TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

"T.I.S.P. Community Meeting 2021"

Berlin, 03.-04.11.2021

Schrems II und die Folgen

Eva Schlehahn

EDV-Unternehmensberatung Floß GmbH

Eva Schlehahn

EDV- Unternehmensberatung Floß GmbH

Hopfengarten 10, 33775 Versmold

Telefon: 05423 964900

E-Mail: eva.schlehahn@floss-consult.de

EDV-Unternehmensberatung
Floß GmbH

- Das Schrems II Urteil
- Folgen für Verantwortliche
- Lösung neue EU-Standardvertragsklauseln?
- Strategie + Transferfolgenabschätzung (TIA)
- Anhang (optional): Verschiedene Fallkonstellationen USA

USA = Drittland ohne hinreichendes Datenschutzniveau

- Deswegen spezifische Legitimation von Datentransfers notwendig
- Eine Lösung war: Datenschutz-Abkommen zwischen EU + USA

Safe Harbor Abkommen in 2015 vom EuGH für unwirksam erklärt

- Sogenanntes „**Schrems I**“ Urteil

Privacy Shield im Juli 2020 vom EuGH für unwirksam erklärt

- Sogenanntes „**Schrems II**“ Urteil
  - Adressiert auch die EU Standardvertragsklauseln

Die Gesetzeslage in den USA

Eine besondere Herausforderung…

- FISA 702 + Cloud Act
  - Gelten für Anbieter elektronischer Kommunikation
  - Gewähren US Ermittlungsbehörden + Geheimdiensten Zugriff auf Daten mittels Herausgabeanordnungen an US Unternehmen
  - Über Cloud Act auch Tochterfirmen in EWR betroffen
  - Rechtsschutz für EU Bürger (-)
  - Oft Schweigeverpflichtungen (National Security Letter, NSL, „gag order“)
  - Rechtsschutz US-Unternehmen gegen NSL (-)

- Generelle Überwachung v. NSA & Co.
  - Executive Order (EO) 12333, Presidential Policy Directive (PPD) 28
  - Siehe Snowden Enthüllungen: Anzapfen von Unterseekabeln, Programme wie PRIMS, UPSTREAM etc.

- Unverhältnismäßige Verarbeitung personenbezogener Daten von EU-Bürger*innen durch amerikanische Behörden
  - Strafverfolgungsbehörden
  - Geheimdienste

- Kein wirksamer Rechtsschutz für EU-Bürger*innen durch das Privacy Shield

= Kein angemessenes Schutzniveau in den USA!

Gültigkeit der EU Standardvertragsklauseln
(engl. Standard Contract Clauses, SCC):
Ja, aber unter Vorbehalt

➢ **Es kommt auf die faktische Einhaltung des Schutzniveaus im Einzelfall an**

Im Fall USA:

- Nachprüfung des Schutzniveaus definitiv notwendig aufgrund der Feststellungen des EuGH

Im Fall UK: KEIN Drittlandstatus

- Angemessenheitsbeschluss der Europäischen Kommission!
- Der erste Versuch scheiterte, der zweite ging durch

- ABER:
  - Unklar, ob dieser Bestand behält (Bemängelung d. EU Parlaments + EDSA, Schrems III?)
  - Auch in Großbritannien umfassende Überwachungsgesetzgebung
  - Gesetzgeberische Abweichungen von der DSGVO zu erwarten -> August 2021: Maßnahmenpaket der Britischen Regierung zur Änderung des Datenschutzrechts
  - Rechtsschutz für EU Bürger unklar


Das Schrems II Urteil
Folgen für Verantwortliche
Lösung neue EU-Standardvertragsklauseln?
Strategie + Transferfolgenabschätzung (TIA)
Anhang (optional): Verschiedene Fallkonstellationen USA

Privacy Shield ist keine Legitimation mehr für Datentransfers

Somit sind alle Anwendungen, welche auf dem Privacy Shield Abkommen beruhen:

- Sofort auf eine andere Rechtsgrundlage zu stellen
- Betrieb auf on premise zu stellen oder
- ABZUSCHALTEN!

Alternative Grundlage EU-Standardvertrag?

Grundsätzlich (+), aber:

- Prüfung der faktischen Einhaltbarkeit
  und
- ggf. ergänzende Garantien erforderlich

➢ Abhängig vom Schutzniveau im jeweiligen Drittland

➢ Es gibt KEINE Übergangsfristen // die Aufsichtsbehörden (AB) fangen derzeit mit koordinierten Prüfungen zur Umsetzung des Schrems II Urteils an

Mindestens 80% der US-Dienste sind somit nicht mehr ohne erneute Betrachtung/Prüfung nutzbar.

Beispiele:

Microsoft Office 365, Amazon AWS, WhatsApp, Google, Facebook, Twitter, Instagram, LinkedIn, Monday.com, Dropbox, HubSpot, Airship…


Das Schrems II Urteil
Folgen für Verantwortliche
Lösung neue EU-Standardvertragsklauseln?
Strategie + Transferfolgenabschätzung (TIA)
Anhang (optional): Verschiedene Fallkonstellationen USA

Durchführungsbeschluss neue Standardvertragsklauseln am 4.6.2021

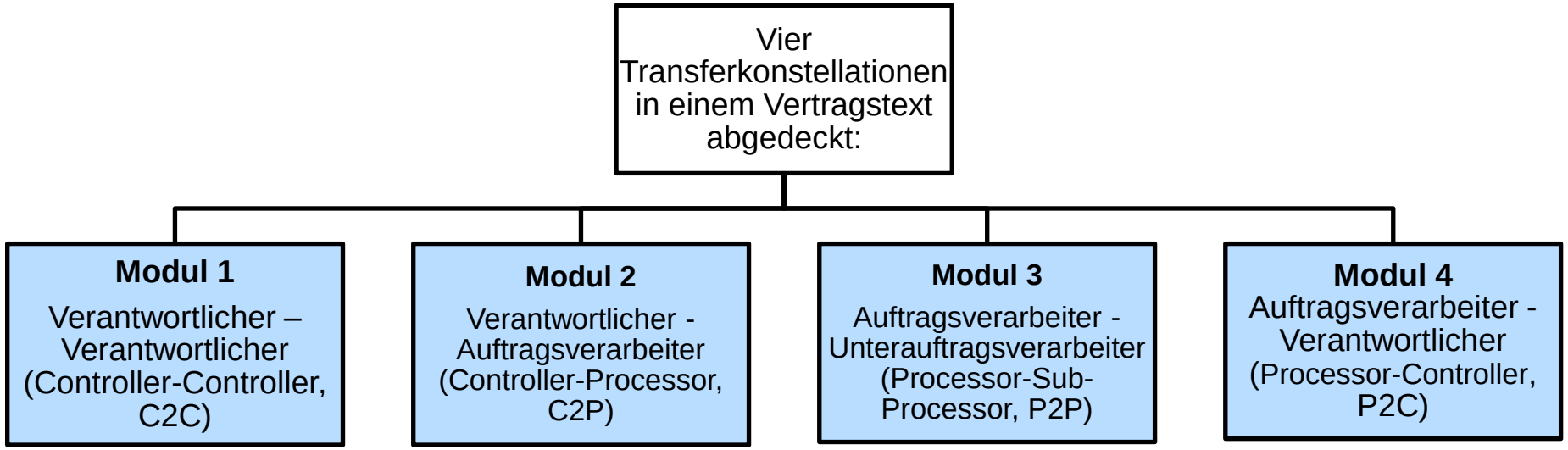
2 Sets von Standardvertragsklauseln:

1. Für Datenübermittlung zw. Verantwortlichen und Auftragsverarbeiter
   - Erstmalig EU-weite einheitliche Vertragsvorlage für Auftragsverarbeitungen innerhalb der EU
   - Nicht verbindlich

2. Für Datenübermittlung in Drittländer
   - Offizielle Veröffentlichung im Amtsblatt am 7. Juni 2021 (OJL 199)
   - Beginn der Übergangsfristen 20 Tage nach Amtsblatt-Veröffentlichung = Fristbeginn 27. Juni 2021
   - Übergangsfrist 18 Monate (3+15)
     - Unwirksamkeit der alten Standardvertragsklauseln: Seit 27 Sept 2021!
     - Update aller alten Verträge bis: 27 Dez 2022

- Anpassung an die DSGVO
  - I.d.R. kein zusätzlicher Auftragsverarbeitungsvertrag nötig, da Anforderungen des Art. 28 DSGVO eingebunden werden
- Garantie für Drittstaatentransfer gemäß Art. 46 Abs. 2 lit. c) DSGVO
- Einbindung Anforderungen des EuGH im Schrems II Urteil (+/-?)

- Erweiterungen im Vergleich zu den bisherigen SCC
  - Bisher gab es in den alten SCC die Konstellationen:
    - Verantwortlicher – Verantwortlicher
    - Verantwortlicher – Auftragsverarbeiter
  - Neu sind nun:
    - Auftragsverarbeiter - Unterauftragsverarbeiter
    - Auftragsverarbeiter - Verantwortlicher



Es sind dann die jeweils für die Vertragspartner relevanten Module auszuwählen und abzuschließen.

☐ Modul 1: Verantwortliche – Verantwortliche (C2C)	☐ Modul 2: Verantwortliche-Auftragsverarbeiter (C2P)	☐ Modul 3: Auftragsverarbeiter-Auftragsverarbeiter (P2P)	☐ Modul 4: Auftragsverarbeiter-Verantwortliche (P2C)

Die Klausel 1, 2 und 4-6 gelten für alle Module. In Klausel 3 ist farblich hervorgehoben, was pro Modul gilt. Klausel 7 ist optional nach Bedarf und dort mit entsprechendem Ankreuz-Häkchen versehen.

ANHANG

STANDARDVERTRAGSKLAUSELN

ABSCHNITT I

Klausel 1 - Zweck und Anwendungsbereich

a) Mit diesen Standardvertragsklauseln soll sichergestellt werden, dass die Anforderungen der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz- Grundverordnung) bei der Übermittlung personenbezogener Daten an ein Drittland eingehalten werden.

b) Die Parteien:

i) die in Anhang I.A aufgeführte(n) natürliche(n) oder juristische(n) Person(en), Behörde(n), Agentur(en) oder sonstige(n) Stelle(n) (im Folgenden „Einrichtung(en)"), die die personenbezogenen Daten übermittelt/n (im Folgenden jeweils „Datenexporteur"), und

ii) die in Anhang I.A aufgeführte(n) Einrichtung(en) in einem Drittland, die die personenbezogenen Daten direkt oder indirekt über eine andere Einrichtung, die ebenfalls Partei dieser Klauseln ist, erhält/erhalten (im Folgenden jeweils „Datenimporteur"),
haben sich mit diesen Standardvertragsklauseln (im Folgenden „Klauseln") einverstanden erklärt.

c) Diese Klauseln gelten für die Übermittlung personenbezogener Daten gemäß Anhang I.B.

d) Die Anlage zu diesen Klauseln mit den darin enthaltenen Anhängen ist Bestandteil dieser Klauseln.

Klausel 2 - Wirkung und Unabänderbarkeit der Klauseln

a) Diese Klauseln enthalten geeignete Garantien, einschließlich durchsetzbarer Rechte betroffener Personen und wirksamer Rechtsbehelfe gemäß Artikel 46 Absatz 1 und Artikel 46 Absatz 2 Buchstabe c der Verordnung (EU) 2016/679 sowie — in Bezug auf Datenübermittlungen von Verantwortlichen an Auftragsverarbeiter und/oder von Auftragsverarbeitern an Auftragsverarbeiter — Standardvertragsklauseln gemäß Artikel 28 Absatz 7 der Verordnung (EU) 2016/679, sofern diese nicht geändert werden, mit Ausnahme der Auswahl des entsprechenden Moduls oder der entsprechenden Module oder der Ergänzung oder Aktualisierung von Informationen in der Anlage. Dies hindert die Parteien nicht daran, die in diesen Klauseln festgelegten Standardvertragsklauseln in einen umfangreicheren Vertrag aufzunehmen und/oder weitere Klauseln oder zusätzliche Garantien hinzuzufügen, sofern diese weder unmittelbar noch mittelbar im Widerspruch zu diesen Klauseln stehen oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneiden.

b) Diese Klauseln gelten unbeschadet der Verpflichtungen, denen der Datenexporteur gemäß der Verordnung (EU) 2016/679 unterliegt.

Klausel 3 – Drittbegünstigte	**Klausel 3 – Drittbegünstigte**	**Klausel 3 – Drittbegünstigte**	**Klausel 3 – Drittbegünstigte**
a) Betroffene Personen können diese Klauseln als Drittbegünstigte gegenüber dem Datenexporteur und/oder dem Datenimporteur geltend machen und durchsetzen, mit folgenden Ausnahmen:	a) Betroffene Personen können diese Klauseln als Drittbegünstigte gegenüber dem Datenexporteur und/oder dem Datenimporteur geltend machen und durchsetzen, mit folgenden Ausnahmen:	a) Betroffene Personen können diese Klauseln als Drittbegünstigte gegenüber dem Datenexporteur und/oder dem Datenimporteur geltend machen und durchsetzen, mit folgenden Ausnahmen:	a) Betroffene Personen können diese Klauseln als Drittbegünstigte gegenüber dem Datenexporteur und/oder dem Datenimporteur geltend machen und durchsetzen, mit folgenden Ausnahmen:
i) Klausel 1, Klausel 2, Klausel 3, Klausel 6, Klausel 7	i) Klausel 1, Klausel 2, Klausel 3, Klausel 6, Klausel 7	i) Klausel 1, Klausel 2, Klausel 3, Klausel 6, Klausel 7	i) Klausel 1, Klausel 2, Klausel 3, Klausel 6, Klausel 7
ii) Klausel 8 — Modul eins: Klausel 8.5 Buchstabe e und Klausel 8.9 Buchstabe b Modul zwei: Klausel 8.1 Buchstabe b, Klausel 8.9 Buchstaben a, c, d und e Modul drei: Klausel 8.1 Buchstaben a, c und d und Klausel 8.9 Buchstaben a, c, d, e, f und g Modul vier: Klausel 8.1 Buchstabe b und Klausel 8.3 Buchstabe b	ii) Klausel 8 — Modul eins: Klausel 8.5 Buchstabe e und Klausel 8.9 Buchstabe b Modul zwei: Klausel 8.1 Buchstabe b, Klausel 8.9 Buchstaben a, c, d und e Modul drei: Klausel 8.1 Buchstaben a, c und d und Klausel 8.9 Buchstaben a, c, d, e, f und g Modul vier: Klausel 8.1 Buchstabe b und Klausel 8.3 Buchstabe b	ii) Klausel 8 — Modul eins: Klausel 8.5 Buchstabe e und Klausel 8.9 Buchstabe b Modul zwei: Klausel 8.1 Buchstabe b, Klausel 8.9 Buchstaben a, c, d und e Modul drei: Klausel 8.1 Buchstaben a, c und d und Klausel 8.9 Buchstaben a, c, d, e, f und g Modul vier: Klausel 8.1 Buchstabe b und Klausel 8.3 Buchstabe b	ii) Klausel 8 — Modul eins: Klausel 8.5 Buchstabe e und Klausel 8.9 Buchstabe b Modul zwei: Klausel 8.1 Buchstabe b, Klausel 8.9 Buchstaben a, c, d und e Modul drei: Klausel 8.1 Buchstaben a, c und d und Klausel 8.9 Buchstaben a, c, d, e, f und g Modul vier: Klausel 8.1 Buchstabe b und Klausel 8.3 Buchstabe b
iii) Klausel 9 — Modul zwei: Klausel 9 Buchstaben a, c, d und e Modul drei: Klausel 9 Buchstaben a, c, d und e	iii) Klausel 9 — Modul zwei: Klausel 9 Buchstaben a, c, d und e Modul drei: Klausel 9 Buchstaben a, c, d und e	iii) Klausel 9 — Modul zwei: Klausel 9 Buchstaben a, c, d und e Modul drei: Klausel 9 Buchstaben a, c, d und e	iii) Klausel 9 — Modul zwei: Klausel 9 Buchstaben a, c, d und e Modul drei: Klausel 9 Buchstaben a, c, d und e

Einschränkungen:

- Relevanz Modul 4?
- SCC laut Kommission nicht anwendbar bei Dienstleistern aus Drittland, die der DSGVO unterfallen

➢ Details zu diesen Punkten gleich ☺

- Abschnitt I (Klauseln 1-7) -> Allgemeines (Zweck, Scope…)
- Abschnitt II (Klauseln 8-13) -> Regelt die Pflichten der Parteien
- Abschnitt III (Klauseln 14 + 15)
  - Lokale Rechtsvorschriften und Pflichten im Falle des Zugangs von Behörden zu Daten -> hier ist das Schrems II Urteil adressiert
- Abschnitt IV Schlussbestimmungen (Klauseln 16-18)
- Anlagen:
  - Anhang I:
    - A. Liste der Parteien
    - B. Beschreibung der Datenübermittlung
    - C. Zuständige Aufsichtsbehörde
  - Anhang II:
    - Technische und organisatorische Maßnahmen, einschließlich zur Gewährleistung der Sicherheit der Daten
  - Anhang III:
    - Liste der Unterauftragsverarbeiter

- Vorrang vor widersprechenden AGB und Hauptverträgen
- Eigene Haftungsregeln, Ausschluss von Haftungsbeschränkungen

- Einbeziehung von Dritten in die Schutzwirkung des Vertrags (Drittbegünstigungsklausel)
- Beitritt von Dritten zum Vertrag vorgesehen (Kopplungsklausel)

- Wahl des anwendbaren (EU-)Rechts und des Gerichtsstandes

- Verpflichtungen des Datenimporteurs
  - zur Abwehr von Regierungsanfragen
  - zur Dokumentation und Information von EU-Verantwortlichen und Aufsichtsbehörden
  - Umfangreiche Rechenschaftspflichten

Möglicherweise juristisch knifflig:

Neuer Baustein Auftragsverarbeiter- Verantwortlicher (Modul 4)

- Offensichtlich sollen Fälle abgedeckt werden, wo Unternehmen mit Sitz in einem Drittland einen Dienstleister in der EU beauftragen
- Also z.B. ein EU-Auftragnehmer, der Daten von Betroffenen aus den USA verarbeiten soll.

➢ Knackpunkt: Unterfällt diese Konstellation überhaupt der Definition des Drittlandtransfers nach Art. 44 DSGVO?

Anwendungsausschluss in dem ErwG 7
Inhalt, grob zusammengefasst:

- SCC -> sollenGarantie bei Drittlandübermittlungen sein.
- Aber sollen nicht genutzt werden, wenn Verarbeitung durch Datenimporteur in den Anwendungsbereich der DSGVO fällt
- Auch wenn Verantwortlicher/Auftragsverarbeiter im Drittland, aber die Verarbeitung in der EU erfolgt bzw. die pbD von Betroffenen in der EU zum Gegenstand hat.

Probleme:

- DSGVO Verständnis von „Drittland-Transfer“?
- Gegenläufigkeit zu Sinn und Zweck der SCC…

Abschnitt III Klausel 14

Bei Drittlandübermittlungen durchzuführen:

Aktive und dokumentierte Prüfung der faktischen Einhaltbarkeit dieser Standardvertragsklauseln durch die Parteien, auch im Hinblick auf die im Drittland geltenden Gesetze

= **Transferfolgenabschätzung (Transfer Impact Assessment, TIA)**

Immer bei den Varianten Module 1-3

Bei Modul 4 (Controller – Processor):

- nur, wenn Auftragsverarbeiter in der EU Daten des Verantwortlichen im Drittland mit personenbezogenen Daten kombiniert, die vom Auftragsverarbeiter in der EU erhoben wurden

Klausel 14

Lokale Rechtsvorschriften und Gepflogenheiten, die sich auf die Einhaltung der Klauseln auswirken

MODUL EINS: Übermittlung von Verantwortlichen an Verantwortliche

MODUL ZWEI: Übermittlung von Verantwortlichen an Auftragsverarbeiter

MODUL DREI: Übermittlung von Auftragsverarbeitern an Auftragsverarbeiter

MODUL VIER: Übermittlung von Auftragsverarbeitern an Verantwortliche*(wenn der in der EU ansässige Auftragsverarbeiter die von dem im Drittland ansässigen Verantwortlichen erhaltenen personenbezogenen Daten mit personenbezogenen Daten kombiniert, die vom Auftragsverarbeiter in der EU erhoben wurden)*

a) Die Parteien sichern zu, keinen Grund zu der Annahme zu haben, dass die für die Verarbeitung personenbezogener Daten durch den Datenimporteur geltenden Rechtsvorschriften und Gepflogenheiten im Bestimmungsdrittland, einschließlich Anforderungen zur Offenlegung personenbezogener Daten oder Maßnahmen, die öffentlichen Behörden den Zugang zu diesen Daten gestatten, den Datenimporteur an der Erfüllung seiner Pflichten gemäß diesen Klauseln hindern. Dies basiert auf dem Verständnis, dass Rechtsvorschriften und Gepflogenheiten, die den Wesensgehalt der Grundrechte und Grundfreiheiten achten und nicht über Maßnahmen hinausgehen, die in einer demokratischen Gesellschaft notwendig und verhältnismäßig sind, um eines der in Artikel 23 Absatz 1 der Verordnung (EU) 2016/679 aufgeführten Ziele sicherzustellen, nicht im Widerspruch zu diesen Klauseln stehen.

- Mitwirkung aller Parteien erforderlich!

Fokus der TIA: Einschätzung der Einhaltbarkeit des Vertrages

Zu berücksichtigende Aspekte:

1. Die besonderen Umstände der Übermittlung

2. Die angesichts der besonderen Umstände der Übermittlung relevanten Rechtsvorschriften und Gepflogenheiten des Bestimmungsdrittlandes
   - Einschließlich Anforderungen zur Offenlegung personenbezogener Daten oder Maßnahmen, die öffentlichen Behörden den Zugang zu diesen Daten gestatten

3. Alle relevanten vertraglichen, technischen oder organisatorischen Garantien

1. **Die besonderen Umstände der Übermittlung**
   - Länge der Verarbeitungskette
   - Anzahl der beteiligten Akteure + der verwendeten Übertragungskanäle
   - Beabsichtigte Datenweiterleitungen
   - Art des Empfängers
   - Zweck der Übermittlung,
   - Kategorien + Format der pbD
   - Wirtschaftszweig, in dem die Übertragung erfolgt
   - Speicherort

2. **Relevante Rechtsvorschriften und Gepflogenheiten des Bestimmungsdrittlandes**
   - Insbesondere Möglichkeiten der Offenlegung bzw. Zugang v. Behörden sowie Rechtsmittel

3. **Alle relevanten vertraglichen, technischen oder organisatorischen Garantien**
   - Hier werden die TOMs relevant sein

Immer Einzelfallbetrachtung erforderlich!

Umfangreiche Mitwirkungspflicht des Datenimporteurs im Drittland

Transferfolgenabschätzung:

Reicht den Aufsichtsbehörden und Gerichten die Risikoabwägung aufgrund von Einschätzungen?

EDSA Stellungnahme vom 18.6.2021: Wohl eher nicht…?

- Ausschluss von Sanktionsrisiken fraglich sowie Klagerisiko (s. noyb)

- Ernsthafte Prüfung der Gesetzeslage im Drittland notwendig
- Haltung zum risikobasierten Ansatz leider immer noch unklar
- Ist detailliert zu dokumentieren:

> *„Reports you will establish will have to include comprehensive information on the legal assessment of the legislation and practices, and of their application to the specific transfers, the internal procedure to produce the assessment (including information on actors involved in the assessment- e.g. law firms, consultants, or internal departments-) and dates of the checks. Reports should be endorsed by the legal representative of the exporter.“*

Daher:

➢ Wenn irgendwie möglich, objektive Faktoren identifizieren und nicht nur auf die Wahrscheinlichkeit eines Zugriffs abstellen

EDSA: Je nach Drittland immer noch ergänzende Garantien (vertraglich, technisch, organisatorisch) notwendig!

➢ Empfehlungen des EDSA zu ergänzenden Garantien bestehen fort


Das Schrems II Urteil
Folgen für Verantwortliche
Lösung neue EU-Standardvertragsklauseln?
Strategie + Transferfolgenabschätzung (TIA)
Anhang (optional): Verschiedene Fallkonstellationen USA

Einzelfallprüfungen aller Drittstaatenübermittlungen, Fragebögen, Checklisten, Audits bei Dienstleistern

↓

Schutzniveau im Drittland und Risiken prüfen (**TIA**)

↓

SCC mit den richtigen Modulen abschließen, Anhänge befüllen

↓

Bei Bedarf ergänzende Maßnahmen etablieren

↓

Kontrolle der Einhaltung von Zusagen + Maßnahmen

↓

Wenn keine ergänzenden Maßnahmen möglich oder Nichteinhaltung der SCC, Aussetzung der Datenübermittlung

↓

Ggf. Meldung an Aufsichtsbehörde

Grundsätzliche Betrachtungen bei den Dienstleister-Audits:

1. Bewertung der Gesetzeslage und des Schutzniveaus im jeweiligen Drittland
   - USA: Sachlage geklärt, detailliertere Bewertung für UK ggf. erforderlich
   - Situation in anderen Drittländern?

2. Wenn ergänzende Maßnahmen notwendig, welche? Wie umsetzbar?

3. Wenn keine Ergänzenden Maßnahmen umsetzbar:
   - Verantwortlicher entscheidet weiteres Vorgehen

In jedem Fall hoher Dokumentationsaufwand

➢ Templates für Audits, TIA, etc. notwendig…

1. Bei Dienstleister in den USA:
   - Anbieter elektronischer Kommunikation (Ja/Nein)?
   - Hier ein Beispiel aus der Fragenliste an Dienstleister

---->

2. Wenn ein Auftragsverarbeiter selbst Subunternehmer einsetzt:
   - Sitzt der Subunternehmer in einem Drittland oder im EWR?
   - Wenn USA: Anbieter elektronischer Kommunikation (Ja/Nein)?

Direkte Anwendung von 50 U.S.C. § 1881a (= FISA 702)

Wenn Sie oder eine andere relevante US-Organisation (für die Verarbeitung Verantwortlicher oder Auftragsverarbeiter) personenbezogene Daten, die an Sie übermittelt werden, verarbeitet oder Zugang zu diesen Daten hat:

1. Fallen Sie oder eine andere relevante US-Organisation (für die Verarbeitung Verantwortlicher oder Auftragsverarbeiter) unter eine der folgenden Definitionen in 50 U.S.C. § 1881(b)(4), die Sie oder die andere(n) Stelle(n) direkt in den Anwendungsbereich von 50 U.S.C. § 1881a (= FISA 702) fallen lassen könnte(n)?

   ☐ Ja
   ☐ Nein
   ☐ Wir sind gesetzlich oder durch eine andere rechtlich verbindliche Regelung verpflichtet, diese Frage nicht zu beantworten

2. Ergänzungsfragen:
   a. Sind Sie oder eine andere relevante US-Organisation (für die Verarbeitung Verantwortlicher oder Auftragsverarbeiter) ein Telekommunikationsunternehmen, und zwar im Sinne der Definition, die in Abschnitt 153 von Titel 47 U.S.C. gegeben ist?

      ☐ Ja
      ☐ Nein
      ☐ Wir sind gesetzlich oder durch eine andere rechtlich verbindliche Regelung verpflichtet, diese Frage nicht zu beantworten

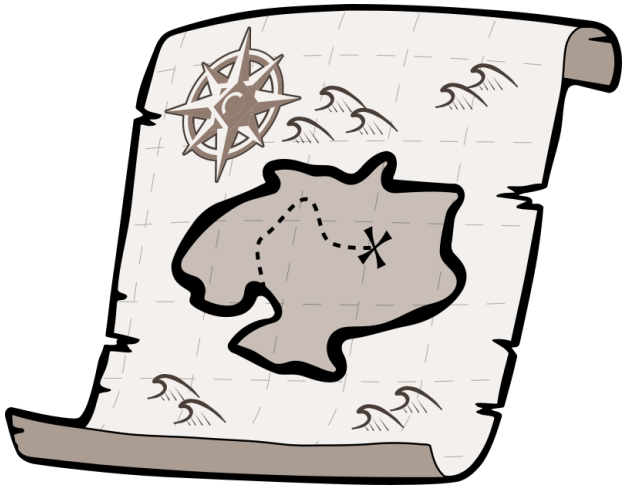
   b. Sind Sie oder eine andere relevante US-Organisation (für die Verarbeitung Verantwortlicher oder Auftragsverarbeiter) ein Anbieter von elektronischen Kommunikationsdiensten, und zwar im Sinne der Definition, die in Abschnitt 2510 von Titel 18 U.S.C. gegeben ist?

      ☐ Ja
      ☐ Nein
      ☐ Wir sind gesetzlich oder durch eine andere rechtlich verbindliche Regelung verpflichtet, diese Frage nicht zu beantworten

Risikoadressierung: Kriterien für Dienstleisteraudits

Welches Drittland ist involviert und wie ist die Rechtslage dort?	
USA, China, Russland, Mittlerer Osten	
Evtl. UK (sofern kein Angemessenheitsbeschluss mit Bestand)	
Um welche Art von Dienstleister handelt es sich?	
Telekommunikationsdienstanbieter, Anbieter elektronischer Kommunikation (E-Mail, Messenger-Dienste, Videokonferenzanbieter usw.), Cloud Service Provider	
Gruppeninterner Datentransfer in einem Dienstleistungsverhältnis, Anbieter von Analyse- oder Trackingdiensten, sonstige IT-Dienste wie z. B. Fernwartung, Support, usw.)	
Welche Daten spielen bei der jeweiligen Verarbeitung eine Rolle?	
Art. 9 DSGVO Daten, Bank- und Finanzdaten, Personaldaten (HR)	
Bestands-/Stammdaten von Kunden oder Arbeitnehmern (Name, Adresse, Kontakt…)	
Nutzungsdaten wie etwa Meta- und Trackingdaten (ohne Standort)	

Vertragliche Maßnahmen
Abschluss der neuen EU-Standardvertragsklauseln
Mit SCC und ggf. ergänzenden Vertragsklauseln die folgenden Zusicherungen des Datenimporteurs abdecken: • Nichtvorhandensein von Backdoors • Rechtswegerschöpfung bei Datenherausgabeanfragen und National Security Letters o.ä. • Alternativ Genehmigungspflicht bei behördlichen Datenzugriffen • Erweiterte Unterstützung bei Gewährleistung von Betroffenenrechten, insbesondere bei Information des Betroffenen • Schadensersatzpflicht gegenüber dem Datenexporteur im Falle der Nichteinhaltung
Technische Maßnahmen
Verschlüsselung -> Transport (in transit) sowie -> Datenträger (at rest)
Getrennte Datenverarbeitung/Mandantentrennung, Geofencing, Beschränkung v. Zugriffen (Rechte/Rollenkonzept…)
Anonymisierung, Pseudonymisierung, Datenminimierung
Organisatorische Maßnahmen
Compliance-Bestätigungen, Zertifizierungen, sonstige Garantien (BCR, CoC…)
Dokumentation von staatlichen Anfragen, Transparenzberichte
Schulungen von Mitarbeitern



Man kann auch versuchen, die Genehmigung einer zuständigen Aufsichtsbehörde für die Datenübermittlung zu bekommen.

-> Unwahrscheinlichste Option von allen ☺

Noch Fragen?

Dann kontaktieren Sie uns gerne!

E-Mail: datenschutz@floss-consult.de
Telefon: 05423 964900


Das Schrems II Urteil
Folgen für Verantwortliche
Lösung neue EU-Standardvertragsklauseln?
Strategie + Transferfolgenabschätzung (TIA)
Anhang (optional): Verschiedene Fallkonstellationen USA

Definition „Anbieter elektronischer Kommunikation“ nach 50 USC § 1881(b)(4):

„*(4) Electronic communication service provider The term “electronic communication service provider” means— (A) a* ***telecommunications carrier****, as that term is defined in section 153 of title 47 ; (B) a* ***provider of electronic communication service****, as that term is defined in section 2510 of title 18 ; (C) a* ***provider of a remote computing service****, as that term is defined in section 2711 of title 18 ; (D)* ***any other communication service provider who has access to wire or electronic communications*** *either as such communications are transmitted or as such communications are stored; or (E)* ***an officer, employee, or agent of an entity described*** *in subparagraph (A), (B), (C), or (D).*”

- Im Folgenden benutzen wir für „Electronic Communications Service Provider“ der Einfachheit halber die Abkürzung ECSP ☺


Fallkonstellation I // Kein ESP
Fallkonstellation II // Ist ESP
US-Anbieter mit Subunternehmern

Mehrheitliche Rechtsprechung in den USA:

Firmen, die eine eigene Webseite zur Firmenpräsentation haben, sind keine ECSPs, auch wenn dort Möglichkeit besteht, mit Kunden Kontakt zu führen.

Mögliche Beispiele:

- Ein Webshop
  - Vgl. Dyer v. Northwest Airlines Corp., 334 F. Supp. 2d 1196, 1199 (D.N.D. 2004)
- Webseite einer Airline
  - Vgl. Jetblue Airways Corp. Privacy Litigation, 379 F. Supp. 2d 299, 309-10 (E.D.N.Y. 2005)

- FISA 702 + Cloud Act sind hier nicht anwendbar
- Aber: KEIN Schutz gegen EO 12333 oder Presidential Policy Directive 28
  - Abgreifen von Daten „in Transit“ durch NSA & Co., etwa bei Unterseekabeln (siehe auch Snowden Affäre)

- Mögliche Maßnahmen:

  - Technisch
    - Verschlüsselung
      - Verschlüsselung sowohl „in transit“ wie auch „at rest“!
    - Audit Trail von Datentransfers + Zugriffen
    - Anonymisierung von Daten, wo machbar

  - Vertraglich
    - Diverse Ergänzungsvereinbarungen zu den SCC, die
      - dem US-Auftragsverarbeiter Pflichten zum Schutz der Daten auferlegen +
      - Schadensersatzansprüche/Vertragsstrafen regeln.

Fallkonstellation I // Kein ESP

Fallkonstellation II // Ist ESP

US-Anbieter mit Subunternehmern

Alle Cloud Service Provider + Internetplattformen zur Kommunikation

Mögliche Beispiele:

- Google mit Diensten wie Hangouts, Googlemail, GoogleDocs,
- Microsoft mit Diensten wie Azure, Office 365 (wenn nicht on premise)
- Amazon mit Cloud Diensten wie AWS

- Achtung:
  - Fluggesellschaft, die Reisebüros ein computergestütztes Reisebuchungssystem zur Verfügung stellt, auf das über separate Computerterminals zugegriffen wird, kann ein Anbieter von ECS sein
    - Vgl. United States v. Mullins, 992 F.2d 1472, 1478 (9th Cir. 1993)

- FISA 702 + Cloud Act anwendbar, neben EO 12333 und PPD 28

- Mögliche Maßnahmen:
  - Technisch
    - Verschlüsselung
      - Verschlüsselung sowohl „in transit“ wie auch „at rest“!
    - Audit Trail von Datentransfers + Zugriffen
    - Wo möglich, Anonymisierung von Daten

  - Knifflig sind hier die vertraglichen Ergänzungsvereinbarungen
    - Siehe Folgefolie
    - Diverse Ergänzungsvereinbarungen zu den SCC, die
      - dem US-Auftragsverarbeiter Pflichten zum Schutz der Daten auferlegen +
      - Schadensersatzansprüche/Vertragsstrafen regeln.

Ergänzend zu den SCCs vertragliche Verpflichtung des Importeurs zur Benachrichtigung des Exporteurs bei Erhalt einer FISA 702 Anordnung.

Aber: Unsicher, ob ausreichend!

- Problem:
  Anordnung durch US-Behörde, dass Stillschweigen bewahrt werden muss (sog. national security letter, NSL, „gag order“)

- Gerichtlich angreifbar, aber langwierig und mit wenig Erfolgsaussichten angesichts der bisherigen Rechtsprechung von US Gerichten

- Möglicher Ausweg:
  Zusicherung des Importeurs, den Exporteur ganz ohne weitere Spezifizierung zu benachrichtigen, wenn er nicht mehr in der Lage ist, die Standardvertragsklauseln und EV einzuhalten.

  - Dies unter Einräumung des generellen Kündigungsrechts und mit ausreichender Vorlaufzeit, bevor (aus welchen Gründen auch immer) Daten gegenüber Dritten offengelegt werden
    (unsicher, da für US-Auftragsverarbeiter rechtlich riskant)

  - Löschung, Kündigung in dem Zeitfenster möglich?

Alternativer Workaround:

- Vertragliche Zusicherung, eines Transparenz Reports, der zumindest die Anzahl der National Security Orders + Directives (inklusive FISA Abfragen), Art der Daten + ersuchende Stelle innerhalb eines Jahres benennt

- Problem: Benennt keine konkreten Fälle, die Betroffenheit ist somit für den Exporteur (und Betroffenen) schwer bis gar nicht einschätzbar.

- Dann höchstens Vergleich mit Anzahl möglicher Betroffener vs. Zahl im Transparenzreport für Risikoabschätzung möglich.

Alternativ oder kumulativ:

Vertragliche Zusicherung, bei Erhalt eines National Security Letters eine zuständige Datenschutzaufsichtsbehörde anzurufen, um das weitere Vorgehen abzuklären.

Fallkonstellation I // Kein ESP

Fallkonstellation II // Ist ESP

US-Anbieter mit Subunternehmern

Mögliches Beispiel:

Eine amerikanische Bank nutzt Amazon AWS für Cloud Speicherkapazität oder Rechenleistung

- Hier Fallkonstellation mit einem ECSP als Subunternehmer

Auftragsverarbeiter zur Weitergabe v. SCC Obliegenheiten verpflichtet, Subunternehmer aber nicht!

Mögliche Lösungen:

- Weitergabe Pflichten SCC + Ergänzungen inkl. techn. Maßnahmen
- Importeur (Auftragsverarbeiter) muss Subunternehmer zusätzliche Pflichten auferlegen
  - Je nachdem ob Subunternehmer wiederum ECSP oder nicht
- Offenlegung von Verträgen mit Subunternehmern
- Benachrichtigungspflicht, wenn neue Subunternehmer
- Regelung Schadensersatzpflichten gegenüber Betroffenen

- Unsicher: Verpflichtung Importeur, Datentransfers an Subunternehmer auf Art. 49 DSGVO zu stützen

- Rechtssicher: Verpflichtung des Importeurs, Subunternehmer aus EWR/Ländern m. Angemessenheitsbeschluss einzusetzen

- Sonst: Wechsel des Auftragsverarbeiters

Folie 03:

- „Goddess of Justice“ von Mardigann, unter CC0 1.0,

Folien 8, 9 + 29:

- „traffic light red dan ge 01“, „traffic light yellow dan 01“ und „traffic light green dan 01“, alle von Anonymous, mit angegebener Quelle Dan Gerhards für OCAL 0.18, unter CC0 1.0

Folie 18+19:

- „Perplexed Female“ von oksmith, unter CC0 1.0

Folie 32:

- „treasure map“ von tzunghaor, unter CC0 1.0