Operationalisierung von Datentransfers in Drittstaaten im Kielwasser datenschutzrechtlicher Gerichtsentscheidungen (insb. sog. Schrems II-Entscheidung)

28. April 2022

ISACA Germany Chapter

Agenda

1. Vorstellung der Fachgruppe und der heutigen Referenten
2. Das Ausgangsproblem:
   Kernpunkte des EUGH-Urteils in der Sache C-311/18 (Schrems II)
3. Zur Motivation:
   Typische use cases eines Datentransfers
4. Der Rahmen des Vorgehens ist abgesteckt:
   Der 6-Punkte Plan des europäischen Datenschutzausschusses
5. Der Plan ist keine Umsetzungsanleitung: Was ist konkret zu tun ?
6. Ausblick: Wird’s besser oder schlimmer ?

ISACA Germany Chapter

Fachgruppe Datenschutz: Vorstellung

- (Wieder-)Gründung im September 2021
- Unser Maxime:
  - Brückenschlag zwischen rechtlicher Regulierung und technischer Umsetzung
  - Ansprechpartner und Verbreiter fundierter Fachinformationen zum Thema Datenschutz im internen und externen Netzwerk von ISACA
- Einige ausgewählte Ziele:
  - Unterstützung bei der Einordnung der vielfältigen, mit Datenschutz und Datensicherheit verbundenen, technischen & organisatorischen Anforderungen
  - Intensive Zusammenarbeit mit gesetzgebenden Gremien in Deutschland/der EU, der Wirtschaft und Wissenschaft

ISACA Germany Chapter

Vorstellung: Ihre heutigen Referenten

Kontaktdaten:
corinna.kulp@bdo.de
+49 -0- 175 6431012

Corinna Kulp
Dipl.-Volkswirtin und Dipl.-Kauffrau

Qualifikationen, u.a.:

CDPSE, CISA, IT-Auditor IDW, CINA

Schwerpunktthemen:

- Datenschutzaudits und Datenschutzmanagement
- IT-Revision (System- und IKS-Prüfung, IT-Governance, Quality Assessment)
- Projektmanagement
- IT-Beratung (Software-Implementierungen/-Wechsel: insb. für elektronische Rechnungsverarbeitung /Dokumentenmanagement und projektbegleitende Qualitätssicherung, Aufbau Interner Kontrollsysteme, Verfahrensdokumentationen)
- IT-Sicherheit

ISACA Germany Chapter

Vorstellung: Ihre heutigen Referenten

Henry M. Hanau
Dipl.-Wirtschaftsinformatiker &
Master of Laws IT-Recht

Qualifikationen, u.a.:

CISA, CGEIT, CDPSE, CIPP/E, ISO 27001 LA, CCSK u.w.m.

Schwerpunktthemen:

- Allgemeiner (DSGVO) und spezieller Datenschutz (Telekommunikation, Telemedien)
- Rechtskonforme digitale Werbung
- Plattform- und Datenökonomie, Cloudcomputing
- IT-Audit und IT-Sicherheit
- Aufbau & Optimierung von Compliance-Managementsystemen (u.a. ISMS, DSMS)

Kontaktdaten:
hmhanau@itc-p.de
+49 -0- 163 1609075

ISACA Germany Chapter

Vorstellung: Ihre heutigen Referenten

Kontaktdaten:
apostel@privacy.consulting
+49 -0- 174 200-9939

Unser Gast: Dr. Oliver Apostel

Rechtsanwalt

Qualifikationen, u.a.:

GDDcert. EU, ISB und DSB für Kreditinstitute, ITGCP

Schwerpunktthemen:

- Datenschutzrecht und Datenschutzmanagement
- IT-Recht
- Telemedien- und Telekommunikationsrecht
- Lauterkeitsrecht
- Vertragsgestaltung und -durchsetzung
- Aufbau und Optimierung von Compliance-Managementsystemen

ISACA Germany Chapter

Das Ausgangsproblem: Kernpunkte des EuGH-Urteils in der Sache C-311/18 (Schrems II)

ISACA Germany Chapter

Schrems II in a nutshell

➢ Ergebnis mit alleiniger US-Relevanz:

- ➢ Der lokal spezifische Angemessenheitsbeschluss namens Privacy Shield ist ungültig, da in den USA kein mit der EU vergleichbares Schutzniveau, gemessen an den verbrieften dortigen Grundrechten, gegeben ist
- ➢ Die Ungültigkeit gilt umgehend - die Abstützung von Datentransfers in die USA auf dieses Instrument entfällt sofort

➢ Ergebnis mit allgemeiner Gültigkeit für Datenübermittlungen in Drittländer:

- ➢ Die sog. Standardvertragsklauseln (SCC) können weiterhin als ein Transferinstrument genutzt werden, der entsprechende Kommissionsbeschluss bleibt bestehen
- ➢ Allerdings stellen sie eine einzelvertragliche Regelung zwischen den beiden isolierten Parteien (Exporteur und Importeur) her - nur zwischen diesen entfaltet sie Bindungswirkung
- ➢ Sollten daher Umstände im Empfängerland die Wirksamkeit des durch die SCC errichteten Schutzniveaus für die vom Export Betroffenen gefährden, sind vom verantwortlichen Exporteur, am besten in Zusammenarbeit mit dem Importeur, zusätzliche ausgleichende Maßnahmen technischer, organisatorischer und vertraglicher Art zu ergreifen
- ➢ Dazu sind die gefährdenden Umstände, denen durch Maßnahmen zu begegnen ist, natürlich zuerst zu identifizieren → Verpflichtung zum Assessment der Rechtslage im Zielland (sog. Transfer Impact Assessent: TIA)

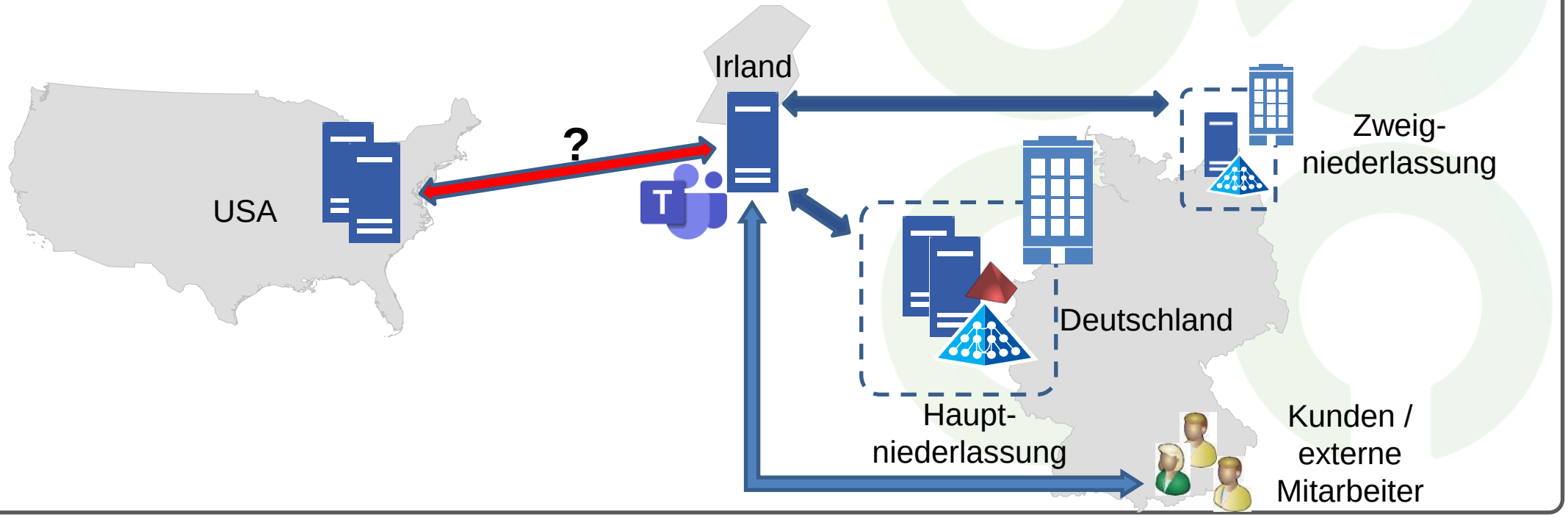
ISACA Germany Chapter

Anwendbarkeit der Vorgaben des EuGH anhand konkreter Einsatzszenarien

ISACA Germany Chapter

Use Case 1 – SaaS
KMU Kundenkommunikation

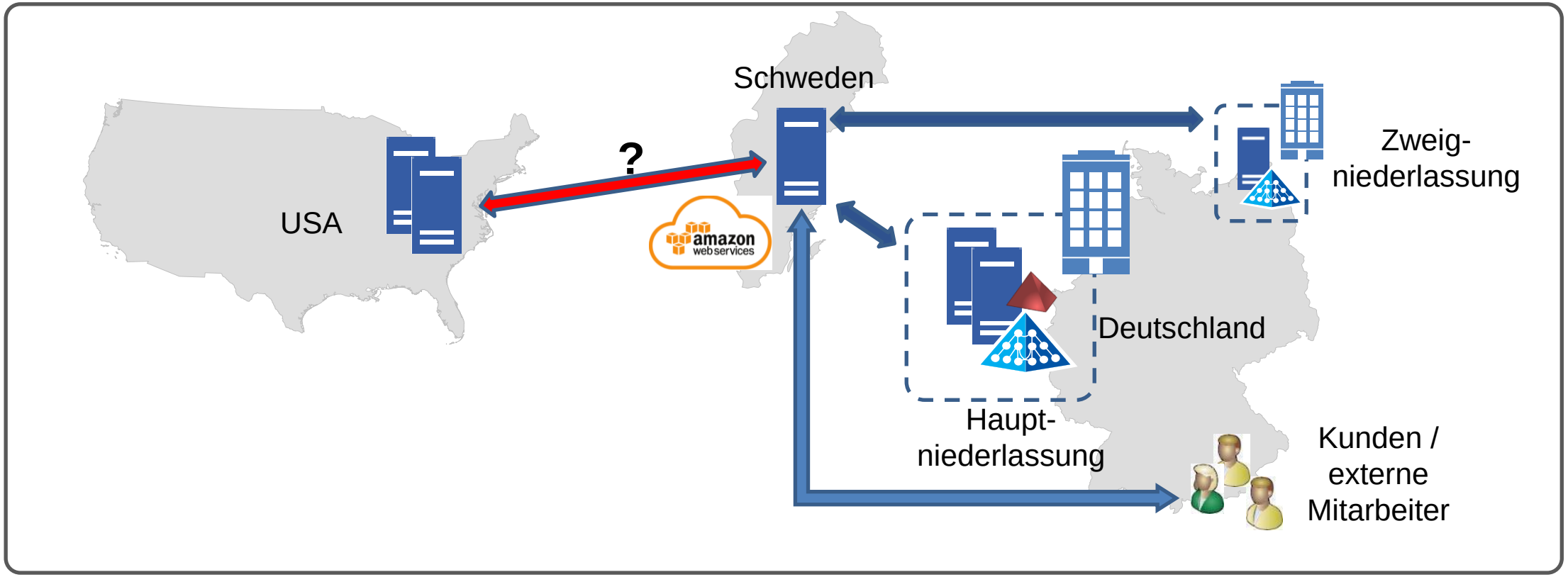
- Kommunikation Video und Chat via Microsoft Teams
- Geschäftszentrale in Deutschland mit eigenem Rechenzentrum
- Kunden und Mitarbeiter sind in Deutschland



ISACA Germany Chapter

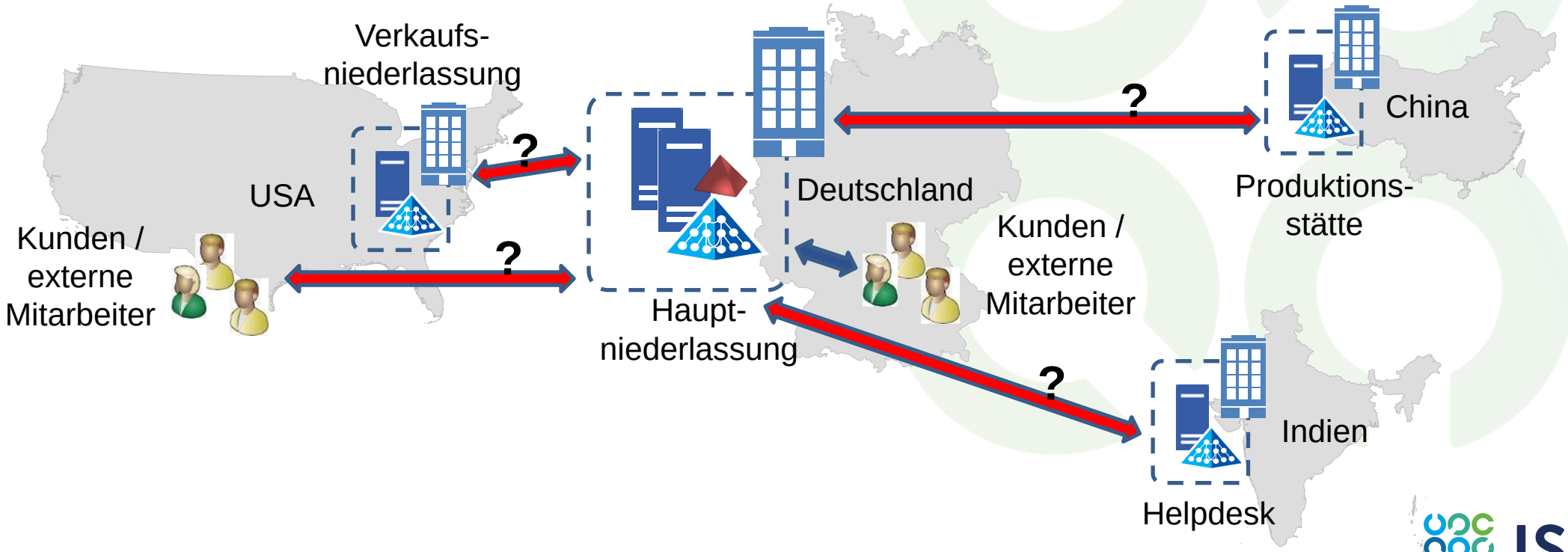
Use Case 2 – IaaS / PaaS
Konzern betreibt eigene Applikation in AWS Cloud

- Betrieb einer selbst entwickelten Applikation in der AWS Cloud
- Geschäftszentrale in Deutschland mit eigenem Rechenzentrum
- Kunden und Mitarbeiter sind in Deutschland



Use Case 3 – Intra Company
Firma mit Betriebsstätten im Außereuropäischen Ausland

- Intra Company Transfers mit Betriebsstätten im außereuropäischen Ausland Geschäftszentrale in Deutschland mit eigenem Rechenzentrum
- Kunden sind in Europa
- Mitarbeiter sind weltweit verteilt, aber größtenteils in Deutschland
- Dateiaustausch / Datenbankzugriffe weltweit



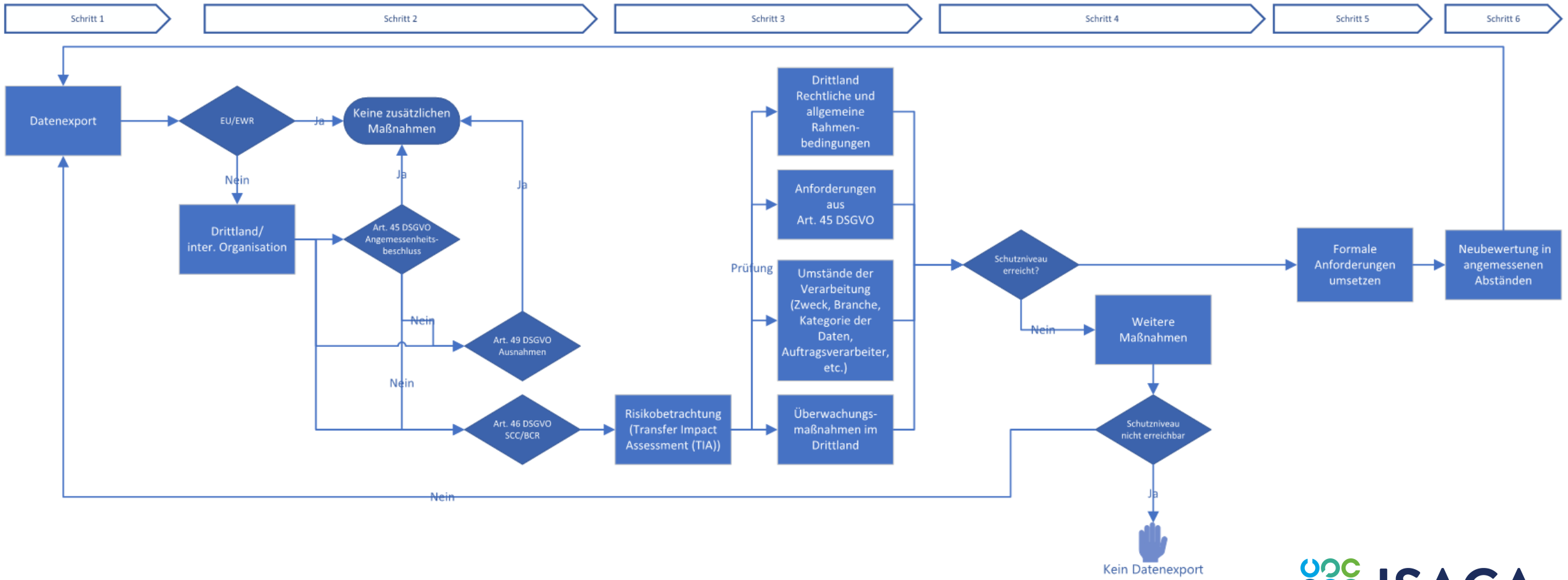
ISACA Germany Chapter

Der Rahmen der Umsetzung ist abgesteckt: der 6-Punkte Plan des europäischen Datenschutzausschusses

ISACA Germany Chapter

Handlungsschritte

Wer ist verpflichtet? : Der für die Verarbeitung Verantwortliche (Exporteur)



ISACA Germany Chapter

Der Plan ist keine Umsetzungsanleitung: Was ist konkret zu tun ?

ISACA Germany Chapter

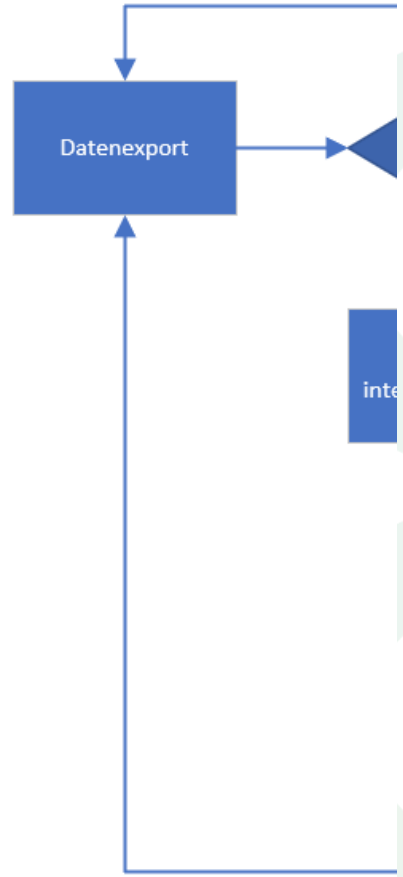
Schritt 1: Datentransfers identifizieren

1.a) Sind überhaupt personenbezogene Daten betroffen?

- Merkmale und Bespiele nach Art. 4 Nr. 1 DSGVO

1.b) Handelt es sich um eine Übermittlung?

- Der für die Verarbeitung Verantwortliche oder Auftragsverarbeiter unterliegt der DSGVO
- Der für die Verarbeitung und damit für den Export Verantwortliche oder Auftragsverarbeiter legt die Daten gegenüber einem anderen Verantwortlichen oder Auftragsverarbeiter (dem Importeur) offen
- Der Importeur ist in einem Drittland außerhalb der EU oder des EWR ansässig (unabhängig, ob er selbst der DSGVO unterfällt (was sein kann))
- Bei Bestandsverhältnissen gute Selektionskriterium in einem gepflegten **Verzeichnis von Verarbeitungstätigkeiten**
  (Auch wenn Art. 30 lit. e DSGVO initial nicht erfüllt, sollten die Kontaktdaten nebst Adresse schon aus Vertragsgründen vorhanden sein; Subauftragsverarbeiter können bei der gesetzlich vorgeschriebenen Due Diligence der ersten Wertschöpfungsstufe nicht im Verborgenen bleiben.)



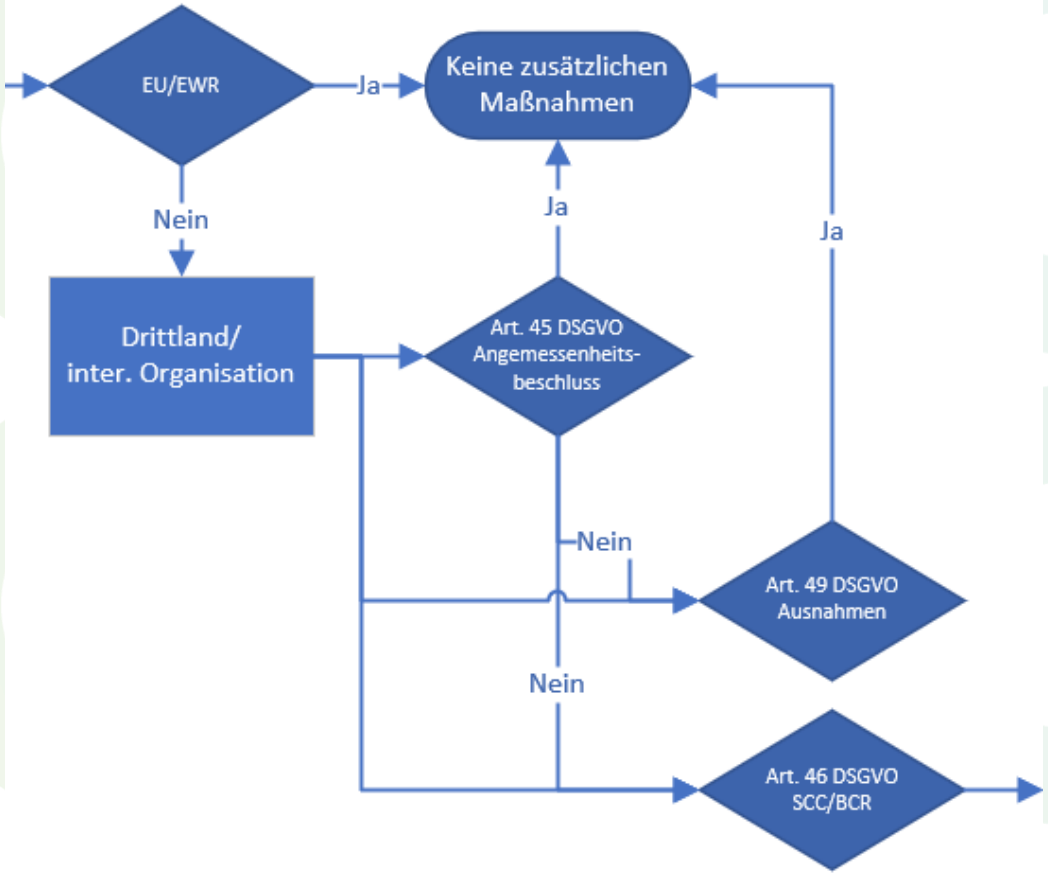
Achtung: Rechtsgrundlage der Übermittlung bestimmen!

ISACA Germany Chapter

Schritt 2: Übermittlungsinstrumente

Mit welchem, seitens der DSGVO vorgesehen, Mittel ist die Aufrechterhaltung des EU-garantierten Datenschutzniveaus (DSN) für den Datenaustausch mit dem Zielland gewährleistet?

- Angemessenheitsbeschluss
  Die EU-Kommission hat formell für das Zielland die Gleichwertigkeit des DSN bestätigt.
  Liste der anerkannten Länder:
  https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en
- Standardvertragsklauseln (SCC)
- Verbindliche interne Datenschutzvorschriften
- Ausnahmen nach Art. 49 DSGVO
  Achtung: eng zu verstehen, insb. Satz 2. Kein Freibrief, sofern die anderen Möglichkeiten nicht realisiert wurden. Ungeeignet für den Regelbetrieb.



ISACA Germany Chapter

Schritt 3: Beurteilung Wirksamkeit ausgewählter Übermittlungs-instrumente i.H.a. Gesamtumstände der Übermittlung (1)

- Kernfrage aus Schrems II: Unterminiert die tatsächliche (Rechts-)Lage im Empfängerland das gewählte Instrument?

- Trotz eingerichtetem Übermittlungsinstrument laufen ggfls. gesetzliche Regelungen im Zielland des Imports der mit dem Instrument verfolgten Absicherung des Transfers zuwider

- Exporteur und Importeur können sich darauf verständigen, diesen Lücken in der Absicherung mit wirksamen Maßnahmen entgegen zu wirken -> dazu muss man diese allerdings identifizieren -> Transfer Impact Assessment (TIA)

Schritt 3: Beurteilung Wirksamkeit ausgewählter Übermittlungs-instrumente i.H.a. Gesamtumstände der Übermittlung (2)

- Handfeste Hinweise ergeben sich schon aus dem Wortlaut der Standardvertragsklauseln (Klausel 14):
  - …einschließlich der Länge der Verarbeitungskette, der Anzahl der beteiligten Akteure und der verwendeten Übertragungskanäle, beabsichtigte Datenweiterleitungen … den Zweck der Verarbeitung, die Kategorien und das Format der übermittelten personenbezogenen Daten … den Speicherort der übermittelten Daten -> die Wertschöpfungskette muss bis zum Ende klar sein -> **Vergegenwärtigung des Ziels der Verarbeitung und Kontaktaufnahme zum Importeur**
  - die angesichts der besonderen Umstände der Übermittlung relevanten Rechtsvorschriften und Gepflogenheiten des Bestimmungsdrittlandes (einschließlich solcher, die die Offenlegung von Daten gegenüber Behörden vorschreiben oder den Zugang von Behörden zu diesen Daten gestatten) sowie die geltenden Beschränkungen und Garantien,
    Kontaktaufnahme zum Importeur; dsbzgl. Veröffentlichungen des Importeurs (zB https://www.microsoft.com/en-us/corporate-responsibility/us-national-security-orders-report?activetab=pivot_1:primaryr2)
  - die Art des Empfängers, der Wirtschaftszweig, in dem die Übertragung erfolgt, eröffnet Möglichkeit eines risikobasierten Ansatzes: wie wahrscheinlich ist es, dass der Importeur etwaigen Maßnahmen in seinem Sitzland unterworfen wird, die den mit der mit dem Instrument verfolgten Absicherung des Transfers zuwider laufen ?
    Kontaktaufnahme zum Importeur
  - **wesentlich Feststellung: gibt es eine zum gewollt eingerichteten DSN konträre Praxis im Zielland , wie wahrscheinlich ist die Realisierung in meinem Übertragungsfall ?**

ISACA Germany Chapter

Schritt 3: Beurteilung Wirksamkeit ausgewählter Übermittlungs-instrumente i.H.a. Gesamtumstände der Übermittlung (3)

- Handfeste Hinweise ergeben sich schon aus dem Wortlaut der Standardvertragsklauseln (Klausel 14):
  - alle relevanten vertraglichen, technischen oder organisatorischen Garantien, die zur Ergänzung der Garantien gemäß diesen Klauseln eingerichtet wurden, einschließlich Maßnahmen, die während der Übermittlung und bei der Verarbeitung personenbezogener Daten im Bestimmungsland angewandt werden
    -> welche mitigierenden Maßnahmen gegen die zuvorigen Feststellungen sind schon ergriffen worden ?

- **Gesamtbewertung, wie wahrscheinlich eine Kenntniserlangung der übermittelten Daten durch eine unbefugte dritte Partei ist -> Einzelfallbetrachtung -> keine Wissenschaft mit diskreten Größen (Bewertungs-Einschätzungsspielräume) -> essentiell: Dokumentation der gesamten Überlegungskette**
  Restrisiko einer abweichenden Einschätzung im behördlichen Überprüfungsfall bleibt gegeben.

- Vorlagen:
  https://iapp.org/resources/article/transfer-impact-assessment-templates/

Schritt 3: Beurteilung Wirksamkeit ausgewählter Übermittlungs-instrumente i.H.a. Gesamtumstände der Übermittlung (4)

- „Pragmatischer“ Ansatz, der allerdings zu Problemen in der Maßnahmenumsetzung führen kann:

  Unmittelbare Annahme eines unzureichenden Schutzniveaus und direkter Übergang zu Schritt 4

ISACA Germany Chapter

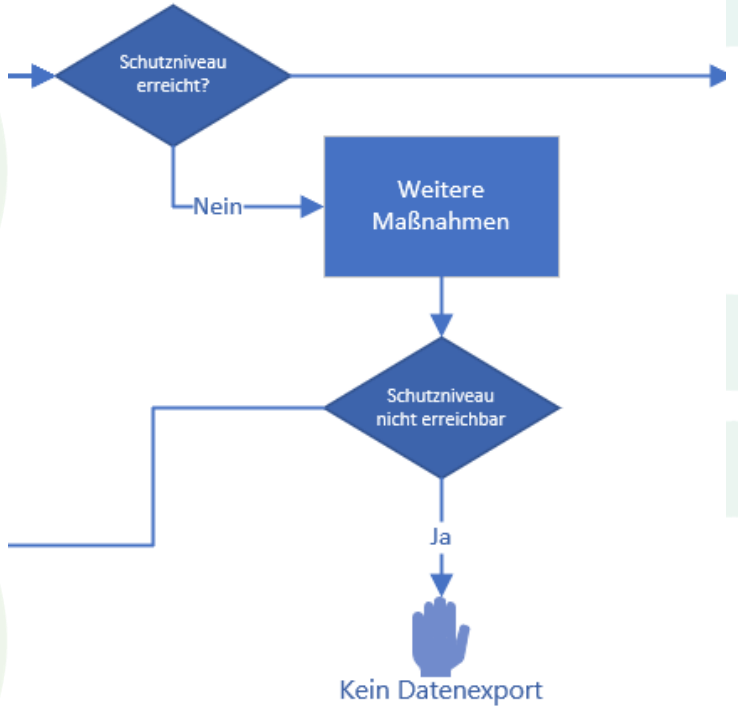
Schritt 4

Weitere Maßnahmen technischer, organisatorischer und vertraglicher Art:

Technische Maßnahmen zur Erschwerung / zum Entzug des Zugriffs durch unbefugte Dritte:

- Vornehmlich: Verschlüsselung (was ist, wenn der Importeur Zugriff auf den Schlüssel benötigt?)

- Organisatorische Maßnahmen:
  - Reduktion der übergebenen Datenmengen
  - Beschränkung der exportierten Datentypen
  - Aufteilen von Verarbeitungsketten
  - Strenge Kontrolle administrativer Zugänge; insb. im Supportfall
- Vertragliche Maßnahmen:
  - „Neue“ SCCs guter Ausgangspunkt, aber genaue Prüfung des Gesamtvertragswerks mit Dienstleister *trotzdem* erforderlich
  - Ggf. ergänzende konkrete Maßnahme im (Leistungs-)Vertrag



ISACA Germany Chapter

Schritt 5: Formale Anforderungen umsetzen

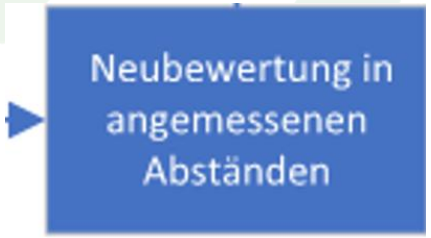
- Betrifft die Anforderung eines formalen Vorgehens durch die für den Exporteur zuständige Aufsichtsbehörde zur Begutachtung/Genehmigung von:
  - Änderungen an den Klauseln der SCCs (i.A. nicht empfehlenswert)
  - Vereinbarung von Maßnahmen zwischen Ex- und Importeur, die Gefahr laufen, das ursprüngliche Ziel (Aufrechterhaltung des Schutzniveaus für die Datenübermittlung) zu unterlaufen (z.B. Verzichtsklauseln): nicht empfehlenswert
  - Zusätzlich erforderlich für alternative Übermittlungsinstrumente, die die sich aus Schrems II ergebenden Anforderungen ebenfalls reflektieren müssen (z.B. verbindliche interne Datenschutzvorschriften)

ISACA Germany Chapter

Schritt 6: Regelmäßige Überprüfung

- Die Bewertung des Drittlandtransfers muss in regelmäßigen Abständen überprüft werden.

- Anlassbezogen, z.B. :
  - Einschränkung gewählter zusätzlicher Maßnahmen im Drittland (Bspw. Kryptoverbot)
  - Meldungen des Importeurs nach Klausel 15 der SCC
  - Bekanntwerden beeinträchtigender gesetzlicher Änderungen im Zielland;
    Verfolgen der Veröffentlichungen der Datenschutzaufsichtsbehörden;
    Newsletter eines Fachverband wie GDD (D) oder IAPP (int.);
    Mitgliedschaft in der Fachgruppe Datenschutz der ISACA Germany



- Regelmäßig in dem Verarbeitungsrisiko angemessenen Abständen (mind. einmal jährlich)

- Kontaktaufnahme zum Importeur

ISACA Germany Chapter

Ausblick: Wird’s besser oder schlimmer ?

ISACA Germany Chapter

Ausblick: Wird’s besser oder schlimmer ?

Didier Reynders • 2.
Commissaire européen à la Justice chez UE
6 Tage •

+ Folgen •••

Privacy Shield : This agreement in principle, as announced by the president of the European Commission , is the result of intense but excellent negotiations with Secretary Raimondo & AG Garland. They took place in the spirit of trust and full confidentiality. I look forward to continuing this collaboration for the next steps

Übersetzung anzeigen

Erste Eckdaten*:

- USA akzeptieren die Einhegung des bisher unbegrenzten Zugriffs ihrer Nachrichtendienste gegenüber EU-Bürgern
  -> Schrems II Defizit der Erforderlichkeit und Angemessenheit

- Zugestehen von Rechtsbehelfen, um Beschwerden von EU-Bürgern gegenüber nachrichtendienstlichen Zugriffen zur Wirksamkeit zur verhelfen (mit eigenem, öffentlich zugänglichem „Data Protection Court“)
  -> Schrems II Defizit der mangelnden rechtsstaatlichen Balance

- Strenge, aus dem geplanten Übereinkommen erwachsende Anforderungen an die eigentlichen Datenimporteure

- Dedizierte Überwachungs- und Überprüfungsmechanismen

*: Fact Sheet der EU und
Pressemitteilung des Weißen Hause vom 25.3.2022

ISACA Germany Chapter

Ausblick: wird’s besser oder schlimmer ?

Didier Reynders • 2.
Commissaire européen à la Justice chez UE
6 Tage •

+ Folgen •••

Privacy Shield : This agreement in principle, as announced by the president of the European Commission , is the result of intense but excellent negotiations with Secretary Raimondo & AG Garland. They took place in the spirit of trust and full confidentiality. I look forward to continuing this collaboration for the next steps

Übersetzung anzeigen

Unklarheiten (ausgewählt):

1. Wie und durch wen wird die Angemessenheit der datengetriebenen Überwachung geprüft und freigegeben? Wird diese Entscheidung dokumentiert und ist sie nachträglich zugänglich ?

2. Auch wenn es einen Rechtsweg geben wird: Wie soll ein Betroffener eines möglichen Verstoßes gegen seine Rechte überhaupt gewahr werden (Informationspflicht oder -möglichkeit)

3. Zu den „Anforderungen“ an Datenimporteure ist noch nichts weiter verlautbart worden

4. Zu Art und Umfang der zu installierenden Überwachungs- und Überprüfungsmechanismen des Gesamtverfahrens ist noch nichts weiter verlautbart worden

Ausblick: wird’s besser oder schlimmer ?

- Stand heute handelt es sich nur um erste Absichtserklärungen
- Ein belastbarer Rechtstext, der in die vorgesehenen Wege der datenschutzrechtlichen Verabschiedung zu leiten ist, liegt aktuell nicht vor
- Der zuvor genannte Prozess der datenschutzrechtlichen Verabschiedung zur Einrichtung rechtlicher Verbindlichkeit ist noch nicht durchlaufen (Zeit ???)
- Wenn verabschiedet, gilt die Vereinbarung nur für Datenexporte in die USA
- Aktuell hat sich an der Situation nichts geändert !

Ausblick: wird’s besser oder schlimmer ?

Risiko weiterhin bestehender zügelloser Zugriffsrechte der US-Behörden trotz aller Beteuerungen → Schrems III ?

"Privacy Shield 2.0"? - First Reaction by Max Schrems

ISACA Germany Chapter

Key Takeaways

ISACA Germany Chapter

Key Takeaways I

- Substantielles Auseinandersetzen mit Problemlage dokumentieren
  - Aktuelles Verzeichnis der Verarbeitungstätigkeiten
  - Identifikation der Übermittlungsverhältnisse
  - Zugriff auf und Kenntnis der zu Grunde liegenden Verträge

- Mit dem jeweiligen Datenimporteur ins Gespräch kommen
  - Hält man dort schon unterstützende Informationen vor (fertige TIAs)?
  - Werden angepasste Verträge unter Einbezug der aktuellen SCCs angeboten ?
  - Wurde ein Mehrbedarf an Maßnahmen darüber hinaus erkannt und klar identifizierbar (Anhänge) vereinbart (insb. Lokationsfestlegungen, Verschlüsselungsoptionen) ?
  - Ist ein Reaktionsprozess auf Seiten des Exporteurs bei etwaigen Meldungen durch den Importeur vorhanden (Klausel 15 der SCC)?

Key Takeaways II:

- Denken Sie an sich aus dem Gesetz ergebende Verbundaufgaben
  - Wahl der richtigen Rechtsgrundlage für die Übermittlung selbst (Art. 6 DSGVO)
  - Anpassen der Pflichtinformationen gegenüber dem Betroffenen (Artt. 13 und 14 Abs. 1 lit. f) DSGVO)
  - Widerspiegeln der Exportverhältnisse im Verzeichnis der Verarbeitungstätigkeiten (Art. 30 Abs. 1 lit. e DSGVO)
- Entwickeln Sie Prozessdisziplin in den Aufgabenfeldern:
  - Eingehen von Exportverhältnissen und Providerauswahl (Due Diligence & Risikomanagement)
  - Turnusmäßige Überprüfung der Situation in den Zielländern der Exportverhältnisse
  - Management der Exportverhältnisse (z.B. Reduktion der Datentransfers oder der Datenimporteure)
  - Dokumentation → Rechenschaftsfähigkeit gemäß Art. 5 Abs. 2 DSGVO!
- Halten Sie Ausschau nach Alternativen und haben Sie eine Exit-Strategie
  Bsp.: https://european-alternatives.eu/categories

Hier endet die zur Veröffentlichung bestimmte Aufzeichnung

Es folgt der vertrauliche Austausch

ISACA Germany Chapter

ISACA®

Germany Chapter