(c) Volker Schroer

# Zusätzliche Schutzmaßnahmen

## Drittlandtransfer: EU-Datenschutzausschuss empfiehlt

In Ergänzung zur Checkliste Drittlandtransfer[1] noch die Empfehlungen zu den zusätzlichen Schutzmaßnahmen der EDSA (EU - Datenschutzausschuss) für Verantwortliche nach dem Urteil „Schrems II“ des EuGH (Link in der Fußleiste zu Empfehlungen 01/2020, 46 Seiten 12/2020)[2]:

*„Der EDSA hat beschlossen, diese Frage von sich aus zu untersuchen und … Empfehlungen zu dem Verfahren zu geben … Der Gerichtshof hat ausgeführt, dass es vor allem dem Datenexporteur obliegt, in jedem Einzelfall – falls angemessen, in Zusammenarbeit mit dem Datenimporteuer – zu prüfen, ob das Recht des Bestimmungsdrittlands nach Maßgabe des Unionsrechts einen im Wesentlichen gleichwertigen Schutz der auf der Grundlage von Standarddatenschutzklauseln übermittelten personenbezogenen Daten gewährleistet, und, soweit erforderlich, über die durch diese Klauseln gebotenen Garantien hinaus zusätzliche Maßnahmen zu ergreifen.“* (= aktives Handeln, keine passive Haltung - Nachweispflicht)

### (1) Einzelne Hinweise zum Verfahrensverzeichnis

- Fernzugriff aus einem Drittland (z. B. im Support-Fall) und/oder zur Speicherung in einer Cloud außerhalb der EU ist als Übermittlung anzusehen. Insbesondere bei einer internationalen Cloud - Infrastruktur ist festzustellen, ob Übermittlung in (welche) Drittländer erfolgt oder vertraglich ausgeschlossen ist.
- IMMER ist die Wirksamkeit des nach Art.46 DS-GVO ausgewählten Übermittlungsinstruments im Hinblick auf die Gesamtumstände zu beurteilen. (ggf. ist ein Rechtsgutachten zu erstellen)
  *PS: Der wissenschaftliche Dienst des Bundestages hat eine Dokumentation (03.08.2020) zum „Zugriff US – amerikanischer Behörden auf Daten“ (Foreign Intelligence Surveillance Act of 1978 (FISA), des USA Patriot Act of 2001, des USA Freedom Act of 2015 sowie des Clarifying Lawful Overseas Use of Data Act von 2018 (CLOUD Act) verfasst.* [3]

- Ergänzung der Standardvertragsklausel (SVK nach Art.46 Abs.2 lit.c, d) sind nicht genehmigungspflichtig, sofern keine Beeinträchtigung der genehmigten SVK besteht.

- Eine zusätzliche Maßnahme ist **nur als effektiv** im Sinne des EuGH - Urteils anzusehen, **sofern** die Maßnahme genau die **festgestellten Rechtsschutzlücken schließt**. Sollte es letztendlich nicht möglich sein, ein im Wesentlichen gleichwertiges Schutzniveau zu erzielen, sind personenbezogenen Daten nicht zu übermitteln.

### (2) Beispiele / Empfehlungen zusätzlicher Schutzmaßnahmen des EDSA

#### *(a) Technische Maßnahmen*

##### *i) Verschlüsselung vor Transfer*

Z. B. ein Backup mit personenbezogenen Daten wird vor Transfer (in eine Cloud) mit einer dem „Stand der Technik“ und den Zeitraum berücksichtigenden Verschlüsselung versehen und der Zugang ist nur über eine im Geltungsbereich der DS-GVO liegenden Berechtigung möglich.

##### *ii) Psydonymisierung vor Transfer*

Vor Übermittlung u/o Analyse wird der Personenbezug derart entfernt, dass ohne Hinzuziehung zusätzlicher Daten eine Identifizierung der Person selbst, noch in einer größeren Gruppe möglich ist. Identifizierung nur über eine im Geltungsbereich der DS-GVO liegenden Berechtigung, die durch technisch – organisatorische Maßnahmen sichergestellt ist.

##### *iii) Transit über ein „Drittland*


Auch wenn die Daten „nur“ über eine Land mit nicht angemessenem Schutzniveau geleitet werden könnten, gilt es einen Zugriffsschutz zu gewährleisten mittels einer Transportverschlüsselung mit dem Zeitraum angemessenem, effektivem Schutz nach dem Stand der Technik und Berechtigungen, die nur im Geltungsbereich der DS-GVO liegen.

---

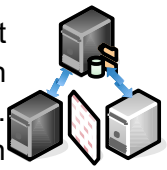
1 *LINK: https://www.volkerschroer.de/DSGVO/2021.04.15.Checkliste.Datentransfer.Drittland.pdf*
2 *Quelle: EDSA – Empfehlung: „Maßnahmen zur Ergänzung von Übermittlungstools …“*
3 *Quelle: Wissenschaftlicher Dienst des Bundestages: „Zugriff US – amerikanischer Behörden auf Daten“*

# Für den eiligen Leser kurz zusammengetragen (2/2)

*iv) Geschützter Empfänger*

Wenn sichergestellt ist, dass der Empfänger im Drittland über einen besonderen Schutz (Geheimhaltungspflicht auch gegenüber Behörden) verfügt, der einem Schutz nach DS-GVO gleich kommt und Zugriff von Dritten ausschließt, ist eine Datentransfer möglich. Voraussetzung ist eine Verschlüsselung nach dem Stand der Technik mit exklusivem Zugriff nur durch Sender und Empfänger. (End – to – End).

*v) Verteilte Verarbeitung (Multi - party Processing)*



Ohne einen Personenbezug herstellen zu können, werden mehrere Auftragsverarbeiter mit der Verarbeitung von Teilmengen der Daten beauftragt, die ihnen und den Landesbehörden (auch gemeinsam) eine Identifizierung von Personen unmöglich machen. Eine Zusammenführung findet nur alleine beim Auftraggeber statt (was einen entsprechenden Nachweis erfordert).

- ✖ Auftragsverarbeitung mit Zugriff auf Personendaten im unsicheren Drittland ist nicht möglich
- ✖ Auch innerhalb einer Unternehmensgruppe u/o eines gemeinsamen Geschäftszwecks können personenbezogen Daten nicht an unsichere Dritte oder Drittländer transferiert werden.

## *(b) Vertragliche Maßnahmen*

Da vertragliche Maßnahmen nur zwischen den Parteien und nicht auch gegenüber dem Drittland wirken, haben vertragliche Maßnahmen (Prüfung Wirksamkeit) unterstützende Wirkung.

*i) Transparenz*

Informationspflicht des Datenempfängers über ihm zugegangene und generelle behördliche Ersuchen, aktuelle rechtliche Regelungen, Zugriffe und Möglichkeiten von Behörden und Nachrichtendiensten, Gerichtsentscheidungen, entsprechende Informationen und Statistiken von Partnern u/o öffentlichen Quellen u. ä. zur aktuellen rechtlichen Einschätzung

*ii) Unterstützungspflichten*

Vertragliche Verpflichtungen keine Hintertüren oder Ähnliches zu programmieren und keine Prozessänderungen für einen Personenbezug für sich selbst oder Dritte vorzunehmen und eine regelmäßige Prüfung zu ermöglichen. Pflicht zur sofortigen Information bei Auskunftsersuchen und Anwendung aller Rechtsmittel sowie ggf. Information und rechtliche Unterstützung der Betroffenen. Dies verbunden mit einer Kündigungsklausel, um im Fall der Fälle den Transfer und die Verarbeitung sofort zu stoppen.

## *(c) Organisatorische Maßnahmen*

Die vom europäischen Datenschutzausschuss vorgeschlagene (möglichen) Maßnahmen zielen auf die Ergänzung und Konkretisierung der Standardvertragsklauseln (SVK) bzw. Standard Contractual Clauses (SCC) ab. Dem Durchführungsbeschluss (EU) 2021/914 der Kommission vom 4. Juni 2021 ist ein / sind genehmigte Muster beigefügt [4]. Der EDSA schlägt dazu konkretisierte Maßnahmen in Bezug auf Transparenz, Rechenschaftspflicht, Datenminimierung, Normen und Verfahren vor. Neben den Einzelmaßnahmen ist sicherlich die Bildung eines gemeinsamen, entsprechend qualifizierten Datenschutzteams aus Juristen und IT – Spezialisten hervorzuheben. Das erleichtert die Einschätzung der aktuellen Lage, ermöglicht schnelle Reaktionen und die lokale Unterstützung für ggf. Betroffene.

## (3) Einschätzung

- ▶ Sofern die „Rechtsschutzlücken“ nicht durch Gerichte, Behörden oder andere vertrauenswürdige Institutionen eindeutig festgestellt wurden, ist m. E. ein Rechtsgutachten durch einen lokalen Juristen fast unumgänglich.
- ▶ Wie der Ausschuss (EDAS) schreibt, bleibt es im Einzelfall zu prüfen, ob mit den zusätzlichen Maßnahmen die festgestellten Lücken im Datenschutz geschlossen werden können.

4 *Link: "Durchführungsbeschluss (EU) 2021/914 der Kommission vom 4. Juni 2021“*