# DSGVO-konforme Datenübermittlung in die USA

## Ein Wegweiser durch den Mythendschungel

**BEITRAG. Datenübermittlung in die USA – Is there a legal way? Die beliebteste Juristenantwort lautet bekanntlich: „Es kommt darauf an." Auch in diesem Fall ist sie zutreffend. Ziel dieses Beitrags ist es, mehrere Wegweiser auf den Pfaden der Prüfung einer DSGVO-konformen Datenübermittlung[1] in Drittländer[2] im Allgemeinen und in die USA im Besonderen zu postieren und darzulegen, ob und unter welchen Umständen die Übermittlung personenbezogener Daten zulässig ist. ecolex 2021/382**

MMag., M.A.I.S. **Theresia Leitinger** ist Rechtsanwaltsanwärterin in der Kanzlei Dr. *Florian Leitinger*.

## A. Ausgangspunkt

### 1. Datenschutz in Europa und den USA

Die Mitgliedstaaten der EU räumen dem *Datenschutz* mit Einführung der DSGVO einen *hohen Stellenwert* ein: Ziel ist es, natürliche Personen in Bezug auf die Verarbeitung ihrer Daten zu schützen.[3] Ein vergleichbares Datenschutzrecht existiert in den USA nicht, die amerikanische Rechtsordnung enthält zahlreiche *Überwachungsgesetze* und Verordnungen, die mit dem europäischen Datenschutz nur unter ausgewählten Umständen kompatibel sind.

Bereits die erste *Schrems*-E des EuGH[4] schob ungeprüften Datenübermittlungen in die USA einen Riegel vor. In dieser E erklärte der EuGH das *Safe-Harbor-Abkommen*[5] zwischen den USA und der EU – aufgrund des Verstoßes gegen den Kernbereich von Art 7 GRC und unzureichender Rechtsschutzmöglichkeiten für Nicht-US-Bürger[6] gegen Art 47 GRC – für nichtig.

Der Versuch einer Reparatur ließ nicht lange auf sich warten: Die EK fasste ein knappes Jahr später, am 1. 8. 2016, erneut einen Angemessenheitsbeschluss, das *EU-US-Privacy-Shield*.[7] Das EU-US-Privacy-Shield war somit noch unter der Anwendbarkeit der RL 95/46/EG[8] in Geltung getreten. Doch auch dieser Angemessenheitsbeschluss währte nicht lange.

Das Urteil des EuGH *Schrems II*[9] erklärte das EU-US-Privacy-Shield nach knapp vierjährigem Bestehen für ungültig und schränkte weitere Legimitationsgründe für die Datenübermittlung in die USA zT stark ein. Bisweilen wurde sogar das *„Aus der Datenübermittlung in die USA"* befürchtet.[10]

### 2. Dezimierte Ausrüstung durch den EuGH anhand Schrems II

**Nun gilt es, für jede Datenübermittlung in die USA eine Einzelfallprüfung zur Zulässigkeit durchzuführen.**

Zur Legitimierung der Datenübertragung in die USA konnten sich Verantwortliche bis *Schrems II* auf *Standardvertragsklauseln (SCC)*[11] nach Art 46 DSGVO, *verbindliche interne Datenvorschriften (BCR)*[12] nach Art 47 DSGVO oder auf die glücklose Nachfolgerin des Safe-Harbor-Abkommens, das *EU-US-Privacy-Shield* nach Art 45 DSGVO, berufen.

Der EuGH unterzog, anders als in *Schrems*,[13] in der E *Schrems II* nun auch die Gültigkeit der E 2010/87/EG[14] der EK einer Überprüfung und erklärte die SCC in Bezug auf Datenübermittlung für unzureichend, wenn diese, etwa aufgrund von Überwachungsgesetzen,[15] nicht eingehalten werden können.[16] Das Ergebnis der E kurz zusammengefasst: Stützte sich die Datenübertragung (nur) auf das Privacy Shield oder SCC ohne weitere Überprüfung, wurde diese Datenübertragung – mit so-

[1] Dieser Beitrag bezieht sich auf die Übermittlung personenbezogener Daten nach Art 4 Z 1 DSGVO.
[2] Anm: Diese umfassen sämtliche Staaten mit Ausnahme der EU und Länder des EWR.
[3] Art 1 Abs 1 DSGVO.
[4] EuGH 6. 10. 2015, C-362/14, *Schrems*.
[5] Entscheidung der Kommission v 26. 7. 2000 gem RL 95/46/EG des EP und des Rates über die Angemessenheit des von den Grundsätzen des „sicheren Hafens" und der diesbezüglichen „Häufig gestellten Fragen" (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA, ABl L 2000/215, 7.
[6] US-Bürger sind durch das 4th Amendment geschützt („*The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated [...]*"); dies gilt für Europäer nicht.
[7] Durchführungsbeschluss (EU) 2016/1250 der Kommission v 12. 7. 2016 gem der RL 95/46/EG des EP und des Rates über die Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes, ABl L 2016/207, 1.
[8] RL 95/46/EG des EP und des Rates v 24. 10. 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl L 1995/281, 31.
[9] EuGH 16. 7. 2020, C-311/18, *Schrems II*.
[10] https://www.it-daily.net/it-sicherheit/datenschutz-grc/25527-schrems-ii-das-aus-fuer-die-datenuebermittlung-in-die-usa (abgerufen am 30. 12. 2020).
[11] Standard Contractual Clauses.
[12] Binding Corporate Rules.
[13] Noch nicht Gegenstand des Verfahrens, weil *Facebook* die Anwendbarkeit der SCC auf das Vertragsverhältnis mit *Schrems* erst nach der ersten Entscheidung behauptete, offenbar um weiterhin eine gültige Datenübertragung argumentieren zu können. Daraufhin erstattete *Schrems* seine zweite Beschwerde.
[14] Beschluss der Kommission vom 5. 2. 2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der RL 95/46/EG des EP und des Rates, ABl L 2010/39, 5.
[15] Siehe dazu C. 2.
[16] EuGH 16. 7. 2020, C-311/18, *Schrems II*, Rn 121.

fortiger Wirkung – unzulässig, denn das Urteil anerkannte weder eine Übergangsfrist noch einen Auslegungsspielraum.[17]

Um eine *DSGVO-konforme Datenübertragung* sicherzustellen, muss man sich nun endgültig weiterer Ausrüstungswerkzeuge bedienen.

## B. Voraussetzungen zur Legitimierung einer Datenübermittlung in ein Drittland

### 1. Zweistufige Prüfung

Zusätzlich zur Rechtmäßigkeitsprüfung der Datenübermittlung anhand *Stufe 1,* nämlich Einhaltung der *Grundsätze des Art 5 DSGVO,* Vorliegen einer *Rechtsgrundlage nach Art 6 DSGVO*[18] sowie die Einhaltung technischer und organisatorischer Maßnahmen *(TOM),* werden an die Übermittlung personenbezogener Daten in ein Drittland nach Art 44 DSGVO zusätzliche Anforderungen (Stufe 2) gestellt: Eine *weitere Legitimierung,* die *Kapitel V der DSGVO* regelt, zur Datenübermittlung in ein Drittland ist notwendig.[19]

**Prüfschema Datenübermittlung in Drittländer**

- ➤ STUFE 1:
  - – Einhaltung der Grundsätze der DSGVO
  - – Rechtsgrundlage nach Art 6 (Art 9)
  - – Einhaltung TOM nach Art 32
- ➤ STUFE 2:
  - – Legitimierung nach Kapitel V: Art 44 + Art 45/Art 46/ Art 47/Art 49
  - – Sonderfall USA
  - – ergänzende Maßnahmen: technisch und vertraglich

### 2. Angemessenheitsbeschluss nach Art 45 DSGVO

Zunächst ist das Vorliegen eines *angemessenen Schutzniveaus,* welches die EK mit einem Angemessenheitsbeschluss des Art 45 DSGVO bestätigt hat, zu prüfen. Im Fall des Bestehens eines solchen Beschlusses bescheinigt die EK dem Drittland ein der EU gleichwertiges Schutzniveau personenbezogener Daten. Liegt ein solcher vor, können Datenübertragungen auf diese Legitimationsgrundlage gestützt werden.

Die EK führt eine Liste jener Länder, aktuell umfasst diese zwölf Staaten, mit vorliegendem Angemessenheitsbeschluss.[20] Nach *Wegfall des Safe-Harbor-Abkommens und des US-EU-Privacy Shield,* beide Angemessenheitsbeschlüsse wurden durch den EuGH in den E *Schrems*[21] und *Schrems* II[22] aufgehoben, befindet sich die USA nicht mehr darunter.

### 3. SCC als geeignete Garantien des Art 46 DSGVO und BCR nach Art 47 DSGVO

*Standarddatenschutzklauseln*[23] *(SCC)* nach Art 46 DSGVO sind einheitliche Vertragswerke, die dem europäischen Datenschutzstandard entsprechen. Werden die von der EK beschlossenen Klauseln vertraglich vereinbart, sind diese keiner gesonderten Überprüfung einer Datenschutzbehörde zu unterziehen.

Ebenso stellen *BCR* nach Art 47 DSGVO, mittels welcher sich Unternehmen in Drittländern selbst ein der DSGVO entsprechendes Datenschutzniveau auferlegen, eine taugliche Legitimitätsgrundlage dar. BCR müssen von der Datenschutzbehörde genehmigt werden.[24]

### 4. Der Joker: Art 49 DSGVO

Kommt keine der vorherigen Legitimitätsgrundlagen in Betracht, kann Art 49 DSGVO in *„Ausnahmen für bestimmte Fälle"* zur Anwendung gelangen. Nach dem Gesetzeswortlaut gilt dies allerdings nur, wenn – ua – die *Übermittlung nicht wiederholt* erfolgt und lediglich eine *begrenzte Zahl von betroffenen Personen* betrifft. Ein Beispiel des *EDSA* hiefür ist die Übermittlung von Kundendaten durch Reisebüros an Hotels in ein Drittland.[25]

## C. Rechtmäßige Datenverarbeitung in den USA

### 1. Mögliche Legitimitätsgrundlagen

Da derzeit kein Angemessenheitsbeschluss mit den USA besteht, muss auf die Legitimitätsgrundlage der SCC nach Art 46 DSGVO oder der BCR nach Art 47 DSGVO zurückgegriffen werden. Die Ausnahmetatbestände des Art 49 DSGVO behalten darüber hinaus weiterhin Gültigkeit, gelangen jedoch nur in Ausnahmefällen zur Anwendung und dürfen daher nicht für regelmäßige Datenverarbeitungen herangezogen werden.

Wie oben ausgeführt, hat der EuGH in *Schrems II* festgehalten, dass im Fall der Anwendung von SCC in jedem Einzelfall zu prüfen ist, ob der Empfänger im Drittland Gesetzen unterliegt, die einem angemessenen Schutz personenbezogener Daten entgegenstehen.[26] Auf SCC allein kann man sich somit bei einer Übermittlung von Daten in die USA nicht mehr berufen, eine *Zusatzprüfung ist zwingend durchzuführen.* Erforderlichenfalls sind weitreichendere Garantien, als von den SCC geboten, zu gewähren.[27]

### 2. Unterliegt der Datenempfänger in den USA einem Gesetz, das mit den Grundsätzen der DSGVO nicht vereinbar ist?

Das für die Vereinigten Staaten geltende Bundesrecht, der *United States Code,*[28] ist in 54 Titel unterteilt. Titel 50 über *War and National Defense* enthält in Kap 36 *Foreign Intelli-*

---

[17] Zur Analyse der Entscheidung *„Schrems* II" s bspw die Empfehlung der *Research Institute AG & Co KG* v 29. 7. 2020, https://www.researchinstitute.at/files/583-memory-business/text/empfehlungen_stellungnahmen/RI_Empfehlungen_EuGH_Schrems%20II_Privacy%20Shield+SCC_29. 07. 2020_DE.pdf (abgerufen am 30. 11. 2020).

[18] Zur Vollständigkeit wird an dieser Stelle darauf hingewiesen, dass für die Verarbeitung besonderer Kategorien personenbezogener Daten selbstverständlich auch im Fall der Drittlandübermittlung die Regelungen des Art 9 und Art 10 DSGVO gelten.

[19] Vgl *Schantz* in *Schantz/Wolff,* Das neue Datenschutzrecht (2017) Rz 755.

[20] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (abgerufen am 1. 12. 2020).

[21] EuGH 6. 10. 2015, C-362/14, *Schrems.*

[22] EuGH 16. 7. 2020, C-311/18, *Schrems II.*

[23] Der Vollständigkeit halber ist zu erwähnen, dass der Begriff Standarddatenschutzklauseln (SDK) der DSGVO entstammt, wobei trotz mittlerweile fast fünfjährigen Bestehens dieser Verordnung noch keine SDK erlassen wurden, wie in Art 46 Abs 2 lit c DSGVO vorgesehen. Art 46 Abs 5 DSGVO regelt allerdings, dass bis zur Kundmachung der SDK die unter der Datenschutz-RL ausgearbeiteten Standardvertragsklauseln (SVK) weiterhin gültig sind. Ein Prüfverfahren für die Einführung der SDK ist gerade in Ausarbeitung. Feedback zu den SDK konnte bis 10. 12. 2020 eingereicht werden; https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Commission-Implementing-Decision-on-standard-contractual-clauses-for-the-transfer-of-personal-data-to-third-countries (abgerufen am 14. 1. 2021).

[24] Art 47 Abs 1 DSGVO.

[25] *EDSA,* Leitlinien 2/2018 zu den Ausnahmen nach Art 49 der Verordnung 2016/679, 10, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_de.pdf (abgerufen am 11. 1. 2021).

[26] EuGH 16. 7. 2020, C-311/18, *Schrems II,* Rn 134.

[27] Auf diese wird in Pkt D genauer eingegangen.

[28] Code of Laws of the United States of America, abrufbar unter https://www.law.cornell.edu/uscode/text (abgerufen am 20. 12. 2020).

*gence Surveillance* die Bestimmung § 1881. Diese Norm regelt, dass bspw elektronische Kommunikationsanbieter unter weitreichende Überwachungsgesetze, nämlich den *Foreign Intelligence Surveillance Act (FISA),*[29] fallen. Dieses Gesetz hat ebenso *Relevanz für Europäer, deren personenbezogene Daten verarbeitet werden,* denn Section 702 regelt *Procedures for Targeting Persons Outside the United States Other Than United States Persons*[30] und zielt darauf ab, *Nicht-US-Bürger außerhalb der Vereinigten Staaten zu überwachen.*

Der Präsident der USA ist ermächtigt, selbständig *Executive Orders* (EO) zu erlassen. Die EO 12.333 über *United States intelligence activities*[31] zur *Überwachung von (elektronischer) Kommunikation* ist eine solche Verordnung, die Massenüberwachungen anordnet.

Unterliegt ein Anbieter in den USA diesen Überwachungsregeln, was auf die meisten der gängigen elektronischen Kommunikationsanbieter zutrifft, ist nach Ansicht des EuGH in *Schrems II* eine *Datenübermittlung aufgrund der Unvereinbarkeit auch bei abgeschlossenen SCC oder zusätzlichen BCR nicht zulässig.*

Unterliegt der Anbieter in den USA nicht diesen Gesetzen, sind zusätzlich zu den SCC technische und organisatorische Maßnahmen zu ergreifen, um sicherzustellen, dass das Schutzniveau der DSGVO auch für die Datenverarbeitung in den USA eingehalten wird. *Eine Datenverarbeitung ist jedoch grundsätzlich* auf Basis der Legitimität von Art 46 oder 47 DSGVO *möglich.*

Es ist daher für *Verantwortliche* dringend geboten, vor Übermittlung personenbezogener Daten in die USA vom Drittanbieter Auskunft darüber zu verlangen, ob dieser dem FISA unterliegt.

### 3. Zusammenfassung

Datenübertragungen in die USA an ein Unternehmen oder eine Organisation, die den *Massenüberwachungsgesetzen* unterliegen, sind aufgrund der Unvereinbarkeit mit den Grundsätzen der europäischen Rechtsordnung[32] *unzulässig,* mit Ausnahme von notwendigen Übertragungen nach Art 49 DSGVO. Auch wenn in der Praxis zusätzliche Vereinbarungen getroffen sowie Einwilligungen eingeholt werden und umfangreiche Rechtsbelehrungen erfolgen, ist eine solche Datenübertragung nicht rechtmäßig, weil eine vertragliche Vereinbarung den US-Verarbeiter aufgrund der Gesetze in den USA nicht binden kann.

Für Verarbeiter, die *nicht Massenüberwachungsgesetzen* unterliegen, gilt es, die weitere *Prüfung* durchzuführen, ob die Verarbeitung auf Basis von *BCR oder SCC* unter *Zuhilfenahme ergänzender und vertraglicher TOM,* die vom Betroffenen nicht autorisierten Zugriff durch US-Behörden ausschließen, zulässig ist.

## D. Technische Ergänzende Maßnahmen (Teil I)

Erfolgt die Datenübertragung an einen Verantwortlichen oder Auftragsverarbeiter in den USA, der nicht den US-Massenüberwachungsgesetzen unterliegt, kann die Verarbeitung zwar ebenfalls nicht mehr auf das Privacy Shield oder ungeprüfte SCC gestützt werden, durch die *zusätzliche Implementierung von TOM und vertraglicher Absicherung* mit dem US-Unternehmen kann jedoch eine DSGVO-konforme Übertragung erreicht werden.

Ergänzende technische Maßnahmen können bspw sein:

- *Verschlüsselung der Datenübermittlung* in die USA („Transit"), damit personenbezogene Daten nicht mittels „Upstreaming" durch US-Behörden eingesehen werden können,[33]
- Verschlüsselung der Daten durch *Datenteilung,* sodass die Daten in zwei voneinander getrennten Verarbeitungsschritten übermittelt werden, die jeweils für sich nicht personenbezogene Daten erhalten,
- *„Zero Knowledge"*-Verschlüsselung, mittels welcher der Zugriff auf Nutzerdaten durch den Provider (zB Auftragsverarbeiter) nicht möglich ist. Diese Verschlüsselungstechnik wird va für Cloudlösungen angeboten.[34]

## E. Vertragliche Ergänzende Maßnahmen (Teil II)

*Die Neuentdeckung des ErwGr 109 DSGVO:* Seit Bestehen der DSGVO empfiehlt ErwGr 109: *„Die Verantwortlichen und die Auftragsverarbeiter sollten* ermutigt werden, mit vertraglichen Verpflichtungen, *die die Standard-Schutzklauseln* ergänzen, *zusätzliche Garantien zu bieten."* Diese Empfehlung wird in der Praxis wohl vermehrt Einzug halten, denn mittels dieser zusätzlichen Verpflichtungen kann die Verantwortliche den in den USA ansässigen Verarbeiter vertraglich zur Einhaltung der datenschutzrechtlichen Bestimmungen der DSGVO anweisen.

Konkrete Empfehlungen durch den *EDSA*[35] befinden sich in Ausarbeitung, der vorläufige Text vom 21. 12. 2020 ist in englischer Sprache abrufbar.[36]

### Schlussstrich

**Die erhoffte „wasserdichte" Einwilligung oder eine andere einheitliche Legitimitätsgrundlage für Datenübermittlung in die USA gibt es nicht. Zu viele unterschiedliche Faktoren gilt es zu beachten. Verantwortliche, die *Datenübermittlungen in die USA* anstreben oder bereits durchführen, sind gut beraten, zunächst zu überprüfen, ob die Übertragung an ein Unternehmen oder eine Organisation in den USA erfolgt, dem FISA oder anderen *Überwachungsgesetzen* unterliegt. Diesfalls ist die Datenübermittlung nach der E *Schrems II fast ausschließlich unzulässig.***

**In anderen Fällen ist es selbst nach Wegfall des EU-US-Privacy Shield mittels anderer Legitimitätsgrundlagen unter Einbeziehung ergänzender technischer und vertraglicher Maßnahmen *möglich,* eine *DSGVO-konforme Datenübermittlung in die USA* sicherzustellen.**

[29] Das 2008 in den USA erlassene Gesetz zur Änderung des FISA aus dem Jahr 1978 enthält in Section 702 weitreichende Bestimmungen, die der US-Regierung die Befugnis erteilen, sämtliche amerikanische Kommunikation über „upstream" und „PRISM" zu überwachen. Section 702 zielt darauf ab, Informationen von Nicht-US-Bürgern, die durch die Fourth Amendment's prohibition geschützt sind, aus Datenbanken abzugreifen, zu sammeln und zu verarbeiten.

[30] Abrufbar unter https://www.govinfo.gov/content/pkg/BILLS-110hr6304pcs/html/BILLS-110hr6304pcs.html (abgerufen am 20. 12. 2020).

[31] Verordnungstext abrufbar unter https://www.archives.gov/federal-register/codification/executive-order/12333.html (abgerufen am 20. 12. 2020).

[32] Art 7 und 47 GRC.

[33] Nach EuGH 16. 7. 2020, C-311/18, *Schrems II,* Rn 183, verstößt die Überwachung durch US-Behörden „im Transit" gegen die Grundrechte der EU.

[34] Anbieter bspw www.boxcryptor.com; www.tresorit.com (jeweils abgerufen am 30. 12. 2020).

[35] *EDSA,* Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf (abgerufen am 30. 12. 2020).

[36] https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer_en (abgerufen am 30. 12. 2020).