Empfehlung nach EuGH Schrems II (EU-US Privacy Shield)

Der **Europäische Gerichtshof** hat am 16. Juli 2020 mit dem Urteil Urteil EuGH C-311/18[1] das **„EU-US-Privacy-Shield“ für unwirksam erklärt**. Das Urteil kennt keine Übergangsfrist und ist in der Begründung so gestaltet, dass es keinen weiteren Spielraum für politische Verzögerungstaktik (wie 2015 nach EuGH Schrems I zur damals aufgehobenen Vorgängerregelung „Safe Harbor“ Abkommen) zulässt. Der Gerichtshof legt mit diesem Urteil ausdrücklich an mehreren Stellen die **Artikel 7 und 8 EU-Grundrechte-Charta** aus, das sind die Grundrechte auf Privatsphäre und Datenschutz. Diese Bestimmungen sind Teil des sog. Primärrechts der EU, der EuGH hat damit auch klare **Schranken für den Unions-Gesetzgeber** formuliert. Was lange ein politisches Gezerre war ist nun durch den EuGH zu Recht geworden. Der daraus entstehende „digitale Handelskonflikt“ zwischen den USA und der EU hat natürlich weiterhin eine politische Dimension, **EU-Unternehmen sind aber nun im Handlungszwang**.

In seinem Urteil prüfte das Gericht auch die **Gültigkeit** der Entscheidung 2010/87/EG der Europäischen Kommission über Standardvertragsklauseln (**Standard Contractual Clauses, "SCC"**) und **hielt diese für gültig**. Allerdings 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 unter Berücksichtigung der Umstände der Übermittlung **zu prüfen, ob dieses Schutzniveau in dem betreffenden Drittland eingehalten wird**, und dass der **Datenimporteur verpflichtet** ist, den Datenexporteur **über die Unfähigkeit zu informieren, die Standarddatenschutzklauseln** und erforderlichenfalls zusätzliche Maßnahmen zu den durch diese Klauseln gebotenen **zu erfüllen.** Der Datenexporteur ist dann seinerseits verpflichtet, die Datenübermittlung auszusetzen und/oder den Vertrag mit dem Datenimporteur zu kündigen.

Die **Zulässigkeit der Übermittlung** personenbezogener Daten in die USA **auf der Basis von SCC hängt vom Ergebnis der Beurteilung im Einzelfall** ab, wobei die Umstände der Übermittlung und zusätzliche Maßnahmen, die Sie ergreifen könnten, zu berücksichtigen sind. Die **ergänzenden Maßnahmen sowie die SCC** müssten nach einer Einzelfallanalyse der Umstände der Übermittlung sicherstellen, dass das US-Recht das angemessene Schutzniveau, das sie garantieren, nicht beeinträchtigt. Das **Urteil begründet** aber **jedenfalls eine Pflicht zur aktiven Prüfung** im Hinblick auf **jede Übermittlung personenbezogener Daten in die USA** durch die Verantwortlichen.

Höchste Priorität kommt jenen Verarbeitungen durch US-Unternehmen zu, die bisher ausschließlich auf „EU-US Privacy Shield“ gestützt waren. Diese sind nach dem Urteil rechtswidrig und sollten möglichst rasch ersetzt werden. Dies betrifft insb. „Google Analytics“[2], auch in der „anonymisierten“ Variante. Hier besteht zB mit Matomo[3] eine datenschutzfreundliche Alternative. **Datenschutzbeauftragte** und -Koordinatoren **sollten dieses Schreiben dringend der Geschäftsführung vorlegen**, zumal hier für Entscheidungsträger auch ein **persönliches Haftungsrisiko besteht**. Zugleich kann mit ein paar relativ einfachen **Handlungen nach dieser Anleitung dieses Risiko deutlich reduziert** oder überhaupt eliminiert werden. Wichtig ist ein aktives Handeln unter Ausnützung der bestehenden Spielräume des Technologiemarktes.

[1] Volltext abrufbar unter http://curia.europa.eu/juris/liste.jsf?language=de&num=C-311/18 (29.07.2020).

[2] Derzeit sind nur die Dienste Google Cloud Platform und G Suite auch auf „EU Model Contract Clauses“ gestützt und bieten daher eine Rechtsgrundlage, https://privacy.google.com/businesses/compliance/?hl=en_US (29.07.2020).

[3] https://matomo.org/ (29.07.2020).

Übereinstimmend mit den FAQs des Europäischen Datenschutz-Ausschusses (EDPB-FAQ[4]) sowie abgestimmt mit den Empfehlungen von noyb.eu[5] zum "Schrems II"-Urteil ist die **dringende Empfehlung des Research Institute** an **jede Organisation,** egal **ob** als für Verarbeitung **Verantwortlicher oder** als **Auftragsverarbeiter**, die folgenden **Schritte zeitnah umzusetzen**:

1. **Alle externen Datenflüsse** (auch an EU-Unternehmen, die ihrerseits Daten an nicht-EU-Unternehmen übermitteln könnten) **auf Datentransfer in Drittländer prüfen**

2. **Rechtsgrundlage prüfen** (zwei Stufen-Prüfung)
   - Auf welcher Rechtsgrundlage der Art 6 bis 9 DSGVO (Einwilligung, Vertragserfüllung, berechtigte Interessen) findet die Verarbeitung statt?
   - Wie wird das angemessene Datenschutzniveau hergestellt? (z.B. Angemessenheitsbeschluss, Ausnahmen Art 49 DSGVO, Privacy Shield, SCC usw.)

3. "Electronic Communication Service Provider"[6] sowie „Cloud Provider“ in den USA und **jeden Datenfluss in die USA, der nicht gegen Abhören durch die NSA gesichert** ist[7], **prüfen**

4. **Verantwortliche/Auftragsverarbeiter im Drittstaat stützen sich auf SCC**:
   - Bei nicht-US-amerikanischen Unternehmen: Sachverhalt im Drittstaat prüfen – Handlungspflicht wenn evident (China? Weißrussland? Andere Regime?)
   - Bei US-Unternehmen: die EuGH Entscheidung „Schrems II“ muss automatisch Zweifel auslösen, ob die SCC eingehalten werden können → Handlungspflichten

5. **Handlungspflichten bei US-Diensten auf Basis von SCC**:
   - Viele US-Dienste sind nach der Aufhebung des „Privacy Shield“ derzeit weiterhin durch SCC gerechtfertigt, zB Microsoft oder Apple. Unseres Erachtens wird diese Rechtfertigung in 6-12 Monaten durch die EU-Datenschutzbehörden vielfach beseitigt.
   - So früh wie möglich, spätestens aber im Herbst nach der Urlaubszeit sollten daher erste Schritte eingeleitet werden, zur Vorbereitung und zur Erfüllung der Pflichten nach Art 24 (Verantwortliche) oder Art 28 (Auftragsverarbeiter) DSGVO.
   - Der erste Schritt ist die offizielle Anfrage an die nach der Prüfung identifizierten US-Unternehmen. Hierzu hat noyb.eu eine Anleitung und Musterfragen entwickelt: https://noyb.eu/de/naechste-schritte-fuer-eu-unternehmen-faqs
   - Nutzen Sie das bearbeitbare Formular[8] und schreiben Sie dem betroffenen US-Unternehmen. Sie erfüllen damit einen wesentlichen Teil Ihrer Pflicht und gewinnen Zeit, in dem Sie den US-Partner in die Verantwortung ziehen. Zugleich wird die weitere Vorgehensweise wesentlich von der Antwort auf Ihre Anfrage bestimmt sein.

[4] https://edpb.europa.eu/sites/edpb/files/files/file1/20200724_edpb_faqoncjeuc31118.pdf (29.07.2020).
[5] https://noyb.eu/de/naechste-schritte-fuer-eu-unternehmen-faqs (29.07.2020).; RI Institutsleiter C. Tschohl ist bei noyb.eu neben M. Schrems und P. Leupold Vorstandsmitglied, war aber nicht operativ am Projekt beteiligt.
[6] Siehe die Liste der jedenfalls betroffenen Anbieter sowie die Musteranfragen bei https://noyb.eu/de/naechste-schritte-fuer-eu-unternehmen-faqs (29.07.2020).
[7] In Bezug auf die US-Rechtsgrundlagen 50 USC § 1881a (= FISA 702) und EO 12.333.
[8] https://noyb.eu/files/CJEU/EU-EU_form_v3.docx (29.07.2020).

Möglichkeiten zur Sicherstellung der Rechtmäßigkeit

1. Soweit möglich und wirtschaftlich vertretbar: Alternativen innerhalb des EWR oder Drittstaaten mit angemessenem Schutzniveau[9] oder „on-premise“-Lösungen wie zB Matomo für Webtraffic-Analysen umsetzen. Wer rasch einen Plan in die Wege leitet, wird auch auf Verständnis treffen, wenn die Umsetzung etwas Zeit in Anspruch nimmt.
2. Nachvollziehbare Erklärung des US-Partners, durch welche technisch-organisatorischen Maßnahmen Daten vor einem Zugriff durch „die NSA“ geschützt werden. Insbesondere bei US-Anbietern mit Rechenzentren in der EU (zB Microsoft) ist auf eine vollständige technische und juristische/organisatorische Trennung der Sphären zwischen dem Betrieb in den USA und in der EU/dem EWR zu achten. Bei einer sauberen Trennung liegt gar keine Verarbeitung im Drittstaat mehr vor.
3. Technologiegestaltung in der eigenen Sphäre: Durch Maßnahmen der Verschlüsselung oder innovative Ansätze des Cloud Computing in verteilten Systemen kann in manchen Fällen ebenso erreicht werden, dass keine personenbezogenen Daten (im rechtlichen Sinn) in Drittstaaten verarbeitet werden. Abhängig von der Bedeutung der bestehenden Systeme kann dies ein sehr guter Lösungsansatz sein.
4. Wenn nichts anderes hilft: Einwilligung des Nutzers auch auf die Verarbeitung in einem unsicheren Drittland erstrecken. Diese Möglichkeit sieht Art 49 Abs 1 lit a DSGVO vor. Die Datenschutzerklärung ist dann ausdrücklich um die Datenübermittlung in ein unsicheres Drittland und die Ausnahme des Art 49 Abs 1 lit a DSGVO zu ergänzen.

Beendigung der Verarbeitung im Drittstaat

In folgenden Fällen sollten die Datenübertragungen in einen Drittstaat gestoppt werden:

- Ihre Organisation oder einer der Partner baut weiterhin ausschließlich auf Privacy Shield die Rechtfertigung eines „angemessenen Datenschutzniveaus“,
- Ihre Organisation übermittelt Daten an einen US "Electronic Communication Service Provider" und es besteht auch keine Ausnahme nach Art 49 DSGVO, oder
- die Datenübermittlung kann auch sonst (insb. durch Technikgestaltung) nicht vor Abhörung durch die NSA geschützt werden.

Wenn Sie trotz einer negativen Beurteilung weiterhin auf Basis von SCC, Binding Corporate Rules (BCR) oder anderen vergleichbare Rechtsinstrumenten Daten in die USA übermitteln wollen, weil es zwingende praktische Gründe dafür gibt, ist zu überlegen, die nationale Datenschutzbehörde einzubeziehen. Bei großen und derzeit praktisch oft alternativlosen Dienstleistern wie Microsoft oder Apple sind hier vor allem auch die europäischen Datenschutzbehörden am Zug.

[9] Siehe dazu den authentischen Überblick der EU Kommission zu den „Angemessenheitsbeschlüssen“, auch auf der deutschen Internetseite offenbar nur in Englisch verfügbar: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_de (29.07.2020).

Zusammenfassung und Ausblick

Kein Unternehmen kann und muss alleine die Probleme der Welt lösen, das wird nicht erwartet. Allerdings ist schon zu erwarten, dass sich ein Unternehmen – insbesondere in der Rolle des für die Verarbeitung Verantwortlichen – um die Herstellung eines rechtmäßigen Zustands aktiv bemüht und dabei auch entsprechende Initiative von Partnern in Drittstaaten einfordert. Dabei sollte vor allem auch eine allfällige Konzernebene motiviert werden, durch ein gemeinsames Vorgehen von Konzerngesellschaften den kritischen Anfragen mehr Gewicht zu verleihen.

Alleine im Wirkungskreis des Research Institutes befinden sich einige Organisationen, die im Hinblick auf deren internationale bzw. konzernmäßige Verbindung auch ordentliches Gewicht über die Republik Österreich hinaus entfalten können. Je mehr diesen Empfehlungen folgen und damit einen Druck auf die digitale US-Wirtschaft entfalten, desto aussichtsreicher ist diese Vorgehensweise. Jedenfalls aber befreit sie vom Vorwurf der Untätigkeit und dämpft damit enorm das eigene Risiko Ihrer Organisation und der Geschäftsführung.

Bitte beachten Sie dabei, dass nach der gefestigten Judikatur des EuGH (insb. „Fashion-ID“ und „Planet49“) häufig auch eine gemeinsame Verantwortung besteht, vor allem bei der Einbindung von „social media plug-ins“ in die eigenen Angebote. Hier besteht oft ein weiteres Risiko einer rechtswidrigen Datenverarbeitung, das vielen Verantwortlichen gar nicht bewusst ist. Im Zusammenhang mit der Aufhebung von Privacy Shield hat sich dieses Risiko nun potenziert.

Die ersten (internen) Schritte sollten daher so früh wie möglich gesetzt werden, insbesondere wenn die Rechtfertigung ausschließlich auf Privacy-Shield gebaut war. Im Hinblick auf US-Partner mit Standard Contractual Clauses (SCC) sollte es aber auch früh genug sein, wenn nach der Urlaubszeit im September die ersten Schritte eingeleitet werden.

Das Team des Research Institute – Smart Rights Consulting und ich stehen Ihnen gerne unterstützend mit unserer Beratung zur Seite. Wir wünschen trotz allen Herausforderungen einen schönen Sommer und gutes Gelingen.

Hochachtungsvoll

Ing. Mag. Dr.iur. Christof Tschohl

Wissenschaftlicher Leiter, ppa

Wien, 29.07.2020

research institute
Amundsenstraße 9, 1170 Wien
Tel: +43 (1) 58 649 83 - 0
E-Mail: office@researchinstitute.at
Web: http://www.researchinstitute.at