Der Landesbeauftragte für den
DATENSCHUTZ und die
INFORMATIONSFREIHEIT
Rheinland-Pfalz

Schrems II und die Folgen. Sicht der Aufsichtsbehörde.

Helmut Eiermann
Stellv. Landesbeauftragter für Datenschutz und Informationsfreiheit Rheinland-Pfalz

Schrems II Juli 2020 (EU-US-Privacy Shield)

„Tausend Mal berührt… und es hat Boom gemacht.“

Schrems I (2015, Safe Harbor)

„Ich dacht' nicht im Traum, dass was passieren kann…“

… und dann ist es 2015 doch passiert …

Schrems I (2015, Safe Harbor)

Pearl Harbor,
Safe Harbor und
datenschutzkonformes
Cloud Computing

GI ITSECMGT, Frankfurt, 26.2.2016

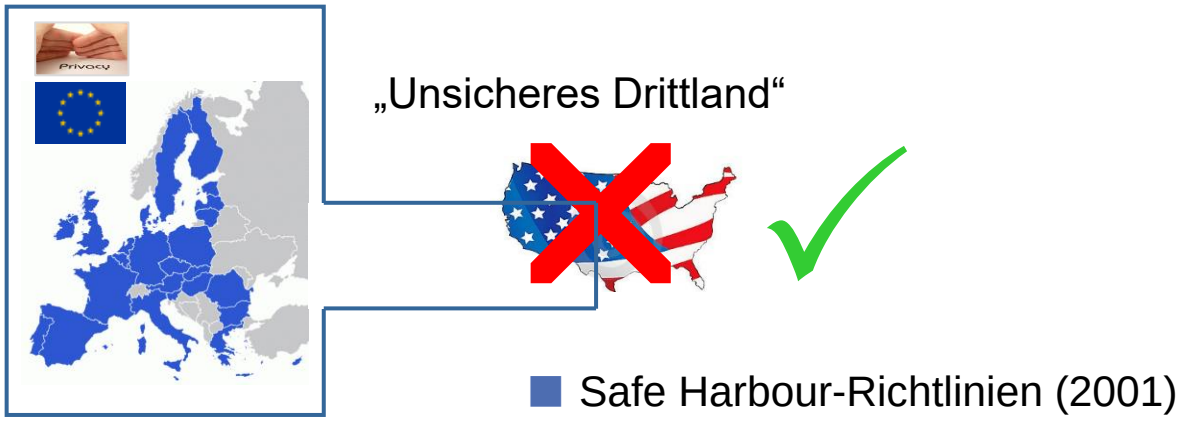
Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz

H. Eiermann Folie 1

Schrems I (2015, Safe Harbor)

Sicherer Datenschutzhafen USA (Safe Harbor)

- DV beschränkt auf den Bereich der EU / EWR

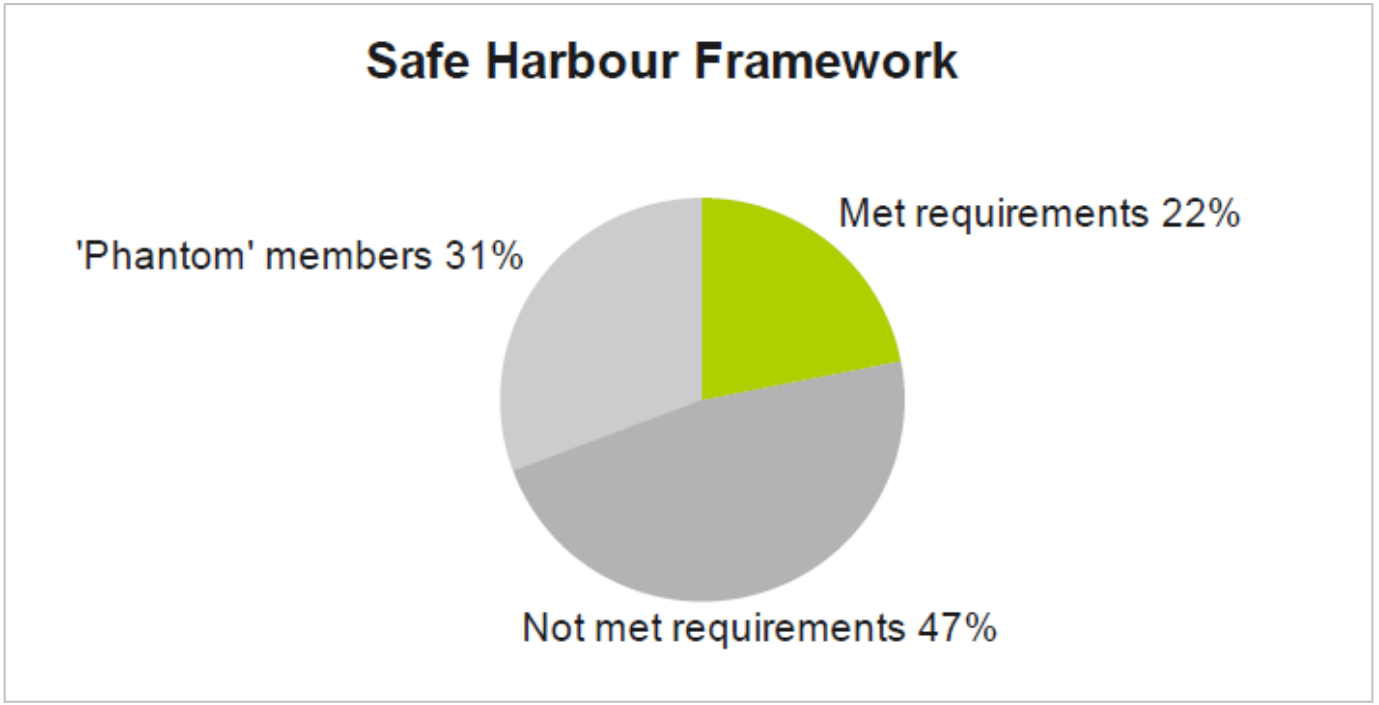


- Safe Harbour-Richtlinien (2001)

Schrems I (2015, Safe Harbor)

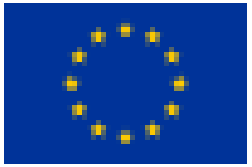
Sicherer Datenschutzhafen USA ? (2008)

Untersuchung zur Verlässlichkeit von Safe Harbour Vereinbarungen



http://www.galexia.com/public/research/assets/safe_harbor_fact_or_fiction_2008/safe_harbor_fact_or_fiction.pdf

Schrems I (2015, Safe Harbor)



Art. 29-Gruppe

„Die von den Zugriffen der ausländischen Behörden betroffenen personenbezogenen Daten unterliegen in den jeweiligen Staaten oft ***keinen datenschutzrechtlichen Restriktionen****, die* ***europäischen Standards*** *auch nur ansatzweise genügen könnten.*

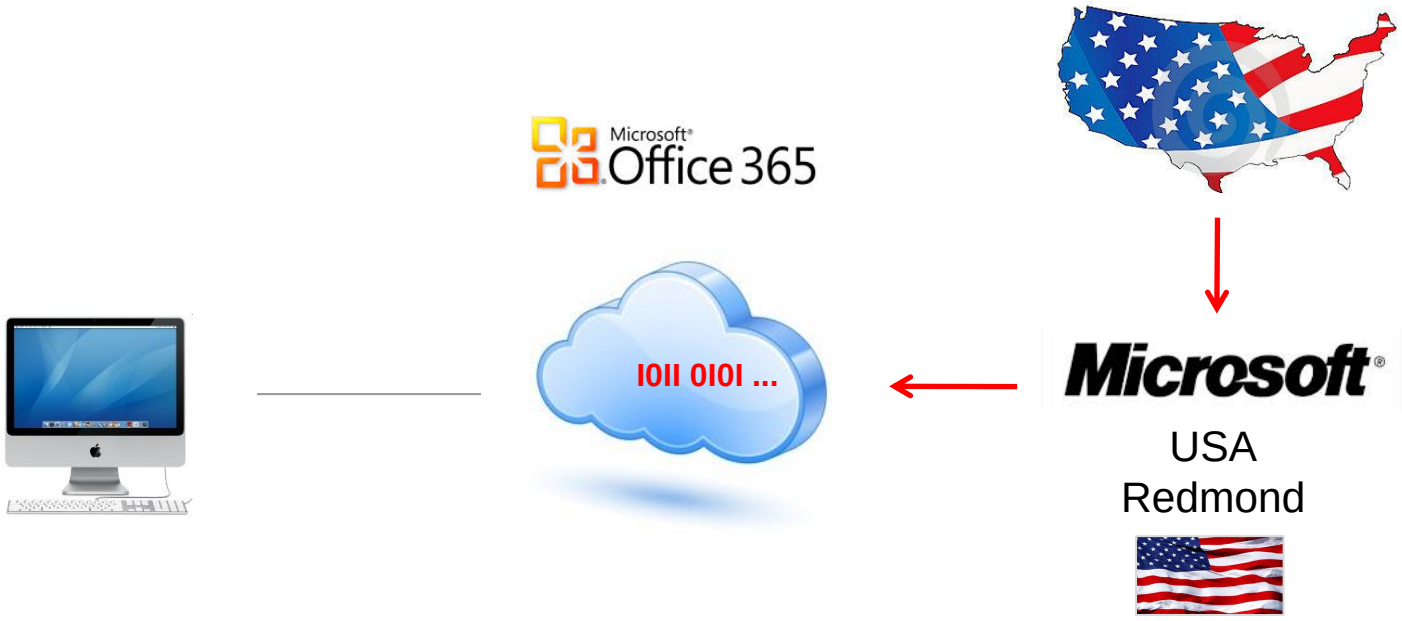
1.1. Privacy Shield

- EuGH, Urt.v.16.7.2020, Rs. C-311/18 („Schrems II“)
- LS 5: Privacy Shield ungültig (invalid)
- Von Beginn an nichtig
- Vorgeschichte: EuGH, Urt.v.6.10.2015, Rs. C-362/14, ECLI:EU:C:2015:650 - Schrems I
  - Datenübermittlungen auf der Grundlage von Safe Harbor
  - Defizite: Verlässlichkeit, fehlende Überprüfung, fehlende unabhängige Aufsichtsstruktur, Rechtslage in den USA

1.2. US-Recht

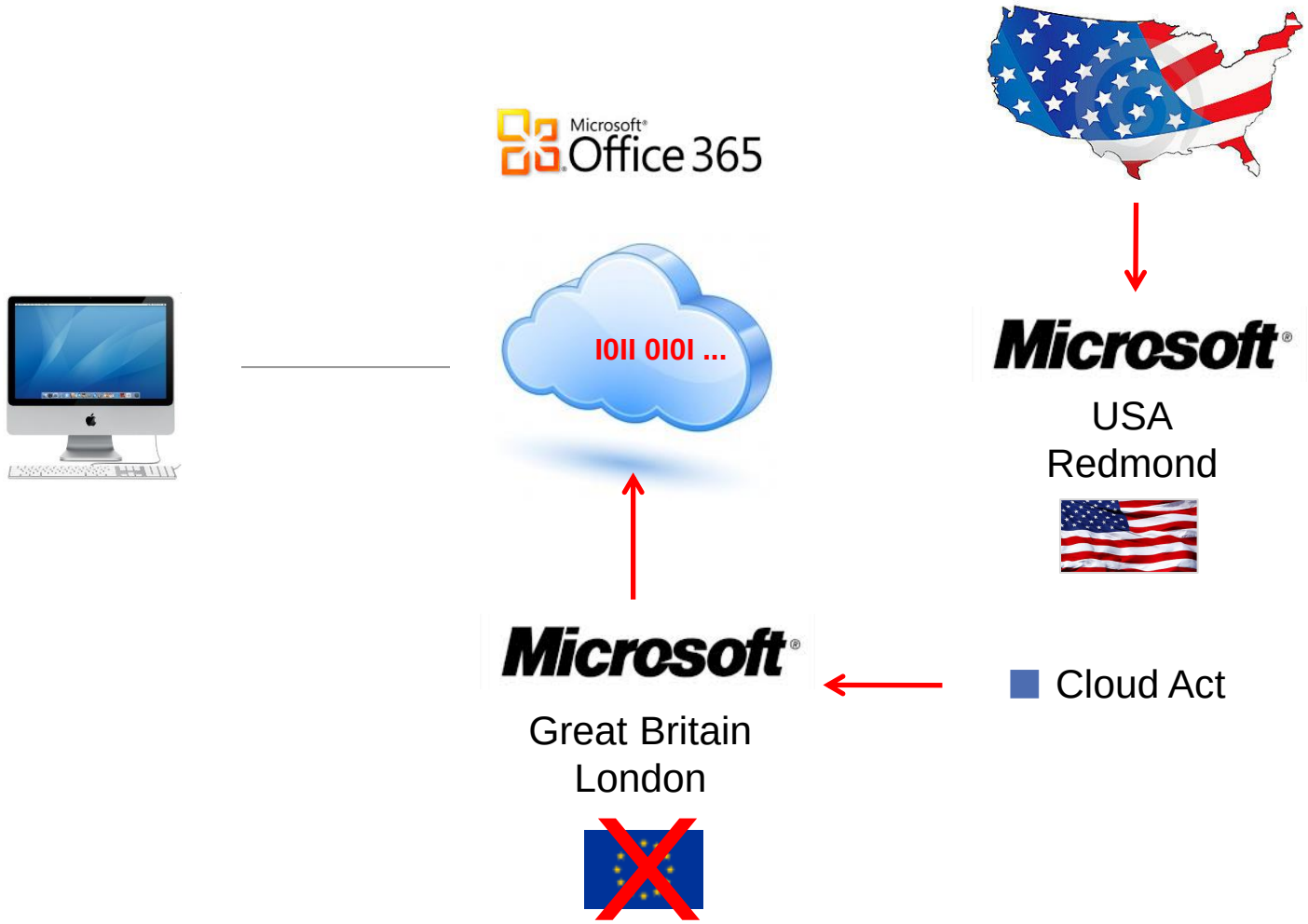
- Section 702 of the FISA (Rn. 180 f.)
  - Keine Einschränkungen des Zugriffs von Behörden
  - Keine Garantien für Nicht-US Bürger
- Executive Order 12333 (Rn. 182)
- Art. 47 GRC verletzt (Rn. 187); Wirksamer Rechtsbehelf

1.1. Privacy Shield

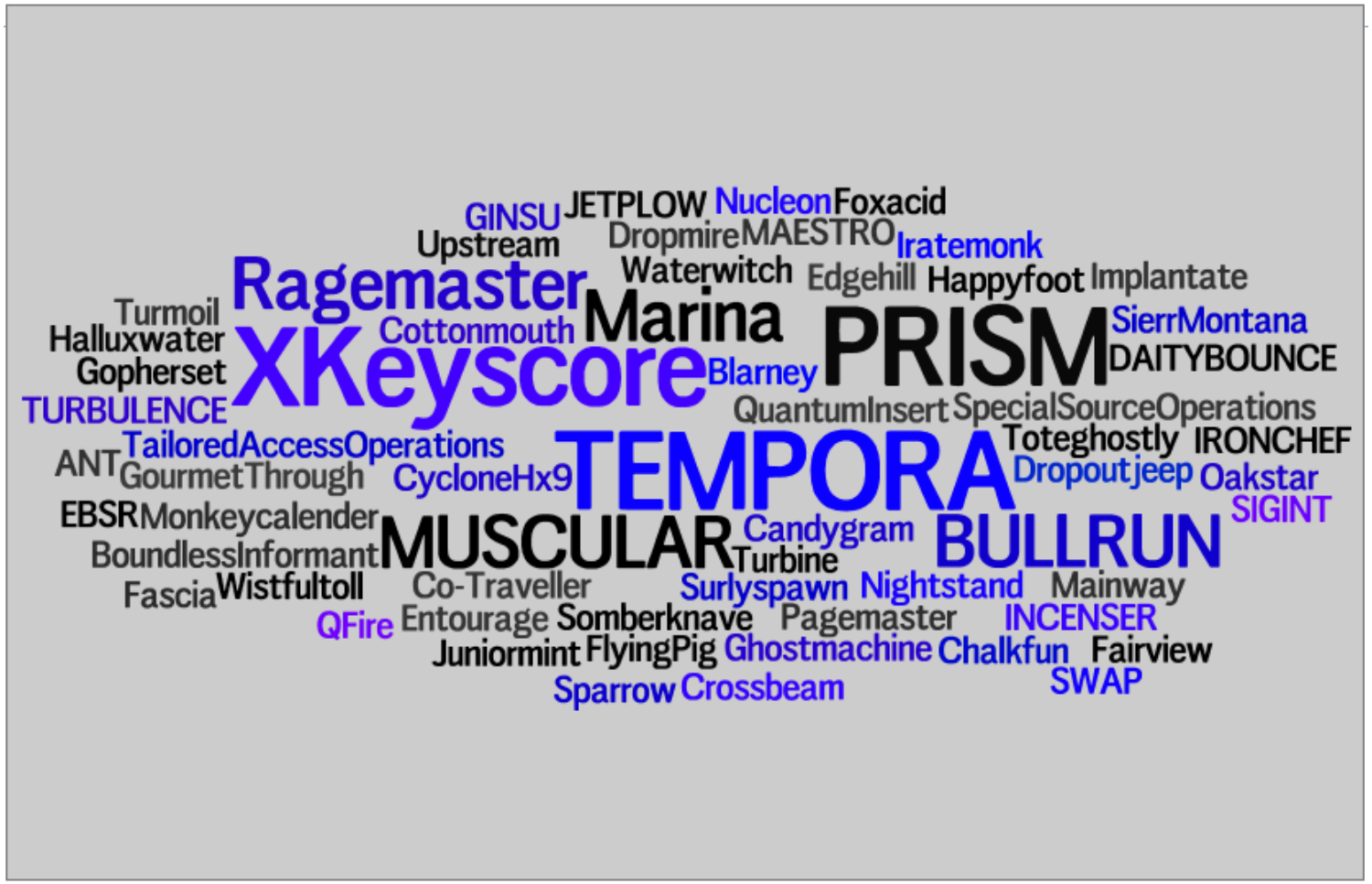


- Patriot Act
- Foreign Intelligence Surveillance Act (FISA) 1881a

1.1. Privacy Shield



Edward Snowdon (Juni 2013)



2.2. Datentransfers in Drittstaaten

Cloud Dienstleister

amazon web services™

iCloud

Google™

hp Cloud Services

Microsoft® Office 365

Windows Azure™

1.3. Drittstaaten

- Angemessenes Schutzniveau (Rn. 105)
  - Vertrag
  - Rechtsordnung des Drittstaates
- Schutzniveau im Drittstaat (Rn. 141 f.)
  - USA! China? Indien? Russland?
- Zwingende Erfordernisse des Rechts des Drittstaates sind anzuerkennen, wenn sie nicht über das in einer demokratischen Gesellschaft erforderliche Maß hinausgehen (vgl. EMRK)

2.1. Datentransfers in Drittstaaten

- Direktbeziehungen (A (EU) → B (extra EU)
- Internationale Kooperationen und Projekte
- Dienstleistungen – Services
  - z.B. Fernwartung

2.2. Datentransfers in Drittstaaten

- Globales arbeitsteiliges Arbeiten
  - Collaboration Tools
- Cloud Lösungen
  - International aufgestellte Anbieter (z.B. Salesforce)
  - Videokonferenzsysteme (MS Teams; Zoom; GotoMeeting, WebEx)
- Software mit Cloud-Funktionen
  - Office 365 (Word; Excel, Onedrive)

Datenübermittlung in die USA

- EU-US-Privacy Shield
  - angemessenes Datenschutzniveau
  - Feststellung durch EU-Kommission

- EU-Standard-Vertragsklauseln (EU SCC) ?
  - ausreichende Garantien
  - Genehmigung durch die Aufsichtsbehörde

- Verbindliche Unternehmensregelungen (BCR) ?
  - ausreichende Garantien
  - Genehmigung durch die Aufsichtsbehörde

- Einwilligung

- Vertragserfüllung im Interesse der Betroffenen

Art. 49 DSGVO
=
Ausnahmefälle

3.1. Standardvertragsklauseln

- Standardvertragsklauseln (SCC) = Standarddatenschutzklauseln (SDPC)
- Verantwortliche müssen die Einhaltung der Rahmenbedingungen für SDPCs kontinuierlich prüfen (Rn. 141 f.)
  - Bloßer Abschluss reicht nicht
- Maßstab: Art. 46 Abs. 1, Abs. 2 lit. c, Art. 47 i.V.m. Art. 7, 8 GRC

3.1. Standardvertragsklauseln

- Falls die Einhaltung der SDPCs infolge der Rechtsordnung des Drittstaates nicht gegeben ist, muss der Verantwortliche die Datenübermittlung aussetzen oder vom Vertrag zurücktreten
- Datenschutzaufsichtsbehörden (Rn. 121) müssen Datenübermittlungen aussetzen oder verbieten, wenn Schutzniveau nicht eingehalten und der Schutz nicht mit anderen Mitteln gewährleistet werden kann
  - Art. 58 Abs. 2 lit. f und j DS-GVO (Anordnung)

3.2. Standardvertragsklauseln plus

- Aufgabe der Verantwortlichen, ihre Datenübermittlungen einzurichten
- “identifying and implementing appropriate supplementary measures of a legal, technical and organizational nature”

3.2. Standardvertragsklauseln plus

- EDPB hat am 10. November 2020 Empfehlungen veröffentlicht

  https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer_de

  - “207 Stellungnahmen in der öffentlichen Anhörung (21.12.20)
  - Konsolidierung im EDPB bis ca. März/April 2021

3.2. Standardvertragsklauseln plus

- Garantien, um etwaige Auswirkungen der Gesetze des Bestimmungsdrittlands auf den Schutz der Daten zu regeln.
- Regelungen für den Datenimporteur dahingehend wie mit verbindlichen Ersuchen von Behörden im Drittland nach einer Weitergabe der übermittelten personenbezogenen Daten umzugehen ist
- Datentransfers nur dann, wenn die Gesetze des Bestimmungsdrittlandes den Datenimporteur nicht daran hindern, diese Klauseln einzuhalten.

3.2. Standardvertragsklauseln plus

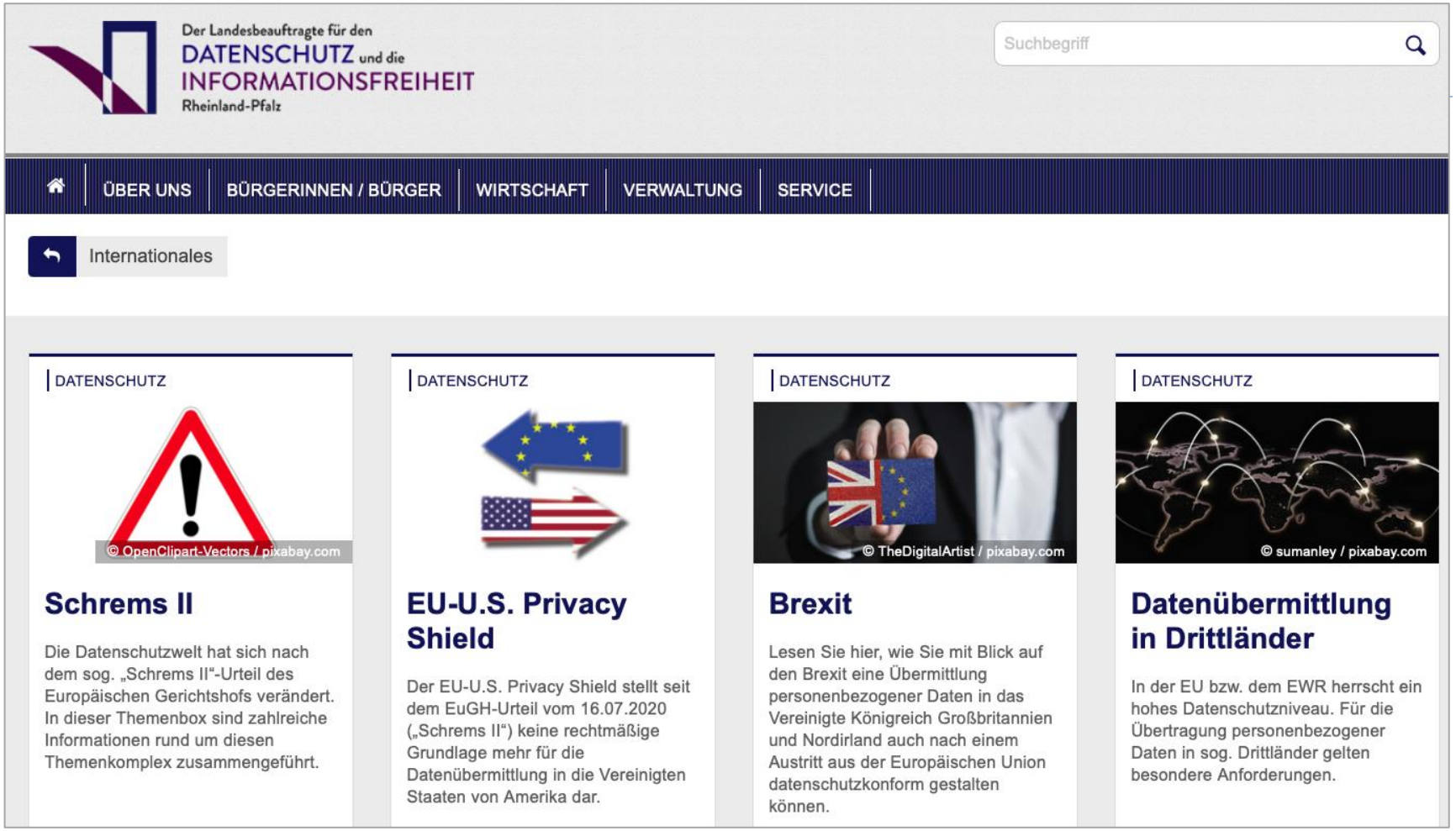
- Pflicht des Datenimporteurs, Betroffene unverzüglich zu informieren, wenn eine ausländische Behörde einen Antrag auf Herausgabe der Betroffenendaten stellt.
- Wird dem Importeur eine Benachrichtigung behördlich untersagt, soll er sich bestmöglich um eine Aufhebung der Untersagung bemühen und im Zweifel alle verfügbaren Rechtsmittel zur Anfechtung des Antrags ausschöpfen

4.1. Vorgehen der DSaufsichtsbehörden

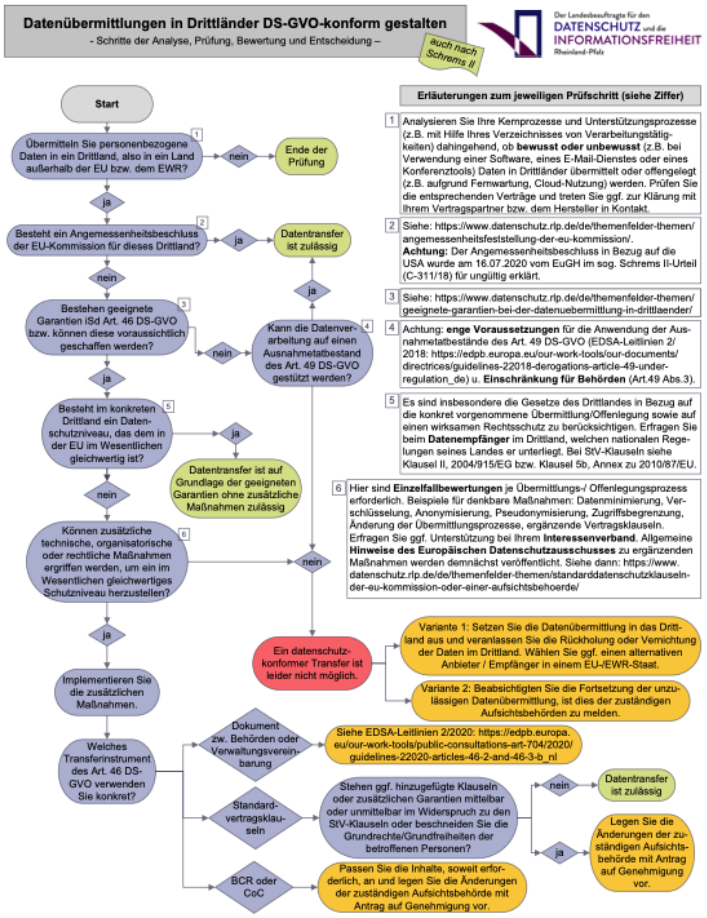
- Privacy Shield entfällt
- Datenübermittlungen auf dieser Grundlage sind rechtswidrig
- Umstellungen müssen eingeleitet sein und so schnell wie möglich vollzogen werden
- Standardvertragsklauseln plus im Einzelfall

4.2. Empfehlungen des LfDI RP

- Datenübermittlungen prüfen
  - Verzeichnis der Verarbeitungstätigkeiten
- Prüfaufträge an die Verantwortlichen
  - Andere Vertragspartner?
  - Lizensierte Subunternehmer?
  - Standardvertragsklauseln
- Prozesse aufsetzen und dokumentieren



https://www.datenschutz.rlp.de/de/themenfelder-themen/internationales/



https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Pruefschritte_Datenuebermittlung_in_Drittlaender_nach_Schrems_II.pdf

4.2. Empfehlungen des LfDI RP

- Bausteine für eine grundrechtskonforme Datenübermittlung:
  - Verschlüsselung

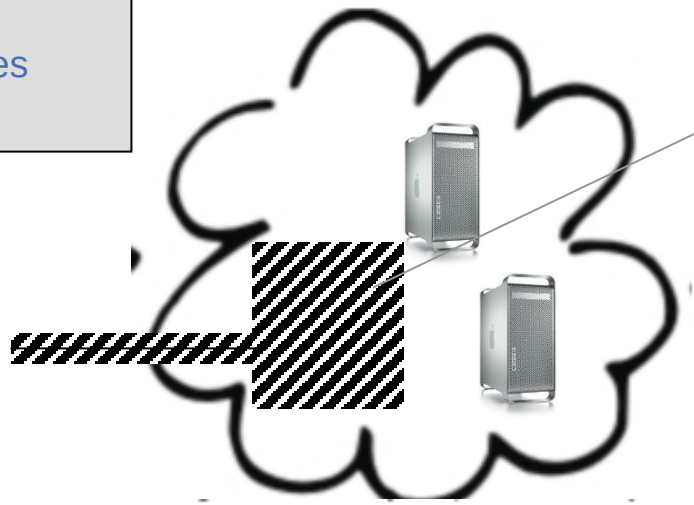
Lösungsansatz Verschlüsselung (IaaS)

- Verfahren
- Schlüssel

unter der Kontrolle des Auftraggebers

Krypto-Reglementierung

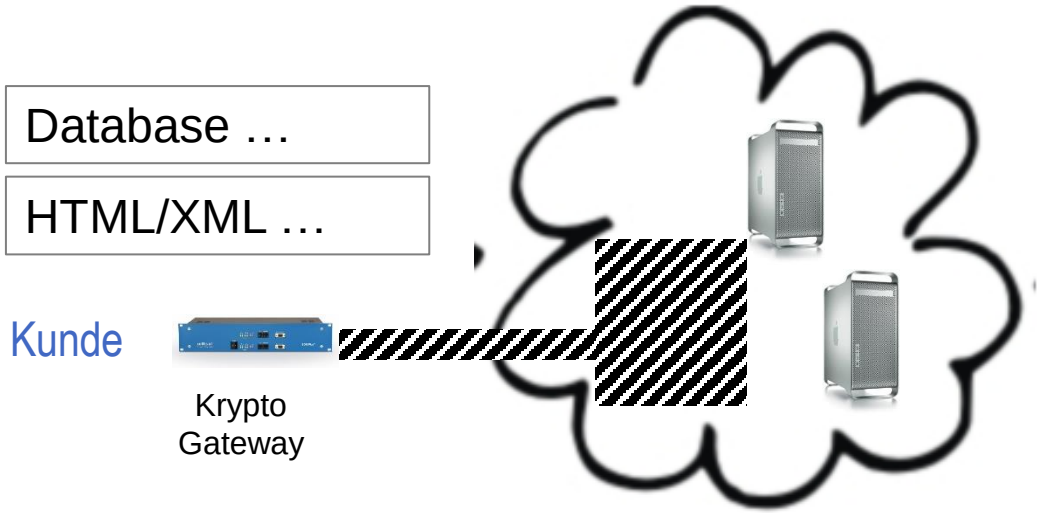
- Key Recovery
- Key Escrowing



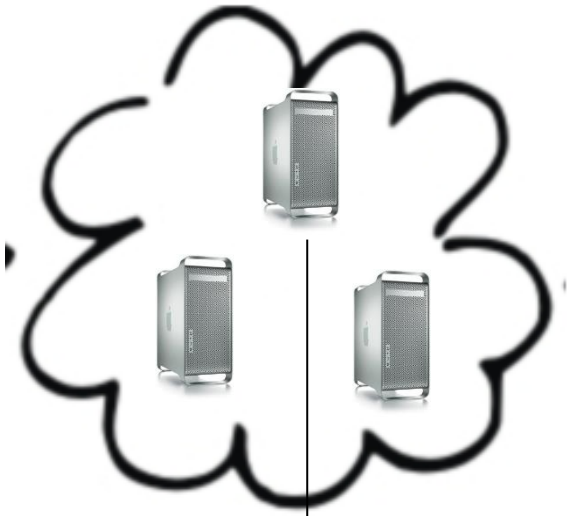
amazon web services

use, whether they be individual consumers or business customers. We offer AWS clients strong encryption as one of many standard security features, and we provide them the option to manage their own encryption keys. We publish security best practices documents on our website and

Lösungsansatz Verschlüsselung (IaaS)



Lösungsansatz Verschlüsselung (IaaS, PaaS)



HTML/XML …

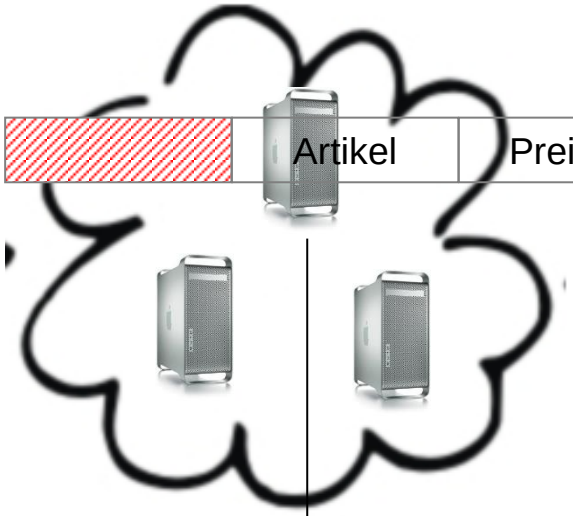
Database …

Krypto Gateway

	Artikel	Preis	Datum		

Name	Artikel	Preis	Datum	E-Mail	Adresse

Lösungsansatz Verschlüsselung (IaaS, PaaS)



Artikel	Preis	Datum

HTML/XML …

Database …

Krypto
Gateway

Name	Artikel	Preis	Datum	E-Mail	Adresse

4.2. Empfehlungen des LfDI RP

- Bausteine für eine grundrechtskonforme Datenübermittlung:
  - Anonymisierung/Pseudonymisierung

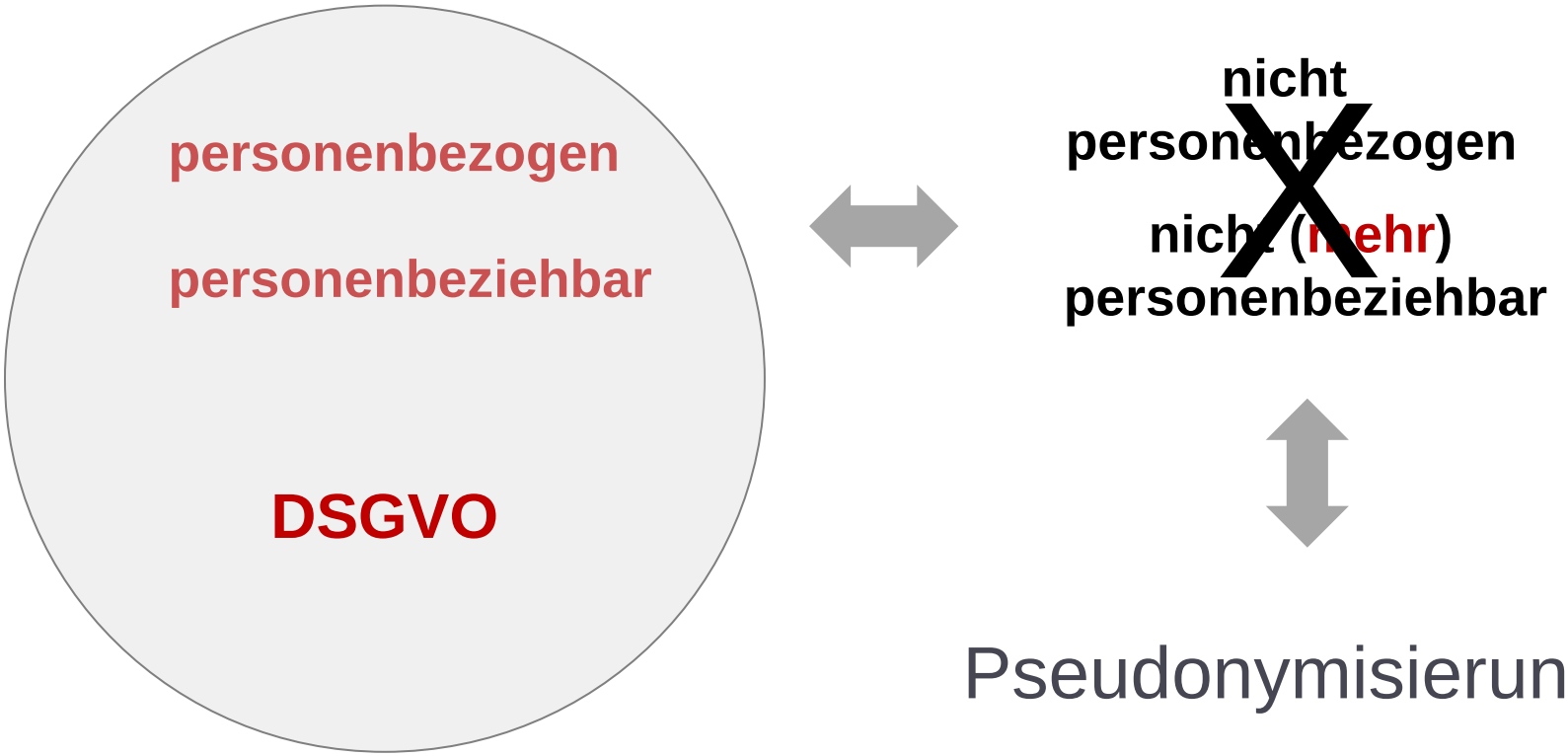
Ausgangspunkt: personenbezogene Daten

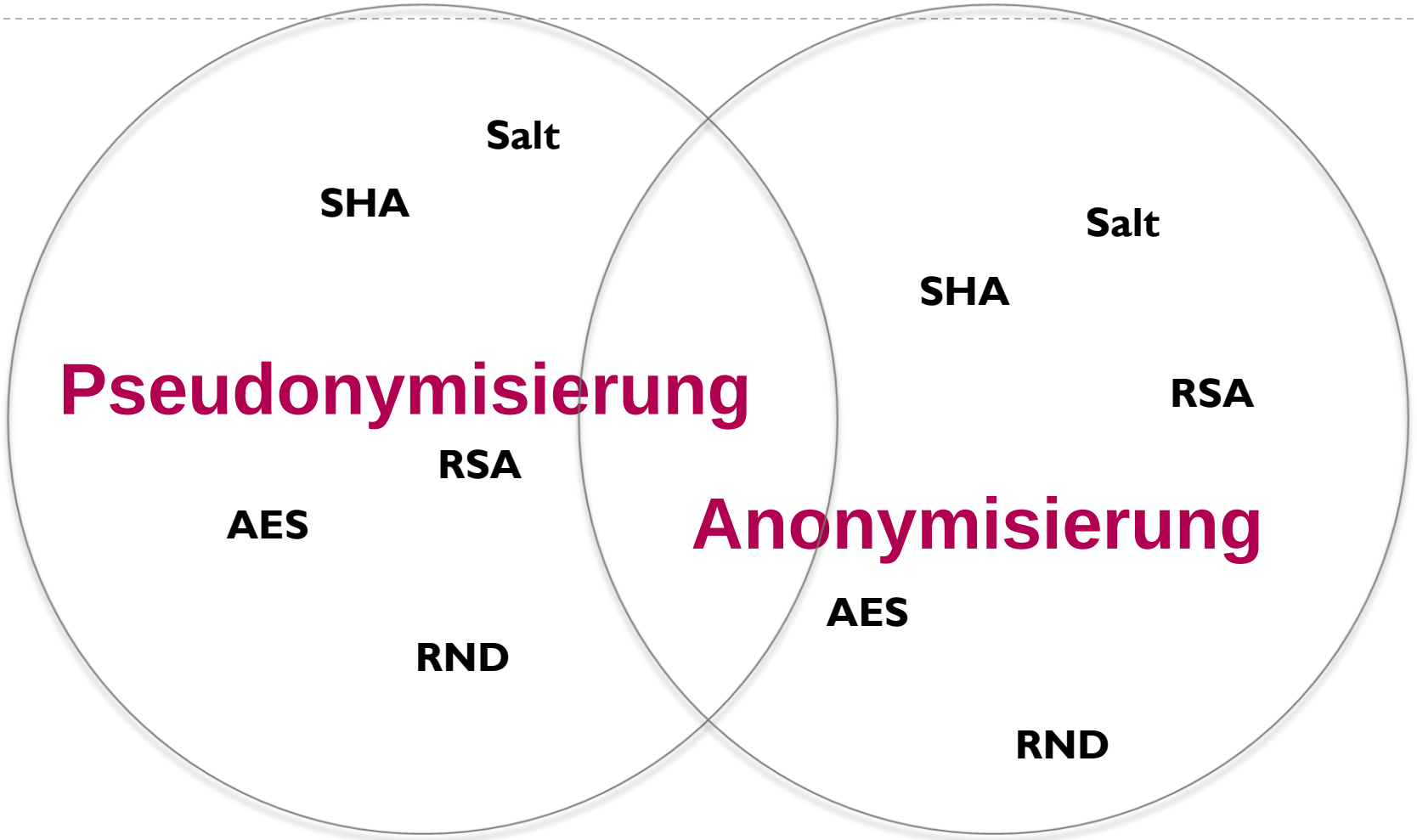
nicht personenbezogen

nicht (mehr) personenbeziehbar

Anonymisierung

Ausgangspunkt: personenbezogene Daten

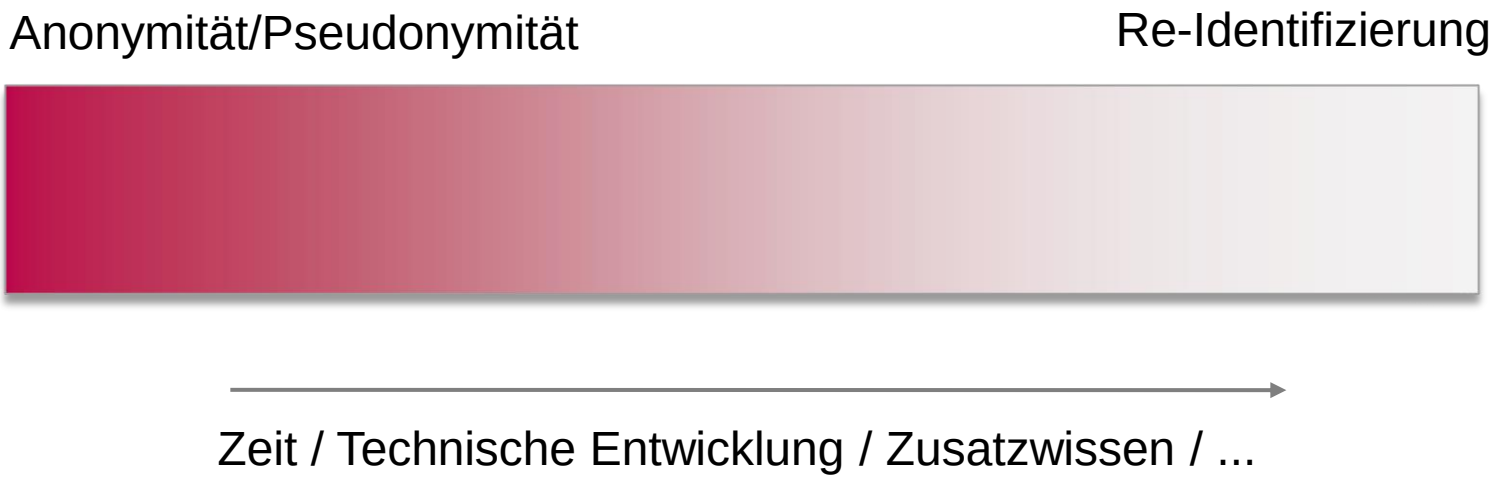



Salt
SHA
Pseudonymisierung
RSA
AES
RND
Salt
SHA
RSA
Anonymisierung
AES
RND

Anonymisierung
Pseudonymisierung

- Kosten
- Zeitaufwand
- Technologische Entwicklung
- Verfügbare Technologien
- **Verknüpfung**
- **Motiv**
- **Wert**
- **Kontakte**
- **Zeitverlauf**
- **Mittel**
- **Interesse**
- **Zugriff**
- **Zusatzwissen**
- **Gelegenheit**

Pseudonymisierung - Güte



- Annahme eines „sicheren **Zeitraums**“ (vgl. BSI-Kryptoempfehlungen)

- Turnusmäßige **Neubewertung** / Audits
- **Re-Anonymisierung/Re-Pseudonymisierung**

4.2. Empfehlungen des LfDI RP

- Bausteine für eine grundrechtskonforme Datenübermittlung:
  - Transparenz der Zugriffe (Informationspflichten)
  - Freigabe-/Widerspruchsregelung
  - Transparenz der Datenübermittlung/Dokumentation

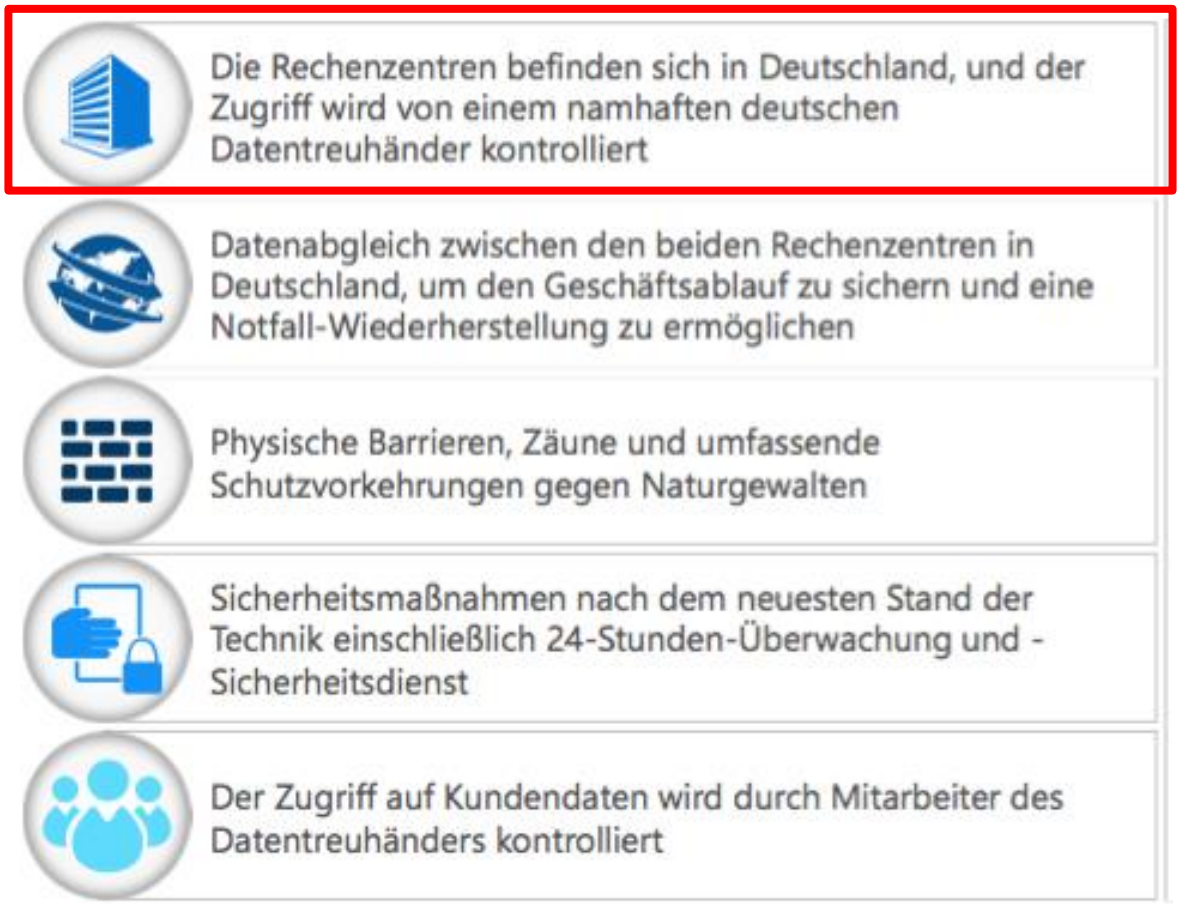
5. Ausblick

- Kreativität bei Rechtsunsicherheit
- Tragweite des risiko-basierten Ansatzes?
- Umstellungen von Geschäftsbeziehungen

Eine Microsoft Cloud mit deutscher Datentreuhand

Die Microsoft Cloud mit deutscher Datentreuhand steht für die Bereitstellung der Microsoft-Dienste Azure, Office 365 sowie Dynamics CRM Online über eigenständige deutsche Rechenzentren. Sie können sich zukünftig für eine neue Cloud entscheiden – mit einem deutschen Datentreuhänder, der unter deutschem Recht agiert. Ihre Daten befinden sich damit nur auf deutschem Boden.

Erfahren Sie mehr


Die Rechenzentren befinden sich in Deutschland, und der Zugriff wird von einem namhaften deutschen Datentreuhänder kontrolliert
Datenabgleich zwischen den beiden Rechenzentren in Deutschland, um den Geschäftsablauf zu sichern und eine Notfall-Wiederherstellung zu ermöglichen
Physische Barrieren, Zäune und umfassende Schutzvorkehrungen gegen Naturgewalten
Sicherheitsmaßnahmen nach dem neuesten Stand der Technik einschließlich 24-Stunden-Überwachung und -Sicherheitsdienst
Der Zugriff auf Kundendaten wird durch Mitarbeiter des Datentreuhänders kontrolliert

Ein deutscher Datentreuhänder kontrolliert den Zugriff auf die Daten

Ein namhafter deutscher Datentreuhänder führt alle Handlungen oder Aufgaben mit Zugriff auf Kundendaten oder auf die Infrastruktur, auf der sich Kundendaten befinden, selbst durch oder überwacht diese.

Role Based Access Control (RBAC)-Tools kontrollieren jeglichen Zugriff auf Kundendaten	Ausschließlich der deutsche Datentreuhänder hat Zugriff auf Server mit Kundendaten	Mitarbeiter von Microsoft haben keinerlei administrative Top-Level-Rechte, um Zugriff auf Kundendaten zu gewähren	Mitarbeiter von Microsoft können sich nicht auf Server mit Kundendaten einloggen

5. Ausblick

- Kreativität bei Rechtsunsicherheit
- Tragweite des risiko-basierten Ansatzes?
- Umstellungen von Geschäftsbeziehungen
- Umstellungen von Geschäftsmodellen
- Flexibilität im Vollzug
- Rechtsrahmen mit klaren Grenzen

Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder – 22.09.2020

Digitale Souveränität der öffentlichen Verwaltung herstellen –

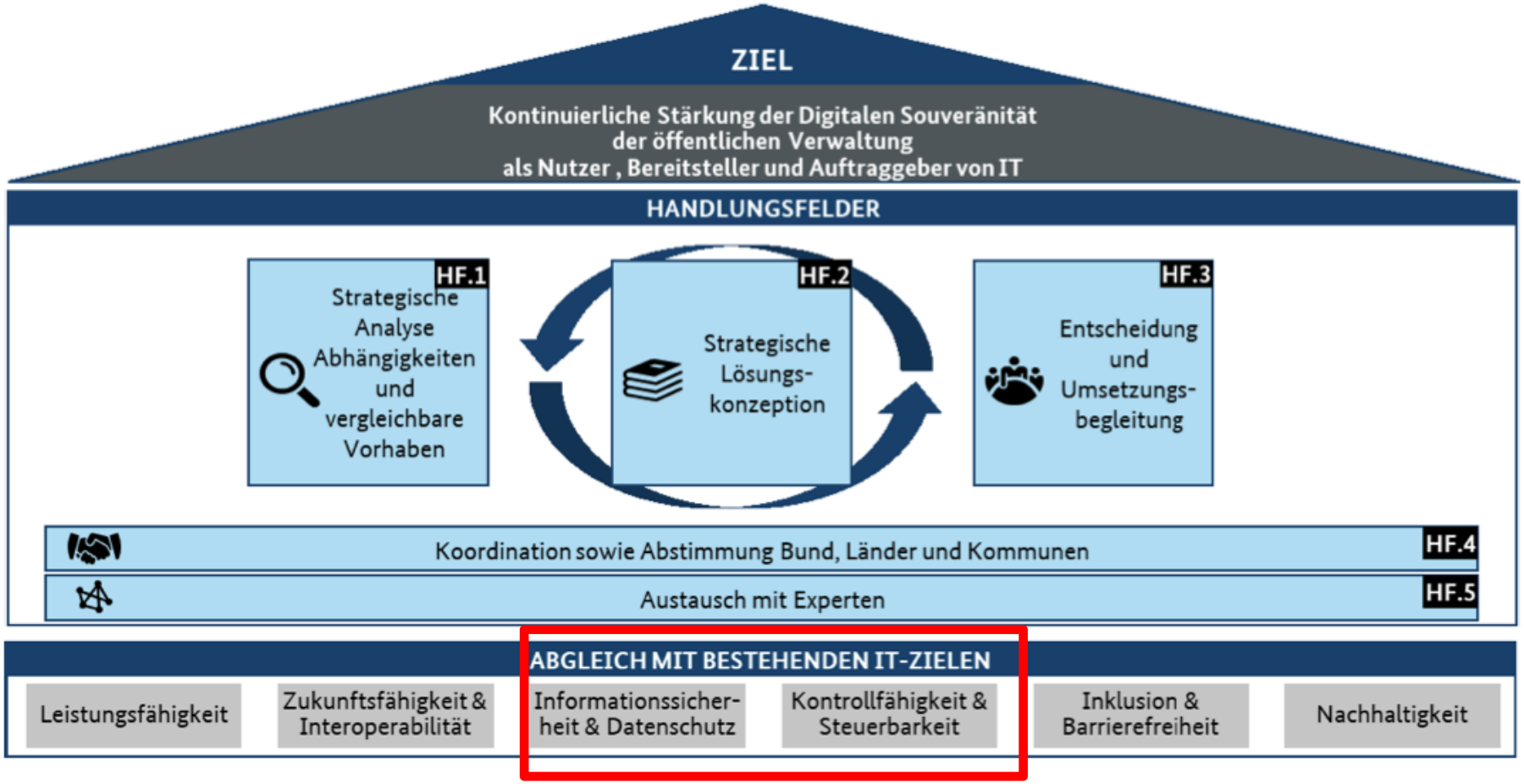
Personenbezogene Daten besser schützen

Stärkung der Digitalen Souveränität der Öffentlichen Verwaltung

Eckpunkte – Ziel und Handlungsfelder

- Version 1.0.1 vom 31. März 2020 –

Beschluss Nr.: 2020/01 des IT-Rats vom 24. März 2020
Beschluss Nr.: 2020/19 des IT-Planungsrats vom 04. Mai 2020


ZIEL
Kontinuierliche Stärkung der Digitalen Souveränität
der öffentlichen Verwaltung
als Nutzer , Bereitsteller und Auftraggeber von IT
HANDLUNGSFELDER
HF.1
Strategische Analyse Abhängigkeiten und vergleichbare Vorhaben
HF.2
Strategische Lösungs-konzeption
HF.3
Entscheidung und Umsetzungs-begleitung
Koordination sowie Abstimmung Bund, Länder und Kommunen
HF.4
Austausch mit Experten
HF.5
ABGLEICH MIT BESTEHENDEN IT-ZIELEN
Leistungsfähigkeit
Zukunftsfähigkeit & Interoperabilität
Informationssicher-heit & Datenschutz
Kontrollfähigkeit & Steuerbarkeit
Inklusion & Barrierefreiheit
Nachhaltigkeit

Der Landesbeauftragte für den
DATENSCHUTZ und die
INFORMATIONSFREIHEIT
Rheinland-Pfalz

Helmut Eiermann

Stellv. Landesbeauftragter für den Datenschutz
und die Informationsfreiheit Rheinland-Pfalz

Postanschrift: Postfach 30 40
55020 Mainz

Büroanschrift: Hintere Bleiche 34
55116 Mainz

Telefon: +49 (6131) 208-2226
Telefax: +49 (6131) 208-2497

E-Mail: h.eiermann@datenschutz.rlp.de

Web: www.datenschutz.rlp.de