Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

Stand: 25.08.2020

Orientierungshilfe: Was jetzt in Sachen internationaler Datentransfer?

Der LfDI gibt Hinweise und legt sein weiteres Vorgehen zum Urteil des Europäischen Gerichtshofs (EuGH) vom 16. Juli 2020, Rechtssache C-311/18 („Schrems II“) fest

I. Worum geht`s?

Hintergrund:

Ein Rechtsstreit zwischen einer Privatperson (Maximilian Schrems) und der irischen Aufsichtsbehörde über die Übermittlung seiner personenbezogenen Daten durch Facebook Irland zum Mutterkonzern von Facebook in die USA

Kernaussagen:

1. ***Die Datenschutz-Grundverordnung (DS-GVO)*** *findet auf die Übermittlung personenbezogener Daten in ein Drittland auch in solchen Fällen* ***Anwendung,*** *in denen es aus Gründen der nationalen Sicherheit oder Verteidigung zu einem Zugriff durch Geheimdienste dieses Landes kommt.*

   Die Ausnahmen des Art. 2 Abs. 2 a, b, d der DS-GVO gelten nur für die Mitgliedstaaten.

2. ***Das sog. „Privacy Shield“****, ein Angemessenheitsbeschluss der Kommission nach Art. 45 DS-GVO (2016/1250 vom 12.07.2016, noch zur Datenschutz-Richtlinie 95/46/EC), mit dem diese 2016 beschlossen hatte, dass die USA unter bestimmten Umständen ein angemessenes Schutzniveau für die Daten natürlicher Personen bieten und so die Übermittlung von Daten in die USA allgemein ermöglicht hatte,* ***ist ab sofort ungültig.***

Aufgrund der Befugnisse der US-Geheimdienste und der Rechtslage in den USA kann ein angemessenes Datenschutz-Niveau nicht sichergestellt werden (u.a.):

- Section 702 des Foreign Intelligence Surveillance Act (FISA) sieht keine Beschränkungen der Überwachungsmaßnahmen der Geheimdienste und keine Garantien für Nicht-US-Bürger vor
- Presidential Policy Directive 28 (PPD-28) gibt Betroffenen keine wirksamen Rechtsbehelfe gegen Maßnahmen der US-Behörden und sieht keine Schranken für die Sicherstellung verhältnismäßiger Maßnahmen vor
- der im Privacy Shield vorgesehene Ombudsmann hat keine genügende Unabhängigkeit von der Exekutive; er kann keine bindenden Anordnungen gegenüber den Geheimdiensten treffen

3. ***Die von der Kommission im Jahr 2010 beschlossenen Standardvertragsklauseln*** *(2010/87/EU vom 05.02.2010), Art. 46 Abs. 2 c* DS-GVO, **sind weiterhin gültig.**
   Aber:
   Es muss ein Schutzniveau für die personenbezogenen Daten sichergestellt sein, das dem in der Europäischen Union entspricht*.*
   - auszulegen im Lichte der EU-Grundrechte-Charta und im Hinblick auf Art. 46 Abs. 1 DS-GVO: geeignete Garantien vom Verantwortlichen und Auftragsverarbeiter, durchsetzbare Rechte und wirksame Rechtsbehelfe für die betroffenen Personen
   - Hier sind also nicht nur die vertraglichen Beziehungen zwischen Datenexporteur und Datenimporteur relevant, sondern auch die Zugriffsmöglichkeit auf die Daten durch Behörden des Drittlandes und das Rechtssystem dieses Landes insgesamt (Gesetzgebung und Rechtsprechung, Verwaltungspraxis von Behörden)

Die Standardvertragsklauseln können allerdings die Behörden des Drittlandes nicht binden und stellen daher in den Fällen, in denen die Behörden nach dem Recht des Drittlandes befugt sind, in die Rechte

der betroffenen Personen einzugreifen <u>ohne zusätzliche Maßnahmen der Vertragspartner</u> keinen angemessenen Schutz dar.

Der Verantwortliche muss für den Einzelfall prüfen, ob das Recht des Drittlandes ein angemessenes Schutzniveau bietet und entsprechende zusätzliche Maßnahmen treffen bzw. mit dem Datenimporteur vereinbaren

- wo der Verantwortliche auch mit zusätzlichen Maßnahmen keinen geeigneten Schutz vorsehen kann, muss er den Transfer aussetzen/beenden
- das gilt insbesondere, wenn das Recht des Drittlandes dem Datenimporteur Verpflichtungen auferlegt, die geeignet sind, vertraglichen Regeln, die einen geeigneten Schutz gegen den Zugriff durch staatliche Behörden vorsehen, zuwider zu laufen

4. *Ist ein solches angemessenes Schutzniveau nicht sichergestellt,* ***muss die Aufsichtsbehörde für den Datenschutz die Datenübermittlung aussetzen oder verbieten****, wenn der Schutz nicht durch andere Maßnahmen hergestellt werden kann*.

II. Wen betrifft die Entscheidung?

Zwar entfaltet das Urteil des EuGH zunächst nur inter partes-Wirkung, ist also erst einmal nur für das vorlegende irische Gericht bindend. **Faktisch** entfaltet es aber bereits jetzt **Bindungswirkung für alle Behörden und Gerichte der Mitgliedstaaten,** die sich mit derselben Auslegungsfrage beschäftigen und die DS-GVO unter Berücksichtigung der Rechtsprechung des EuGH auslegen und anwenden müssen.

Erklärt der EuGH einen Gemeinschaftsrechtsakt (wie das **Privacy Shield**) für ungültig, sind daran alle Gerichte und Behörden in allen Mitgliedstaaten

gebunden und demnach auch **alle** dem EU-Recht unterworfenen **Unternehmen** (erga omnes-Wirkung).

Insofern betrifft die Entscheidung alle öffentlichen Stellen oder Unternehmen, die Daten in die USA transferieren, insbesondere, wenn sie die Übermittlung dabei bisher auf das Privacy Shield gestützt haben, aber auch, wenn sie dafür Standardvertragsklauseln genutzt haben (wie genau, dazu sogleich)**.**

Beispiele (nicht abschließend):

- Sie stehen in Handelsbeziehung mit Unternehmen, die einen Sitz in den USA haben und tauschen mit diesen personenbezogene Daten über Kunden (Lieferadressen, Beschwerden, Bestellungen etc.) oder Ihre Beschäftigten (Verträge, Netzwerke, etc.) aus.
- Sie speichern Daten in einer Cloud, die von einem Unternehmen in den USA außerhalb der EU gehostet wird.
- Sie nutzen ein Videokonferenzsystem eines US-amerikanischen Anbieters, der Daten der Teilnehmenden erhebt und in die USA übermittelt.

Gleichzeitig enthält das Urteil allgemeine Aussagen zur Nutzung von Standardvertragsklauseln für eine Übermittlung von Daten in Drittländer, sodass **auch alle öffentlichen Stellen oder Unternehmen, die Daten nicht in die USA, sondern <u>in ein anderes Drittland übermitteln</u>, von der Entscheidung betroffen sind.**

Bsp.: Sie übermitteln Daten in das Vereinigte Königreich.

Die Auswirkungen der Gerichtsentscheidung sind daher **denkbar umfassend**.

III. Was bedeutet die Entscheidung konkret?/ Was ist zu tun?

1.) Wenn Sie Daten in die USA übermitteln oder sich eines Auftragsverarbeiters bedienen, der Daten in die USA übermittelt:

⇒ das **Privacy Shield** stellt **keine gültige Rechtsgrundlage** für die Übermittlung mehr dar, **trotzdem durchgeführte Datentransfers sind rechtswidrig und können Bußgelder und Schadensersatzforderungen nach sich ziehen**

⇒ **eine Übermittlung auf Grundlage von Standardvertragsklauseln ist zwar denkbar,** wird die Anforderungen, die der EuGH an ein wirksames Schutzniveau gestellt hat, **jedoch nur in seltenen Fällen erfüllen**:

Der Verantwortliche muss hier **zusätzliche Garantien** bieten, die einen Zugriff durch die US-amerikanischen Geheimdienste effektiv verhindern und so die Rechte der betroffenen Personen schützen; dies wäre in folgenden Fällen denkbar:

- **Verschlüsselung, bei der nur der Datenexporteur den Schlüssel hat und die auch von US-Diensten nicht gebrochen werden kann**
- **Anonymisierung oder Pseudonymisierung, bei der nur der Datenexporteur die Zuordnung vornehmen kann**

⇒ eine **Übermittlung nach Art. 49 DS-GVO ist denkbar**; jedoch ist hier der **insgesamt restriktive Charakter dieser Vorschrift** zu beachten, vgl. dazu auch die Leitlinien 2/2018 zu den Ausnahmen nach Artikel 49 der Verordnung 2016/679 des Europäischen Datenschutzausschusses (EDSA) vom 25.05.2018, abrufbar unter https://edpb.europa.eu/our-work-tools/our-documents/smjernice/guidelines-22018-derogations-article-49-under-regulation_de :

- Wortlaut des Titels „Ausnahmen für bestimmte Fälle“: **Ausnahmecharakter von Artikel 49** als Abweichung vom Regelverbot der Übermittlung in Drittstaaten bei Nichtvorliegen eines angemessenen Datenschutzniveaus
- für Art. 49 Abs. 1 UAbs. 1 b, c und e DS-GVO (für Vertrag oder zur Geltendmachung von Rechtsansprüchen erforderlich) zusätzlich: **Wortlaut EG 111: „gelegentlich“** erfolgende Datenübermittlungen, nicht systematisch wiederholend

- **noch restriktiver: Art. 49 Abs. 1 UAbs. 2** für Fälle, in denen keine Ausnahme für bestimmte Fälle vorliegt (Übermittlung nicht wiederholt, nur eine begrenzte Zahl von betroffenen Personen, erforderlich für die Wahrung der zwingenden berechtigten Interessen des Verantwortlichen, kein Überwiegen des Interesses oder der Rechte und Freiheiten der betroffenen Person)
- **für Behörden** gelten zudem gem. Art. 49 Abs. 3 DS-GVO die Art. 49 Abs. 1 UAbs. 1 a, b und c sowie UAbs. 2 nicht bei Ausübung ihrer hoheitlichen Befugnisse

2.) Wenn Sie Daten in ein anderes Drittland übermitteln:
Hier sollten Sie die Rechtslage in dem genannten Land überprüfen, insbesondere hinsichtlich der Zugriffsmöglichkeiten des Geheimdienstes und der dem Betroffenen zustehenden Rechte und Rechtsschutzmöglichkeiten und auch hier die unter IV. genannten Ergänzungen der Garantien der Standardvertragsklauseln aufnehmen

IV. Wo und wie anfangen?/ Checkliste

Sie sollten jetzt unverzüglich

- ✓ eine **Bestandsaufnahme** machen, in welchen Fällen Ihr Unternehmen/Ihre Behörde personenbezogene Daten in Drittländer exportiert;
  darunter können auch Zugriffsmöglichkeiten von privaten oder öffentlichen Stellen in Drittstaaten auf bei Ihnen vorgehaltene Daten zählen, ein physischer Export der Daten ist also nicht erforderlich.

- ✓ **sich mit Ihrem Dienstleister/Vertragspartner im Drittland in Verbindung setzen** und ihn über die Entscheidung des EuGH und deren Konsequenzen informieren

- ✓ **sich über die Rechtslage im Drittland informieren** (öffentliche Stellen wie die Datenschutz-Aufsichtsbehörden, der Europ. Datenschutz-

Ausschuss (EDSA), die EU-Kommission oder das Auswärtige Amt sollten dazu Hilfestellungen geben können)

- ✓ **überprüfen, ob es für das Drittland einen Angemessenheitsbeschluss nach Art. 45 DS-GVO gibt**
  Für die USA wurde dieser nun für ungültig erklärt, aber für Argentinien, Kanada, Japan, Neuseeland oder die Schweiz besteht diese Möglichkeit z.B. noch, s. eine ausführliche Liste hier: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en :ggfls. können Sie sich auch auf verbindliche interne Datenschutzvorschriften gemäß Artikel 47 (BCRs) berufen

- ✓ **überprüfen, ob Sie die von der Kommission beschlossenen Standardvertragsklauseln für das jeweilige Land nutzen können (Art. 46 Abs. 2c DS-GVO)** – diese sind abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32010D0087**.**

  Dies ist zu verneinen, wenn Behörden oder sonstige Stellen des Drittlandes in unverhältnismäßiger Art und Weise in die Rechte der betroffenen Personen eingreifen können (z.B. ein massenhafter Abruf von Daten ohne Information der Betroffenen und ohne verfahrensrechtliche Sicherungen wie einen Richtervorbehalt) und es keinen wirksamen Rechtsschutz für die Betroffenen gibt.

  Für die USA wurde dies vom EuGH verneint. Eine Übermittlung von Daten mithilfe der Standardvertragsklauseln ist in die USA daher nur in eng begrenzten Fällen mithilfe zusätzlicher Garantien (z.B. Verschlüsselung, s.o. und sogleich) möglich.

- ✓ überprüfen, ob Sie die Daten mithilfe der **Standardvertragsklauseln und zusätzlicher Garantien** in das jeweilige Land übertragen können,

Dies beinhaltet insbesondere die Überlegung, ob Sie die Übertragung bzw. den Zugriff durch andere relativ vermeiden können
(Verschlüsselung, Vereinbarung, dass die Daten innerhalb des

Geltungsbereichs der DS-GVO gehostet werden oder dass keine Datenübertragung in die USA vorgenommen wird)

Um Ihren Willen zu einem rechtskonformen Handeln zu demonstrieren und zu dokumentieren, sollten Sie zudem **Kontakt mit dem jeweiligen Empfänger der Daten aufnehmen** und sich insbesondere über folgende **Änderung der Bestimmungen der Standardvertragsklauseln verständigen:**

- **Abänderung Anhang Klausel 4f:** Information der betroffenen Person nicht nur bei der Übermittlung besonderer Datenkategorien, sondern bei jeglicher Datenübermittlung (vor oder so bald wie möglich nach der Übermittlung), dass ihre Daten in ein Drittland übermittelt werden, das kein angemessenes Schutzniveau im Sinne der Verordnung (EU) 2016/679 bietet
- **Abänderung Anhang Klausel 5d i:** Pflicht des Datenimporteurs, nicht nur den Datenexporteur, sondern auch die betroffene Person unverzüglich zu informieren über alle rechtlich bindenden Aufforderungen einer Vollstreckungsbehörde zur Weitergabe der personenbezogenen Daten; ist diese Informationsweitergabe anderweitig untersagt, beispielsweise durch ein strafrechtliches Verbot zur Wahrung des Untersuchungsgeheimnisses bei strafrechtlichen Ermittlungen, müssen Sie sich mit der Aufsichtsbehörde LfDI in Verbindung setzen und das weitere Vorgehen abklären
- **Ergänzung von Anhang Klausel 5 d** um die Verpflichtung des Datenimporteurs, den Rechtsweg gegen eine Weitergabe von personenbezogenen Daten zu beschreiten und die Offenlegung der personenbezogenen Daten gegenüber den jeweiligen Behörden zu unterlassen, bis er von einem zuständigen Gericht letztinstanzlich zur Offenlegung rechtskräftig verurteilt wurde
- **Abänderung von Anhang Klausel 7 Abs. 1, nur Aufnahme von b):** Befassung der Gerichte des Mitgliedstaats, in dem der Datenexporteur sich niedergelassen hat, mit dem Streitfall, für den Fall, dass eine betroffene Person gegenüber dem Datenimporteur

Rechte als Drittbegünstigte und/oder Schadenersatzansprüche aufgrund der Vertragsklauseln geltend macht

- **Aufnahme des in Anhang 2 genannten Beispiels für eine Entschädigungsklausel:**

Haftung

Die Parteien erklären sich damit einverstanden, dass, wenn eine Partei für einen Verstoß gegen die Klauseln haftbar gemacht wird, den die andere Partei begangen hat, die zweite Partei der ersten Partei alle Kosten, Schäden, Ausgaben und Verluste, die der ersten Partei entstanden sind, in dem Umfang ersetzt, in dem die zweite Partei haftbar ist.

Die Entschädigung ist abhängig davon, dass

a) der Datenexporteur den Datenimporteur unverzüglich von einem Schadenersatzanspruch in Kenntnis setzt und

b) der Datenimporteur die Möglichkeit hat, mit dem Datenexporteur bei der Verteidigung in der Schadenersatzsache bzw. der Einigung über die Höhe des Schadenersatzes zusammenzuarbeiten.

Wenn nach diesen Prüfschritten die Datenübermittlung nicht zulässig wäre, bleibt als letztes Mittel die Übermittlung von Daten nach der Ausnahmevorschrift des Art. 49 DS-GVO.

Dies kann insbesondere in Betracht kommen bei Datenübermittlungen im Konzern oder bei Einzelvertragsbeziehungen. Hier wäre zu prüfen, ob der restriktive Charakter der Norm der Übermittlung nicht entgegensteht.

Im Zentrum des weiteren Vorgehens des LfDI Baden-Württemberg wird die Frage stehen, ob es neben dem von Ihnen gewählten Dienstleister/Vertragspartner nicht **auch zumutbare Alternativangebote ohne Transferproblematik** gibt. Wenn Sie uns nicht davon überzeugen können, dass der von Ihnen genutzte Dienstleister/Vertragspartner mit Transferproblematik kurz- und mittelfristig unersetzlich ist durch einen zumutbaren Dienstleister/Vertragspartner ohne Transferproblematik, dann wird der Datentransfer vom LfDI Baden-Württemberg **untersagt** werden.

Uns ist bewusst, dass mit dem Urteil des EuGH u.U. extreme Belastungen für einzelne Unternehmen einhergehen können. Der LfDI wird sein weiteres Vorgehen

am Grundsatz der Verhältnismäßigkeit ausrichten. Wir werden die Entwicklung weiter beobachten und unsere Positionen dementsprechend laufend überprüfen und fortentwickeln.