Republik Österreich
Datenschutzbehörde

Transatlantische Datenflüsse

MMag. Elisabeth Wagner

17. Österreichischer IT-Rechtstag

5. Mai 2023

Inhalt

- Leitlinien des EDSA (5/2021) zum Zusammenspiel zwischen der Anwendung von Artikel 3 DSGVO und den Bestimmungen über internationalen Datentransfer gemäß Kapitel V der DSGVO
- Stellungnahme des EDSA (5/2023) zum Entwurf eines Durchführungsbeschlusses der Europäischen Kommission über die Angemessenheit des Schutzes personenbezogener Daten gemäß dem EU-U.S.-Datenschutzrahmen
- Report der 101 Task Force des EDSA
- Verbindliche Entscheidung des EDSA (1/2023) über den Entscheidungsentwurf der irischen Datenschutzbehörde über die Rechtmäßigkeit der Datenübermittlung in die USA durch Meta Platforms Ireland Limited (Meta IE) für seinen Facebook-Dienst

EDSA Leitlinien 5/2021

- Kapitel V der DSGVO
- Artikel 44 DSGVO: *Bedingungen / Instrumente* des Kapitel V der DSGVO
  - Angemessenheitsbeschluss der Europäischen Kommission - Artikel 45 DSGVO
  - geeignete Garantien des Exporteurs (Verantwortlicher oder Auftragsverarbeiter) - Artikel 46 DSGVO
    - Standardvertragsklauseln (SCCs);
    - Verbindliche unternehmensinterne Vorschriften (BCR)
    - Verhaltensregeln
    - Zertifizierungsmechanismen
    - Ad-hoc-Vertragsklauseln
    - Internationale Abkommen/Verwaltungsvereinbarungen
  - Ausnahmen für bestimmte Fälle – Artikel 49 DSGVO

EDSA Leitlinien 5/2021

Republik Österreich
Datenschutzbehörde

3 kumulative Kriterien

1) Ein Verantwortlicher oder ein Auftragsverarbeiter ("Exporteur") unterliegt für die *betreffende Verarbeitung der DSGVO*.

2) Der *Exporteur stellt* einem anderen Verantwortlichen, einem gemeinsam Verantwortlichen oder einem Auftragsverarbeiter ("Importeur") personenbezogene Daten, die Gegenstand dieser Verarbeitung sind, *durch Übermittlung oder auf andere Weise zur Verfügung.*

3) Der *Importeur* befindet sich in einem *Drittland*, unabhängig davon, ob dieser Importeur für die betreffende Verarbeitung gemäß Artikel 3 DSGVO unterliegt oder eine internationale Organisation ist.

1. Kriterium: Exporteuer unterliegt der DSGVO

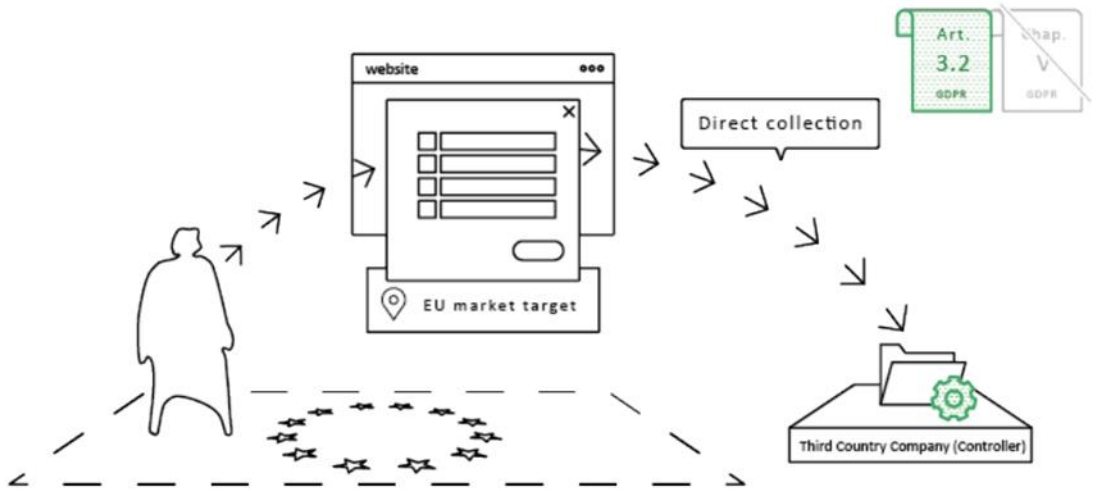
- Verantwortlicher unterliegt für die Verarbeitung Artikel 3 DSGVO.
- Auch Verantwortliche oder Auftragsverarbeiter, die nicht in der EU niedergelassen sind, aber gemäß Artikel 3 Abs. 2 DSGVO erfüllen.
- DSGVO und Kapitel V gilt auch für Datenverarbeitung durch Botschaften und Konsulate der EU-Mitgliedstaaten außerhalb der EU→ Artikel 3 Abs. 3 DSGVO

2. Kriterium: Exporteuer stellt Importeur personenbezogene Daten durch Übermittlung oder auf andere Weise zur Verfügung

- „zur Verfügung stellen“
- Keine Übermittlung
  - „interne“ Verarbeitung
  - es gibt keinen "Exporteur", z. B. wenn die Daten direkt von der betroffenen Person an den Empfänger weitergegeben werden.

2. Kriterium: Exporteuer stellt Importeur personenbezogene Daten durch Übermittlung oder auf andere Weise zur Verfügung

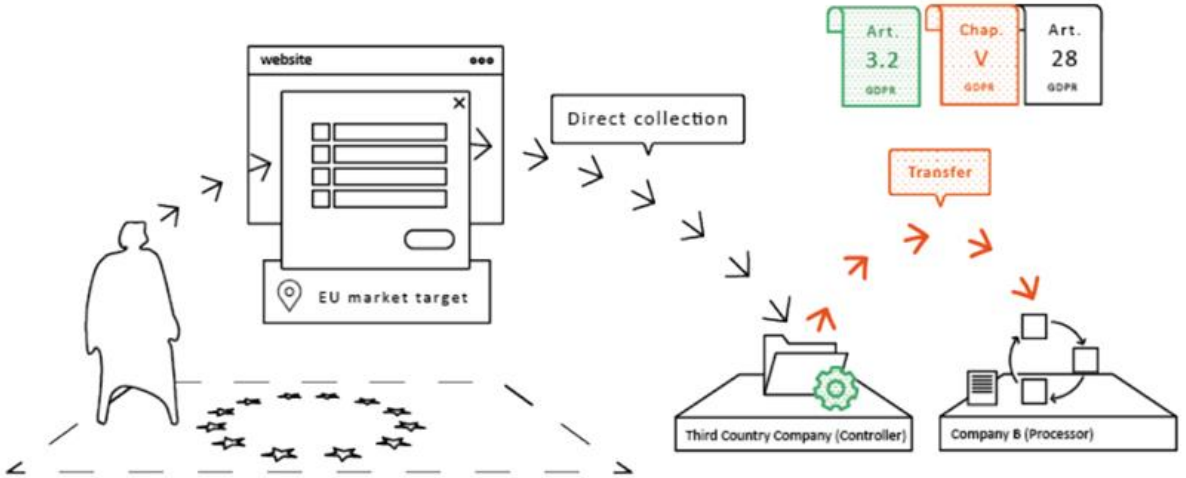
- **Beispiel 1:** Verantwortlicher in einem Drittland unterliegt der DSGVO und erhebt Daten direkt von einer betroffenen Person in der EU → kein Datentransfer



Sämtliche Grafiken sind den EDSA Leitlinien 5/2021 entnommen.

2. Kriterium: Exporteuer stellt Importeur personenbezogene Daten durch Übermittlung oder auf andere Weise zur Verfügung

- **Beispiel 2:** Verantwortlicher in einem Drittland unterliegt der DSGVO, erhebt Daten direkt bei einer betroffenen Person in der EU und beauftragt einen Auftragsverarbeiter außerhalb der EU mit einigen Verarbeitungstätigkeiten → Datentransfer an Auftragsverarbeiter nach Kapitel V und Art. 28 DSGVO einzuhalten.

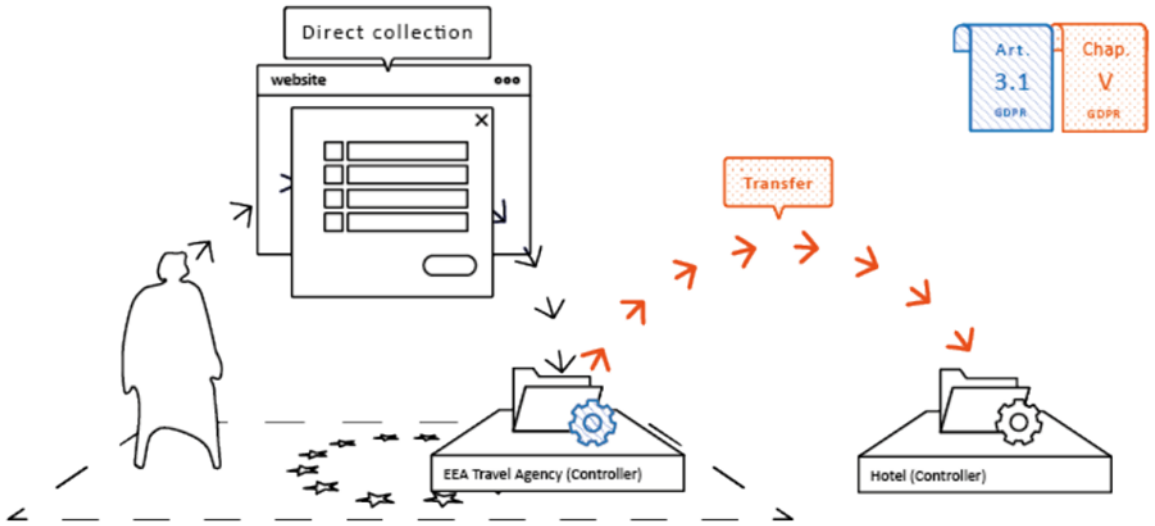


2. Kriterium: Exporteuer stellt Importeur personenbezogenen Daten durch Übermittlung oder auf andere Weise zur Verfügung

- **Beispiel 3:** Verantwortlicher in einem Drittland unterliegt nicht der DSGVO, erhält Daten direkt von einer betroffenen Person in der EU und beauftragt einen Auftragsverarbeiter außerhalb der EU mit einigen Verarbeitungstätigkeiten → kein Datentransfer nach Kapitel V

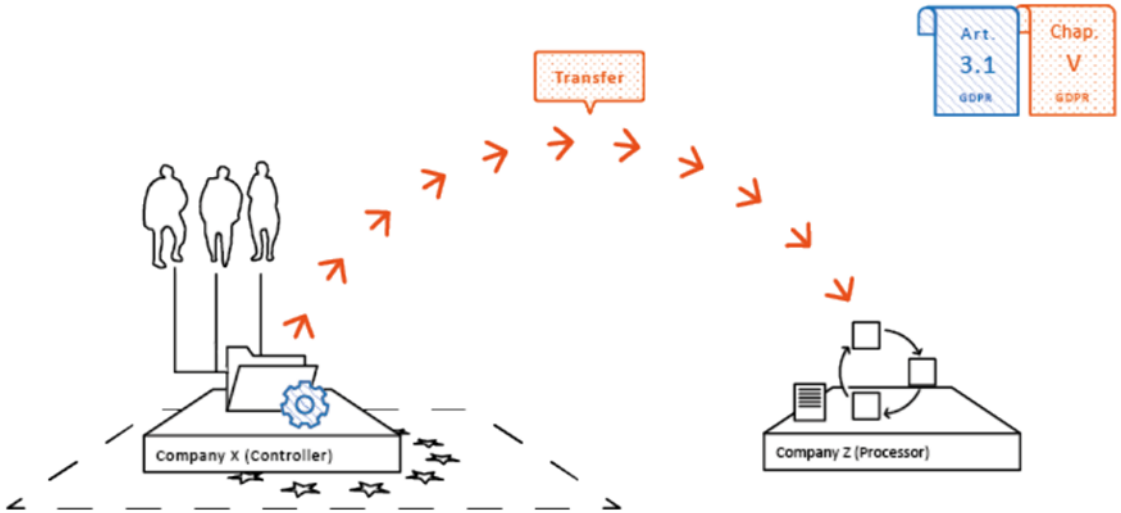
2. Kriterium: Exporteuer stellt Importeur personenbezogenen Daten durch Übermittlung oder auf andere Weise zur Verfügung

- **Beispiel 4:** Von einer EWR-Plattform gesammelte Daten werden an einen Verantwortlichen in einem Drittland weitergeleitet → Datentransfer nach Kapitel V



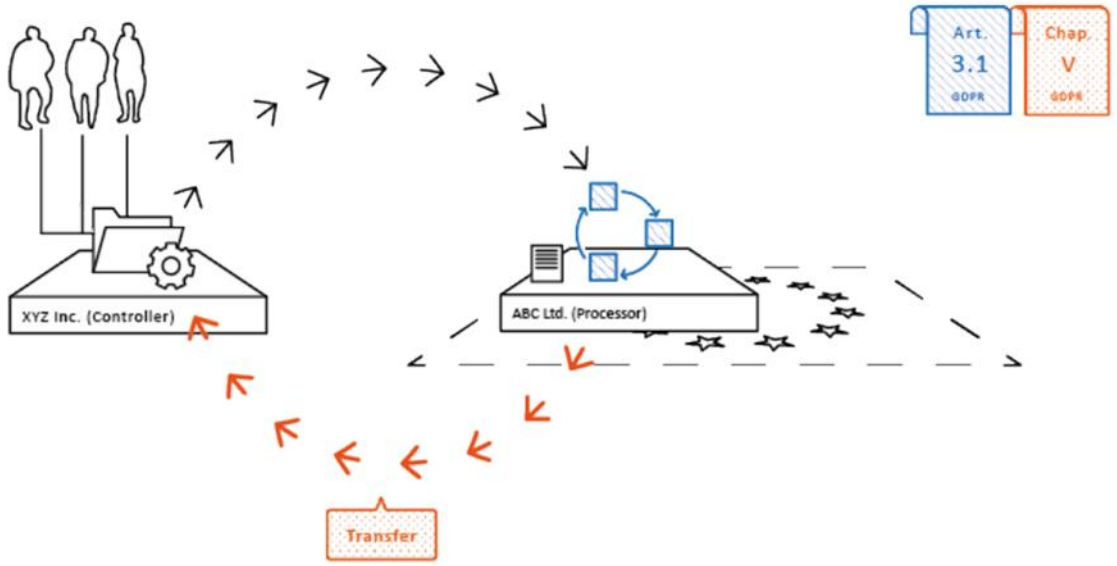
2. Kriterium: Exporteuer stellt Importeur personenbezogenen Daten durch Übermittlung oder auf andere Weise zur Verfügung

- **Beispiel 5:** Verantwortlicher in der EU sendet Daten an einen Auftragsverarbeiter in einem Drittland → Datentransfer nach Kapitel V



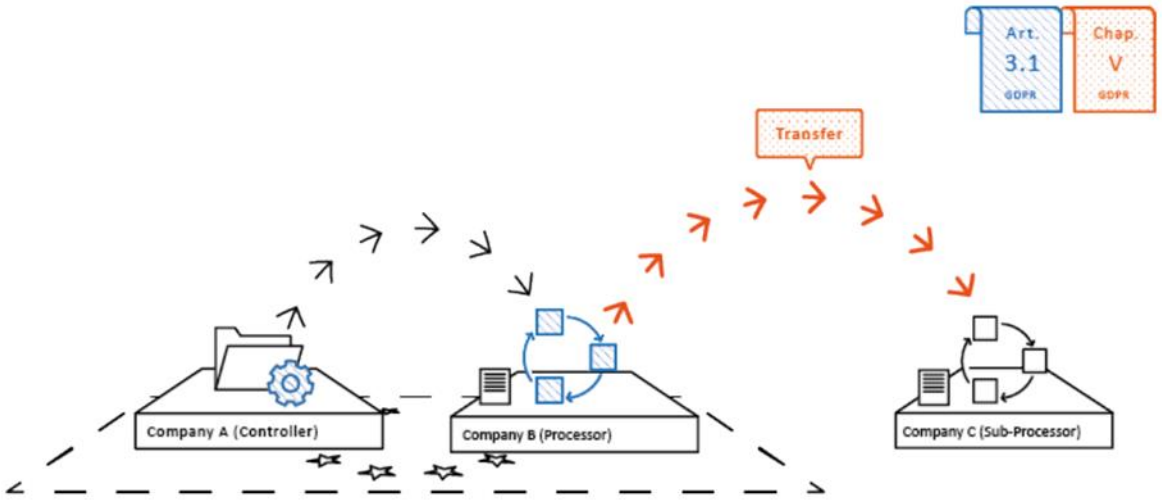
2. Kriterium: Exporteuer stellt Importeur personenbezogenen Daten durch Übermittlung oder auf andere Weise zur Verfügung

- **Beispiel 6:** Auftragsverarbeiter in der EU sendet Daten zurück an seinen Verantwortlichen in einem Drittland → Datentransfer nach Kapitel V



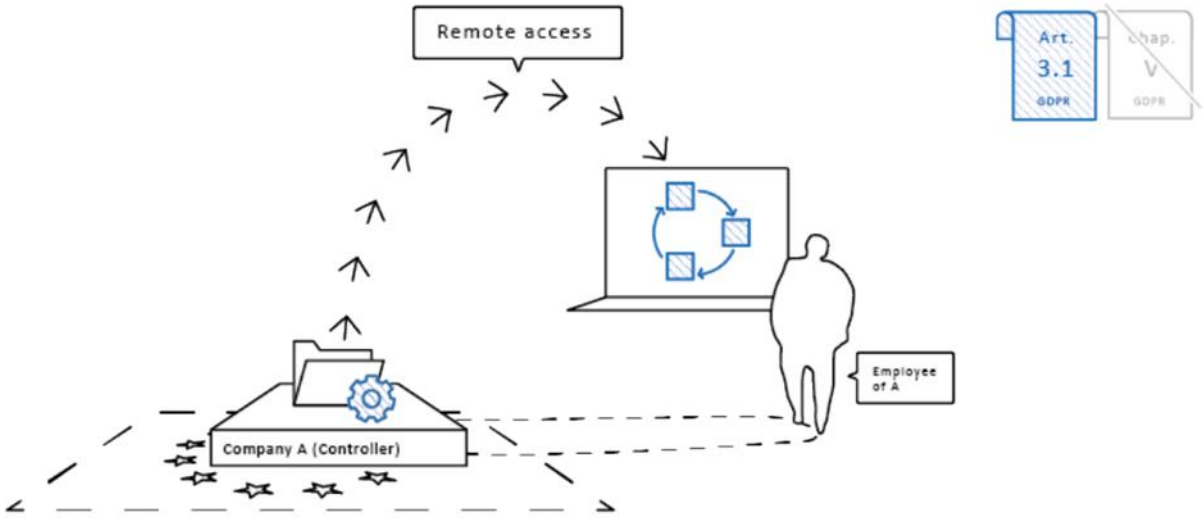
2. Kriterium: Exporteuer stellt Importeur personenbezogenen Daten durch Übermittlung oder auf andere Weise zur Verfügung

- **Beispiel 7:** Auftragsverarbeiter in der EU übermittelt Daten an einen Sub-Auftragsverarbeiter in einem Drittland → Datentransfer nach Kapitel V



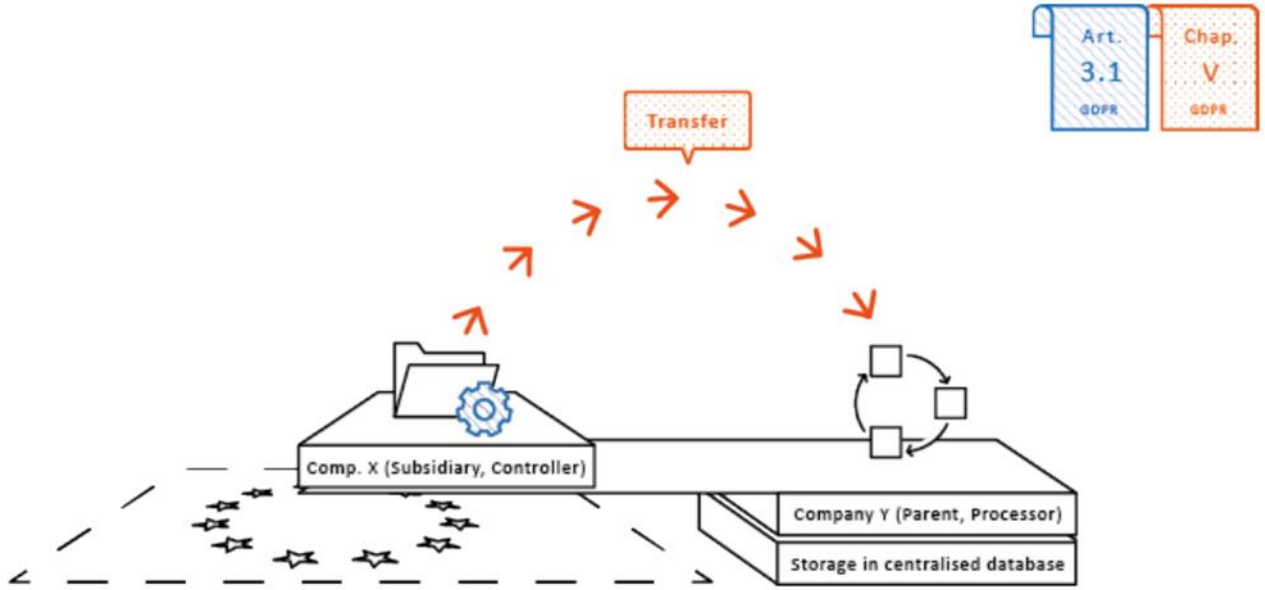
2. Kriterium: Exporteuer stellt Importeur personenbezogenen Daten durch Übermittlung oder auf andere Weise zur Verfügung

- **Beispiel 8:** Angestellter eines Verantwortlichen in der EU begibt sich auf eine Geschäftsreise in ein Drittland → kein Datentransfer nach Kapitel V



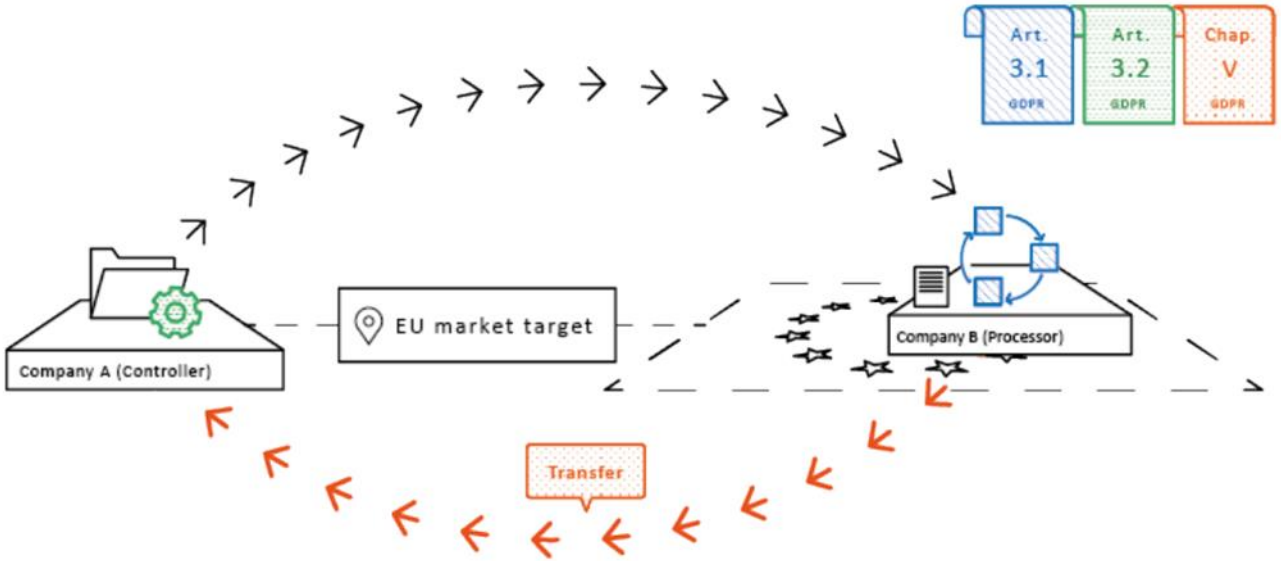
2. Kriterium: Exporteuer stellt Importeur personenbezogenen Daten durch Übermittlung oder auf andere Weise zur Verfügung

- **Beispiel 9:** Tochtergesellschaft (Verantwortlicher) in der EU teilt Daten mit ihrer Muttergesellschaft (Auftragsverarbeiter) in einem Drittland → Datentransfer nach Kapitel V



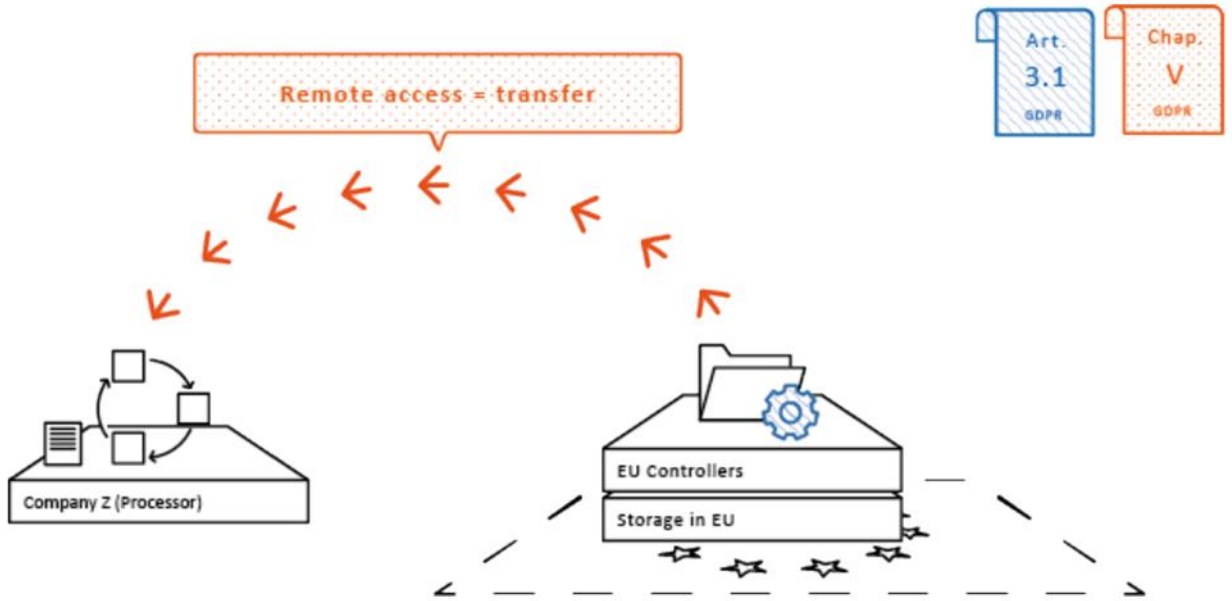
3. Kriterium: Importeur befindet sich in einem Drittland, unabhängig, ob er Art. 3 DSGVO unterliegt oder eine internationale Organisation ist

- **Beispiel 10:** Auftragsverarbeiter in der EU sendet Daten zurück an seinen Verantwortlichen in einem Drittland → Datentransfer nach Kapitel V



3. Kriterium: Importeur befindet sich in einem Drittland, unabhängig, ob er Art. 3 DSGVO unterliegt oder eine internationale Organisation ist

- **Beispiel 11:** Fernzugriff auf Daten in der EU durch einen Auftragsverarbeiter aus einem Drittland, der im Auftrag eines Verantwortlichen in der EU handelt → Datentransfer nach Kapitel V



Stellungnahme des EDSA (5/2023) zum EU-U.S.-Datenschutzrahmen

Republik Österreich Datenschutzbehörde

- Art. 70 Abs. 1 lit. s DSGVO
- Art. 45 Abs. 1 DSGVO - Datenübermittlung an ein Drittland oder eine internationale Organisation ohne weitere Instrumente oder einer besonderen Genehmigung erlaubt.
- 13. Dezember 2022 - Entwurf des Angemessenheitsbeschlusses für den „EU-US-Datenschutzrahmen“ - „EU-U.S. Data Privacy Framework“
- Lob für Verbesserungen, aber auch Bedenken

Stellungnahme des EDSA (5/2023) zum EU-U.S.-Datenschutzrahmen

Republik Österreich Datenschutzbehörde

Allgemeine Datenschutzgrundsätze

- Update der *Prinzipien* des EU-US-Datenschutzrahmens

ABER

  - keine wesentlichen Änderungen dieser Prinzipien sowie Rechtsbehelfe für betroffene Personen
  - zu weitgefasste Ausnahmen zum Auskunftsrecht
  - Fehlen von Schlüsseldefinitionen
  - mangelnde Klarheit über die Anwendung der Grundsätze für Auftragsverarbeiter

- spezifische Schutzmaßnahmen in den Bereichen der *automatisierten Entscheidungsfindung und des Profiling*

ABER

  - Notwendigkeit von spezifischen Vorschriften

Stellungnahme des EDSA (5/2023) zum EU-U.S.-Datenschutzrahmen

Republik Österreich Datenschutzbehörde

Zugriff von US-Behörden auf die aus der EU übermittelten personenbezogenen Daten für Zwecke der nationalen Sicherheit

- erheblichen Verbesserungen durch Durchführungsverordnung vom 7. Oktober 2022 („Executive Order [EO] 14086) von Präsident Biden
- Konzepte der *Notwendigkeit und Verhältnismäßigkeit* und *neuer Rechtschutzmechanismus* für EU-Bürger:

NEU

  - *„Civil Liberties Protection Officer“ (CLPO)* →
  - *„Data Protection Review Courts“ (DPRC)* →
  - *„Privacy and Civil Liberties Oversight Board“ (PCLOB*)

ABER

- allgemeine Standardantwort des DPRC

Stellungnahme des EDSA (5/2023) zum EU-U.S.-Datenschutzrahmen

Republik Österreich Datenschutzbehörde

<u>Zugriff von US-Behörden auf die aus der EU übermittelten personenbezogenen Daten für Zwecke der nationalen Sicherheit</u>

- EO 14086 sieht Liste *spezifischer Zwecke für Datensammlung* vor.

ABER

  - nicht unbedingt öffentliche Aktualisierung möglich
  - Fehlen einer unabhängigen *vorherigen* Genehmigung als auch einer systematischen unabhängigen *nachträglichen* Überprüfung von „bulk collection“ durch ein Gericht oder eine gleichwertige unabhängige Stelle

- weitere Überprüfungen mindestens alle *drei Jahre*

Report der 101 Task Force

- Koordinierung der 101 Beschwerden zu "Google Analytics" und "Facebook Business“
- <u>Datentransfer</u>
  - Keine Einhaltung von Kapitel V DSGVO, wenn die Übermittlung nach dem 16. Juli 2022 auf das „EU-U.S. Privacy Shield“ gestützt wurde.
  - *Keine Rückwirkung* der Standarddatenschutzklauseln gemäß Artikel 46 Abs. 2 lit. c DSGVO
  - *Verschlüsselung* durch den Datenimporteur ist uU. keine geeignete Maßnahme.
  - *Anonymisierungsfunktionen* sind keine geeignete Maßnahmen, wenn Anonymisierung erst nach der Datenübermittlung erfolgt.
  - Falls Auftragsverarbeiter Datenexporteur im Namen des Verantwortlichen (des Website-Betreibers) ist → Verantwortliche ist ebenso verantwortlich und haftet gemäß Kapitel V DSGVO.
  - Verantwortliche muss sicherstellen, dass der Auftragsverarbeiter ausreichende Garantien gemäß Artikel 28 DSGVO bietet.

Report der 101 Task Force

- Grundsatz der Rechenschaftspflicht
  - *Prüfungspflicht* der DSGVO-Konformität eines Tools durch Webseiten-Betreiber.
  - → *Nachweispflicht*, sonst Verstoß gegen Artikel 5 Abs. 2 und Artikel 24 Abs. 1 DSGVO.
  - auch Anbieter von Tools müssen kontinuierliche Einhaltung der DSGVO sicherstellen - als Verantwortlicher oder gemäß Art. 28 DSGVO.

- Rollenzuweisung
  - *Haftung* des Website-Betreibers möglich
  - Entscheidung für ein bestimmtes Tool → Festlegung der "Zwecke und Mittel" gemäß Artikel 4 Absatz 7 DSGVO
  - *Einzelfallanalyse objektiver Faktoren* → keine Einschränkung durch Abschluss von Vereinbarungen gemäß Artikel 28 oder Artikel 26 DSGVO

Report der 101 Task Force

- <u>Ergebnis der Beschwerden</u>
  - One-Stop-Shop-Verfahren, aber auch rein nationale Verfahren
  - *Anweisung* an Webseiten-Betreiber
    - Anforderungen von Kapitel V DSGVO zu erfüllen, und
    - erforderlichenfalls die fragliche Übermittlung zu stoppen.
  - Entscheidungen ohne Aussetzungsanordnung, falls Nutzung der fraglichen Instrumente vorher eingestellt wurde.
  - *zusätzliche Hinweise und praktische Empfehlungen* im Hinblick auf alternative Lösungen durch einige Aufsichtsbehörden
  - Noch offene Verfahren

Verbindlicher Beschluss des EDSA 1/2023

- 13. April 2023 - verbindlichen Beschluss zu einem Entscheidungsentwurf der irischen Datenschutzbehörde über die Rechtmäßigkeit der Datenübermittlung in die USA durch Meta Platforms Ireland Limited (Meta IE) für ihren Facebook-Dienst

- Entscheidung der Irischen Aufsichtsbehörde: Verbot des Datentransfers von Nutzerdaten aus Europa in die USA

- Entscheidung des EDSA, ob die endgültige Entscheidung der irischen Datenschutzbehörde
  - ein *Bußgeld und/oder*
  - eine *zusätzliche Anordnung* zur Anpassung der Verarbeitung enthalten muss.

- Finale Entscheidung der irischen Aufsichtsbehörde Mitte Mai 2023

Republik Österreich
Datenschutzbehörde

Danke für Ihre Aufmerksamkeit!