

**KONSEQUENZEN
DES SCHREMS II
URTEILS IN DER
PRAXIS:
LÖSUNGSANSÄTZE
DES BITKOM**

Fachtagung Datenschutz im
Gesundheitswesen
am 06. Mai 2021



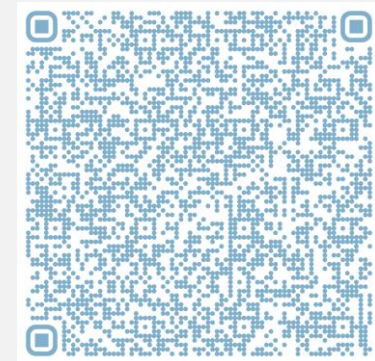
HEIKO GOSSEN
Geschäftsführer



migosens GmbH
Wiesenstraße 35
45473 Mülheim an der Ruhr
Tel. 0208 / 99395110
heiko.gossen@migosens.de



stellv. Vorsitzender des Bitkom AK Datenschutzes
Datenschutzauditor (TÜVCert)
Lead Auditor ISO 27001 i.A. der TÜV Rheinland
Cert GmbH
ehem. Datenschutzbeauftragter der Telefónica
Deutschland GmbH und Postbank Systems AG
Network Security Engineer



„UNSERE MITARBEITER SIND **JURISTEN, TECHNIKER, INFORMATIKER, KAUFLEUTE UND PROZESSMANAGER**. SOMIT KÖNNEN WIR ALLE ASPEKTE EINER FACHLICHEN HERAUSFORDERUNG UMFASSEND BETRACHTEN UND LÖSUNGEN MIT WEITBLICK ANBIETEN.“

Heiko Gossen, Geschäftsführer



Unser Serviceportfolio gliedert sich in vier Bereiche

migosens



datenschutz

Beratung

Audits (intern/extern)

Externer DSB

TK-Datenschutz



managementsysteme*

Beratung

(27001 / 9001 / 22301)

Audits (intern)

Externer ISB / QMB

Einführung ISMS

QMS und *i*DSMS®



akademie

DSB-Ausbildung

Projekte und Prozesse

Informationssicherheit

Integrierte Managementsysteme



worksmart

Führung und Zusammenarbeit

Organisationsentwicklung

Arbeitsumfeld gestalten

ERFAHRUNG. WISSEN. BERATUNG.

* ein Angebot der migosens management GmbH

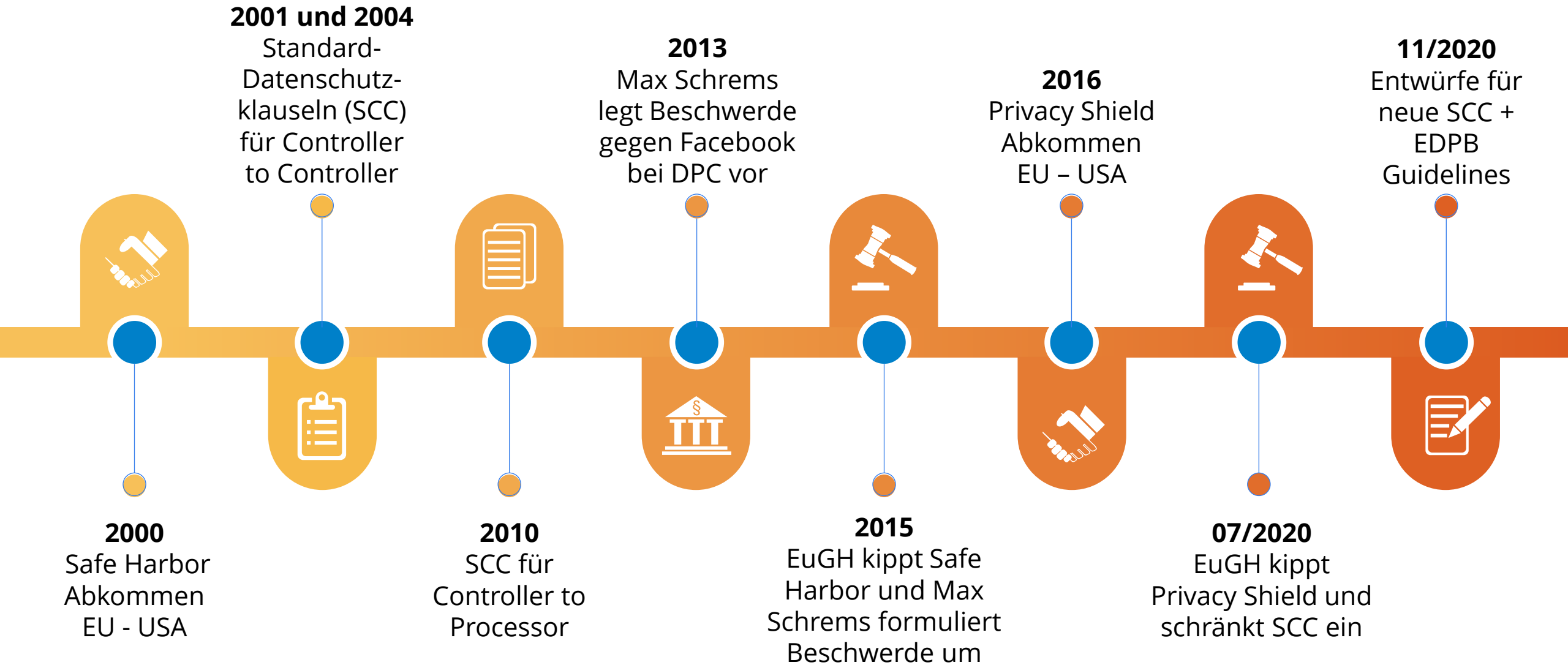
The image shows two women in a professional setting, likely a meeting room. They are looking at a large digital display wall. The woman on the left is wearing glasses and a dark top, pointing towards the screen. The woman on the right is wearing a yellow top and has her hand raised as if explaining something. The screen displays various data visualizations, including a world map and several circular progress indicators with percentages. The overall atmosphere is collaborative and focused on data analysis.

migosens

WIR WOLLEN GEMEINSAM BESSER WERDEN

Unser Wissen zu teilen ist die höchste
Wertschätzung und der sicherste Weg
Richtung Zukunft









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



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

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



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



SCC ist nicht geeignet, um diesen Mangel zu beheben

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

Frage 8



Zuständige **Aufsichtsbehörde** ist **verpflichtet**, eine auf **Standarddatenschutzklauseln gestützte Übermittlung** in ein **Drittland auszusetzen** oder zu verbieten, wenn sie der Auffassung ist, dass die **Klauseln in diesem Drittland nicht eingehalten** werden (können) und dass der nach dem Unionsrecht erforderliche Schutz der übermittelten Daten nicht durch andere Mittel gewährleistet werden kann.

Fragen 7 und 11



Geeignete Garantien nach Art. 46 Abs. 2 Buchst. c der DSGVO können in von der Kommission erlassenen Standarddatenschutzklauseln bestehen. Nach diesen Bestimmungen **müssen aber nicht sämtliche Garantien zwangsläufig in einem Beschluss der Kommission** wie dem SDK-Beschluss vorgesehen sein.

Verantwortlicher muss prüfen, ob das Recht des Bestimmungsdrittlands einen angemessenen Schutz der auf der Grundlage von Standarddatenschutzklauseln übermittelten personenbezogenen Daten gewährleistet, und erforderlichenfalls mehr Garantien als die durch diese Klauseln gebotenen zu gewähren

Ist dieser Schutz nicht gegeben, ist die Übermittlung auszusetzen oder zu beenden.

Fragen 4, 5, 9 und 10



Das Gericht hat u.a. Zweifel
an der Wirksamkeit und
Unabhängigkeit des
Ombudsmanns



Die Kommission hat bei ihrer Feststellung in Art. 1 Abs. 1 des DSS-Beschlusses, dass die Vereinigten Staaten für personenbezogene Daten, die im Rahmen des EU-US-Datenschutzschilds aus der Union an Organisationen in diesem Drittland übermittelt würden, ein angemessenes Schutzniveau gewährleisten, die Anforderungen verkannt, die sich aus Art. 45 Abs. 1 der DSGVO im Licht der Art. 7, 8 und 47 der Charta ergeben.

Ungültigkeit des gesamten Beschlusses zum „Privacy Shield“





- EU Kommission stellt Entwürfe für neue Standard-Datenschutzklauseln Ende 2020 zur öffentlichen Konsultation
- Genauer Zeitpunkt der Verabschiedung unklar

- SECTION I - Allgemeines
- SECTION II – Verpflichtungen der Parteien, aufgeteilt in vier Module
 1. Transfer controller to controller
 2. Transfer controller to processor
 3. Transfer processor to processor
 4. Transfer processor to controller
- SECTION III – FINAL PROVISIONS

SECTION I

Clause 1: Zweck und Anwendungsbereich

- (a) Zweck dieser Standardvertragsklauseln ist es, **die Einhaltung der Anforderungen der Datenschutz-Grundverordnung** für die Übermittlung personenbezogener Daten in ein Drittland sicherzustellen.

SECTION II

Clause 2: Lokale Gesetze, die sich auf die Einhaltung der Klauseln auswirken

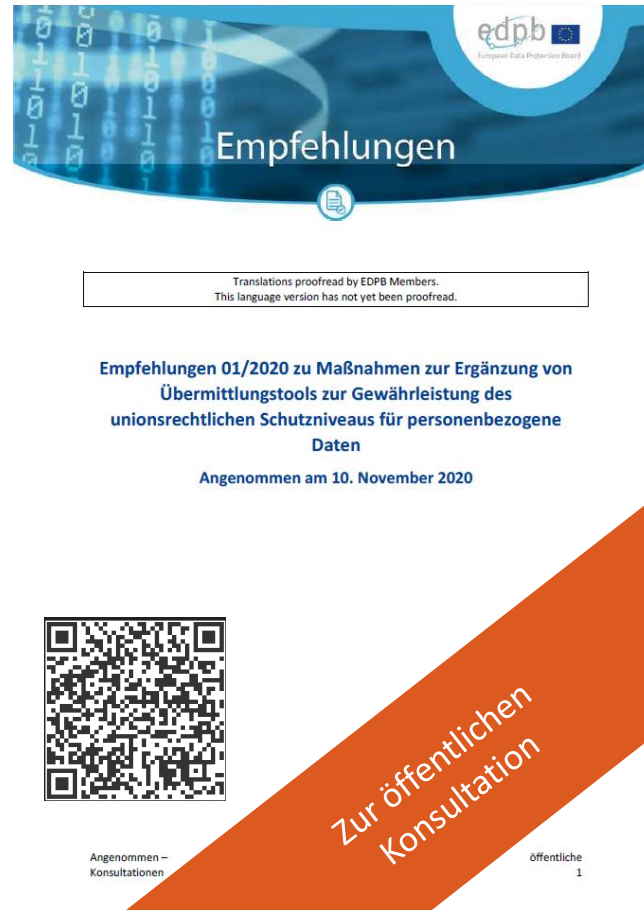
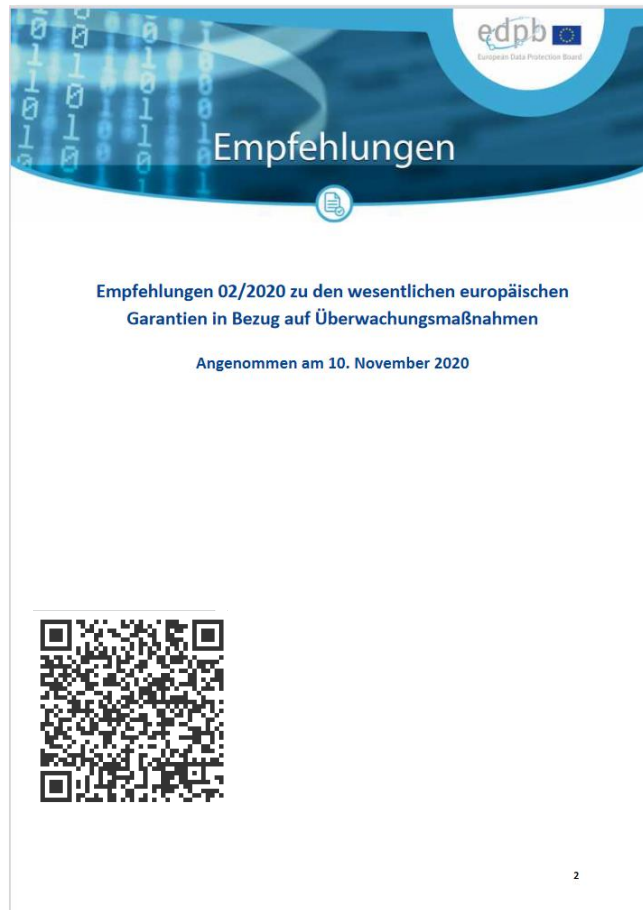
- a) Die Parteien sichern zu, dass **sie keinen Grund zu der Annahme haben**, dass **die anwendbaren Gesetze [..] den Datenimporteur daran hindern**, seine Verpflichtungen gemäß diesen Klauseln zu erfüllen.

SECTION III

Clause 1: Nichteinhaltung der Klauseln und Kündigung

- (a) Der **Datenimporteur informiert den Datenexporteur unverzüglich**, wenn er diese Klauseln, aus welchen Gründen auch immer, **nicht einhalten** kann.
- (b) Verstößt der Datenimporteur gegen diese Klauseln oder ist er nicht in der Lage, diese Klauseln einzuhalten, **setzt der Datenexporteur** die Übermittlung personenbezogener Daten an den Datenimporteur **aus**.

Helfen die Empfehlungen des Europäischen Datenschutz-Ausschusses?



- Empfehlungen 02/2020 zu den wesentlichen europäischen Garantien in Bezug auf Überwachungsmaßnahmen
 - ▶ Angenommen am 10. November 2020
- Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten
 - ▶ Angenommen am 10. November 2020
 - ▶ Öffentliche Konsultation

A

Auf klaren, präzisen und zugänglichen Vorschriften beruhende Datenverarbeitung

B

Nachweis der Erforderlichkeit und Angemessenheit im Hinblick auf die verfolgten legitimen Ziele

C

Vorhandensein eines unabhängigen Aufsichtsmechanismus

D

Vorhandensein wirksamer Rechtsbehelfe für den Bürger



Erläuterungen

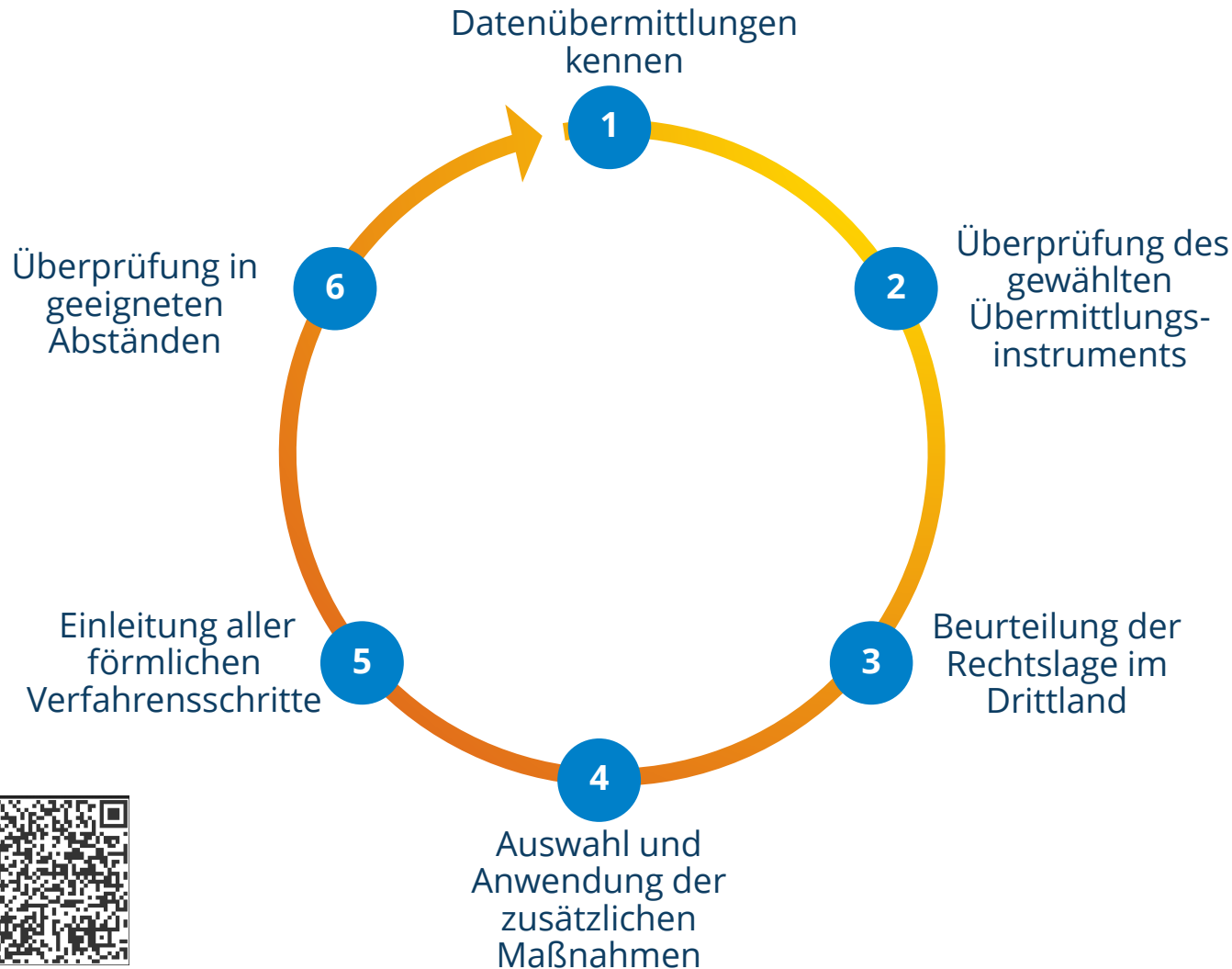
Insbesondere, wenn die Rechtsvorschriften, die den Datenzugriff staatlicher Stellen regeln, unklar oder nicht allgemein zugänglich sind.

Wenn es keine Rechtsvorschriften gibt, sollte der Datenexporteur auf andere relevante und objektive Umstände abstellen.

Subjektive Faktoren – etwa, ob ein nicht mit dem unionsrechtlichen Schutzniveau in Einklang stehender Datenzugriff staatlicher Stellen auf seine Daten wahrscheinlich ist – dürfen nicht berücksichtigt werden.

Diese Bewertung erfordert eine gründliche Prüfung und Dokumentation, da der Datenexporteur für die auf dieser Grundlage getroffene Entscheidung rechenschaftspflichtig ist.





Anhang 2: Beispiele für zusätzliche Maßnahmen



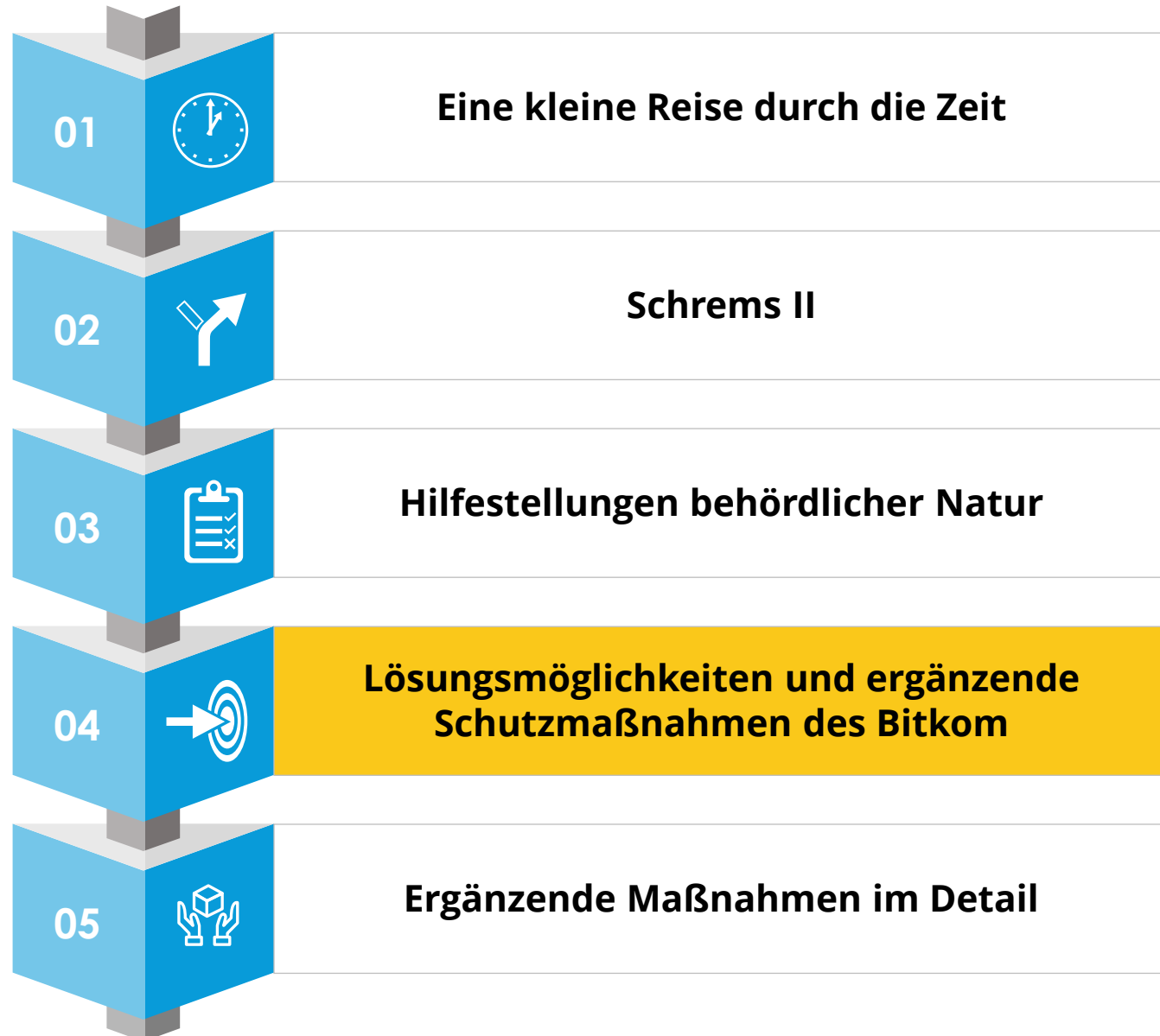
„Eine **zusätzliche Maßnahme ist nur als effektiv** im Sinne des Schrems II-Urteils des Gerichtshofs anzusehen, sofern und soweit die Maßnahme **genau die Rechtsschutzlücken schließt**, die der Datenexporteur bei seiner Prüfung der Rechtslage im Drittland festgestellt hat.“



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

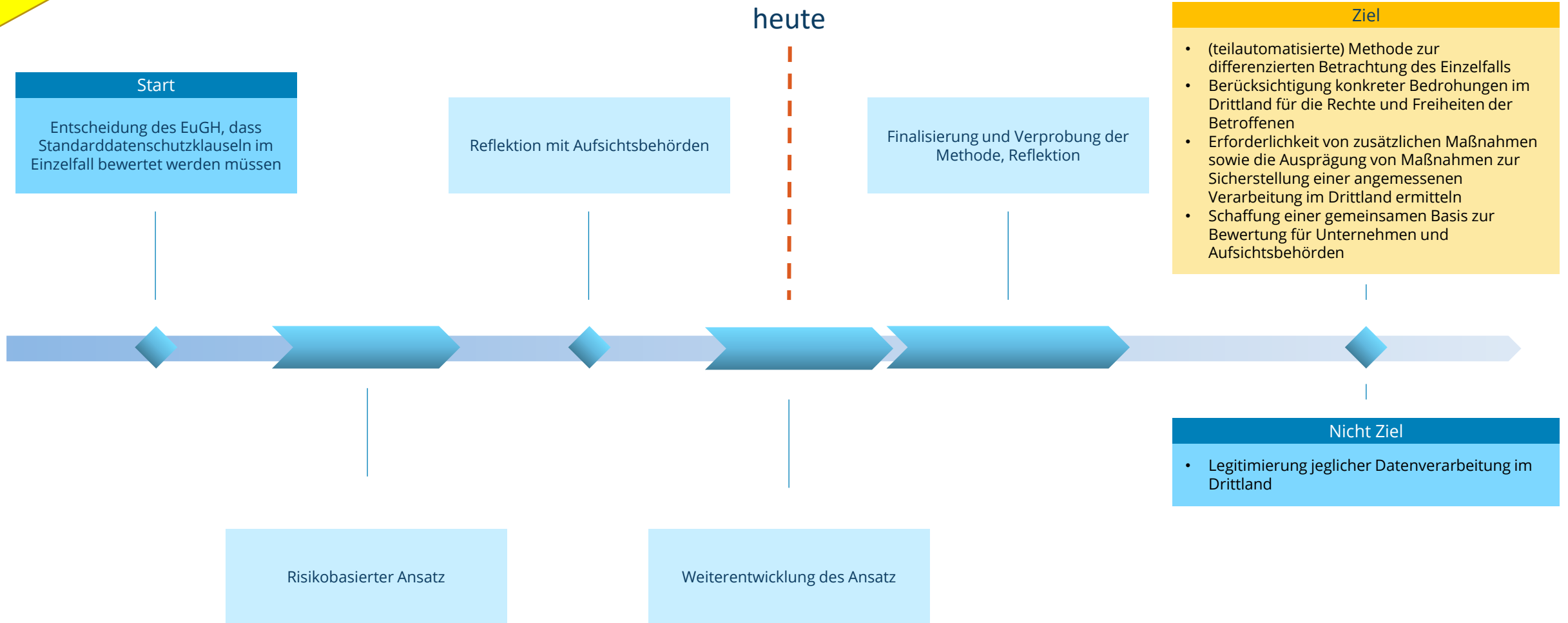


Technische Maßnahmen
Zusätzliche vertragliche Maßnahmen
Organisatorische Maßnahmen



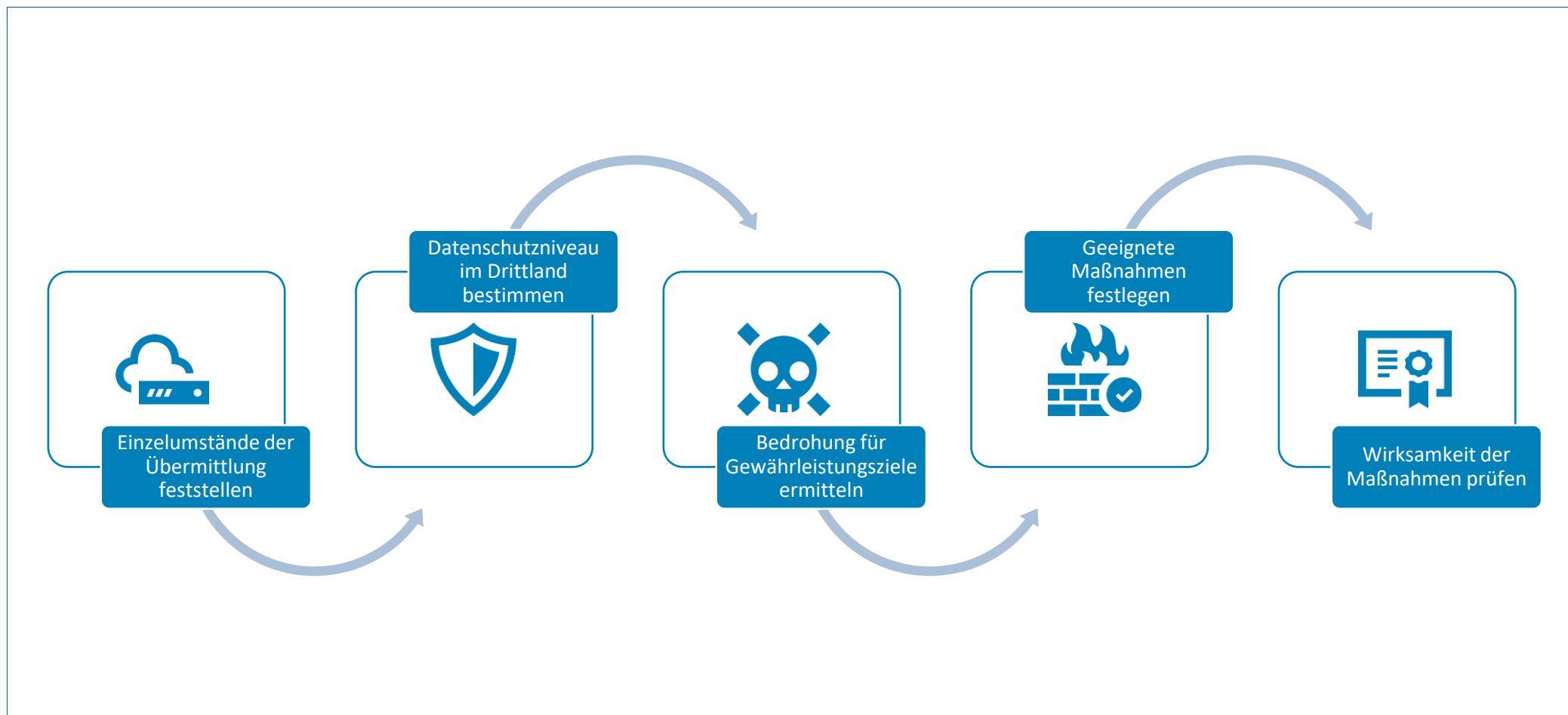
work in progress: Zwischenstand Bitkom AK Datenschutz

Stand:
30. April
2021

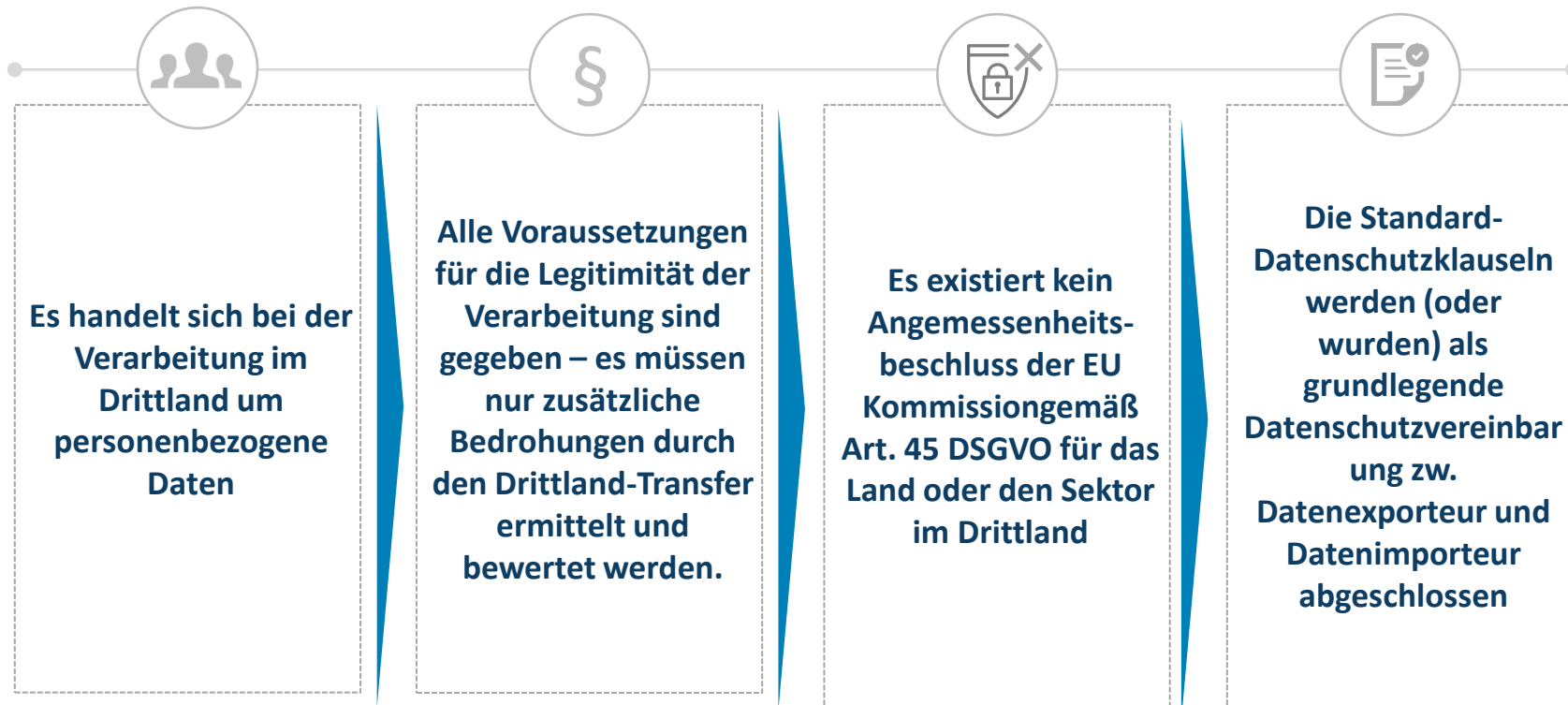


Das Grundprinzip in 5 Schritten

Stand:
30. April
2021



Stand:
30. April
2021



Die Gewährleistungsziele des SDM als „kleinster gemeinsamer Nenner“



Schritt 1: Ermittlung des Übermittlungsprofils

Stand:
30. April
2021

Übermittlungsszenario

Übermittlungsszenario	Übermittlungsprofil	Text
pbDaten stammen nicht ausschließlich aus öffentlichen Quellen	<ul style="list-style-type: none"> Vertraulichkeit Verfügbarkeit Integrität Intervenierbarkeit Transparenz 	Im Hinblick auf Verfügbarkeit und Integrität der Daten sollte der Betroffene allenfalls Erwartungen an die öffentliche Quelle haben. Die Herausforderung der Intervenierbarkeit aber auch der Transparenz stellen sich auch in dieser Konstellation.
Betroffener hat in Drittland-übermittlung nicht eingewilligt?	<ul style="list-style-type: none"> Vertraulichkeit Verfügbarkeit Integrität Intervenierbarkeit Transparenz 	Der Umstand einer vorliegenden Einwilligung des Betroffenen, die die Drittland explizit beinhaltet, kann sich positiv auf alle Gewährleistungsziele auswirken.
kein ausschließlicher Remote-Zugriff auf Systeme des Exporteurs?	<ul style="list-style-type: none"> Vertraulichkeit Verfügbarkeit Integrität Intervenierbarkeit Transparenz 	Remote-Zugriffe auf Systeme des Verantwortlichen/Datenexporteurs erhöht grundsätzlich die Möglichkeiten zur Ausübung von Kontrolle.
Erfolgt Speicherung im Drittland?	<ul style="list-style-type: none"> Vertraulichkeit Verfügbarkeit Integrität Intervenierbarkeit Transparenz 	Auswirkung grundsätzlich auf alle Gewährleistungsziele, Intervenierbarkeit aufgrund des faktischen Kontrollverlustes evtl. etwas stärker.
Übermittlung erfolgt außerhalb des Konzerns?	<ul style="list-style-type: none"> Vertraulichkeit Verfügbarkeit Integrität Intervenierbarkeit Transparenz 	Innerhalb eines Konzerns sind effektivere Maßnahmen möglich (Richtlinien, Prozesse, Anweisungen), welche die Risiken für fast alle Gewährleistungsziele mitigieren können.
Weiterübermittlung im Drittland?	<ul style="list-style-type: none"> Vertraulichkeit Verfügbarkeit Integrität Intervenierbarkeit Transparenz 	Der mit der Weiterübermittlung im Drittland verbundene faktische und potenziell rechtliche Kontrollverlust beeinträchtigt das Übermittlungsprofil. Weiterübermittlung in andere Drittländer löst eigene Prüfung aus.
Keine besonderen Maßnahmen zum Schutz d. Vertraulichkeit?	<ul style="list-style-type: none"> Vertraulichkeit Verfügbarkeit Integrität Intervenierbarkeit Transparenz 	Wir fassen hier diverse Möglichkeiten des Vertraulichkeitsschutzes (bspw. Verschlüsselung) zusammen; andere Gewährleistungsziele (außer Integrität) bleiben davon unberührt.
Daten unterliegen besonderen Vertraulichkeitsanforderungen?	<ul style="list-style-type: none"> Vertraulichkeit Verfügbarkeit Integrität Intervenierbarkeit Transparenz 	Besondere Anforderungen wie bspw. das Fernmeldegeheimnis können in Abhängigkeit der Regelungen im Drittland relevant werden.

Systematik

Reduzierung der Parameter des Übermittlungsprofils auf entscheidende Aspekte

Generelle Betrachtung, welcher Parameter sich auf welches Gewährleistungsziel auswirkt

Legende

konkrete Bedrohung

generelle Bedrohung

reduzierte Bedrohung

nicht relevant

Schritt 2: Abgleich mit Länderprofil

Stand: 30. April 2021

Zielland

Länderprofil	keine vergleichbaren Regelungen zum Richtervorbehalt?	keine wirksamen verwaltungsrechtl. Rechtsmittel für Betroffenen?	keine wirksamen zivilrechtl. Rechtsmittel für Betroffenen?	keine wirksamen Rechtsmittel für Datenimporteure?	Unabhängigkeit der Gerichte nicht gewährleistet?	Unvereinbare Geheimdiensttätigkeiten bekannt?	Regelungen zur Schaffung von "Hintertüren"?
	↓	↓	↓	↓	↓	↓	↓
	<ul style="list-style-type: none"> Vertraulichkeit Verfügbarkeit Integrität Intervenierbarkeit Transparenz 	<ul style="list-style-type: none"> Vertraulichkeit Verfügbarkeit Integrität Intervenierbarkeit Transparenz 	<ul style="list-style-type: none"> Vertraulichkeit Verfügbarkeit Integrität Intervenierbarkeit Transparenz 	<ul style="list-style-type: none"> Vertraulichkeit Verfügbarkeit Integrität Intervenierbarkeit Transparenz 	<ul style="list-style-type: none"> Vertraulichkeit Verfügbarkeit Integrität Intervenierbarkeit Transparenz 	<ul style="list-style-type: none"> Vertraulichkeit Verfügbarkeit Integrität Intervenierbarkeit Transparenz 	<ul style="list-style-type: none"> Vertraulichkeit Verfügbarkeit Integrität Intervenierbarkeit Transparenz
	z.B. kein Richtervorbehalt für Zugriffe oder gerichtl. Überprüfung	kein verwaltungsrechtlicher Rechtsweg/Rechtsmittel verfügbar gg. ggf. rechtswidrigen Datenzugriff	kein zivilrechtlicher Rechtsweg/Rechtsmittel (z.B. Schadenersatz) verfügbar gg. ggf. rechtswidrigen Datenzugriff	Verwaltungsrechtlicher oder zivilrechtlicher Rechtsweg/Rechtsmittel nicht verfügbar für Verarbeiter/Importeur	Generelle Rechtsstaatlichkeit im Drittland und Unabhängigkeit der Gerichte, Freiheit von unzulässiger Beeinflussung (Beeinflussung außerhalb des Verfahrensrechts)	Sind besonders problematische Geheimdienstaktivitäten bekannt geworden, die auch nach nationalem Recht unzulässig wären? Bestehen besonders belastende zwischenstaatliche Vereinbarungen über die Geheimdiensttätigkeit?	Verpflichtungen nach nationalem Recht zur Schaffung von Hintertüren oder den Zugriff auf personenbezogene Daten oder Systeme zu erleichtern (EDPB Guidelines 103)?

Systematik

Prüfung der Bedrohungslage im Drittland anhand entscheidender Aspekte (Parameter)

Generelle Betrachtung, welcher Parameter sich auf welches Gewährleistungsziel auswirkt

Legende

- konkrete Bedrohung
- generelle Bedrohung
- reduzierte Bedrohung
- nicht relevant

Schritt 3: Prüfung der Schnittstellen ergibt Bedrohungsprofil

Stand:
30. April
2021

		Länderprofil						
		keine vergleichbaren Regelungen zum Richtervorbehalt?	keine wirksamen verwaltungsrechtl. Rechtsmittel für Betroffenen?	keine wirksamen zivilrechtl. Rechtsmittel für Betroffenen?	keine wirksamen Rechtsmittel für Datenimporteure?	Unabhängigkeit der Gerichte nicht gewährleistet?	Unvereinbare Geheimdiensttätigkeiten bekannt?	Regelungen zur Schaffung von "Hintertüren"?
		1	0	1	0	1	1	1
Übermittlungsprofil								
pbDaten stammen nicht ausschließlich aus öffentlichen Quellen	0							
Betroffener hat in Drittland-übermittlung nicht eingewilligt?	1	Vertraulichkeit Verfügbarkeit Integrität Intervenierbarkeit Transparenz	Vertraulichkeit Verfügbarkeit Integrität Intervenierbarkeit Transparenz	Vertraulichkeit Verfügbarkeit Integrität Intervenierbarkeit Transparenz	Vertraulichkeit Verfügbarkeit Integrität Intervenierbarkeit Transparenz	Vertraulichkeit Verfügbarkeit Integrität Intervenierbarkeit Transparenz	Vertraulichkeit Verfügbarkeit Integrität Intervenierbarkeit Transparenz	Vertraulichkeit Verfügbarkeit Integrität Intervenierbarkeit Transparenz
kein ausschließlicher Remote-Zugriff auf Systeme des Exporteurs?	1	Vertraulichkeit Verfügbarkeit Integrität Intervenierbarkeit Transparenz	Vertraulichkeit Verfügbarkeit Integrität Intervenierbarkeit Transparenz	Vertraulichkeit Verfügbarkeit Integrität Intervenierbarkeit Transparenz	Vertraulichkeit Verfügbarkeit Integrität Intervenierbarkeit Transparenz	Vertraulichkeit Verfügbarkeit Integrität Intervenierbarkeit Transparenz	Vertraulichkeit Verfügbarkeit Integrität Intervenierbarkeit Transparenz	Vertraulichkeit Verfügbarkeit Integrität Intervenierbarkeit Transparenz
Erfolgt Speicherung im Drittland?	0							
Übermittlung erfolgt außerhalb des Konzerns?	1	Vertraulichkeit Verfügbarkeit Integrität Intervenierbarkeit Transparenz	Vertraulichkeit Verfügbarkeit Integrität Intervenierbarkeit Transparenz	Vertraulichkeit Verfügbarkeit Integrität Intervenierbarkeit Transparenz	Vertraulichkeit Verfügbarkeit Integrität Intervenierbarkeit Transparenz	Vertraulichkeit Verfügbarkeit Integrität Intervenierbarkeit Transparenz	Vertraulichkeit Verfügbarkeit Integrität Intervenierbarkeit Transparenz	Vertraulichkeit Verfügbarkeit Integrität Intervenierbarkeit Transparenz
Weiterübermittlung im Drittstaat?	0							
Keine besonderen Maßnahmen zum Schutz d. Vertraulichkeit?	1	Vertraulichkeit Verfügbarkeit Integrität Intervenierbarkeit Transparenz	Vertraulichkeit Verfügbarkeit Integrität Intervenierbarkeit Transparenz	Vertraulichkeit Verfügbarkeit Integrität Intervenierbarkeit Transparenz	Vertraulichkeit Verfügbarkeit Integrität Intervenierbarkeit Transparenz	Vertraulichkeit Verfügbarkeit Integrität Intervenierbarkeit Transparenz	Vertraulichkeit Verfügbarkeit Integrität Intervenierbarkeit Transparenz	Vertraulichkeit Verfügbarkeit Integrität Intervenierbarkeit Transparenz
Daten unterliegen besonderen Vertraulichkeitsanforderungen?	0							

beispielhaft

Systematik

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

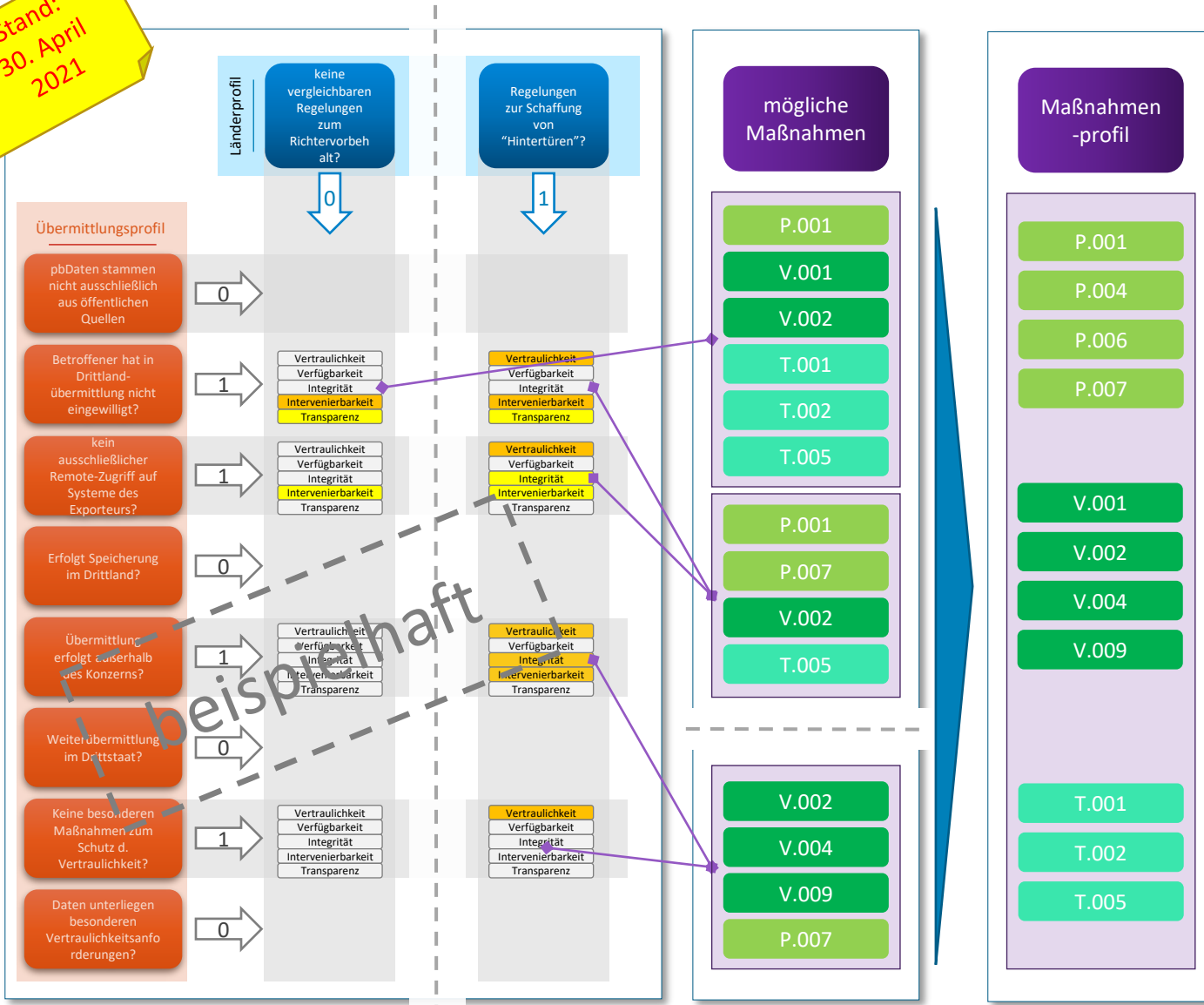
Ermittlung eines Bedrohungsprofils für die Gewährleistungsziele

Legende

konkrete Bedrohung	generelle Bedrohung	reduzierte Bedrohung	nicht relevant
--------------------	---------------------	----------------------	----------------

Schritt 4: Ableitung von Maßnahmen

Stand:
30. April
2021




Systematik

Bei jeder Bedrohung eines Gewährleistungsziels kann geprüft werden, welche Maßnahmen sich zur Mitigation der Bedrohung eignen.

Hieraus entsteht ein Set an Maßnahmen abhängig von den Einzelparametern des Übermittlungs- sowie des Länderprofils in ihrer Kombination.

Schritt 6: Prüfung der Geeignetheit von Maßnahmen

Stand:
30. April
2021



	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. Nexenio ein Spinoff des Hasso-Plattner-Instituts macht sich mit BDrive die Vorteile der RAID-Technologie innerhalb der Cloud zunutze. Zu speichernde Daten werden hierbei in mehrere Fragmente unterteilt und auf verschiedene Cloudprovider verteilt. Auf diese Weise führt der Ausfall von Cloud-Providern oder die Manipulation 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 Innentäter verfälscht werden.
Wirksamkeit	Die hoch verfügbare Speicherung von Daten innerhalb der Cloud gehört zu den Kernfunktionalitäten von Cloud-Anbietern. RAID werden die elementaren Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit gewährleistet, ohne dass kritische Verantwortungsbereiche an die Cloud-Provider abgetreten werden müssen.
Umzusetzen durch	Verantwortlichen/Datenexporteur/Datenimporteur
Gewährleistungsziele	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).

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.

Festlegung der konkreten Umsetzung von Maßnahmen

Stand:
30. April
2021



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



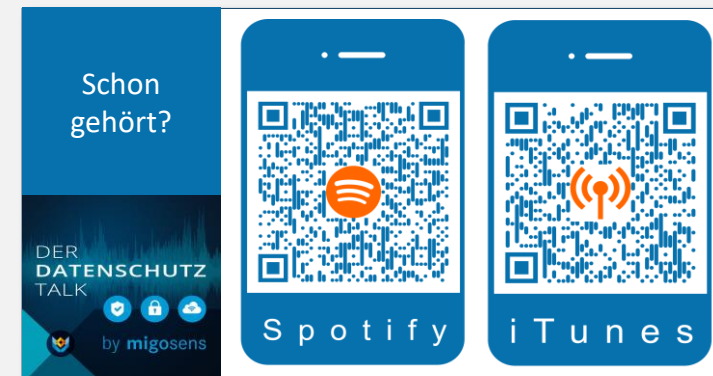
HEIKO GOSSEN
Geschäftsführer



migosens GmbH
Wiesenstraße 35
45473 Mülheim an der Ruhr
Tel. 0208 / 99395110
heiko.gossen@migosens.de



stellv. Vorsitzender des Bitkom AK Datenschutzes
Datenschutzauditor (TÜVCert)
Lead Auditor ISO 27001 i.A. der TÜV Rheinland
Cert GmbH
ehem. Datenschutzbeauftragter der Telefónica
Deutschland GmbH und Postbank Systems AG
Network Security Engineer





P.001 Überprüfung Datenimporteur durch Verantwortlichen

Stand:
30. April
2021



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



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

P.003 Transparenzberichte des Datenempfängers/Datenimporteurs

Stand:
30. April
2021



Transparenzberichte können sowohl generell als auch spezifisch sein. Ziel der Berichte ist es, eine Transparenz über die Häufigkeit der Zugriffe durch (öffentliche) Stellen in der Vergangenheit herzustellen, z.B. in Form von Statistiken auf der Webseite des Datenimporteurs oder im geschlossenen Benutzerbereich, z.B. über die jeweilige Admin-Konsole des Verantwortlichen abrufbar. Diese Berichte müssen regelmäßig aktualisiert werden.

Die Häufigkeit bzw. die evtl. auch nicht erfolgten Zugriffe können dem Datenexporteur ein Lagebild darüber geben, wie wahrscheinlich ein Zugriff auf die eigenen Daten ist – auch wenn diese Transparenzbericht in der Regel keine Rückschlüsse auf konkrete Datenbestände zulassen.

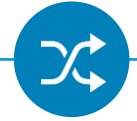
Veröffentlicht der Dienstleister diese Transparenzberichte bereits für Zeiträume vor dem erstmaligen Transfer, kann die Einsicht in die vergangenen Jahre eine hilfreiche Grundlage für die Bewertung der Erforderlichkeit für weitere Schutzmaßnahmen sein.



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.

Maßnahme hat mehrfache mittelbare Wirkung für höheres Datenschutzniveau beim Verarbeiter und höheren Schutz für die Betroffenen:

1. Transparenzberichte ermöglichen es dem Datensender/Datenexporteur eine abstrakte und teilweise konkrete Risikoeinschätzung bzgl. der Datenverarbeitung im Drittland und Bedrohung durch staatlichen Zugriff was wiederum Auswahl erforderlicher, geeigneter Maßnahmen mit direkter Wirksamkeit ermöglicht.
2. Die Maßnahme zwingt Datenempfänger/-importeure durch die Erstellung von Transparenzberichten zur umfassenden Implementierung sowie Dokumentation risikominimierender Maßnahmen u.a. bzgl. Umgang/Begrenzung konkreter Zugriffe/Zugriffsanfragen durch Dritte. Soweit der Datenempfänger/-importeure einen Transparenzbericht führt, muss er diesen auch inhaltlich zutreffend führen.
3. Maßnahme ermöglicht ggf. konkreten Vergleich der Risiken unterschiedlicher Verarbeiter/Datenimporteure
4. ...



Umzusetzen durch:

- Datenimporteure



Wirkt auf Gewährleistungsziele:

- Transparenz

P.005 Externe Testate und Zertifizierungen, Prüfberichte anerkannter Verhaltensregeln

Stand:
30. April
2021



Bei der Auswahl des Datenempfängers /-importeurs wird darauf geachtet, dass dieser die behaupteten technisch-organisatorischen Maßnahmen durch geeignete externe Testate und Zertifizierungen, inklusive der Prüfberichte von anerkannten Verhaltensregeln, untermauern kann.

Hierbei können je nach Umständen andere Testate und Zertifizierungen im Einzelfall relevant sein. Eine Übersicht einiger gängiger internationalen Standards mit Bezug zu Datenschutzfragen sind in der Anlage zu dieser Maßnahme tabellarisch aufgeführt.

Stand heute gibt es keine Testate / Zertifizierungen, die ausdrücklich einen Drittstaatentransfer legitimieren können, obgleich die DS-GVO derartige Mechanismen erlaubt, etwa anerkannte Verhaltensregeln nach Art. 40 DS-GVO oder Zertifikate nach Art. 42 DS-GVO. Es gibt bereits erste Initiativen, die sich aus dieser Perspektive dem Sachverhalt widmen und zwar im Wege einer Verhaltensregel im Bereich des Cloud Computings.

Ein zertifiziertes Management-System trifft streng genommen keine Aussage über die konkrete Umsetzung einzelner Maßnahmen, es trifft aber eine Aussage über das Vorliegen von Prozessen und Regeln, die geeignet sind, angemessene Maßnahmen festzulegen, umzusetzen und zu überprüfen. Es kann also von einer gesteigerten Wahrscheinlichkeit der Angemessenheit ausgegangen werden, da die Entscheidung über die Maßnahmen einem standardisierten Prozess unterliegt.

...



Entsprechend des erwarteten Risikos erscheint es sinnvoll, dass der Datensender / -exporteur sich nicht ausschließlich auf die vertraglichen Zusicherungen des Datenempfängers / -importeurs verlässt. Eine individuelle Prüfung ist nicht nur aufwändig, sondern kann unter Umständen selbst ein Risiko der Datensicherheit beim Datenempfänger /-importeur darstellen. Ein zielführender Kompromiss ist der Rückgriff auf externe Testate und Zertifikate, inklusive der Prüfberichte von anerkannten Verhaltensregeln, betreffend der zugesicherten Maßnahmen.

Soweit ein solches Testat nicht ausdrücklich ein solches nach Art. 46 Abs. 2 Buchst. e bzw. f betrifft, rechtfertigen diese Testate einen Drittstaatentransfer nicht unmittelbar.

Eine gewissenhafte Prüfung und Dokumentation der Ergebnisse sind unerlässlich.



- Datenexporteur (Prüfung und Bewertung von Zertifikaten)
- Datenimporteur (Aufrechterhaltung Zertifizierung)



- Vertraulichkeit
- Transparenz
- Verfügbarkeit
- Integrität

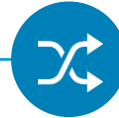
Stand:
30. April
2021



Datenexporteur klassifiziert intern Datenkategorien in Bezug auf ihren Schutzbedarf. Diese Maßnahme ergänzt die Maßnahme P006.



Es handelt sich um eine organisatorische Maßnahme (daher begrenzte Wirksamkeit gegeben), die zur Risikominimierung bei der Datenübermittlung beitragen kann, je nachdem welchen Schutzbedarf die übermittelten Daten aufgrund ihrer Sensitivität aufweisen.



Umzusetzen durch:

- Datenexporteur



Wirkt auf Gewährleistungsziele:

- Vertraulichkeit
- Transparenz
- Intervenierbarkeit

Beispiel

Klassifizierung	P1 - no PII (Standardwert)	P2 - Simple PII	P3 - Extended PII	P4 - Sensitive PII
Beschreibung	Generell werden keine pbD verarbeitet	Bearbeitungsvorgänge von pbD, deren Missbrauch keine besondere Beeinträchtigung der Rechte von betroffenen Personen nach sich zieht, oder öffentlich zugängliche Daten. Zusätzlich müssen auch der Zweck und die gesamten Umstände der Datenbearbeitung zu keinem besonderen Risiko führen können.	Personendaten, deren Missbrauch zu einer Beeinträchtigung für die Rechte und Freiheiten der betroffenen Personen führen kann. Bei dieser Beurteilung sind neben der Art der Daten auch der Zweck und die Umstände der Datenverarbeitung zu beurteilen.	Personendaten, deren Missbrauch zu einer erheblichen Beeinträchtigung für die Rechte und Freiheiten der betroffenen Personen führen kann. Bei dieser Beurteilung sind neben der Art der Daten auch der Zweck und die Umstände der Datenverarbeitung zu beurteilen.
Beispiele		<ul style="list-style-type: none"> • Name • Vorname • Adresse • E-Mail-Adresse • Geburtsdatum 	Alle personenbezogene Daten, die nicht in die Kategorie P2 oder P4 fallen. Z.B.: <ul style="list-style-type: none"> • Mitarbeiterbeurteilungen • Lohndaten • Umsatzdetails pro Kunden 	Besondere Kategorie von Personendaten: <ul style="list-style-type: none"> • Ethnie • Politische Gesinnung • Religiöse oder philosophische Weltanschauungen • Gewerkschaftszugehörigkeit • Genetische oder

T.001 Ende-zu-Ende-Verschlüsselung (E2EE)

Stand:
30. April
2021



Der Begriff Ende-zu-Ende-Verschlüsselung (End-to-End-Encryption - kurz E2EE) bezeichnet eine durchgehende Verschlüsselung im Bereich der Übertragung von Informationen. Dabei liegt der Fokus bei der E2EE auf der Durchgängigkeit der Verschlüsselung zw. Sender und Empfänger einer Nachricht. Die Schlüssel zur Ver- und Entschlüsselung sind i.d.R. nur dem (ersten) Sender und (endgültigen) Empfänger bekannt. Alle weiteren an dem Austausch der Information Beteiligten sind die Schlüssel nicht bekannt und damit die übertragene Information nicht zugänglich.

Bezogen auf eine Verarbeitung von personenbezogenen Daten in einem Drittstaat können Sender und Empfänger jedoch auch identisch sein.

Nicht jede Form der Verarbeitung in einem Drittstaat lässt jede Form der Verschlüsselung zu. Verarbeitungen z.B. im Bereich von Software-as-a-Service (SaaS), bei denen es gerade darauf ankommt, dass der Verarbeiter im Drittstaat die Klartext-Daten verarbeiten muss, ist eine E2EE i.d.R. nicht möglich.

Aber auch abgestufte Möglichkeiten der Verschlüsselung können bereits eine Reduzierung der Risiken für die Freiheiten und Rechte der Betroffenen bedeuten. Liegen die Schlüssel zur Ver- und Entschlüsselung auch beim Dienstleister im Drittstaat, hängt der Grad der Vertraulichkeit der Informationen in weiten Teilen vom Schlüsselmanagement ab.

...



E2EE kann eine der wirksamsten Maßnahmen hinsichtlich möglicher Bedrohungen im Drittland sein. Durch eine wirksame Verschlüsselung kann Unbefugten im Drittland der Zugang zu den Informationen verwehrt und eine Nutzung der Daten zu anderen Zwecken ausgeschlossen werden. Jedoch hängt die Wirksamkeit der Maßnahme sehr stark von den verwendeten Algorithmen, der technischen Implementierung und dem Schlüsselmanagement ab. Besonders wirksam ist die Maßnahme, wenn die vollständige Schlüsselverwaltung und -speicherung in Europa verbleibt und auch für ausländische Behörden keine Durchgriffsbefugnisse bestehen, die eine Herausgabe der Schlüssel erzwingen würde.



Umzusetzen durch:

- Datenexporteur



Wirkt auf Gewährleistungsziele:

- Vertraulichkeit
- Integrität



Bei der Pseudonymisierung werden eindeutige Identifikationsmerkmale durch ein Pseudonym (zumeist ein Code, bestehend aus einer Buchstaben- oder Zahlenkombination) ersetzt, um die Feststellung der Identität des Betroffenen auszuschließen oder wesentlich zu erschweren.

Die Pseudonymisierung ermöglicht also – unter Zuhilfenahme eines Schlüssels – die Zuordnung von Daten zu einer Person, was ohne diesen Schlüssel nicht oder nur schwer möglich ist, da Daten und Identifikationsmerkmale getrennt sind. Entscheidend ist also, dass eine Zusammenführung von Person und Daten noch möglich ist.

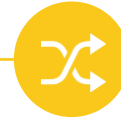
Je aussagekräftiger die Datenansammlung ist (z. B. Einkommen, Krankheitsgeschichte, Wohnort, Größe), desto größer ist die theoretische Möglichkeit, diese auch ohne Code einer bestimmten Person zuzuordnen und diese identifizieren zu können. Um die Anonymität gegenüber dem Verarbeiter/Dritten zu wahren, müssten diese Daten gegebenenfalls getrennt oder verfälscht werden, um die Identitätsfeststellung zu erschweren.

Die funktionale Trennung der Pseudonymisierung in die drei möglichen Funktionen eines Verantwortlichen möglich:

- 1) Durchführer der Pseudonymisierung
- 2) Halter der Zuordnungsregel und
- 3) Verarbeiter der pseudonymisierten Daten ...



Pseudonymisierte Daten mit separierter Zuordnungsregel entsprechen einer Art „temporären Anonymisierung“, die Daten können auch außerhalb des EWR verarbeitet werden, ohne die Freiheiten und Rechte der Betroffenen zu gefährden. Die Löschung der Zuordnungsregel entspricht einer Anonymisierung. Bei der Bewertung der Wirksamkeit bzw. der Angemessenheit der Maßnahme ist vor allem in Anbetracht der Gesamtheit der Daten zu achten, inwieweit sich auch ohne Zuordnungsregeln – ggf. auch unter Einbeziehung anderer Quellen – die Daten auf einzelne Betroffene zurückführen lassen.



Umzusetzen durch:

- Datenexporteur



Wirkt auf Gewährleistungsziele:

- Vertraulichkeit

T004 Trusted Execution Environment (TEE)

Stand:
30. April
2021



Moderne Rechnersysteme teilen sich Speicher (RAM, Festplatte, Cache) und Rechenkerne (CPU, Grafikkarte) für sämtliche Anwendungsbereiche. So läuft privilegierter Softwarecode, beispielsweise Dienste des Betriebssystems, in der gleichen technischen Umgebung, wie Nutzeranwendungen. Computerviren nutzen diesen Umstand, um kritische Anwendungsbereiche aus der Nutzerumgebung heraus zu manipulieren oder abzuhören. Virtualisierung oder Sandboxing sind Maßnahmen zur logischen Trennung von Anwendungen. Sie funktionieren allerdings nur so lange keine privilegierten Rechte existieren. Solche können durch Schwachstellen erlangt (Privilege Escalation Attack) oder bewusst vergeben worden sein (Innentäter).

Sichere Ausführungsumgebungen (TEE) bieten eine dedizierte Hardwareumgebung für die Ausführung kritischer Anwendungen, die auch von Anwendungen oder Nutzern mit privilegierten Rechten nicht manipuliert oder abgehört werden können. In der Regel wird die Abtrennung bestimmter Bereiche des Systems von der CPU gewährleistet. Sie stellt z.B. durch Verschlüsselung den Schutz kritischer Speicherbereiche und den sicheren Übergang der unsicheren in die vertrauenswürdige Umgebung durch einen speziellen Befehlssatz sicher. Mit Hilfe von Attestierungen kann nicht nur die Identität einer Anwendung, sondern auch ihre Integrität und die Gewährleistung ihrer Ausführung innerhalb des TEE kryptographisch belegt werden. Beispiele für TEEs sind Intel Software Guard Extensions (SGX) oder ARM TrustZone. Auch mobile Endgeräte wie Smartphones, ...



Durch den Einsatz von Sicherheitshardware zur Separierung unsicherer von sicheren Rechnerbereiche können kritische Anwendungen auch in Umgebungen ausgeführt werden, in denen eine Gefährdung durch boshafte privilegierte Nutzer existiert.

Diese Technik schützt bspw. Daten vor behördlichen Zugriffen bei Verarbeitung in virtualisierten Infrastrukturen, bei denen der Betrieb der Infrastruktur beim Datenimporteur, der Betrieb der Anwendung jedoch beim Datenexporteur selbst liegt.



Umzusetzen durch:

- Datenimporteur



Wirkt auf Gewährleistungsziele:

- Vertraulichkeit
- Integrität

Stand:
30. April
2021



Die Konfiguration von Sicherheitsloggings (auch „Sicherheitsprotokollierung“) und eines aktiven Monitorings (z.B. durch ein SIEM – Security Incident & Event Management System) der Protokolle zur Identifizierung helfen bei der Detektion von behördlich angeordneten Zugriffen auf Daten. Die Zugriffe lassen sich mit dieser Maßnahme zwar nicht verhindern, aber zumindest detektieren. Dies kann bspw. durch ein Erfassen von Zugriffen auf die Verschlüsselungsinformationen oder die Verwendung bestimmter Nutzerkonten erfolgen. Die Sicherheitsloggings müssen so konfiguriert werden, dass

- die Logfiles selbst nicht manipuliert werden können (z.B. durch Erfassung auf separaten Systemen außerhalb der Kontrolle des Datenimporteurs, Speicherung auf WORM-Medien) und
- die Deaktivierung des Loggings selbst zwingend zu einem Protokolleintrag führt.

Mit dem Datenimporteur sollte ferner festgelegt werden, wie geplante Zugriffe (z.B. zu Wartungszwecken) dokumentiert oder ggf. sogar vorab genehmigt werden.

Die genauen Metriken und Parameter des Loggings müssen im Einzelfall festgelegt werden, zum Beispiel zeitlich beschränkte Zugriffe, Angabe des Zwecks des Zugriffs, Genehmigungsverfahren und begleiteter Zugriff.



Erst mit Monitoring können untypische Zustände und Verläufe detektiert und auf diese entsprechend reagiert werden.

Werden auffällige Zugriffe identifiziert und der Datenimporteur kann oder darf diese nicht erklären, muss von einem unbefugten Zugriff ausgegangen werden. Ob, sofern es sich um einen behördlichen Zugriff gehandelt hat, dieser nach angemessenen rechtsstaatlichen Prinzipien erfolgt ist, kann dadurch nicht beantwortet werden.

Allerdings kann der Betroffene informiert werden und die Einlegung von Rechtsmitteln geprüft werden.

Werden keine auffälligen Zugriffe identifiziert, kann mit sehr hoher Wahrscheinlichkeit davon ausgegangen werden, dass kein behördlicher Zugriff stattgefunden hat.



Umzusetzen durch:

- Datenimporteur



Wirkt auf Gewährleistungsziele:

- Transparenz
- Intervenierbarkeit

T.009 Ausschließliche Nutzung von sicheren und nicht proprietären Krypto-Algorithmen

Stand:
30. April
2021



Vertrauenswürdige Kryptographie lebt vom Prinzip von Kerckhoff, welches besagt, dass die Sicherheit eines Verschlüsselungsverfahrens auf der Geheimhaltung des Schlüssels beruht anstatt auf der Geheimhaltung des Verschlüsselungsalgorithmus. Diesem Prinzip inhärent ist das Vorgehen kryptographische Algorithmen durch die Allgemeinheit, d.h. die Fachcommunity überprüfen zu lassen.

Das Gegenteil zu diesem Vorgehen stellt die Geheimhaltung des Verschlüsselungsalgorithmus dar – auch „Security through obscurity“ genannt. Eine Ausprägung dieses Prinzips sind proprietäre Algorithmen, die nicht durch die allgemeine Fachcommunity überprüft werden können/konnten. Hier muss sich der Nutzer einzig auf die Aussagen des Herstellers verlassen. Das Sicherheitsniveau eines Verschlüsselungsverfahrens kennzeichnet den Aufwand, den ein Angreifer betreiben muss, um an den Klartext zu gelangen. Das Sicherheitsniveau steigt mit der Anzahl der Möglichkeiten, die für die Auswahl des Schlüssels zur Verfügung stehen (der Bit-Länge).

Umsetzung:

Es sollte daher vor und regelmäßig während der Verarbeitung geprüft und sichergestellt werden, dass die eingesetzten Verschlüsselungsalgorithmen als sicher gelten.

Hilfestellung bietet hier bspw. das BSI mit der Übersicht der aktuell als sicher einzustufenden Algorithmen (QR).



Das Prinzip der durch die Fachcommunity evaluierten Algorithmen hat sich bewährt – zum Beispiel beim derzeit führenden symmetrischen Algorithmus AES – und gilt als vertrauenswürdiger als das Prinzip Proprietät.

Für die Wirksamkeit der Maßnahme muss daher regelmäßig und anhand verlässlicher Quellen die Aktualität eines verwendeten Verschlüsselungsalgorithmus geprüft werden. Dazu gehören neben dem eingesetzten Algorithmus selbst auch die eingestellten Parameter wie Schlüssellänge, Größe des Bildraums für Hashfunktionen, Sicherheit von Austauschverfahren für Schlüssel u.Ä.) sowie die gesamte Schlüsselverwaltung.



Umzusetzen durch:

- Datenexporteur



Wirkt auf Gewährleistungsziele:

- Vertraulichkeit
- Integrität

V.001 Eindeutige vertragliche Regelungen zum Umgang mit Behördenanfragen

Stand:
30. April
2021



Vereinbarung eindeutiger, vertraglicher Regelungen, Selbstverpflichtungen und Standards zum Umgang mit Datenauskunftersuchen durch Behörden des Ziellands

Implementierung eindeutiger vertraglicher Verpflichtungen mit dem Anbieter, durch:

- a. Identifikation des geeigneten Regelungsorts für die vertragliche Vereinbarung eindeutiger Regeln zum Umgang mit Datenauskunftersuchen durch Behörden des Ziellands (z.B. im Hauptvertrag, AVV, Anhang zum AVV, in SCC Ergänzungsvereinbarung oder durch Bezugnahme im jeweiligen Vertrag auf BCR). Hierbei muss sichergestellt werden, dass die vertraglichen Regelungen zum Umgang mit Datenauskunftersuchen durch Behörden des Ziellands durchsetzbar sind.
- b. Der Vorrang dieser Regeln im Widerspruchsfall mit anderen Dokumenten ist sicherzustellen..Die diversen Verträge und Anlagen (Hauptvertrag, AVV, SCC, BCR, etc.) enthalten oft widersprüchliche Vorrangsklauseln. Häufig geht der Hauptvertrag (z.B. Cloud Service Subscription Vertrag) allen Anlagen vor. Es muss aber sichergestellt werden, dass das Dokument mit den eindeutigen Regelungen zur Datenverarbeitung und insbesondere zum Umgang mit Behördenanfragen im Fall eines Widerspruchs/Regelungslücke jedem anderen Dokument vorgeht.

work in progress



Maßnahme hat mittlere mittelbare Wirkung für höheres Datenschutzniveau beim Verarbeiter und höheren Schutz für die Betroffenen:

Eindeutige rechtliche Verpflichtungen mit Vorrang im Konfliktfall sind elementare Grundvoraussetzung für alle weiteren, spezifischeren Maßnahmen und für die Implementierung eines höheren Datenschutzniveaus sowie den Schutz Betroffener. Maßnahme hat daher eine abstrakte hohe direkte Wirksamkeit.



Umzusetzen durch:

- Datenimporteure



Wirkt auf Gewährleistungsziele:

- Vertraulichkeit
- Transparenz
- Intervenierbarkeit

V.002 Prüfpflichten des Datenimporteurs bei Offenlegungsanfragen

Stand:
30. April
2021



1. Eindeutige, über das ohnehin erforderliche Maß hinausgehende, vertragliche Verpflichtung des Verarbeiters / Datenimporteurs zur detaillierten formellen und (soweit möglich) sachlichen Prüfung der Offenlegungsanfrage durch qualifizierte Rechtsanwälte
2. Eindeutige, über das ohnehin erforderliche Maß hinausgehende, vertragliche Verpflichtung des Verarbeiters / Datenimporteurs zur formellen und sachlichen Prüfung durch qualifizierte Rechtsanwälte/Rechtsabteilung, ob Offenlegungsanfragen zu weit geht oder unangemessen sind.

work in progress



Maßnahme hat mehrfache mittlere mittelbare Wirkung für höheres Datenschutzniveau beim Verarbeiter und höheren Schutz für die Betroffenen:

1. Maßnahme führt zu Implementierung funktionaler Prozesse und Kriterien zur Prüfung und Umgang mit Zugriffsanfragen die es ermöglicht ganz oder teilweise rechtswidrige Zugriffe/Zugriffsanfragen zu identifizieren und entsprechend der vereinbarten Verfahren zwischen Datensender/-exporteur und Datenempfänger/-importeuer zu reagieren.
2. mittelbare Erhöhung des Datenschutzniveaus, in dem sich die Behörden ggf. andere Adressaten für Ihre Zugriffsanfragen suchen werden, bei denen keine detaillierte formell / sachliche Prüfung und gegebenenfalls Zurückweisung des Offenlegungsantrags zu erwarten ist.
3. Maßnahme ermöglicht ggf konkreten Vergleich der Risiken unterschiedlicher Verarbeiter/Datenimporteure und damit Auswahl des Verarbeiters mit dem höchsten Datenschutzniveau.
4. Maßnahme hat bereits hohe praktische Wirksamkeit da von einigen Anbietern verwendet.



Umzusetzen durch:

- Datenimporteur



Wirkt auf Gewährleistungsziele:

- Vertraulichkeit
- Transparenz
- Intervenierbarkeit

Stand:
30. April
2021



1. unverzügliche Information des Verantwortlichen über erhaltene Offenlegungsanfragen von Sicherheitsbehörden und Regierungen (soweit rechtlich erlaubt) inkl. Nennung der gesetzlichen Grundlagen (Exportkontrolle, Geldwäsche, FISA 702 etc.) und aller weiteren Informationen die zur Prüfung/Geltendmachung von Rechtsmitteln notwendig sind.
2. unverzügliche Information der Betroffenen durch den Verantwortlichen (sofern rechtlich erlaubt) jeweils erhaltene Offenlegungsanfragen (Request) von Sicherheitsbehörden und Regierungen (soweit rechtlich erlaubt) inkl. Nennung der gesetzlichen Grundlagen (Exportkontrolle, Geldwäsche, FISA 702 etc.) und aller weiteren Informationen die zur Prüfung/Geltendmachung von Rechtsmitteln notwendig sind.
3. Regelmäßige Information des Verantwortlichen über Status Quo der Prüfung/Rechtsmittel/Maßnahmen zum Schutz der Daten (soweit rechtlich erlaubt)

work in progress



Maßnahme hat mehrfache hohe mittelbare Wirkung für höheres Datenschutzniveau beim Verarbeiter und höheren Schutz für die Betroffenen:

1. durch Informationspflichten Ergreifung werden konkrete direkte Maßnahmen ermöglicht um die konkret betroffenen Daten und/oder Rechte des Betroffenen schützen zu können.
2. Maßnahme führt zu Implementierung funktionaler Prozesse zur Prüfung, Umgang mit und Information über Zugriffsanfragen die Datenschutzniveau erhöhen.
3. Maßnahme ermöglicht ggf konkreten Vergleich der Risiken unterschiedlicher Verarbeiter/Datenimporteure und damit Auswahl des Verarbeiters mit dem höchsten Datenschutzniveau.



Umzusetzen durch:

- Datenimporteur



Wirkt auf Gewährleistungsziele:

- Vertraulichkeit
- Transparenz
- Intervenierbarkeit

Stand:
30. April
2021



1. Verpflichtung des Adressaten der Offenlegungsanfrage, eine Aufhebung (etwa durch Widerspruch gegen die Offenlegungsanfrage oder oder anderen Mitteln des vorläufigen Rechtsschutzes) oder Beschränkung der Offenlegungsanfrage (etwa durch restraint orders oder protective orders) zu erwirken, sofern nach dem Recht im Drittland möglich und unter Heranziehung eines objektiven Maßstabs nicht offensichtlich ohne Aussicht auf Erfolg, ohne dass dem Adressaten der Offenlegungsanfrage dabei ein subjektiver Ermessensspielraum zugeht

work in progress



Die Maßnahme hat mehrfache hohe unmittelbare und mittelbare Wirkung für ein höheres Datenschutzniveau beim Verarbeiter und einen höheren Schutz für die Betroffenen, da:

1. die Offenlegung der personenbezogenen Daten verzögert / ggf. eingeschränkt erfolgt und für die anfragende Behörde deutlich erschwert wird;
2. die unreflektierte Erfüllung von rechtswidrigen oder unangemessenen Offenlegungsanfragen und darauf beruhender Datenherausgaben verhindert wird;
3. die Maßnahme zur Implementierung funktionaler Prozesse zur Einlegung von Rechtsmitteln führt, wodurch das Datenschutzniveau abstrakt erhöht wird;
4. eine mittelbare Erhöhung des Datenschutzniveaus daraus folgen kann, dass sich die zuständigen Behörden im Drittland ggf. andere Adressaten für ihre Zugriffsanfragen suchen werden, bei denen keine vorläufigen Rechtsmittel gg. Offenlegungsanfragen zu erwarten sind;
5. die Maßnahme einen konkreten Vergleich der Risiken unterschiedlicher Importeure ermöglicht und damit die Auswahl des Importeurs mit dem höchsten Datenschutzniveau erlaubt.



Umzusetzen durch:

- Datenimporteure



Wirkt auf Gewährleistungsziele:

- Intervenierbarkeit

V.007 Erhöhte Haftungsbegrenzungen zulasten des Datenimporteurs

Stand:
30. April
2021



Vereinbarung unbegrenzter Haftung im Innenverhältnis zwischen Datenexporteur und Datenimporteur für Verstöße des Datenimporteurs gegen die SCC (Clause 7 (a) SCC: any breach of these Clauses) oder Verpflichtungen zum Schutz der Betroffenen (Clause 7 (c) SCC: any breach of the third party beneficiary rights) wie insbesondere zusätzliche Maßnahmen bzgl. Drittlandsübermittlung; z.B. per

- Verweis, dass Art. 82 (4), (5) DSGVO explizit auch für diese Verstöße gelten; oder
- Klarstellung, dass sich Regresshaftung im Innenverhältnis nach Clause 7 (b) SCC richtet (= voller Ersatz des tatsächlich erlittenen Schadens „Liability as between the Parties is limited to actual damage suffered.“); oder
- Klarstellung, dass an anderen Stellen vereinbarte vertragliche Haftungsausschlüsse oder Begrenzungen (z.B. im Hauptvertrag oder AVV) für diese Verstöße nicht gelten; oder

Alternativ:

Vereinbarung einer deutlich höheren Haftungsbegrenzung („Supercap“) im Innenverhältnis zwischen Datenexporteur und Datenimporteur für Verstöße des Datenimporteurs gegen die SCC (Clause 7 (a) SCC: any breach of these Clauses) oder Verpflichtungen zum Schutz der Betroffenen (Clause 7 (c) SCC: any breach of the third party beneficiary rights) wie insbesondere zusätzliche Maßnahmen bzgl. Drittlandsübermittlung;



Maßnahme hat eine relevante Wirkung für ein höheres Datenschutzniveau beim Verarbeiter und einen höheren Schutz für die Betroffenen, da:

1. sich Verstöße des Datenimporteurs gegen die SCC oder Verpflichtungen zum Schutz der Betroffenen wie insbesondere zusätzliche Maßnahmen bzgl. Drittlandübermittlung für Datenimporteur finanziell nachteilig spürbar auswirken und er daher signifikante Anstrengungen unternehmen wird, die Verpflichtungen einzuhalten; ...
2. die Vereinbarung unbegrenzter Haftung vom LFDI Baden-Württemberg als nötige Maßnahmen definiert sind (QR). Deswegen kann argumentiert werden, dass die Aufsichtsbehörden hier eine relevante Wirksamkeit sehen können.



Umzusetzen durch:

- Datenexporteur



Wirkt auf Gewährleistungsziele:

- Vertraulichkeit
- Transparenz
- Intervenierbarkeit

work in progress

V.008 Drittbegünstigungsklausel

Stand:
30. April
2021



Diese Maßnahme richtet sich auch zum Teil an die Durchgriffsrechtekette, ist allerdings im Grunde weiter. Der Datenexporteur/Verantwortliche und der Betroffene sind häufig nicht direkte Vertragspartner (in der Kette). Es könnte aber notwendig sein, dass der Datenexporteur/Verantwortliche und insbesondere die Betroffenen bestimmte Rechte eingeräumt bekommen.

Die Maßnahme soll die Regelungen bzgl. der Drittbegünstigung des Verantwortlichen/Datenexporteurs sowie der Betroffenen, die bereits in den Standardvertragsklauseln enthalten sind, ergänzen.

work in progress



Die DSGVO legt nur dem Datenexporteur bestimmte Pflichten auf. In der "Kette" ist es notwendig und praxistauglich, diese Pflichten vertraglich durchzustufen. Jedoch birgt jede weitere Stufe das inhärente (wenn auch nicht unbedingt hohe) Risiko, dass der Datenempfänger-/importeure den Verpflichtungen nicht vollumfänglich nachkommt. Eine solche Drittbegünstigungsklausel kann diese Risiken reduzieren, in dem die Kontroll- und Durchsetzungsberechtigten numerativ erweitert werden.



Umzusetzen durch:

- Datenimporteure



Wirkt auf Gewährleistungsziele:

- Intervenierbarkeit

V.011 Sicherstellung der Vollstreckbarkeit etwaiger Urteile in empfangender Jurisdiktion

Stand:
30. April
2021



Das zugrundeliegende materielle Recht für die datenschutzrechtlich relevanten Abschnitte der vertraglichen Regelungen ist die DSGVO. Die bloße Anwendbarkeit der DSGVO bedeutet indessen nicht automatisch, dass diese im Streitfall auch faktisch vom angerufenen Gericht beachtet wird und ein erwirkter Titel durchsetzbar ist. Unabhängig davon, ob ein Gerichtsstand innerhalb oder außerhalb des EWR vereinbart wird, sollte daher sichergestellt werden, dass die rechtliche Beurteilung auf Basis der DSGVO stattfindet und ein gerichtlich erwirkter Titel durchsetzbar ist. Darüber hinaus sollte darauf geachtet werden, dass die Verarbeitung ausschließlich oder wenigstens primär auf der Basis der DSGVO erfolgt und andere Gesetze (auch zum Datenschutzrecht) ausgeschlossen werden. Hierdurch kann ein conflict of law - zumindest teilweise - vermieden werden.

work in progress



Dies ist grundlegende Voraussetzung zur Sicherstellung der weiteren Maßnahmen dieser Matrix, da nur durch hinreichend Vorabprüfung der Vollstreckbarkeit weitere vertragliche Schutzmaßnahmen überhaupt durchsetzbar sind.



Umzusetzen durch:

- Datenexporteur



Wirkt auf Gewährleistungsziele:

- Intervenierbarkeit

V.014 Verbindliche vertragliche Pflichten des Datenimporteurs zum "Warrant Canary"-Verfahren

Stand:
30. April
2021



Verpflichtung des Importeurs, soweit rechtlich im Drittland erlaubt, regelmäßig (z.B. mindestens alle 24 Stunden) eine kryptographisch signierte Nachricht zu veröffentlichen, die den Datenexporteur darüber informiert, dass der Datenimporteur ab einem bestimmten Datum und Zeitpunkt keinen Auftrag zur Offenlegung von Personendaten oder ähnlichem an Behörden erhalten hat.

work in progress



Es ist von einer hohen Wirksamkeit auszugehen: Die Versendung der Nachricht erfolgt automatisiert und ist einfach (günstig) umsetzbar; ; Eine schnelle Information über einen möglichen Zugriff ist sichergestellt und ermöglicht sofortiges Vorgehen durch den Datenexporteur und/oder Betroffenen – je nach Jurisdiktion, in der dies möglich ist.

Evtl ist auch Prüfung auf fehlende Meldung durch Verantwortlichen automatisiert durchführbar was sofortige Reaktion ermöglicht.

Die Maßnahme hat potenziell eine große, praktische Wirkung auf ein höheres Datenschutzniveau beim Datenempfänger/-importeure und einen höheren Schutz für die Betroffenen:

1. Durch eine schnelle, zuverlässige und regelmäßige Information mit minimalem Zeitverlust wird nahezu eine sofortige Ergreifung direkter Maßnahmen ermöglicht, um konkret betroffene Daten und/oder Rechte des Betroffenen schützen zu können.
2. Die Maßnahme ermöglicht eine voll automatisierte, kostengünstige und skalierbare Implementierung funktionaler Prozesse zur Prüfung, zum Umgang mit und zur Information über Zugriffsanfragen, die das Datenschutzniveau erhöhen (insbesondere für technologisch führende Cloud/SaaS Provider)
3. Die Maßnahme ermöglicht ggf. einen konkreten Vergleich der Risiken unterschiedlicher Datenempfänger/-importeure und damit die Auswahl des Datenempfängers/-importeurs mit dem höchsten Datenschutzniveau.



Umzusetzen durch:

- Datenimporteur



Wirkt auf Gewährleistungsziele:

- Transparenz