Urteil des EuGH zu grenzüberschreitenden Datenübermittlungen aus der EU in Drittländer – was nun?

Daniela Fábián Masoch, Lucas Maciejewski

3. August 2020

Am 16. Juli 2020 verkündete der Gerichtshof der Europäischen Union (EuGH) sein Urteil in der Rechtssache C-311/18 — *Data Protection Commissioner v. Facebook Irland und Maximillian Schrems* (Schrems II). In diesem Fall ersuchte M. Schrems die Kommission, die Übermittlung seiner personenbezogenen Daten durch Facebook Irland an die in den USA ansässige Facebook Inc. zu verbieten oder auszusetzen, mit der Begründung, dass dieses Drittland kein angemessenes Schutzniveau gewährleiste. Dieses Urteil hat weitreichende Konsequenzen für jegliche Datenübermittlung aus der EU in Drittländer.

Die Ergebnisse der Entscheidung des EuGH

1. Privacy Shield

Der EuGH hob den Beschluss 2016/1250 der Europäischen Kommission über die Übermittlung personenbezogener Daten in die USA (Privacy Shield) mit sofortiger Wirkung auf. Der Grund für diese Entscheidung liegt im Kern darin, dass das US-Recht (insbesondere Abschnitt 702 Foreign Intelligence Surveillance Act (FISA) und die Executive Order 12333) gemäss der Einschätzung des EuGH kein angemessenes Schutzniveau bietet, das dem in der EU im Wesentlichen gleichwertig ist (in Bezug auf angemessene Schutzvorkehrungen, durchsetzbare Rechte und wirksame Rechtsbehelfe, die gemäss DSGVO erforderlich sind).

In der Schweiz hat der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) das Urteil des EuGH zur Kenntnis genommen. Das Urteil ist nicht direkt auf die Schweiz und damit nicht auf den CH-US Privacy Shield anwendbar. Der EDÖB wird das Urteil im Detail prüfen und zu gegebener Zeit dazu Stellung nehmen. Während der CH-US-Privacy Shield derzeit noch gültig ist, ist zu erwarten, dass die Behörde dem EuGH-Urteil folgen und auch den CH-US-Privacy Shield für ungültig erklären wird (wie sie es auch 2015 nach der Ungültigerklärung der Safe-Harbor-Vereinbarung getan hat).

2. Standardvertragsklauseln (SCC)

Der EuGH bestätigte die prinzipielle Gültigkeit des Kommissionsbeschlusses 2010/87/EG über Standardvertragsklauseln (SCC), betonte jedoch die Verantwortung des Datenexporteurs und des Datenimporteurs für die Durchführung einer Einzelfallanalyse des innerstaatlichen Rechts des Datenimporteurs, insbesondere in Bezug auf den Zugang von Behörden und Rechtsbehelfe, um festzustellen, ob die Rechte der betroffenen Personen im Drittland ein angemessenes Schutzniveau geniessen, das dem in der Union gleichwertig ist. Ist dies nicht der Fall, muss der Datenexporteur zusätzliche wirksame Schutzmassnahmen ergreifen oder die betreffende Datenübermittlung aussetzen. Solche zusätzlichen Schutzmassnahmen können technische Massnahmen wie die Verschlüsselung der Daten im Transit und im Ruhezustand, vertragliche Absicherungen oder organisatorische Massnahmen umfassen. Der EuGH legt jedoch nicht fest, welche Art von zusätzlichen Schutzmassnahmen ergriffen werden sollen, und lässt somit die Unternehmen in Ungewissheit. Weitere Leitlinien werden in naher Zukunft erwartet.

Die vom EuGH hervorgehobenen Verpflichtungen sind nicht neu. Sie sind sowohl in den «Controller to Processor SCC» als auch in den «Controller to Controller SCC» bereits enthalten. Der EuGH appelliert an die bestehenden Verpflichtungen von Unternehmen, die personenbezogene Daten auf der Grundlage der SCC aus der EU in ein Drittland ohne Angemessenheitsentscheid der EU-Kommission exportieren bzw. importieren, und betont, dass die reine Unterzeichnung der SCC nicht ausreicht, sondern dass die Parteien im Einzelfall prüfen müssen, ob die SCC im Empfängerland eingehalten werden können.

Die Entscheidung des EuGH betrifft im Prinzip die «Controller to Processor SCC». Dieselben Argumente gelten jedoch auch für die Übermittlung personenbezogener Daten aus der EU in ein Drittland auf der Grundlage der «Controller to Controller SCC» oder verbindlicher interner Datenschutzvorschriften (Binding Corporate Rules, BCR).

Unternehmen, die diese Analyse nicht durchführen und gegebenenfalls personenbezogene Daten auf der Grundlage von SCC in ein Drittland übermitteln, in dem der Datenempfänger aufgrund dem EU-Recht nicht gleichwertiger lokaler Gesetzgebung nicht in der Lage ist, die SCC effektiv einzuhalten, verstossen gegen die Anforderungen der DSGVO (selbst wenn die SCC unterzeichnet wurden) und riskieren somit hohe Geldstrafen von bis zu EUR 20'000'000 oder 4% des Jahresumsatzes des vorangehenden Geschäftsjahres, je nachdem, welcher der Beträge höher ist. Zudem können solche Datenübermittlungen von den zuständigen Aufsichtsbehörden verboten oder ausgesetzt werden

Relevante Klauseln in den aktuellen SCC

Controller to Processor SCC vom 5. Februar 2010 (2010/87/EU)

Klausel 4 (a): Der Datenexporteur erklärt sich bereit und garantiert, dass die Verarbeitung der personenbezogenen Daten einschließlich der Übermittlung entsprechend den einschlägigen Bestimmungen des anwendbaren Datenschutzrechts durchgeführt wurde und auch weiterhin so durchgeführt wird (...) und nicht gegen die einschlägigen Vorschriften dieses Staates verstößt.

Klausel 5: Der Datenimporteur erklärt sich bereit und garantiert, dass:

(a): er die personenbezogenen Daten nur im Auftrag des Datenexporteurs und in Übereinstimmung mit dessen Anweisungen und den vorliegenden Klauseln verarbeitet; dass er sich, falls er dies aus irgendwelchen Gründen nicht einhalten kann, bereit erklärt, den Datenexporteur unverzüglich davon in Kenntnis zu setzen, der unter diesen Umständen berechtigt ist, die Datenübermittlung auszusetzen und/oder vom Vertrag zurückzutreten;

b): er seines Wissens keinen Gesetzen unterliegt, die ihm die Befolgung der Anweisungen des Datenexporteurs und die Einhaltung seiner vertraglichen Pflichten unmöglich machen, und eine Gesetzesänderung, die sich voraussichtlich sehr nachteilig auf die Garantien und Pflichten auswirkt, die die Klauseln bieten sollen, dem Datenexporteur mitteilen wird, sobald er von einer solchen Änderung Kenntnis erhält; unter diesen Umständen ist der Datenexporteur berechtigt, die Datenübermittlung auszusetzen und/oder vom Vertrag zurückzutreten;

Controller to Controller SCC vom 27. Dezember 2004 (2004/915/EG)

Klausel I (b): Der Datenexporteur gibt folgende Zusicherungen: Er hat sich im Rahmen des Zumutbaren davon überzeugt, dass der Datenimporteur seine Rechtspflichten aus diesen Klauseln zu erfüllen in der Lage ist.

Klausel II (c): Der Datenimporteur gibt folgende Zusicherungen: Zum Zeitpunkt des Vertragsabschlusses bestehen seines Wissens in seinem Land keine entgegenstehenden Rechtsvorschriften, die die Garantien aus diesen Klauseln in gravierender Weise beeinträchtigen; er benachrichtigt den Datenexporteur (der die Benachrichtigung erforderlichenfalls an die Kontrollstelle weiterleitet), wenn er Kenntnis von derartigen Rechtsvorschriften erlangt.

Reaktionen der Datenschutzbehörden

Inzwischen haben mehrere Datenschutzbehörden sowie der Europäische Datenschutzbeauftragte (Stellungnahme vom 17. Juli 2020), der Europäische Datenschutzausschuss (EDSA) (Stellungnahme vom 17. Juli 2020) und die Deutsche Datenschutzkonferenz (DSK) (Pressemitteilung vom 28. Juli 2020) erste Leitlinien für den künftigen Umgang mit Datenübermittlungen herausgegeben. Auf der Website der IAPP ist eine Übersicht aller bisher veröffentlichten Leitlinien mit Links zu den entsprechenden Dokumenten veröffentlicht.

Einige Datenschutzbehörden wie die deutschen Datenschutzbehörden in Berlin (Pressemitteilung vom 17. Juli 2020) und Hamburg (Pressemitteilung vom 16. Juli 2020) haben rigorose Erklärungen zur Rechtswidrigkeit von Datenübermittlungen auf der Grundlage der SCC in die USA abgegeben. Die Berliner Datenschutzbehörde fordert gar sämtliche ihrer Aufsicht unterstehenden Verantwortlichen auf, Daten nicht mehr in die USA zu übermitteln, sondern umgehend zu Dienstleistern mit Sitz in der EU oder einem anderen Drittland mit einem angemessenen Schutzniveau zu wechseln.

Der EDSA hat zusätzlich zu seiner Erklärung FAQ herausgegeben. Weitere Leitlinien, insbesondere hinsichtlich der zusätzlich zu ergreifenden Schutzmassnahmen, werden erwartet.

Was Unternehmen tun können

Es ist zu erwarten, dass der EDSA, die EU-Kommission und die Aufsichtsbehörden weitere Leitlinien zu den «zusätzlichen Schutzmassnahmen» bereitstellen und dass die EU-Kommission überarbeitete SCC herausgibt. Datenexporteure und -importeure sollten jedoch bereits Massnahmen in Betracht ziehen, um ein angemessenes Schutzniveau bei der Übermittlung personenbezogener Daten aus der EU in Drittländer zu gewährleisten:

1. Verfolgung der weiteren Entwicklung und insbesondere der vom EDSA, der EU-Kommission und Aufsichtsbehörden herausgegebenen Leitlinien und die Herausgabe überarbeiteter SCC.
2. Ermittlung und Dokumentation aller grenzüberschreitenden Datenübermittlungen innerhalb der Unternehmensgruppe sowie an Dienstleister und andere Geschäftspartner mit Sitz ausserhalb der EU/CH:
    a. Wenn personenbezogene Daten auf der Grundlage des EU-US Privacy Shield grenzüberschreitend übermittelt werden, sollten alternative rechtliche Mechanismen bestimmt werden, um solche Übermittlungen nach der DSGVO zu ermöglichen (z.B. SCC unter den vom EuGH festgelegten Bedingungen oder eine der rechtlichen Ausnahmeregelungen nach Art. 49 DSGVO). Verträge sollten entsprechend angepasst werden. Zudem sollte ein Plan erstellt werden, der alle Schritte, Verantwortlichkeiten und Fristen festlegt, einschliesslich der allfälligen Kündigung des EU-US Privacy Shield unter Beachtung der entsprechenden Benachrichtigungspflichten.
    b. Wenn personenbezogene Daten auf der Grundlage der SCC (einschliesslich konzerninterner Datenübermittlungsvereinbarungen) grenzüberschreitend übermittelt werden, sollte der Datenexporteur gemeinsam mit dem Datenimporteur prüfen, ob die Rechtsvorschriften des Empfängerlands einen angemessenen Schutz der im Rahmen der SCC übermittelten personenbezogenen Daten nach EU-Recht gewährleisten. Insbesondere sollte geprüft werden, ob der Datenimporteur Gesetzen und Praktiken unterliegt, die den Datenzugriff durch öffentliche Behörden erlauben (wie z.B. nach Art. 702 FISA in den USA), und der Datenimporteur daher möglicherweise nicht in der Lage ist, den SCC nachzukommen. In diesem Fall sollte der Datenexporteur eine Datenschutz-Risikoeinschätzung durchführen, um die Wahrscheinlichkeit einer Offenlegung der Daten oder eines Zugriffs auf die Daten, die Datensensibilität, das Datenvolumen und die Aufbewahrungsfristen zu beurteilen, sowie zusätzliche, über die SCC hinausgehende Schutzmassnahmen in Betracht ziehen, wie beispielsweise vertragliche und technische Massnahmen wie Datenverschlüsselung im Transit und im Ruhezustand. Wenn solche zusätzlichen Massnahmen nicht möglich sind, sollte der Datenexporteur die Übermittlung personenbezogener Daten aussetzen oder beenden oder die zuständige Aufsichtsbehörde benachrichtigen, die jede weitere Datenübermittlung verbieten kann.
    c. Wenn die Übertragung auf BCR beruht, sollte die gleiche Analyse wie bei den SCC durchgeführt werden.
    d. Wenn die Übermittlung auf einer der gesetzlichen Ausnahmeregelungen gemäss Art. 49 DSGVO beruht, wie z.B. die ausdrückliche Einwilligung oder die Erforderlichkeit zur Erfüllung eines Vertrags, sind vorerst keine weiteren Schritte erforderlich.
3. Die Analyse, das Ergebnis und alle unternommenen Schritte sollten ausführlich dokumentiert werden.
4. Überprüfung und Anpassung von Due-Diligence-Prozessen und Vertragsvorlagen:
    a. Um eine angemessene Konformitäts- und Risikobewertung durchführen zu können, sollte der Due-Diligence-Prozess und der Fragebogen zur datenschutzrechtlichen Bewertung von Dienstleistern überarbeitet und mit Fragen über die Existenz von Gesetzen und Praktiken zur Überwachung und zum Datenzugriff, denen der Datenimporteur unterliegt, ergänzt werden. Besondere Aufmerksamkeit sollte auch den internen Regeln und Verfahren des Datenimporteurs hinsichtlich der Behandlung von Anträgen von Behörden und der Benachrichtigung des Datenexporteurs gewidmet werden. Zudem sollten in Zukunft alle Datenimporteure, d.h. nicht nur Auftragsdatenverarbeiter, sondern auch Verantwortliche, evaluiert werden.
    b. Die Vertragsvorlagen sollten bezüglich der grenzüberschreitenden Datentransfers überarbeitet werden, um die primären Verpflichtungen des Datenexporteurs/-importeurs aus den SCC sowie die Behandlung von Anträgen der Behörden auf Zugang zu personenbezogenen Daten hervorzuheben. Zudem sollte jeglicher Verweis auf das Privacy Shield Framework gelöscht werden.

5. Dienstleistungsanbieter (Datenimporteure) können ihre Kunden unterstützen, indem sie die lokalen Gesetze gründlich analysieren, um die Angemessenheit des Schutzniveaus in Bezug auf die EU-Gesetze zu überprüfen und die Einhaltung der SCC zu gewährleisten. Ein solches Vorgehen kann auch dazu beitragen, die Wettbewerbsfähigkeit zu erhalten.
6. Einführung (oder Überarbeitung) interner Richtlinien und Verfahren, um grenzüberschreitende Datenübermittlungen im Einklang mit der DSGVO und dem Urteil des EuGH zu regeln.
7. Langfristig können Unternehmen erwägen, auf robustere Datentransfermechanismen umzusteigen, wie sie in Art. 46 DSGVO vorgesehen sind, z.B. von den EU-Aufsichtsbehörden genehmigte BCR (für Auftragsdatenverarbeiter und Verantwortliche), Verhaltenskodex oder Zertifizierungsmechanismen.