Schrems-II-Urteil des EuGH und die Folgen

EDSA – Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (Papier beschlossen am 10.11.2020)

EDSA-Roadmap für Datenexporteure:

Schritt 1: Prüfe Deine Datentransfers in Drittländer (Mapping)

Schritt 2: Identifiziere Deine Transfer-Tools (Instrumente im Sinne von Kapitel V DSGVO)

Schritt 3 – bei Artikel-46-Tools: Prüfe, ob die darin gegebenen Garantien angesichts der Rechtslage und Praxis in Drittland tatsächlich eingehalten werden können

Schritt 4 – wenn Antwort zu Schritt 3 „nein“ ist: Prüfe, ob zusätzliche Maßnahmen ergriffen werden können

Schritt 5 – Verfahrensfragen für den Fall „zusätzlicher Maßnahmen“

Schritt 6 – regelmäßige Reevaluierung des Schutzniveaus im Drittland

Schritt 1 – Prüfe Deine Datentransfers in Drittländer

- Ausgangspunkt: Verzeichnis der Verarbeitungstätigkeiten, ggf. Informationspflichten nach Artt. 13, 14 DSGVO
- auch Weiter-Übermittlungen (onward transfers) sind zu berücksichtigen (also auch Übermittlungen durch den ersten Empfänger in einem Drittland an weitere Empfänger (z.B. Unterauftragsverarbeiter) in Drittländern
- prüfe, ob Transfers auf das Erforderliche begrenzt sind (Grundsatz der Datenminimierung)
- Erinnerung: Fernzugriff (remote access) aus einem Drittland ist rechtlich eine Übermittlung in ein Drittland!
  - z.B. Wartung, Support

Schritt 2 – Identifiziere Deine Transfer-Tools im Sinne von Kapitel V DSGVO

- Bei Transfer in ein Drittland mit Angemessenheitsbeschluss (Art. 45 DSGVO): keine weiteren Schritte erforderlich
- Artikel-46-Transfertools (Standarddatenschutzklauseln, Binding Corporate Rules, Ad-Hoc-Datenexportvertrag,…)
- Ausnahmen nach Art. 49 DSGVO

Bei Transfers auf Basis von Transfertools nach Art. 46: Gehe zu Schritt 3

Schritt 3: Prüfe, ob die im Art.-46-Transfertool gegebenen Garantien angesichts von Recht und Praxis im Drittland eingehalten werden können

- Dieser entscheidende Prüfschritt wurde vom EuGH im Schrems-II-Urteil betont
- Für diese Prüfung ist der Datenexporteur zuständig, bei Bedarf in Zusammenarbeit mit dem Datenimporteur
- Zu prüfen ist, ob die Daten, die transferiert werden, unter Regelungen Drittland fallen, die die Einhaltung der Garantien aus dem Transfer-Tool negativ beeinträchtigen.
  - besonderes Augenmerk auf Regelungen, die den Behörden im Drittland Möglichkeiten des Zugangs zu den transferierten Daten eröffnen
- u.a. kann es auf Art und Kategorien der Daten ankommen, da sowohl
  - allgemeine Regelungen/Gesetze im Drittland zu berücksichtigen sind (z.B. Datenzugriffsregelungen im Bereich Strafverfolgung, Nachrichtendienste
  - als auch sektorale Regelungen/Gesetze, z.B. spezifische Datenzugangsmöglichkeiten für Aufsichtsbehörden in bestimmten Sektoren im Drittland

Schritt 3: Prüfe, ob die im Art.-46-Transfertool gegebenen Garantien angesichts von Recht und Praxis im Drittland eingehalten werden können

- Datenzugangsmöglichkeiten von Behörden dürfen nicht über das hinausgehen, was nach EU-Recht akzeptabel ist.
  - Standard ist hier Art. 52 EU-Grundrechtecharta (klare gesetzliche Basis erforderlich, Verhältnismäßigkeit)
  - Näheres dazu im „European Essential Guarantees“-Papier des EDSA (am 11.11.2020 überarbeitet und neu veröffentlicht)
- Das Recht im Drittland muss betroffenen Rechtsschutzmöglichkeiten gegen Datenzugriffe gewähren (vgl. Art. 47 EU-GRCh).
- Datenzugangsmöglichkeiten, die die EU-Standards einhalten, stehen nicht im Widerspruch zu den Artikel-46-Transfertools, wirken sich also nicht negativ auf die darin gegebenen Garantien aus.

Schritt 3: Prüfe, ob die im Art.-46-Transfertool gegebenen Garantien angesichts von Recht und Praxis im Drittland eingehalten werden können

- Zwei mögliche Ergebnisse der Prüfung:
  - (a) Rechtslage und Praxis des Drittlands haben keine negativen Auswirkungen auf die Garantien aus dem Transfertool.
    - In diesem Fall kann der Datenexport ohne weitere Maßnahmen durchgeführt werden.
  - (b) Rechtslage und Praxis im Drittland wirken sich negativ auf die Garantien aus dem Transfertool aus
    - in diesem Falle: gehe zu Schritt 4
    - Beispiel hierfür laut EDSA (unter Berufung auf EuGH, Schrems II:) die Regelungen im US-Gesetz FISA Section 702

Schritt 4: Prüfung, ob zusätzliche Maßnahmen möglich sind; wenn ja, sind diese anzuwenden

- Einzelfallbetrachtung notwendig dazu, ob und ggf. welche „zusätzlichen Maßnahmen“ möglich sind, um das Minus an Schutz, das aus der Situation im Drittland resultiert, zu kompensieren
- ganz grundsätzlich können Maßnahmen technischer, organisatorischer oder vertraglicher Art in Betracht gezogen werden
- Aber: vertragliche und organisatorische Maßnahmen alleine können in aller Regel das Problem von Datenzugängen durch drittstaatliche Behörden nicht kompensieren,
  - da die Behörden nicht daran gebunden werden können
  - sondern können allenfalls ergänzend zu evtl. möglichen technischen Maßnahmen als Lösung in Betracht kommen (Rn. 48)

Schritt 4: Prüfung, ob zusätzliche Maßnahmen möglich sind; wenn ja, sind diese anzuwenden

- Können keine effektiven zusätzlichen Maßnahmen gefunden werden, muss die Übermittlung unterbleiben bzw. beendet werden.
  - ggf. bereits übermittelte Daten müssen zurückgeholt oder vernichtet werden.
- Will der Exporteur „dennoch“ die Übermittlung durchführen, muss er die Aufsichtsbehörde informieren
  - Diese hat aber nicht die Aufgabe, den Transfer „irgendwie noch möglich zu machen“
  - Sondern wird den Transfer unter diesen Umständen förmlich untersagen
- Achtung: Die Aufsichtsbehörden haben nicht die allgemeine Aufgabe einer Beratung im Einzelfall für jegliche Vorschläge/Ideen für potentielle „zusätzliche Maßnahmen“
  - Das wäre nicht leistbar.
  - Die Verantwortung der Einschätzung der Wirksamkeit „zusätzlicher Maßnahmen“ liegt vielmehr beim Datenexporteur! Es gibt auch keine Notifizierungs- oder Abstimmungspflicht mit der Aufsichtsbehörde
  - wird zwar nicht explizit im Papier gesagt, ergibt sich aber als Gegenschluss

Schritt 5 – Verfahrensschritte, wenn zusätzliche Maßnahmen identifiziert wurden

- **bei Standarddatenschutzklauseln (SCCs)**
  - „zusätzliche Maßnahmen“ machen den Datentransfer nicht genehmigungsbedürftig, solange sie nicht im Widerspruch zu den SCCs stehen
  - In aller Regel dürfte das bei „zusätzlichen Maßnahmen“ so sein, da sie ja gerade ein Plus an Schutz gewährleisten sollen.
- **Bei BCR und Ad-Hoc-Datentransferverträge (ad hoc contractual clauses)**
  - Die Aussagen des Schrems-II-Urteils beanspruchen auch Geltung für BCR und ad hoc Clauses, da diese wie SCC rein vertragliche Instrumente sind.
  - Der EDSA wird zu BCR im Rahmen der Überarbeitung der Papiere zu den BCR (Working Papers 256, 257) Details mitteilen.
  - Nach vorläufiger Meinung des BayLDA gehören „zusätzliche Maßnahmen“ nicht zum Prüfungsumfang der Aufsichtsbehörden bei der Genehmigung einer BCR, denn sie sind (dritt-)länderspezifisch und ggf. sogar Datenimporteur-spezifisch.

Schritt 6 – regelmäßige Reevaluierung

- Der Datenexporteur muss die Entwicklung im Drittland laufend verfolgen, bei Bedarf in Kooperation mit dem Datenimporteur (Begründung: Rechenschaftspflicht)
- Bei Neuentwicklungen, die sich negativ auf die Garantien und/oder auf die „zusätzlichen Maßnahmen“ auswirken, muss die Übermittlung beendet werden.

Beispiele für „zusätzliche Maßnahmen“ (Annex 2 des EDSA-Papiers)

Der EDSA betont, dass es sich bei den genannten Beispielen nicht um „Patentrezepte“ oder one-fits-all-Ansätze und auch nicht um eine abschließende Liste handelt, sondern nur um eine Art Toolbox, aus der je nach Fall ggf. ausgewählt werden kann – und dass es aber Fälle gibt, in denen u.U. keine effektiven Maßnahmen gefunden werden können, um die Defizite auszugleichen.

- Maßnahmen technischer Art
- Maßnahmen organisatorischer Art
- Maßnahmen vertraglicher Art

Beispiele für „zusätzliche Maßnahmen“ (Annex 2 des EDSA-Papiers)

- **Technische Maßnahmen**
  - Hier geht es um die Verhinderung des Datenzugriffs durch Behörden (sofern dieser über das hinausgeht, was nach EU-Recht akzeptabel ist)
  - Oder aber Maßnahmen, die zwar den Datenzugriff als solchen evtl. nicht verhindern, jedoch dafür sorgen, dass betroffene Personen
    - nicht identifiziert werden können
    - und auch nicht „singularisiert“ werden können
    - d.h. dass selbst wenn die Behörde zwar Zugang zu den Daten nehmen kann, „sie mit den Daten überhaupt nichts anfangen kann, was irgendeine Auswirkung auf betroffene Personen haben könnte

Beispiele für „zusätzliche Maßnahmen“ (Annex 2 des EDSA-Papiers)

- **Technische Maßnahmen**
  - Mögliche Datenzugriffe kann es geben
    - Während des Übermittlungsvorgangs (data in transit), also z.B. in Kabeln
    - Nachdem die Daten beim Empfänger angekommen sind

Beispiele für „zusätzliche Maßnahmen“ (Annex 2 des EDSA-Papiers)

Use Case 1 – (reine) Speicherung/Backup von Daten; für die Funktionalität ist kein Zugang zu Klartext-Daten erforderlich

- Die Daten müssen vor der Übermittlung stark verschlüsselt werden
- Verschlüsselungs-Algorithmus und dessen Parametrisierung (z.B. Schlüssellänge) entspreched dem Stand der Technik…
- Stärke der Verschlüsselung berücksichtigt die Dauer des notwendigen Schutzes
- Korrekte Implementierung des Verschlüsselungsalgorithmus
- Verlässliches Schlüssel-Management
- Schlüssel verbleiben beim Datenexporteur oder jedenfalls einem damit Beauftragen in der EU
- also Schlüssel darf nicht beim Datenimporteur sein

Fazit: In *diesem* Use Case ist es also denkbar, mit Hilfe von Verschlüsselung den Transfer zu ermöglichen.

Beispiele für „zusätzliche Maßnahmen“ (Annex 2 des EDSA-Papiers)

Use Case 2 – Transfer pseudonymisierter Daten

- ist durchaus eine kontrovers diskutierte Konstellation, da pseudonymisierte Daten immer noch Personenbezug aufweisen
- D.h. bei Datenzugriffe durch Behörden geht es darum, zu verhindern, dass die Daten in irgendeiner Weise für die Behörden „nutzbar“ sind

Voraussetzungen für Wirksamkeit der Pseudonymisierung

- Die „Zuordnungsliste“ verbleibt allein beim Datenexporteur bzw. ggf. Beauftragtem in der EU.
- akzeptabel sind nur Situationen, in denen ein Datenzugriff unter keinen Umständen irgendwelche negativen Folgen für Betroffene führen kann; die Behörden dürfen nicht in der Lage sein, anhand der (pseudonymisierten) Daten den Betroffenen irgendwie zu „singularisieren“
- …

Fazit: Bei Pseudonymisierung ist eine Einzelfallbetrachtung angezeigt, ob sie in concreto als „zusätzliche Maßnahme“ geeignet ist oder nicht.

Beispiele für „zusätzliche Maßnahmen“ (Annex 2 des EDSA-Papiers)

Use Case 3 – Verschlüsselte Daten, die durch Drittland durchgeleitet und in ein sicheres Drittland (Art. 45 DSGVO) übermittelt werden

Hier geht es um die Verhinderung von Datenzugriffen während des Transits durch ein „unsicheres“ Drittland, insbesondere über das Internet.

- Transportverschlüsselung
- Entschlüsselung im unsicheren Drittland muss ausgeschlossen sein
- keine Backdoors
- Algorithmus und Parametrisierung (Schlüssellänge…) sind Stand der Technik und berücksichtigen die Ressourcen und Fähigkeiten drittstaatlicher (Sicherheits-)Behörden
- u.a. (Näheres siehe im EDSA-Papier)

Beispiele für „zusätzliche Maßnahmen“ (Annex 2 des EDSA-Papiers)

Use Case 4, betrifft einen gewissen Sonderfall – Empfänger, der besonderen Schutz genießt

Hier geht es um Empfänger im Drittland, die nach dortigem Recht einen besonderen Schutz genießen.

- Es muss feststehen, dass das Recht des Drittlands den Empfänger vor behördlichen Datenzugriffen, die nach EU-Recht nicht akzeptabel wären, schützt (z.B. bestimmte Berufsgeheimnisträger)
- Und dass die Daten, um die es geht, davon umfasst sind
  - eventuelle Auftragsverarbeiter berücksichtigen!
- Daten werden vor der Übermittlung verschlüsselt, der Schlüssel ist beim (besonders geschützten) Datenempfänger
- u.a. (siehe EDSA-Papier)

Beispiele für „zusätzliche Maßnahmen“ (Annex 2 des EDSA-Papiers)

Use Case 5 – Multi-Party Processing - Daten werden an mehrere Auftragsverarbeiter in unterschiedlichen Drittländern übermittelt

- die Daten werden so aufgeteilt, dass jeder „Teilset“ nicht mehr einer bestimmten oder bestimmbaren Person zugeordnet werden kann
- Multi-party computation dergestalt, dass die Trennung der Information auch während der gemeinsamen Verarbeitung gewahrt bleibt.
- keine „Kollaboration“ zwischen Sicherheitsbehörden in den einzelnen betroffenen Drittländern, die es ihnen erlauben würde, die Teilsets zusammenzufügen
- u.a. (vgl. EDSA-Papier)

Achtung: Nun Beispiele, in denen KEINE „zusätzliche Maßnahmen“ gefunden werden können (Annex 2 des EDSA-Papiers)

Use Case 6 – Übermittlung an Cloud Service Provider, die Zugang zu Klartext-Daten benötigen

Sehr praxisrelevant, betrifft wohl die meisten Software-as-a-Service-Anwendungen!

- Wenn der Empfänger oder ein Subdienstleister für die Funktionalitäten der Dienstleistung Zugang zu unverschlüsselten Daten benötigt,
- und drittstaatliche Behörden Zugriffsrechte haben, die über das nach EU-Recht zulässige Maß überschreiten,
- Können Transportverschlüsselung und auch (zwischenzeitliche) Data-at-Rest-Verschlüsselung nicht helfen,
  - Da wegen der Notwendigkeit des Datenzugriffs durch den Empfänger auf unverschlüsselte Daten die Verschlüsselung ja zeitweise aufgehoben werden muss.

Fazit: in diesen – sehr relevanten – Fällen gibt es nach derzeitigem Stand keine wirksamen „zusätzlichen Maßnahmen“

Achtung: Nun Beispiele, in denen KEINE „zusätzliche Maßnahmen“ gefunden werden können (Annex 2 des EDSA-Papiers)

Use Case 7 – Fernzugriff (Remote Access) für geschäftliche Zwecke

Gemeint sind hier z.B. gemeinsam genutzte Datenbanken in Unternehmensgruppen

Vorbemerkung:

- *bitte immer bedenken: Problematisch sind Datentransfers nur dann, wenn der Datenempfänger unter eine gesetzliche Regelung im Drittland fällt, die Datenzugriffe durch dortige Behörden jenseits des nach EU-Recht Zulässigen ermöglicht.*
  - *bei Empfängern in den USA insbesondere etwa „Electronic Communication Service Providers“ (ECSP), da diese unter FISA Section 702 fallen*
- *bei Datenbanken / gemeinsame Systeme im Konzern ist zu prüfen, ob der US-Datenempfänger darunter fällt*
- *Dies kann aber z.B. schon der Fall sein, wenn ein E-Mail-Server angeboten wird (ist aber im Einzelnen zu prüfen!)*
  - *Der EDSA hat KEINE Prüfung des Anwendungsbereichs von FISA Sect. 702 vorgenommen und plant dies auch nicht in absehbarer Zeit, soweit ersichtlich.*

Achtung: Nun Beispiele, in denen KEINE „zusätzliche Maßnahmen“ gefunden werden können (Annex 2 des EDSA-Papiers)

Use Case 7 – Fernzugriff (Remote Access) für geschäftliche Zwecke

Szenario:

- Datentransfer durch Bereitstellung der Daten in ein gemeinsam genutztes Informationssystem
- Datenempfänger kann nach eigenem Belieben für eigene Zwecke auf die Daten zugreifen

Fazit: in diesen – sehr relevanten – Fällen gibt es nach derzeitigem Stand keine wirksamen „zusätzlichen Maßnahmen“

Beispiele für „zusätzliche Maßnahmen“ (Annex 2 des EDSA-Papiers)

Vertragliche Maßnahmen, organisatorische Maßnahmen (Rn. 92 ff. des EDSA-Papiers)

- EDSA betont, dass vertragliche / organisatorische Maßnahmen alleine keine effektiven „zusätzlichen Maßnahmen“ gegen Datenzugriffsmöglichkeiten von Behörden darstellen
- können daher, je nach Fall, beim Thema „Datenzugriffe durch Behörden im Drittland“ lediglich u.U. als Ergänzung zu technischen Maßnahmen in Betracht kommen
- Bei Problemen anderer Art als „Datenzugriffe durch Behörden“ können vertragliche / organisatorische Maßnahmen aber u.U., als „zusätzliche Maßnahmen“ in Betracht kommen.

Beispiele (im Sinne einer Toolbox)

- Verstärkte Berichtspflichten / Transparenzpflichten für den Datenimporteur betreffend Datenzugriffe durch Behörden
  - z.B. Aufnahme einer Anlage zum SCC, in der der Datenimporteur Informationen zur Rechtslage in Sachen Nachrichtendienste liefert

Beispiele für „zusätzliche Maßnahmen“ (Annex 2 des EDSA-Papiers)

Vertragliche Maßnahmen, organisatorische Maßnahmen (Rn. 92 ff. des EDSA-Papiers)

Beispiele (Fortsetzung):

- Versicherung des Importeurs, keine „Backdoors“ für Behörden zu liefern
- Verstärkte Verpflichtungen des Importeurs, den Exporteur über Änderungen der Rechtslage im Drittland zu informieren, bevor solche in Kraft treten
- „Warrant Canary“ – regelmäßige Bestätigung durch den Importeur, dass er keine Aufforderung zur Offenlegung von Daten an Behörden erhalten hat (-> das Fehlen einer solchen Meldung bedeutet, dass es eine Aufforderung gab)
- Verpflichtung des Importeurs, die Rechtmäßigkeit von Datenoffenlegungs-Anordnungen nach dem Recht des Drittlands zu prüfen und bei Zweifeln dagegen gerichtlich vorzugehen
- Verpflichtung des Importeures, die Behörde zu informieren, dass die Offenlegung gegen seine Pflichten aus dem Transfer-Tool verstoßen würde
- Verpflichtung des Exporteurs und/oder Importeurs, betroffene Personen bei der Ausübung ihrer Rechte zu unterstützen

Beispiele für „zusätzliche Maßnahmen“ (Annex 2 des EDSA-Papiers)

Vertragliche Maßnahmen, organisatorische Maßnahmen (Rn. 92 ff. des EDSA-Papiers)

- Ernennung eines Teams, das für das Thema „Datenoffenlegungen von Daten aus der EU gegenüber Behörden“ zuständig ist
- Dokumentation aller Anforderungen zur Offenlegung von Daten aus der EU, Offenlegung an den Datenexporteur
- Transparency Reports
- …

Beispiele für „zusätzliche Maßnahmen“ (Annex 2 des EDSA-Papiers)

Das Papier des EDSA ist nun in eine Öffentliche Konsultation gegeben worden:

https://edpb.europa.eu/edpb_en ,

dort unter

„Our Work and Tools“

/ GDPR: Guidelines, Recommendations, Best Practices,

-> Recommendations 01/2020 on measures that supplement transfer tools…
(https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer_en)

Bis 30.11.2020 können alle Interessierten das Papier kommentieren.

Das bedeutet aber **nicht** irgendeine Grace Period / Übergangszeit für die Umstellung der Datenverarbeitungen.

WAS HEISST DAS NUN?

Empfehlungen für Datenexporteure bei Übermittlungen in Drittländer

1.) Bestandsaufnahme aller Übermittlungen Drittländer machen:

- In welche Länder wird übermittelt?
- Welche Daten?
- Welches „Instrument“ wird für die jeweilise Übermittlung genutzt?
  - angemessenes Datenschutzniveau (Art. 45)?
  - Vertragliche Garantie-Instrumente nach Art. 46, z.B. Standarddatenschutzklauseln, BCR,…?
  - Ausnahmeerlaubnisse nach Art. 49?

WAS HEISST DAS NUN?

Empfehlungen für Datenexporteure bei Übermittlungen in Drittländer

2.) Klärung der Rechtslage im Drittland, insbesondere betreffend Datenzugriffsmöglichkeiten dortiger Behörden

- Kontaktaufnahme mit dem jeweiligen Datenimporteur (Empfänger)
- Darstellung der Problematik
- Frage, in welchem Umfang Behörden dort Zugriff auf die übermittelten Daten nehmen können – i.d.R. wird man um eine genauere rechtliche Analyse / Gutachten nicht herumkommen
- Klären im Einzelfall, anhand des konkreten Datentransfers, inwieweit gerade in diesem Fall Zugriffsmöglichkeiten der Drittstaatsbehörden bestehen (
  - bei USA – zentrale Frage: Klären, ob der Empfänger unter die Pflichten zur Zugangsgewährung an Nachrichtendienste nach FISA Section 702 fällt
  - **Achtung: Auch die Weiterübermittlung an Sub-Dienstleister prüfen!**

WAS HEISST DAS NUN?

Empfehlungen für Datenexporteure bei Übermittlungen in Drittländer

3.) Risikoanalyse für den konkreten Datentransfer

- Können Drittstaatsbehörden Zugriff gerade auf diese Daten nehmen? In welchem Umfang?
- Entsprechen die Zugriffsmöglichkeiten dem Standard des EU-Rechts (Erforderlichkeit, Verhältnismäßigkeit) – hierzu meist nähere rechtliche Analyse nötig -> Anfordern!
- Haben die betroffenen Personen Rechtsschutzmöglichkeiten? – auch hier meist nähere Analyse nötig
- Wenn im Ergebnis kein vergleichbares Schutzniveau mit der EU besteht, muss nach zusätzlichen Maßnahmen gesucht werden, z.B. Verschlüsselung.
- Wenn auch diese nicht ausreichen, ist der Transfer **unzulässig**.
- Wenn der Transfer fortgesetzt werden soll, muss die Datenschutzbehörde informiert werden (siehe EDSA-FAQ zu Schrems II).
    - Diese wird aber den Transfer, wenn kein mit der EU vergleichbares Schutzniveau gewährleistet ist, untersagen bzw. beenden.

Noch Fragen?

Vielen Dank