



RA Hon. Prof Dr. Clemens Thiele • Salzburg

Ist der Datentransfer in die USA am Ende? – Zur Unzulässigerklärung des EU Privacy Shield – Analyse der Entscheidung EuGH 16. 7. 2020, C-311/18 mit Praxistipps

» jusIT 2020/70

✦ EU-US-Datenschutzschild; Standardvertragsklauseln; Ombudsmechanismus; Datenschutzrecht, EU; USA; Privacy Shield; Datenübermittlung; Drittstaat; Facebook; Drittlandübermittlung; Übermittlung; Schrems II-Fall; Datenschutz, angemessener; Angemessenheit; Schutzniveau, angemessenes, keines; Kontrollstelle, nationale; Befugnisse; Rechtsschutz; Überwachungsmechanismus; Kontrollmechanismus; US-Geheimdienste

§ GRC: Art 7, 8, 45 ff; VO (EU) 2016/679: Art 46 Abs 3 lit a, Art 47, 49; Beschluss (EU) 2016/1250 der Kommission; Beschluss 2010/87 der EU-Kommission

Der EU-US Privacy Shield genügt nicht den Vorgaben der DSGVO und ist ungültig. Ein transatlantischer Datentransfer auf Basis von Standardvertragsklauseln bleibt hingegen zulässig. Der Beitrag erörtert das EuGH-Urteil *Schrems II* und seine Folgen für die Datenschutzpraxis.

1. Verfahrensgang

Nachdem auf Initiative des österreichischen Datenschutzaktivisten *Mag. Maximilian Schrems* hin das sogenannte „Safe-Harbor-Abkommen“ 2000/520/EG der Kommission für ungültig erklärt¹ und durch das sogenannte „Privacy Shield“ (EU) 2016/1250 ersetzt worden war, stützte Facebook die Datenübermittlung nicht (nur) auf den Privacy Shield der Kommission, sondern auf die im Beschluss zu den Standardvertragsklauseln 2010/87/EU enthaltenen Klauseln.

Der weiterhin in der Klägerrolle tätige *Schrems* forderte daraufhin von der zuständigen irischen Datenschutzbehörde (*Data Protection Commissioner Ireland*) ein Übermittlungsverbot. Denn Facebook Inc. war und ist im Rahmen verschiedener Überwachungsprogramme zur massenhaften Weiterübermittlung etwa an NSA und FBI ohne mit Art 7, 8 und 47 GRC vergleichbarem Schutz verpflichtet. Im gegen den DPC Ireland notwendigen Gerichtsverfahren legte der High Court Ireland die Sache (neuerlich)

dem EuGH vor. Das irische Gericht verwies auf Erkenntnisse aus einem anderen Verfahren, nach denen für die Überwachungsprogramme PRISM bzw. UPSTREAM der Zugriff auf Inhalts- und Verkehrsdaten außerhalb des Hoheitsgebiets sich aufhaltender Nicht-US-Staatsbürger auf Section 702 des Foreign Intelligence Surveillance Act (iF: FISA 702) gestützt würde. Den nicht dem FISA unterliegenden Zugriff der NSA auf Datenströme über Seekabel außerhalb des US-Hoheitsgebiets erlaube das Präsidialdekret E.O. 12333 ohne jede gerichtliche Kontrolle. Letztlich hatte der EuGH im Vorlageweg über die Zulässigkeit des internationalen Datenexports in die USA und über die Gültigkeit des Privacy Shield zu entscheiden.

2. Die Entscheidung der Großen Kammer

Das über 200 Randzahlen umfassende Urteil gelangt zur klaren Aussage: In den USA besteht entgegen der Feststellung der EU-Kommission in ihrem vorbehaltlos nichtigen Privacy-Shield-Beschluss kein angemessenes Datenschutzniveau. Dessen Gewährleistung ggf durch Standardvertragsklauseln ist vom verantwortlichen Datenexporteur nachzuweisen bzw letztlich von der Aufsichtsbehörde kritisch zu prüfen. Die Große Kammer hat vereinfacht festgehalten, dass die Überwachung durch amerikanische Behörden im Prinzip uferlos sei, weshalb die Daten von UnionsbürgerInnen in den USA nicht ausreichend geschützt wären. Auch bestehe für UnionsbürgerInnen kein angemessener Rechtsschutz gegen die Überwachung durch amerikanische Nachrichtendienste.

Im Ergebnis erklärt der EuGH den Durchführungsbeschluss (EU) 2016/1250 der Kommission vom 12. 7. 2016 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes für ungültig.

¹ EuGH 6. 10. 2015, C-362/14 (*Schrems*), AnwBl 2015, 586 (*Steinbrecher*) = ARD 6473/5/2015 (*Vogt-Majarek/Spring*) = ecolex 2015, 1117 ([*Leissler/Wolffbauer*] =) *Dako* 2015/60, 115 (*Schrems*) = JB Datenschutzrecht 2015, 9 (*Kunnert*) = *juridikum* 2015, 412 (*Kettemann*) = *jusIT* 2015/95, 234 (*Jahnel*) = MR-Int 2015, 79 (*Orantek*) = ÖJZ 2015/144, 1125 (*Berger/Maderbacher*) = RdW 2015/591, 691 (*Retter/Marko*) = SWK 2015, 1470 (*Gruber*) = ecolex 2016, 115 (*Pachinger*) = JAP 2016/2017/4, 31 (*Radlgruber*) = JB Öffentliches Recht 2016, 209 (*Kunnert*) = RdW 2016/347, 460 (*Gruber*).

Der Beschluss 2010/87 der EU-Kommission über Standardvertragsklauseln ist hingegen gültig. Dabei aber – und auch das stellten die Luxemburger RichterInnen klar – garantiert die Verwendung der Klauseln nicht automatisch die Rechtmäßigkeit der Datenübermittlung in das Zielland. Das festzustellen unterliegt auch der Kontrolle derjenigen, die Daten in die USA übermitteln, und nachprüfend den Datenschutzbehörden.

3. Das Wesentliche in Kurzform

3.1. Zum Schutzniveau bei Angemessenheitsprüfung

Das EU-Höchstgericht hat bereits in der Rs *Tele2 Sverige und Watson ua* ausgesprochen, dass die Befugnisse der nationalen Behörden im Bereich der nationalen Sicherheit im Rahmen der Prüfung sowohl für die Vertragsklauseln als auch für den Privacy Shield zu beachten und an Art 7 und 8 GRC zu messen sind.² Die Datenweitergabe stellt unabhängig von der späteren Datenverwendung einen Grundrechtseingriff dar. Das löst das Erfordernis einer verhältnismäßigen und den Kern der Privatsphäre bzw des Kommunikationsgeheimnisses wahren den gesetzlichen Befugnis nach Art 8 Abs 2 iVm Art 52 Abs 1 Satz 2 GRC aus. Der auf das absolut Notwendige beschränkte Umfang des Eingriffs muss gesetzlich klar und präzise festgelegt sein. Erforderliche Garantien gegen Missbrauchsgefahren sind umso bedeutsamer bei automatisierter Datenverarbeitung. Art 45 Abs 2 lit a DSGVO macht dazu deutlich, dass bei der Drittlandübermittlung Betroffenenrechte wirksam durchsetzbar bleiben müssen.

3.2. Verhältnismäßigkeitsprüfung

In Prüfung der Verhältnismäßigkeit befand die Große Kammer, dass Section 702 FISA keine Einschränkungen der Überwachungsprogramme oder Garantien für Nicht-US-Personen zulässt. Dies hatte bereits die EU-Kommission in ErwGr 109 zu ihrem Privacy-Shield-Beschluss vermerkt. Ebenso mangelte es gegenüber den amerikanischen Behörden an gerichtlich durchsetzbaren Rechten für Unionsbürger (gegenteilig noch ErwGr 67 und 77 Privacy-Shield-Beschluss). Im Ergebnis bestehen in den USA keine zu Art 52 Abs 1 GRC gleichwertigen Verhältnisse.

3.3. Kein gleichwertiger Rechtsschutz

Auch die Gleichwertigkeit des Rechtsschutzes verneinte die Große Kammer eindeutig. Es fehle an wirksamen Rechtsbehelfen iSv Art 45 Abs 2 lit a DSGVO (vgl auch ErwGr 104 DSGVO). Entgegen ErwGr 115 und 116 Privacy-Shield-Beschluss gewährleiste auch die nach dem Privacy-Shield vorgesehene Ombudsperson keinen gleichwertigen Rechtsschutz. Da sie dem US-Außenministerium untersteht und nicht zu verbindlichen Entscheidungen

gegenüber den Nachrichtendiensten berechtigt ist, fehlt die von Art 47 Abs 1, Abs 2 GRC geforderte Gleichwertigkeit.

4. Tipps für die Praxis

Eine Datenübermittlung wie etwa für Google Analytics, Microsoft 365 oder Amazon Web Services lässt sich seit dem 16. 7. 2020 (und streng genommen auch davor) nicht mehr auf den Privacy Shield stützen. Entsprechende Datenschutzerklärungen sind jetzt anzupassen. Den Defiziten bei Verhältnismäßigkeit und Rechtsschutz aufgrund zwingenden US-Rechts kann mangels Gestaltungsspielraums nicht durch bloße privatrechtliche Regelung der Übermittlung begegnet werden. Dies gilt entsprechend für Binding Corporate Rules nach Art 47 DSGVO. Daher wird der High Court Ireland im Ausgangsverfahren bei unveränderter US-Rechtslage wohl ein Übermittlungsverbot bejahen.

Anders als vor fünf Jahren nach der Safe-Harbor-Entscheidung hat der EDSA bereits am 24. 7. 2020 bekannt gegeben, dass Datenverarbeitungen auf der Grundlage des ungültigen Privacy Shield unverzüglich, dh ohne „Gnadenfrist“ von wenigen Monaten, umzustellen sind.³

Für die Beratungspraxis ist Folgendes zu beachten: Besteht kein vergleichbares Datenschutzniveau und lässt es sich gegen zwingendes Recht des Drittstaats auch nicht privatrechtlich herstellen, verweist der EuGH in der vorliegenden Entscheidung für die Übermittlung auf Art 49 DSGVO. Die dort vorgesehenen Ausnahmefälle zur Drittstaatenübermittlung (zB ausdrückliche Einwilligung, Vertragserfüllung, Wahrung von Rechtsansprüchen usw) sind jedoch eng auszulegen und kaum auf regelmäßige Transfers anwendbar.⁴ Insb sind im Fall der ausdrücklichen Einwilligung umfassende Risikoaufklärung, Erforderlichkeit (vgl Koppelungsverbot nach Art 7 Abs 4 DSGVO) und die Freiwilligkeit zu erfüllen (vgl ErwGr 43 DSGVO). An Letzterem kann es nicht nur beim Behördenkontakt oder Beschäftigungsverhältnis fehlen, sondern auch im Fall einer marktbeherrschenden Stellung im Software- oder Social Media-Bereich.

Es ist daher dringend zu empfehlen, eine Datenübermittlung an US-ansässige Unternehmen, US-Server sowie Anbieter mit US-Bezug zu vermeiden oder lediglich noch unter besonderen Begleitmaßnahmen zu tolerieren.

Zu berücksichtigen ist zudem, dass Standardvertragsklauseln, die von der Europäischen Kommission erlassen wurden und in denen die datenschutzrechtlichen Pflichten der beteiligten Unternehmen festgelegt werden, nicht jede Drittlandübermittlung rechtfertigen können. Bei der Nutzung von Standardvertragsklauseln hat nämlich das datenübermittelnde Unternehmen eigenständig im Einzelfall zu beurteilen, ob das Schutzniveau der DSGVO im Drittland eingehalten werden kann. Für

² So bereits EuGH 21. 12. 2016, C-203/15, C-698/15 (*Tele2 Sverige und Watson ua*), *jusIT* 2017/10, 31 (*Jahnel*) = *ÖJZ* 2017/37, 281 (*Lehofer*); EuGH 2. 10. 2018, C-207/16 (*Ministerio Fiscal*), *ZfIR* 2019, 59 (*Seiser*).

³ EDSA, FAQ zu EuGH C-311/18, abrufbar unter https://edpb.europa.eu/sites/edpb/files/files/file1/20200724_edpb_faqoncjec31118_en.pdf (8. 9. 2020).

⁴ Deutlich EDSA 25. 5. 2018, Leitlinien 2/2018; zutr *Denk*, Entscheidungsanmerkung, *ZfIR* 2020, 315 (325).

die USA wurde dieser Rechtsrahmen bereits durch den EuGH beurteilt. Die Gründe, die zur Aufhebung des EU-US Privacy Shield geführt haben, sind dieselben, die gegen die Zulässigkeit der Datenübermittlung auf Basis von Standardvertragsklauseln sprechen. Dies gilt insb für jene US-Empfänger, die den einschlägigen sicherheitsbehördlichen und geheimdienstlichen Befugnisgesetzen (ua FISA 702) unterliegen, die den Sicherheitsbehörden ohne richterlichen Beschluss Zugriff auf die Daten gewähren. Unter FISA 702 fallen jedenfalls US-Unternehmen, die ein Telekommunikationsunternehmen betreiben. Dies gilt auch für US-Anbieter, die solche lediglich in Anspruch nehmen. UU könnten sogar auch EU-/EWR-Anbieter darunterfallen, sofern ein US-Bezug gegeben ist.

Kurz zusammengefasst bedeutet dies, dass kaum Fälle denkbar sind, in denen die USA einen DSGVO-konformen Rechtsrahmen bieten. Somit sind Standardvertragsklauseln idR auch kein Ausweg, um personenbezogene Daten in die USA zu übermitteln.

Demzufolge appellieren aufmerksame Rechtsanwender an Verantwortliche, folgende Maßnahmen bei Drittlandübermittlungen, insb in die USA, zu ergreifen:

- Prüfen Sie, ob und in welchem Rahmen personenbezogene Daten in die USA (zB an US-Anbieter oder Anbieter mit US-Bezug, wie Amazon, Mail Chimp, Microsoft, Apple, Google, WhatsApp, Instagram, Facebook, Dropbox, Cloudflare, Verizon) übermittelt werden.
- Gruppieren Sie die Datenverarbeitungen nach der Rechtsgrundlage für die Datenübermittlung:
 - *EU-US Privacy Shield*: Für diese Datenübermittlung ist dringend eine andere Rechtsgrundlage zu finden.
 - *Standardvertragsklauseln*: Prüfen Sie, ob der Empfänger oder einer seiner Dienstleister den sicherheitsbehördlichen und geheimdienstlichen Befugnisgesetzen (FISA 702) unterliegt. Ist dies der Fall, sind Datenübermittlungen nicht auf diese Rechtsgrundlage zu stützen.
 - *Bei bloß gelegentlich und nicht wiederholter Drittlandübermittlung*: Prüfen Sie, ob eine der Ausnahmen gem Art 49 DSGVO vorliegt.
 - *Bei nicht bloß gelegentlicher Übermittlung*: Die Datenübermittlung kann uU – auch wenn der Europäische Datenschutzausschuss anderer Ansicht ist – auf eine der Ausnahmen in Art 49 DSGVO gestützt werden, da der EuGH explizit auf diese besondere Ausnahme hinweist. Diese Rechtfertigung birgt allerdings dennoch ein hohes Risiko für den Verantwortlichen.

- Ist kein Rechtfertigungsgrund für die Drittlandübermittlung vorhanden, ist die Übermittlung dringend auszusetzen und nach alternativen Anbietern in der EU bzw im EWR (ohne US-Bezug) zu suchen. Ansonsten ist alternativ vom Verantwortlichen zu beurteilen, ob das Risiko einer datenschutzrechtlichen Sanktionierung durch die Datenschutzbehörde eingegangen werden will. Diese Vorgehensweise ist jedoch keinesfalls zu begrüßen.

5. Fazit

Zusammenfassend lässt sich die komplexe Entscheidung des EuGH zum EU-US Privacy Shield als ebenso erfolglosem Nachfolgemodell zum Safe Harbor Principle wie folgt charakterisieren: Eine Datenübermittlung an Drittländer per Standardvertragsklauseln ist zulässig, aber nach dem EU-US Privacy Shield ungültig. Inhalt des Abkommens ist, dass in der EU ansässige Unternehmen personenbezogene Daten an ihre Geschäftspartner in den USA übermitteln dürfen. In dem konkreten Fall ging es um die Weitergabe von personenbezogenen Daten durch die Facebook Ireland Ltd an die in den USA ansässige Facebook Inc. Die Beratungspraxis ist jetzt mehr gefragt denn je.



Der Autor:

RA Hon.-Prof. Dr. **Clemens Thiele**, LL.M. Tax (GGU) studierte US-amerikanisches Steuerrecht in San Francisco; Gründer der RA-Kanzlei EUROLAWYER® in Salzburg; Fachbuch-Autor; gerichtlich beeideter Sachverständiger für Urheberfragen aller Art, insb Neue Medien und Webdesign.

Publikationen des Autors:

Standardkommentar zum RATG³ (2011); gemeinsam mit Elisabeth Staudegger Mitherausgeber des Jahrbuchs Geistiges Eigentum 2012 bis 2019; Co-Autor in Kotschy (Hrsg), RdW Spezial: DSGVO (2019) zum wirklichen Rechtsschutz für Betroffene im zivilen Klagsweg; zahlreiche Beiträge in Fachzeitschriften zu Themen des Informationsrechts.

✉ Anwalt.Thiele@eurolawyer.at
<http://www.eurolawyer.at>

🌐 lesen.lexisnexis.at/autor/Thiele/Clemens

Foto: D. Wild



Alle Infos für Ihre Beratung

Coronavirus: Laufende Updates, alle rechtlichen Infos & Analysen



Lexis.at/corona-infopoint

