

# Konsequenzen des Schrems II Urteils in der Praxis: Lösungsansätze des Bitkom

Fachtagung Datenschutz im Gesundheitswesen  
am 12. Mai 2022

# Ihre heutigen Ansprechpartner



**Heiko Gossen**

Geschäftsführender Gesellschafter  
migosens GmbH  
E [heiko.gossen@migosens.de](mailto:heiko.gossen@migosens.de)



**Markus Stamm**

Senior Legal Counsel Legal &  
Compliance | Nokia  
E [markus.stamm@nokia.com](mailto:markus.stamm@nokia.com)

# Agenda



# Ausgangssituation: Beschwerde Max Schrems vom 1.12.2015



**Facebook Inc.** sei zur **Herausgabe** von personenbezogenen **Daten** an **FBI und NSA** verpflichtet

- **Section 702** des **FISA** und **E.O. 12333**
- **Geringe gerichtliche Hürden** für die Auslandsaufklärung im Rahmen der PRISM und UPSTREAM Programme



**Unvereinbar mit Art. 7 und 8** der Grundrechtscharta der EU



**Keine ausreichenden Rechtsbehelfe** nach **Art. 47** der Charta

- **Rechtsschutz** für **Nicht-US-Bürger** deutlich **eingeschränkt**
- Hohe **Hürden** die **Klagebefugnis nachzuweisen**



**SCC ist nicht geeignet**, um diesen Mangel zu beheben

# Rechtssache C311/18 – elf Fragen an den EuGH

## Frage 1



**Anwendbarkeit der DSGVO**, wenn die Daten bei ihrer **Übermittlung oder im Anschluss** daran von den Behörden eines Drittlands **für Zwecke der öffentlichen Sicherheit, der Landesverteidigung und der Sicherheit des Staates** verarbeitet werden können, ist **gegeben**.

## Fragen 2, 3 und 6



Das im Drittland **erwartete Schutzniveau** richtet sich nach **Art 44 DSGVO**, wonach alle Bestimmungen des Kapitel V anzuwenden sind, „um sicherzustellen, dass das durch diese Verordnung gewährleistete Schutzniveau für natürliche Personen nicht untergraben wird.“

Der Fortbestand des hohen Schutzniveaus soll gewährleistet bleiben

Schutzniveau muss nicht identisch sein, aber gleichwertig mit dem in der Charta garantierten Niveau

„Messlatte“  
Angemessenheitsbeschluss

Rechtsstaatlichkeit,

die Achtung der Menschenrechte und Grundfreiheiten,

Im betreff. Land geltenden einschlägigen Rechtsvorschriften – auch in Bezug auf öff. Sicherheit, [..]

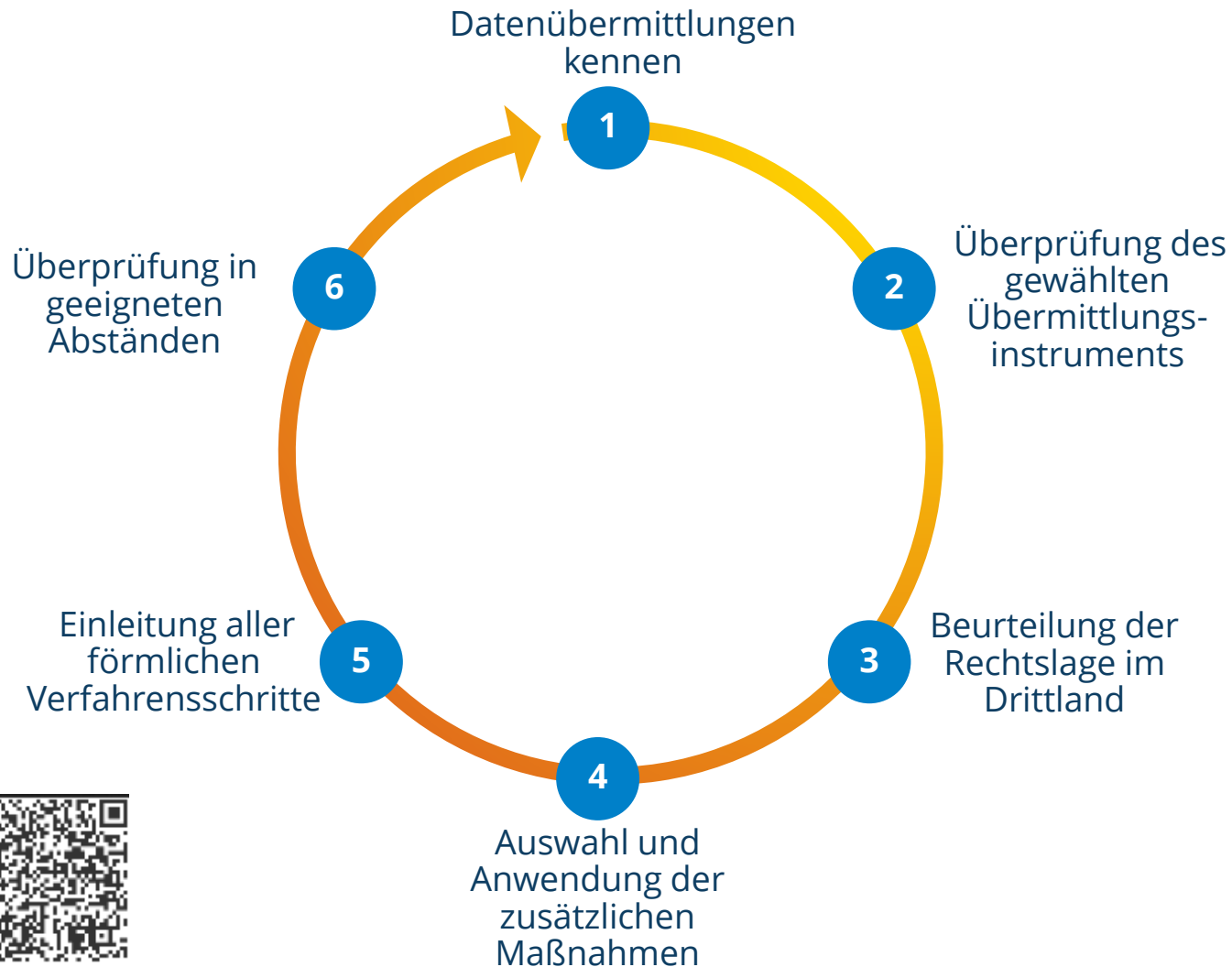
sowie Zugang der Behörden zu personenbezogenen Daten



# Agenda



# EDSA-Empfehlungen zu Maßnahmen zur Ergänzung zur Gewährleistung des Schutzniveaus



## Anhang 2: Beispiele für zusätzliche Maßnahmen



„Eine **zusätzliche Maßnahme** ist nur als **effektiv** im Sinne des Schrems II-Urteils des Gerichtshofs anzusehen, sofern und soweit die Maßnahme **genau die Rechtsschutzlücken schließt**, die der Datenexporteur bei seiner Prüfung der Rechtslage im Drittland festgestellt hat.“



7 Anwendungsfälle  
Anwendungsfälle 1-5 „lösbar“  
Anwendungsfälle 6-7 „nicht lösbar“



Technische Maßnahmen  
Zusätzliche vertragliche Maßnahmen  
Organisatorische Maßnahmen

# DSGVO Erwägungsgrund 108

Bei Fehlen eines Angemessenheitsbeschlusses sollte der Verantwortliche oder der Auftragsverarbeiter als **Ausgleich für den in einem Drittland bestehenden Mangel an Datenschutz geeignete Garantien** für den Schutz der betroffenen Person vorsehen.

Diese geeigneten Garantien können darin bestehen, dass auf [...] Standarddatenschutzklauseln [...] zurückgegriffen wird.

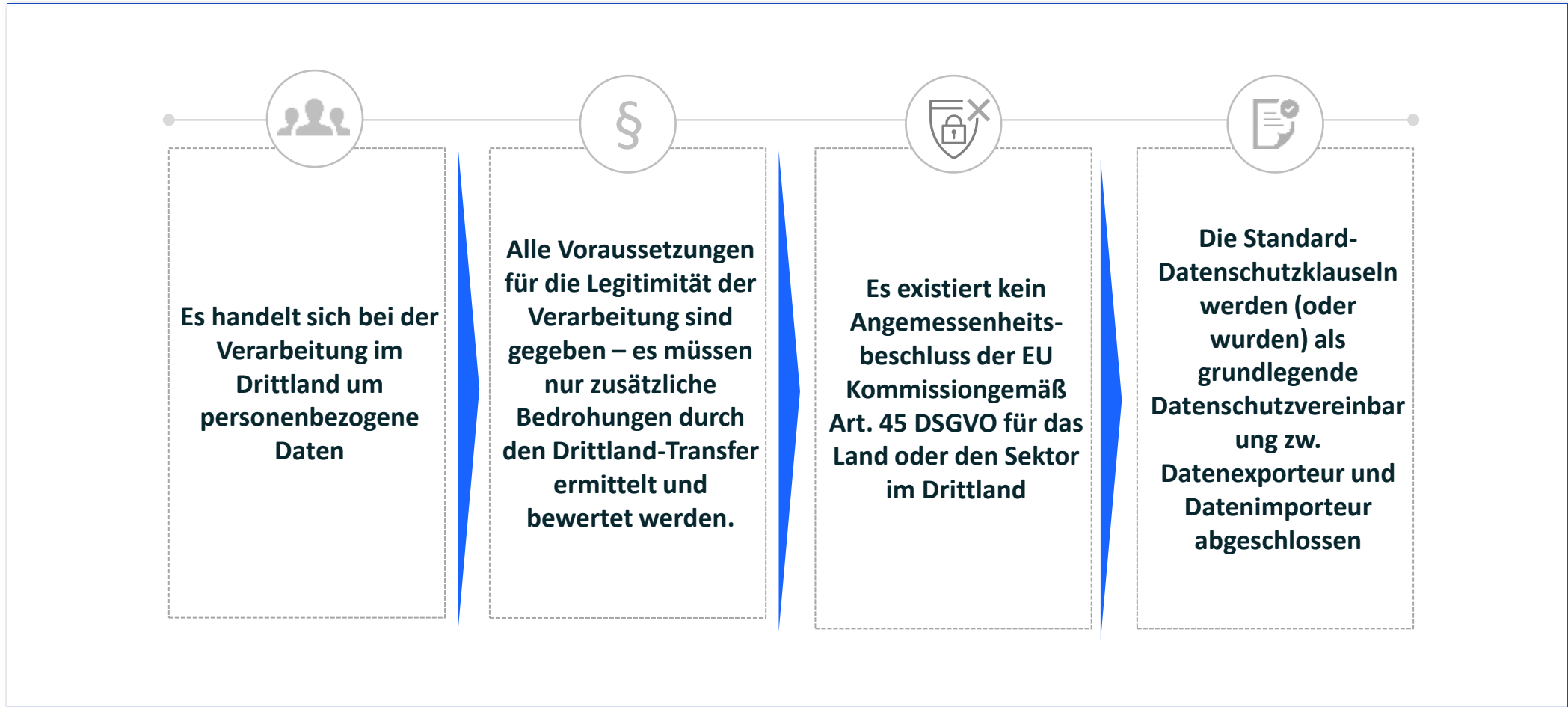
Diese Garantien sollten sicherstellen, dass die Datenschutzvorschriften und die Rechte der betroffenen Personen auf eine der Verarbeitung innerhalb der Union **angemessene Art und Weise** beachtet werden;

dies gilt auch hinsichtlich der Verfügbarkeit von durchsetzbaren Rechten der betroffenen Person und von wirksamen Rechtsbehelfen [...] in der Union oder in einem Drittland.

Sie sollten sich insbesondere auf die Einhaltung der allgemeinen Grundsätze für die Verarbeitung personenbezogener Daten, die Grundsätze des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen beziehen.



# Vorab: Prüfung der Eingangsvoraussetzungen



# Die gesamte TIA muss in einen Gesamtprozess integriert werden

## Das Kernprinzip unserer TIA-Methode in 5 Schritten



# Die Gewährleistungsziele des SDM als „kleinster gemeinsamer Nenner“



# Hinterlegung von Drittlandsprofilen

#	Ausprägung	Zusammenfassung (wird im TIA-Bericht mit ausgegeben und soll im Kern die Gesamt-Bewertung begründen)	#	Relevanz für das Drittlandsprofil	Parameter
<b>Bestehen legale Restriktionen für Privacy by design, Privacy by default oder die Datensicherheit im Drittland?</b>					
1	Ja	Es bestehen legale Restriktionen für Privacy-by-Design im Drittland. Im Rahmen der Strafverfolgung und der Terrorismusbekämpfung bestehen Verpflichtungen für Telekommunikationsanbieter zur Schaffung von Zugriffsmöglichkeiten für die nationalen Dienste. Diese umfassen auch Nicht-US-Bürger.	1.1	Restriktionen für den Privacy-by-Design-Grundsatz	Existieren im Zielland gesetzliche oder anderweitige regulatorische Anforderungen, die auf eine Schwächung von Privacy by Design / by Default abzielen, z.B. indem unprotokollierte Schnittstellen für Behörden zwecks Zugriff auf Kommunikationsinhalte etabliert oder kompromittierte Verschlüsselungsprotokolle genutzt werden müssen?
			1.2	Restriktionen für den Privacy-by-Design-Grundsatz	Gibt es im Zielland andere rechtliche Vorgaben, die den Datenimporteur daran hindern, angemessene technische und organisatorische Maßnahmen im Sinne des Art. 32 DSGVO zu ergreifen?
<b>Fällt der gesetzliche Rahmen für (präventive, repressive, strategische) Zugriffe auf personenbezogene Daten durch Hoheitsträger in Hinblick auf: (i) Regelungsdichte (ii) Formale Anforderungen</b>					
2	Nein	Zugriffe durch Hoheitsträger unterliegen definierten Kriterien und Freigabeprozessen. Recherche und Überwachungsmaßnahmen im Rahmen der Strafverfolgung sind geregelt und bedürfen der behördlichen Autorisierung.	2.1	Eingeschränkte Geltung des Grundsatzes der Gesetzmäßigkeit bei Datenzugriffen	Wird das Prinzip des "Vorbehalts des Gesetzes" bei Zugriffen auf personenbezogene Daten durch Hoheitsträger in relevanter Weise untergabelt?
			2.2	Eingeschränkte Geltung des Grundsatzes der Gesetzmäßigkeit bei Datenzugriffen	Weichen gegebenenfalls existierende gesetzliche Erlaubnistatbestände das Prinzip der Verhältnismäßigkeit bezüglich Datenzugriffen auf?
			2.3	Eingeschränkte Geltung des Grundsatzes der Gesetzmäßigkeit bei Datenzugriffen	Mangelt es im Zielland an richterlichen Vorab-Kontrollen bei geplanten Zugriffen durch Geheimdienstbehörden?
<b>Besteht eine relevante eingeschränkte Möglichkeit der nachträglichen Information von Zugriffen an Exporteur oder Betroffenen?</b>					
3	Ja	Die nachträgliche Information über Zugriffe an Exporteur oder Betroffenen sind im Drittland eingeschränkt. So erlaubt die geheimdienstliche Überwachung im Rahmen der Terrorismusbekämpfung unter geregelten Umständen die Sammlung und Auswertung personenbezogener Daten von U.S. Bürgern und Nicht-U.S. Bürgern ohne deren Wissen zum Schutz der USA.	3.1	Einschränkungen des Transparenzgrundsatzes	Gibt es im Drittland gesetzliche Verpflichtungen, die den Datenimporteur von der Benachrichtigung des Dataexporteurs über einen Zugriff durch Hoheitsträger abhalten?
			3.2	Einschränkungen des Transparenzgrundsatzes	Gibt es im Drittland gesetzliche Verpflichtungen, die den Datenimporteur und/oder den Dataexporteur von einer Benachrichtigung der betroffenen Person über einen Zugriff durch Hoheitsträger abhalten?
			3.3	Einschränkungen des Transparenzgrundsatzes	Gibt es im Drittland gesetzliche Verpflichtungen, die den Dataimporteur grundsätzlich daran hindern, seine Verpflichtungen aus Ziffer 7.6 der Standardvertragsklauseln (Dokumentation und Einhaltung der Klauseln) zu erfüllen?
			3.4	Einschränkungen des Transparenzgrundsatzes	Gibt es im Drittland gesetzliche Verpflichtungen, die den Dataimporteur an der Benachrichtigung und an der

## Systematik

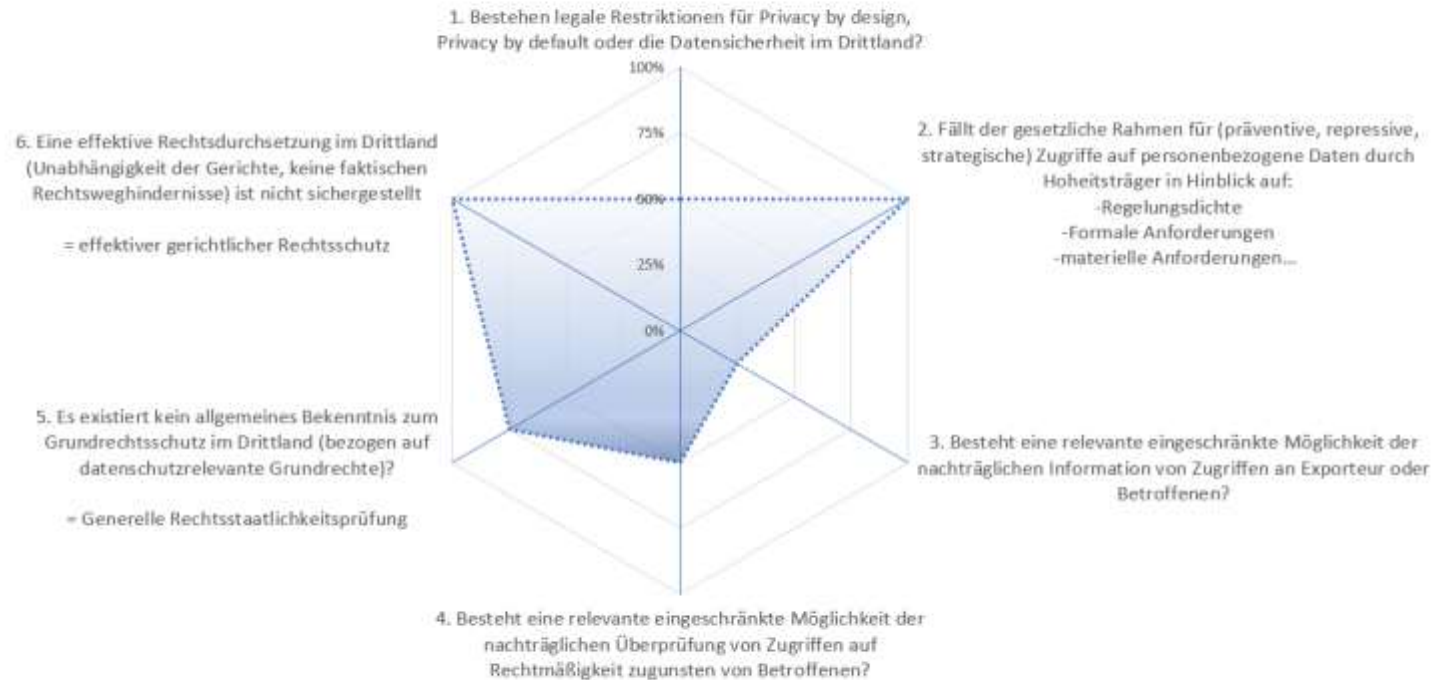
Betrachtung von 25 Einzelfragen je Drittland und Bewertung (ja/nein)

Verdichtung auf 6 Parameter (ja/nein)

Ausgabe der Zusammenfassung im Report

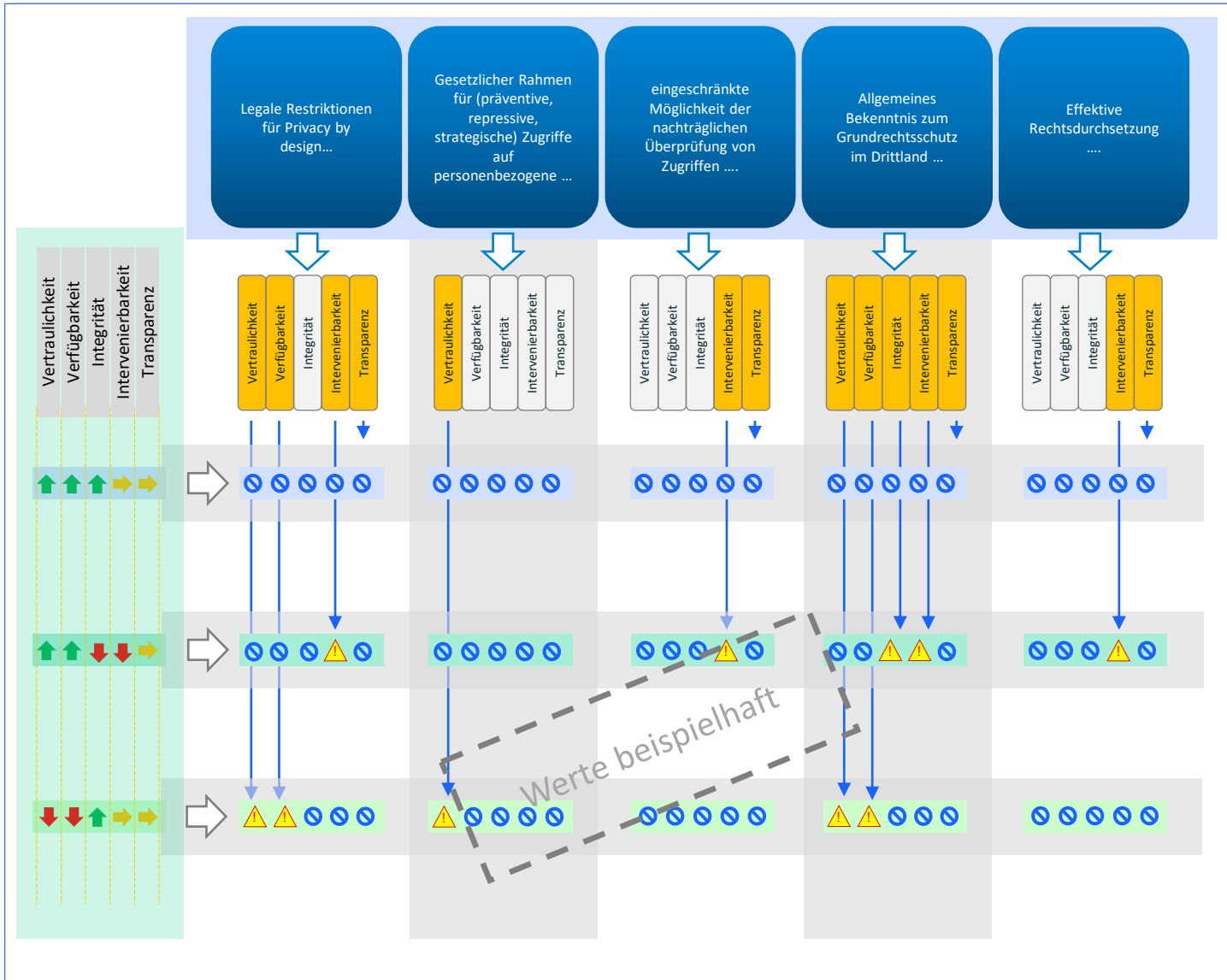
# Status Drittlandsprofile

## ÜBERSICHT USA



Land	Status
Australien	100%
Indien	100%
Kolumbien	100%
USA	100%
Brasilien	99%

# Länderprofil und Übermittlungsdetails ergeben Bedrohungsprofil

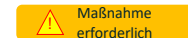


## Systematik

Prüfung der Auswirkungen auf die Gewährleistungsziele an den Schnittstellen der Matrix (sofern Parameter zutreffend)

Ermittlung eines Bedrohungsprofils für die Gewährleistungsziele

Legende



# Agenda



# Deep Dive USA

## 1. Bestehen legale Restriktionen für Privacy by design, Privacy by default oder die Datensicherheit im Drittland?

Ergebnis: Ja

Es bestehen legale Restriktionen für Privacy-by-Design im Drittland. Im Rahmen der Strafverfolgung und der Terrorismusbekämpfung bestehen Verpflichtungen für Telekommunikationsanbieter zur Schaffung von Zugriffsmöglichkeiten für die nationalen Dienste. Diese umfassen auch Nicht-US-Bürger.

#	Parameter	Teil-Ausprägung
1.1	Existieren im Zielland gesetzliche oder anderweitige regulatorische Anforderungen, die auf eine Schwächung von Privacy by Design / by Default abzielen, z.B. indem unprotokollierte Schnittstellen für Behörden zwecks Zugriff auf Kommunikationsinhalte etabliert oder kompromittierte Verschlüsselungsprotokolle genutzt werden müssen?	Ja
1.2	Gibt es im Zielland andere rechtliche Vorgaben, die den Datenimporteur daran hindern, angemessene technische und organisatorische Maßnahmen im Sinne des Art. 32 DSGVO zu ergreifen?	Nein



# Deep Dive USA

2. Fällt der gesetzliche Rahmen für Zugriffe auf personenbezogene Daten durch Hoheitsträger in Hinblick auf Regelungsdichte, Formale Anforderungen und materielle Anforderungen hinter das EU-Niveau zurück?

Ergebnis: Nein

Zugriffe durch Hoheitsträger unterliegen definierten Kriterien und Freigabeprozessen. Recherche und Überwachungsmaßnahmen im Rahmen der Strafverfolgung sind geregelt und bedürfen der behördlichen Autorisierung.

#	Parameter	Teil-Ausprägung
2.1	Wird das Prinzip des "Vorbehalts des Gesetzes" bei Zugriffen auf personenbezogene Daten durch Hoheitsträger in relevanter Weise untergeben?	Nein
2.2	Weichen gegebenenfalls existierende gesetzliche Erlaubnistatbestände das Prinzip der Verhältnismäßigkeit bezüglich Datenzugriffen auf?	Nein
2.3	Mangelt es im Zielland an richterlichen Vorab-Kontrollen bei geplanten Zugriffen durch Geheimdienstbehörden?	Nein

# Deep Dive USA

## 3. Besteht eine relevante eingeschränkte Möglichkeit der nachträglichen Information von Zugriffen an Exporteur oder Betroffenen?

Ergebnis: Ja

Die nachträgliche Information über Zugriffe an Exporteur oder Betroffenen sind im Drittland eingeschränkt.

So erlaubt die geheimdienstliche Überwachung im Rahmen der Terrorismusbekämpfung unter geregelten Umständen die Sammlung und Auswertung personenbezogener Daten von U.S. Bürgern und Nicht-U.S. Bürgern ohne deren Wissen zum Schutz der USA.

#	Parameter	Teil-Ausprägung
3.1	Gibt es im Drittland gesetzliche Verpflichtungen, die den Datenimporteur von der Benachrichtigung des Dataexporteurs über einen Zugriff durch Hoheitsträger abhalten?	Ja
3.2	Gibt es im Drittland gesetzliche Verpflichtungen, die den Datenimporteur und/oder den Dataexporteur von einer Benachrichtigung der betroffenen Person über einen Zugriff durch Hoheitsträger abhalten?	Ja
3.3	Gibt es im Drittland gesetzliche Verpflichtungen, die den Dataimporteur grundsätzlich daran hindern, seine Verpflichtungen aus Ziffer 7.6 der Standardvertragsklauseln (Dokumentation und Einhaltung der Klauseln) zu erfüllen?	Ja
3.4	Gibt es im Drittland gesetzliche Verpflichtungen, die den Dataimporteur an der Benachrichtigung und an der Unterstützung des Datenexporteurs im Fall der Verletzung des Schutzes personenbezogener Daten hindern (Ziffer 9 Standardvertragsklauseln)?	Nein

# Deep Dive USA

## 4. Besteht eine relevante eingeschränkte Möglichkeit der nachträglichen Überprüfung von Zugriffen auf Rechtmäßigkeit zugunsten von Betroffenen?

Ergebnis: Ja

Es besteht eine teilweise eingeschränkte Möglichkeit für den Betroffenen der nachträglichen Überprüfung der Rechtmäßigkeit von Zugriffen im Drittland.

Insbesondere für Nicht-US-Bürger bestehen nur eingeschränkte Möglichkeiten des Rechtswegs

#	Parameter	Teil-Ausprägung
4.1	Fehlt es im Zielland an Institutionen, welche die Rechtmäßigkeit von Behörden beim Umgang mit/Zugriff auf personenbezogenen Daten beaufsichtigen?	Nein
4.2	Fehlt es im Zielland überhaupt an einer Institution, die den Schutz personenbezogener Daten - oder eines vergleichbaren Schutzgutes - überwacht?	Nein
4.3	Mangelt es im Zielland an formalen Rechtsbehelfen gegen die Verletzung relevanter datenschutzrechtlicher Bestimmungen durch Hoheitsträger?	Nein
4.4	Mangelt es im Zielland an der Möglichkeit der nachträglichen gerichtlichen Überprüfbarkeit von Datenzugriffen durch Behörden bzw. entsprechenden darauf abzielenden Aufforderungen.	ja
4.5	Mangelt es im Zielland an der Möglichkeit zivilrechtlichen Rechtsschutzes wegen potenziell unzulässiger Datenzugriffe durch Behörden (etwa zwecks der Geltendmachung von Schadensersatzansprüchen)?	Ja
4.6	Sieht das Rechtssystem im Zielland generell eine Beschränkung der Berechtigung zur Geltendmachung von Ansprüchen (Aktivlegitimation) auf materiellen oder immateriellen Schadensersatz vor?	ja
4.7	Ist (verwaltungs- oder zivilrechtlicher) Rechtsschutz für den Datenimporteuer gegen Datenzugriffe durch Hoheitsträger ausgeschlossen?	Nein
4.8	Wird der gegebenenfalls gewährte (verwaltungs- oder zivilrechtliche) Rechtsschutz dem Datenexporteur und/oder den EU-Bürgern vorenthalten ?	Ja

# Deep Dive USA

## 5. Es existiert kein allgemeines Bekenntnis zum Grundrechtsschutz im Drittland bezogen auf datenschutzrelevante Grundrechte? (Generelle Rechtsstaatlichkeit)

Ergebnis: Nein

Ein allgemeines Bekenntnis zum Grundrechtsschutz im Drittland besteht.

Jedoch sind die USA Mitglied im Dienste-Verbund "Five Eyes".

#	Parameter	Teil-Ausprägung
5.1	Erfährt der Anspruch an die Geltung universeller Menschen- und Bürgerrechte im Zielland grundlegende Einschränkungen?	Nein
5.2	Distanziert sich das Zielland von der UN Menschenrechtskonvention.	Nein
5.3	Bestehen grundsätzliche Zweifel an der Achtung der Menschenrechte und Grundfreiheiten im Drittland, was z.B. durch Sanktionen der UN und/oder der EU objektiviert werden?	Nein
5.4	Ist das Zielland auf Ebene von Nachrichtendiensten Mitglied in einem internationalen Dienste-Verbund (z.B. "Five Eyes")?	Ja

# Deep Dive USA

## 6. Eine effektive Rechtsdurchsetzung im Drittland (Unabhängigkeit der Gerichte, keine faktischen Rechtsweghindernisse) ist nicht sichergestellt? = effektiver gerichtlicher Rechtsschutz

Ergebnis: Nein

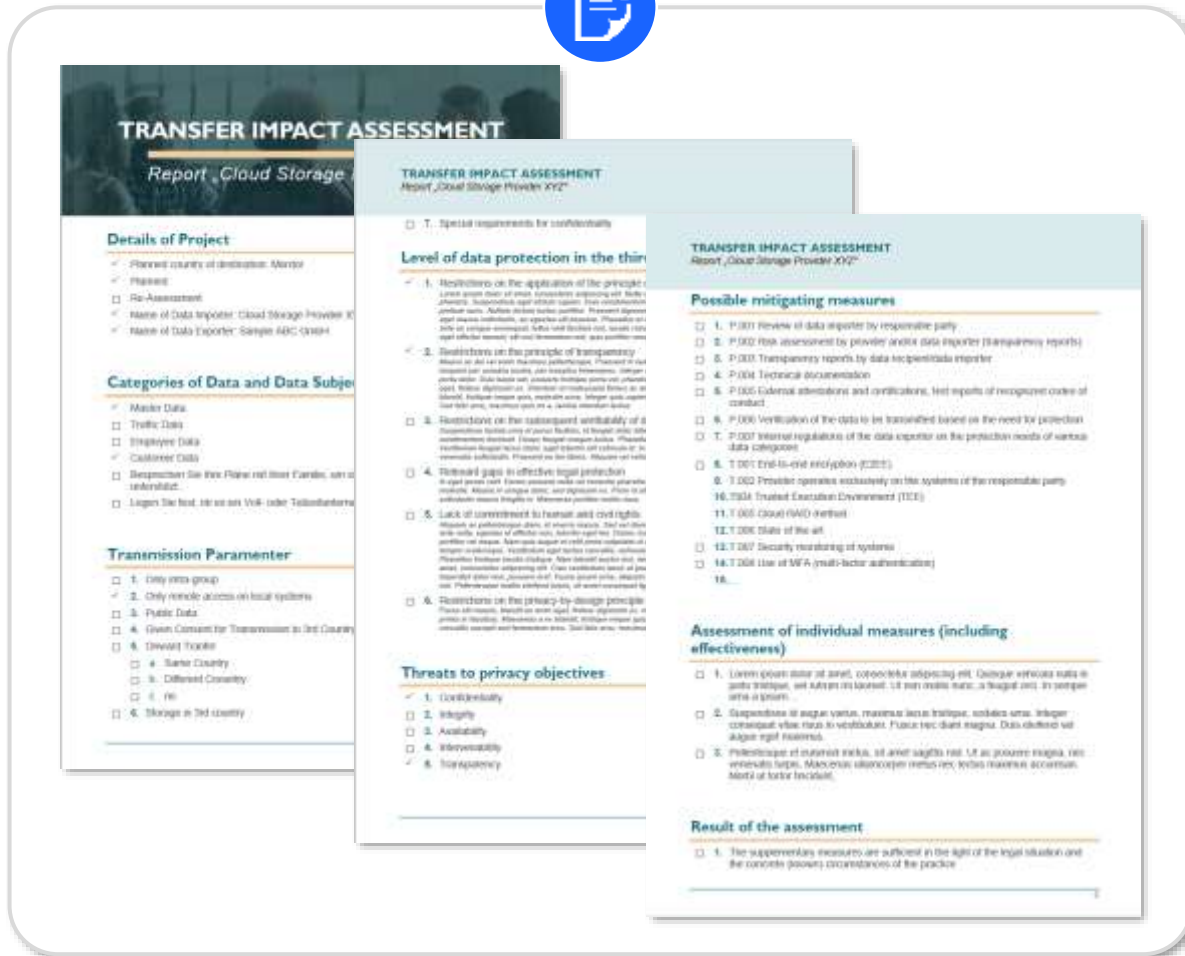
Ein effektiver gerichtlicher Rechtsschutz im Drittland ist gegeben. Die Vollstreckung ausländischer Urteile in den USA ist unter bestimmten Voraussetzungen vorgesehen und möglich. Die Unabhängigkeit der Gerichte ist gegeben.

#	Parameter	Teil-Ausprägung
6.1	Erfahren allgemeine Rechtsstaatsprinzipien (Bindung der Verwaltung an Recht und Gesetz, Bindung der Gerichte an das Gesetz, Rechtsweggarantie) im Zielland grundlegende Einschränkungen?	Nein
6.2	Existieren im Zielland Einschränkungen im Hinblick auf die Unabhängigkeit der Gerichte?	Nein
6.3	Existieren im Zielland praktische/tatsächliche Beschränkungen für den effektiven Rechtsschutz (etwa durch Anwaltszwang, überbordende Bürokratie, komplizierte Verfahren, etc.)?	Nein
6.4	Bestehen substantielle Hindernisse bei der Vollstreckbarkeit von Urteilen von Gerichten innerhalb der EU durch Gerichte im Zielland?	Nein

# Agenda



# Das Tool liefert einen Rechenschaftsbericht als Ergebnis



— Vom Ende her gedacht —

Erstellung eines einfach zu bedienenden Tools

Zusammenfassung der wichtigsten Informationen in einem entsprechenden Bericht

**Bewertung** der einzelnen Bedrohungen und ergänzenden Maßnahmen **verbleibt beim Exporteur/Verantwortlichen**

Nachweis der Wirksamkeit der ergänzenden Maßnahmen

Erfüllung der notwendigen Rechenschaftspflicht



# Festlegung der konkreten Umsetzung von Maßnahmen



P.001	Überprüfung Datenimporteur durch Verantwortlichen
P.002	Risikobewertung durch Anbieter
P.003	Transparenzberichte des Datenempfängers/Datenimporteurs
P.004	Technische Dokumentation
P.005	Externe Testate und Zertifizierungen, Prüfberichte anerkannter Verhaltensregeln
P.006	Überprüfung der zu übermittelnden Daten anhand des Schutzbedarfs
P.007	Interne Regelungen des Datenexporteurs zum Schutzbedarf verschiedener Datenkategorien



T.001	Ende-zu-Ende-Verschlüsselung (E2EE)
T.002	Anbieter arbeitet auf den Systemen des Verantwortlichen
T.003	Pseudonymisierung
T.004	Trusted Execution Environment (TEE)
T.005	Cloud-RAID-Verfahren
T.006	Stand der Technik
T.007	Sicherheits-Monitoring von Systemen (vorher: Härtung von Systemen)
T.008	Nutzung von MFA (Multi-Faktor-Authentifizierung)
T.009	Ausschließliche Nutzung von sicheren und nicht proprietären Kryptoalgorithmen



V.001	Regelungen zum Umgang mit Behördenanfragen
V.002	Prüfungspflichten des Datenimporteur bei Offenlegungsanfragen
V.003	Informationspflichten bei Offenlegungsanfragen
V.004	Pflicht zur Ergreifung Rechtsmittel gg. Offenlegungsanfragen
V.005	Unterstützungspflicht bei Gewährung individueller Rechte
V.006	Maßnahmen und Verpflichtungen bzgl. Umgang mit Offenlegungsanfragen
V.007	Haftungs- und Freistellungsverpflichtung zulasten Datenimporteur
V.008	Drittbegünstigungsklausel
V.009	Durchgriffsrechte / Berichtspflichten "in der Kette"
V.010	Ergänzende Informations- und Dokumentationspflichten bei Offenlegungsanfragen (Transparenzbericht)
V.011	Sicherstellung der Vollstreckbarkeit etwaiger Urteile
V.012	Vertragliche Verpflichtungen zur Einführung geeigneter Garantien zur Erhöhung des Schutzniveaus
V.013	Hinterlegung
V.014	"Warrant Canary"-Verfahren (passive Informationspflicht)
V.015	Zusicherung bzgl. Erleichterung des Zugriffs für Behörden



## Systematik

Die Maßnahmen teilen sich in die drei Bereiche


- ▶ prozessual
- ▶ technisch
- ▶ vertraglich

Jede Maßnahme kann auf ein oder mehrere Gewährleistungsziele wirken

Für jede Maßnahme wird beschrieben, wer diese (oder welche Teile davon) umsetzen muss



# Schritt 6: Prüfung der Geeignetheit von Maßnahmen



	Beschreibung
Maßnahmen-ID	T.005 Cloud-RAID-Verfahren
Beschreibung (Anforderung/Umsetzung)	Ein Redundant Array of Inexpensive Disks (RAID) ist eine Technologie zur Zusammenfassung mehrerer physischer zu einem einzelnen logischen Speicher. Es dient in erster Linie dem Schutzziel Verfügbarkeit, indem es unter anderem die Möglichkeit bietet, den Betrieb der logischen Umgebung auch beim Ausfall physischer Speicher fortzusetzen. Nebenbei ein Spilloff des Hardware-Plattens-Instanz macht sich mit Hilfe der Vorteile der RAID-Technologie innerhalb der Cloud zunutze. Zu speichernde Daten werden hierbei in mehrere Fragmente unterteilt und auf verschiedene Cloud-Provider verteilt. Auf diese Weise führt ein Ausfall von Cloud-Providern oder die Migration von Cloud-Speicher nicht zum Verlust der Ursprungsdaten. Durch die nutzerspezifische Verschlüsselung werden darüber hinaus die Schutzziele Vertraulichkeit und Integrität gewährleistet. Es ist einzelnen Cloud-Anbietern weder möglich, Rückschlüsse auf die Ursprungsdaten aus einzelnen Fragmenten zu gewinnen, noch können Inhalte durch böswillige Insider verifiziert werden. Die hochverfügbare Speicherung und Redundanz innerhalb der Cloud gehört zu den Kernfunktionen von Cloud-Anbietern. RAID werden als elementare Schutzmaßnahmen für Vertraulichkeit, Integrität und Verfügbarkeit gewährleistet, ohne dass kritische Verantwortungsbereiche an die Cloud-Provider übertragen werden müssen.
Wirksamkeit	Vertraulichkeit, Integrität und Verfügbarkeit
Umgesetzt durch	Verantwortlichen/Dateiexporteur/Dateiimporteur
Gewährleistungsebene	Vertraulichkeit

Beschreibung der Maßnahme & was bei Umsetzung zu beachten/wichtig ist

Wie und worauf wirkt die Maßnahme

## Systematik

Jede Maßnahme muss hinsichtlich der Wirksamkeit gegen die konkrete Bedrohung aufgrund der rechtlichen Situation im Drittstaat bewertet werden.

in Diskussion: wie Bewertungsmaßstäbe oder Mindestanforderungen aussehen können, um in Abhängigkeit der konkreten Umstände von „geeigneten Garantien“ sprechen zu können (C311/18, Art. 46 DSGVO i.V.m. ErwG 108).

## P.001 Überprüfung Datenimporteur durch Verantwortlichen



Zur Bewertung, ob die Standard-Datenschutzklauseln ein angemessenes Schutzniveau im Drittland für den konkreten Dienstleister bieten können, kann eine individuelle Bewertung des Dienstleisters hilfreich sein. Neben einer initialen Befragung und Auswertung muss auch eine turnusmäßige Wiederholung erfolgen. In folgende Schritte lässt sich die Maßnahme aufteilen:

1. Fragebogen-Versand an Anbieter und/oder Datenimporteur vor Beauftragung zur Einschätzung / Verifizierung der konkreten Bedrohungen bzgl. Datenzugriff durch Sicherheitsbehörden und für Rechte und Freiheiten der Betroffenen
2. Einschätzung / Verifizierung (genannter) konkreter Bedrohungen bzgl. Wahrscheinlichkeit Datenzugriff durch Sicherheitsbehörden und für Rechte und Freiheiten der Betroffenen bei Anbieter und/oder Datenimporteur durch Verantwortlichen, bzw. seiner Anwälte/DSB (basierend auf Fragebogen, Informationen, Fachkenntnissen, Erfahrungen)
3. Regelmäßige, standardisierte Abfrage / Nachkontrolle der konkreten Bedrohung bei Anbieter und/oder Datenimporteur
  - a. in Form vertraglicher Verpflichtung des Anbieters regelmäßig unaufgefordert über Änderungen, Neuigkeiten die Auswirkung auf Bedrohung haben zu informieren (z.B. in neuem Transparenzreport)
  - b. Verantwortlicher sollte regelmäßig (jährlich) Abfragen/Fragebogen versenden oder neuen Transparenzreport anfordern

Beispiel



Die Maßnahme kann einen Zugriff durch Behörden auf Daten nicht verhindern. Sie unterstützt den Verantwortlichen bei der Bewertung, ob ein entsprechender Zugriff im Drittland wahrscheinlich ist. Ferner ist der Abgleich mit vorherigen Antworten des Dienstleisters wichtig, um Indikatoren zu erhalten, ob während der laufenden Zusammenarbeit ggf. Zugriffe durch Behörden auf die Daten stattgefunden haben könnten.

Daher hat die Maßnahme mehrfache mittelbare Wirkung für ein höheres Datenschutzniveau beim Datenimporteur und höheren Schutz für die Betroffenen.

1. Sicherstellung Zuverlässigkeit
2. Bewertungshilfe für weitere Maßnahmen
3. Vergleich verschiedener Datenimporteure
4. ...



Umzusetzen durch:

- Datenexporteur



Wirkt auf Gewährleistungsziele:

- Vertraulichkeit
- Transparenz
- Intervenierbarkeit

# Sanity-Check

Maßnahmenrelevanz: 110

Nummer P.002

Bezeichnung Risikobewertung durch Anbieter

Wirkung: indirekt

Erläuterung  
Wirksamkeit: Maßnahme liefert keine Hinweise auf konkrete Zugriffe bestimmter Daten. Daher kann Maßnahme nur zur Bewertung der Eintrittswahrscheinlichkeit eines Zugriffs dienen (entweder vor erstmaliger Übermittlung oder im Rahmen der lfd. Zusammenarbeit).

Maßnahme wird nicht angewandt

Begründung:

Maßnahme ist angesichts der Kritikalität der Daten und der Bedrohungslage im Drittland nach eingehender Betrachtung als nicht erforderlich bewertet wurde. Ein adäquates Schutzniveau für die Rechte und Freiheiten der Betroffenen kann mit den verbleibenden Maßnahmen erreicht werden

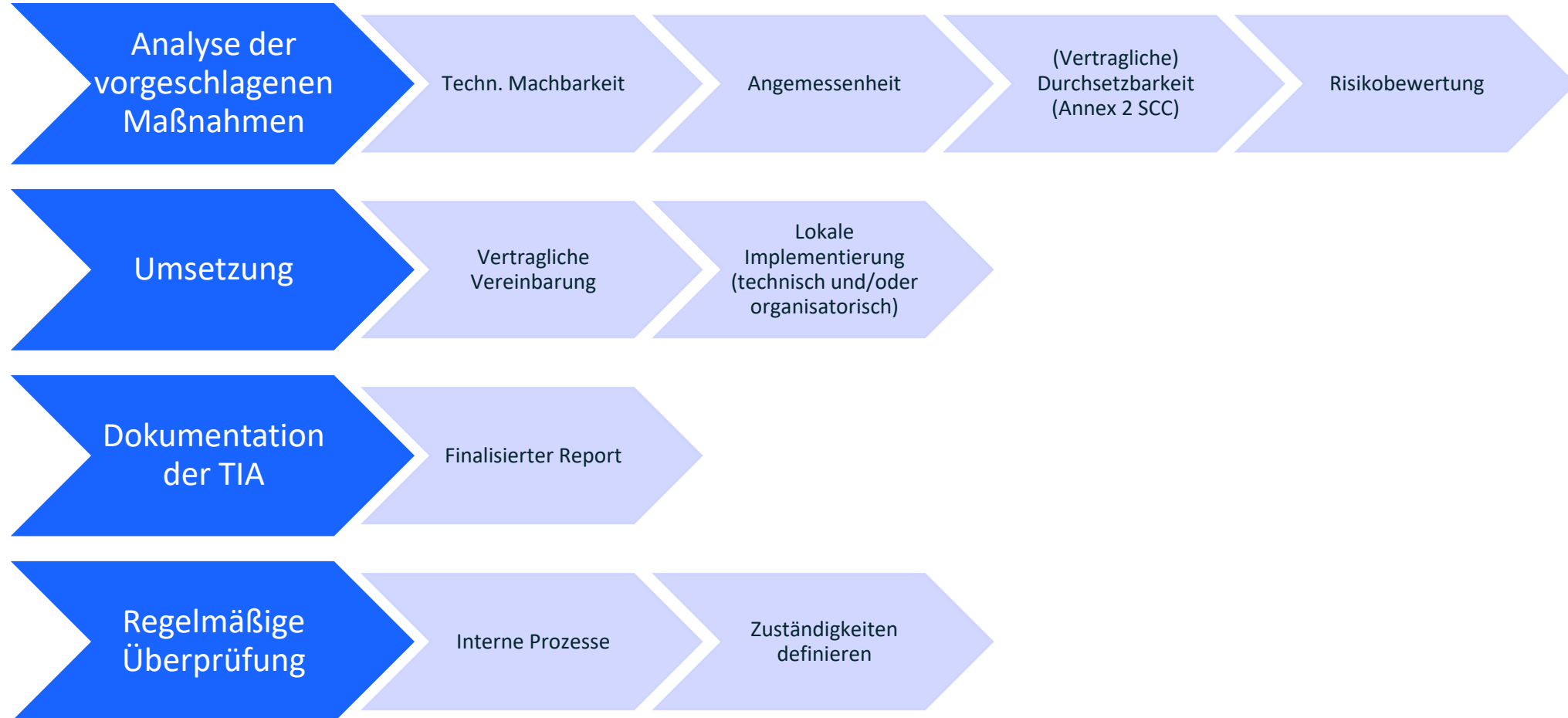
## Systematik

Nach Eingabe aller Parameter werden alle relevanten Maßnahmen vorgeschlagen.

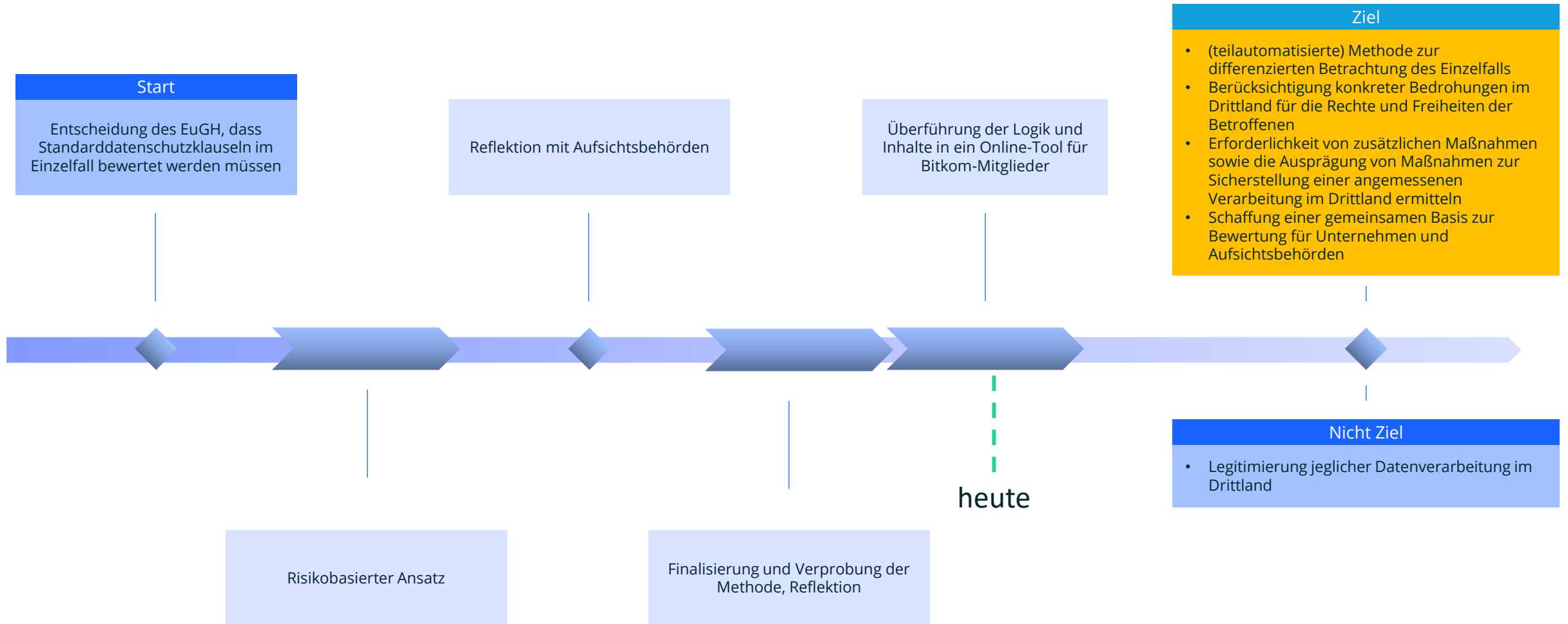
Der Anwender kann nun daraus Maßnahmen abwählen (mit kurzer Begründung – Freitext oder Auswahl noch offen)

Ausgabe der Eingaben, des Drittlandprofils und der Maßnahmen als Report in editierbarem Format

# Aufgabe des Verantwortlichen



# work in progress: Zwischenstand



# Beispiel Videokonferenzsystem mit Anbieter in den USA

In welches Land soll der Datentransfer stattfinden?	USA
<b>Umstände der Übermittlung:</b>	
Bestehen besondere Anforderungen an die Vertraulichkeit (z.B. Art. 9 DSGVO, Fernmeldegeheimnis)	ja
Sind die betroffenen Daten ausschließlich aus öffentlichen Quellen erhoben?	nein
Liegt eine wirksame Einwilligung aller Betroffenen zur Übermittlung dieser Daten nach USA vor?	nein
Erfolgt eine persistente Speicherung der Daten im Drittland? *	ja
Erfolgt die Übermittlung ausschließlich in Form eines Remote-Zugriffes aus USA heraus auf Systeme im EWR, ohne dass eine Speicherung im Drittland vorgesehen ist? **, **	nein
Erfolgt die Übermittlung rein konzernintern?	nein
Werden oder sollen die Daten innerhalb von USA an Dritte/weitere Empfänger übermittelt werden?	ja
* Dass diese beiden Parameter für ein- und dieselbe Datenübermittlung gleichzeitig ausgeprägt sind, ist eher ausgeschlossen. Dies dient ausschließlich der Erläuterung des Prinzips.	
** Damit dieses Privileg wirksam wird, müssen allerdings ausreichende Maßnahmen zur Beschränkung des Zugriffs getroffen sein.	



Relevanz	ID	Bezeichnung
900	T.001	Ende-zu-Ende-Verschlüsselung (E2EE)
700	T.003	Pseudonymisierung
500	T.004	Trusted Execution Environment (TEE)
500	T.005	Cloud-RAID-Verfahren
500	T.008	(Verteilte) Nutzung von MFA (Multi-Faktor-Authentifizierung)
400	T.002	Anbieter arbeitet auf den Systemen des Verantwortlichen
300	P.006	Überprüfung der zu übermittelnden Daten anhand des Schutzbedarfs
300	V.001	Verbindliche vertragliche Regelungen zum Umgang mit Behördenanfragen
300	V.002	Verbindliche vertragliche Prüfungspflichten des Verarbeiters / Datenimporteur bei Offenlegungsanfragen
		Verbindliche vertragliche Prüfungspflichten des Verarbeiters / Datenimporteur