2010/87/EU der Kommission sowie Paragraph 5(a) des Beschlusses 2001/497/EG der Kommission und Anhang Set II(c) des Beschlusses 2004/915/EG der Kommission. In Bezug auf die BCR siehe Abschnitt 6.3 WP256 rev.01 (vom EDPB gebilligt) und Abschnitt 6.3 WP257 rev.01 (vom EDPB gebilligt).