



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

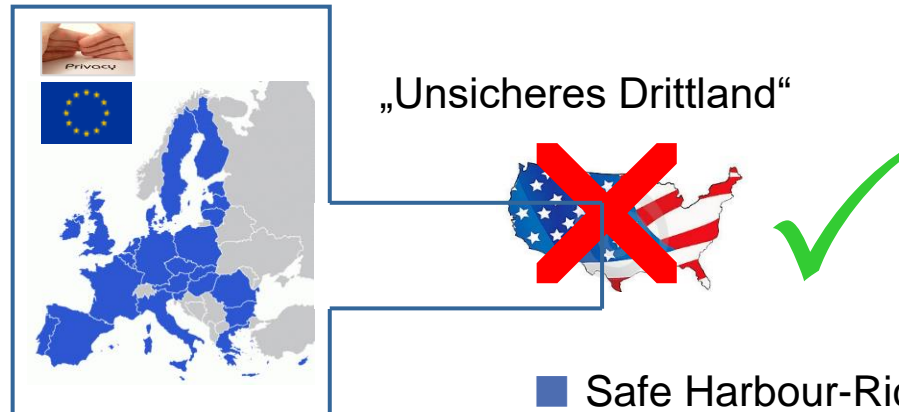


GI ITSECMGT, Frankfurt, 26.2.2016

Schrems I (2015, Safe Harbor)

Sicherer Datenschutzhafen USA (Safe Harbor)

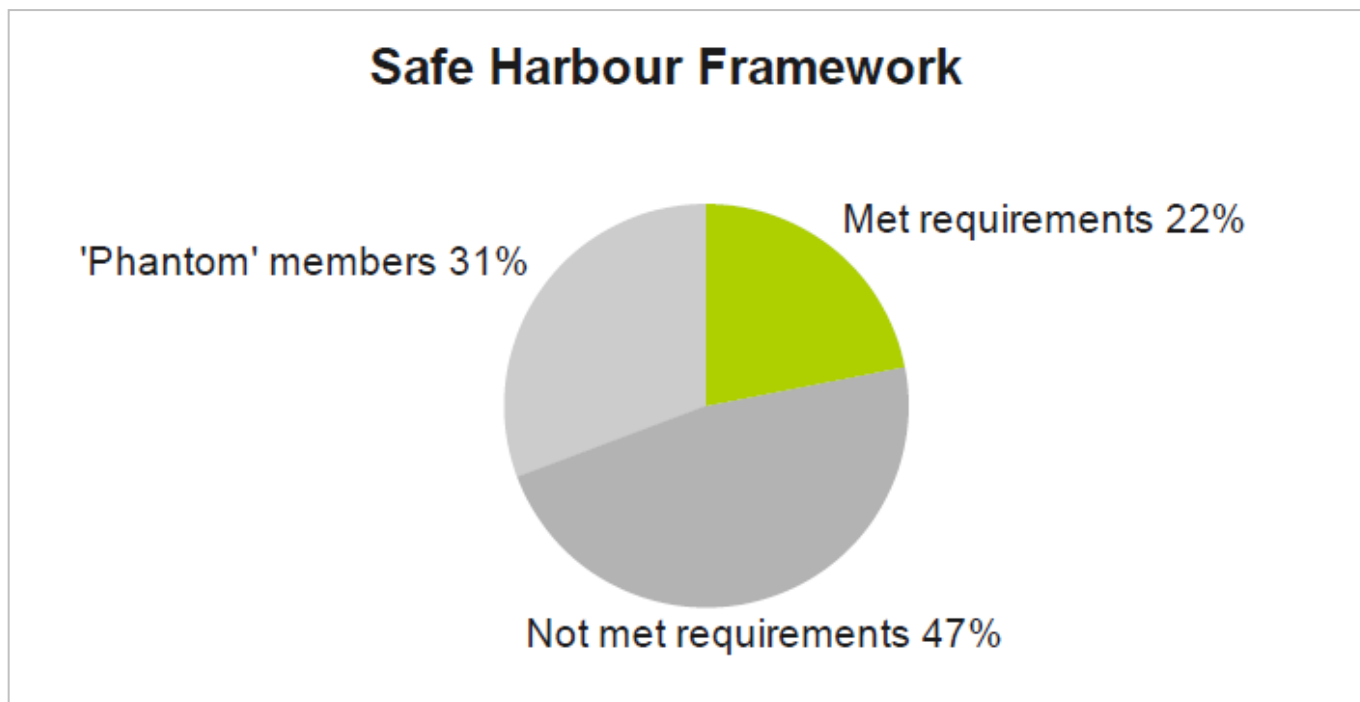
- DV beschränkt auf den Bereich der EU / EWR



Schrems I (2015, Safe Harbor)

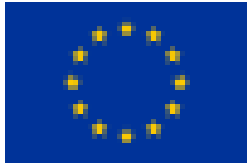
Sicherer Datenschutzhafen USA ? (2008)

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.*

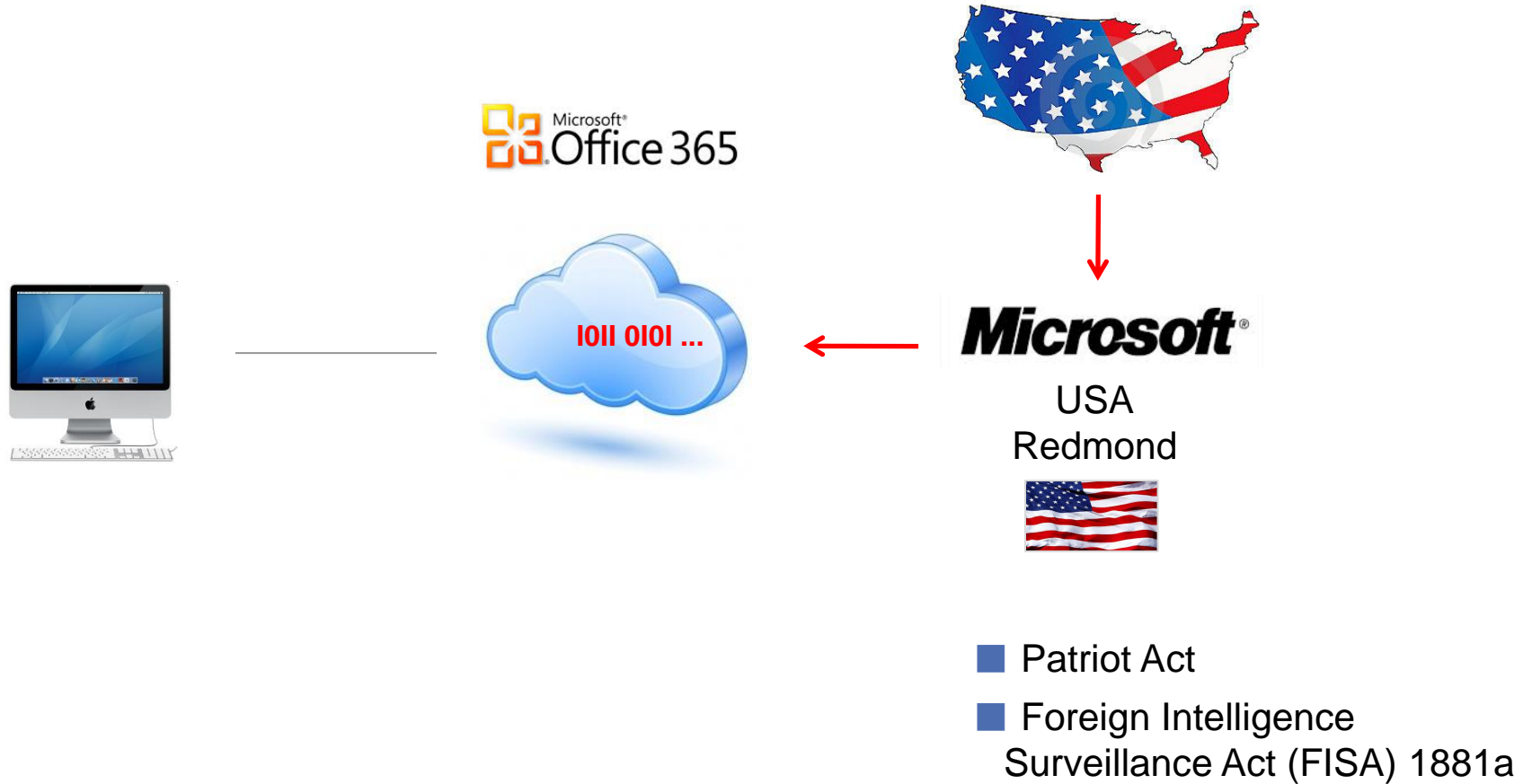
1.1. Privacy Shield

- ▶ 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



1.1. Privacy Shield



Edward Snowden (Juni 2013)



2.2. Datentransfers in Drittstaaten

Cloud Dienstleister



iCloud



Cloud Services



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 Bestimmungs Drittlands 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 Bestimmungs Drittlandes 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 Betroffenenendaten 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?
 - ▶ Lizenzierte Subunternehmer?
 - ▶ Standardvertragsklauseln
- ▶ Prozesse aufsetzen und dokumentieren



DATENSCHUTZ



© OpenClipart-Vectors / pixabay.com

Schrems II

Die Datenschutzwelt hat sich nach dem sog. „Schrems II“-Urteil des Europäischen Gerichtshofs verändert. In dieser Themenbox sind zahlreiche Informationen rund um diesen Themenkomplex zusammengeführt.

DATENSCHUTZ



EU-U.S. Privacy Shield

Der EU-U.S. Privacy Shield stellt seit dem EuGH-Urteil vom 16.07.2020 („Schrems II“) keine rechtmäßige Grundlage mehr für die Datenübermittlung in die Vereinigten Staaten von Amerika dar.

DATENSCHUTZ



© TheDigitalArtist / pixabay.com

Brexit

Lesen Sie hier, wie Sie mit Blick auf den Brexit eine Übermittlung personenbezogener Daten in das Vereinigte Königreich Großbritannien und Nordirland auch nach einem Austritt aus der Europäischen Union datenschutzkonform gestalten können.

DATENSCHUTZ



© sumanley / pixabay.com

Datenübermittlung in Drittländer

In der EU bzw. dem EWR herrscht ein hohes Datenschutzniveau. Für die Übertragung personenbezogener Daten in sog. Drittländer gelten besondere Anforderungen.

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



Datenübermittlungen in Drittländer DS-GVO-konform gestalten

- Schritte der Analyse, Prüfung, Bewertung und Entscheidung -



- Erläuterungen zum jeweiligen Prüfschritt (siehe Ziffer)**
- 1 Analysieren Sie Ihre Kernprozesse und Unterstützungsprozesse (z. B. mit Hilfe Ihres Verzeichnisses von Verarbeitungstätigkeiten) dahingehend, ob **bewusst oder unbewusst** (z. B. bei Verwendung einer Software, eines E-Mail-Dienstes oder eines Konferenztools) Daten in Drittländer übermittelt oder offengelegt (z. B. aufgrund Fernwartung, Cloud-Nutzung) werden. Prüfen Sie die entsprechenden Verträge und treten Sie ggf. zur Klärung mit Ihrem Vertragspartner bzw. dem Hersteller in Kontakt.
 - 2 Siehe: <https://www.datenschutz.rlp.de/de/themenfelder-themen/angemessenheitsfeststellung-der-eu-kommission/>. **Achtung:** Der Angemessenheitsbeschluss in Bezug auf die USA wurde am 18.07.2020 vom EuGH im sog. Schrems II-Urteil (C-311/18) für ungültig erklärt.
 - 3 Siehe: <https://www.datenschutz.rlp.de/de/themenfelder-themen/angemessenheitsgarantien-bei-der-datenuebermittlung-in-drittlaender/>.
 - 4 **Achtung: enge Voraussetzungen** für die Anwendung der Ausnahmebestände des Art. 49 DS-GVO (EDSA-Leitlinien 2/2018: https://edpb.europa.eu/our-work-tools/our-documents/directrices/guidelines-2018-derogations-article-49-under-regulation_de) u. **Einschränkung für Behörden** (Art. 49 Abs. 3).
 - 5 Es sind insbesondere die Gesetze des Drittlandes in Bezug auf die konkret vorgenommene Übermittlung/Offenlegung sowie auf einen wirksamen Rechtsschutz zu berücksichtigen. Erfragen Sie beim Dateneempfänger im Drittland, welchen nationalen Regelungen seines Landes er unterliegt. Bei StV-Klauseln siehe Klausel II, 2004/915/EG bzw. Klausel 5b, Annex zu 2010/87/EU.
 - 6 Hier sind **Einzelfallbewertungen** je Übermittlungs-/Offenlegungsprozess erforderlich. Beispiele für denkbare Maßnahmen: Datenminimierung, Verschlüsselung, Anonymisierung, Pseudonymisierung, Zugriffsbegrenzung, Änderung der Übermittlungsprozesse, ergänzende Vertragsklauseln. Erfragen Sie ggf. Unterstützung bei Ihrem **Interessenverband**. Allgemeine Hinweise des Europäischen Datenschutzausschusses zu ergänzenden Maßnahmen werden demnächst veröffentlicht. Siehe dann: <https://www.datenschutz.rlp.de/de/themenfelder-themen/standarddatenschutzklauseln-der-eu-kommission-oder-einer-aufsichtsbehoerde/>.

Variante 1: Setzen Sie die Datenübermittlung in das Drittland aus und veranlassen Sie die Rückholung oder Vernichtung der Daten im Drittland. Wählen Sie ggf. einen alternativen Anbieter / Empfänger in einem EU-EWR-Staat.

Variante 2: Beabsichtigen Sie die Fortsetzung der unzulässigen Datenübermittlung, ist dies der zuständigen Aufsichtsbehörden zu melden.

Siehe EDSA-Leitlinien 2/2020: https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-2020-articles-46-2-and-46-3-b_nl

Siehen ggf. hinzugefügte Klauseln oder zusätzlichen Garantien mittelbar oder unmittelbar im Widerspruch zu den StV-Klauseln oder beschreiben Sie die Grundrechte/Grundfreiheiten der betroffenen Personen?

Passen Sie die Inhalte, soweit erforderlich, an und legen Sie die Änderungen der zuständigen Aufsichtsbehörde mit Antrag auf Genehmigung vor.

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

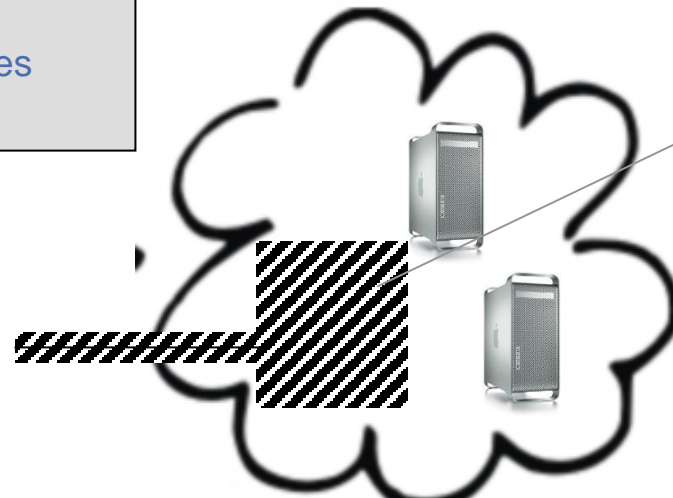
Lösungsansatz Verschlüsselung (IaaS)

- Verfahren
- Schlüssel

unter der Kontrolle des Auftraggebers

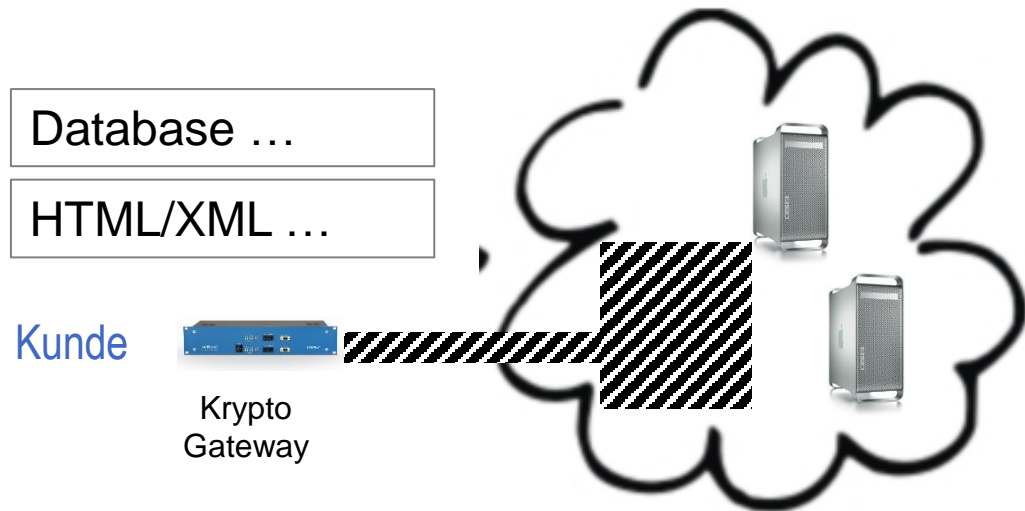
Krypto-Reglementierung

- Key Recovery
- Key Escrowing

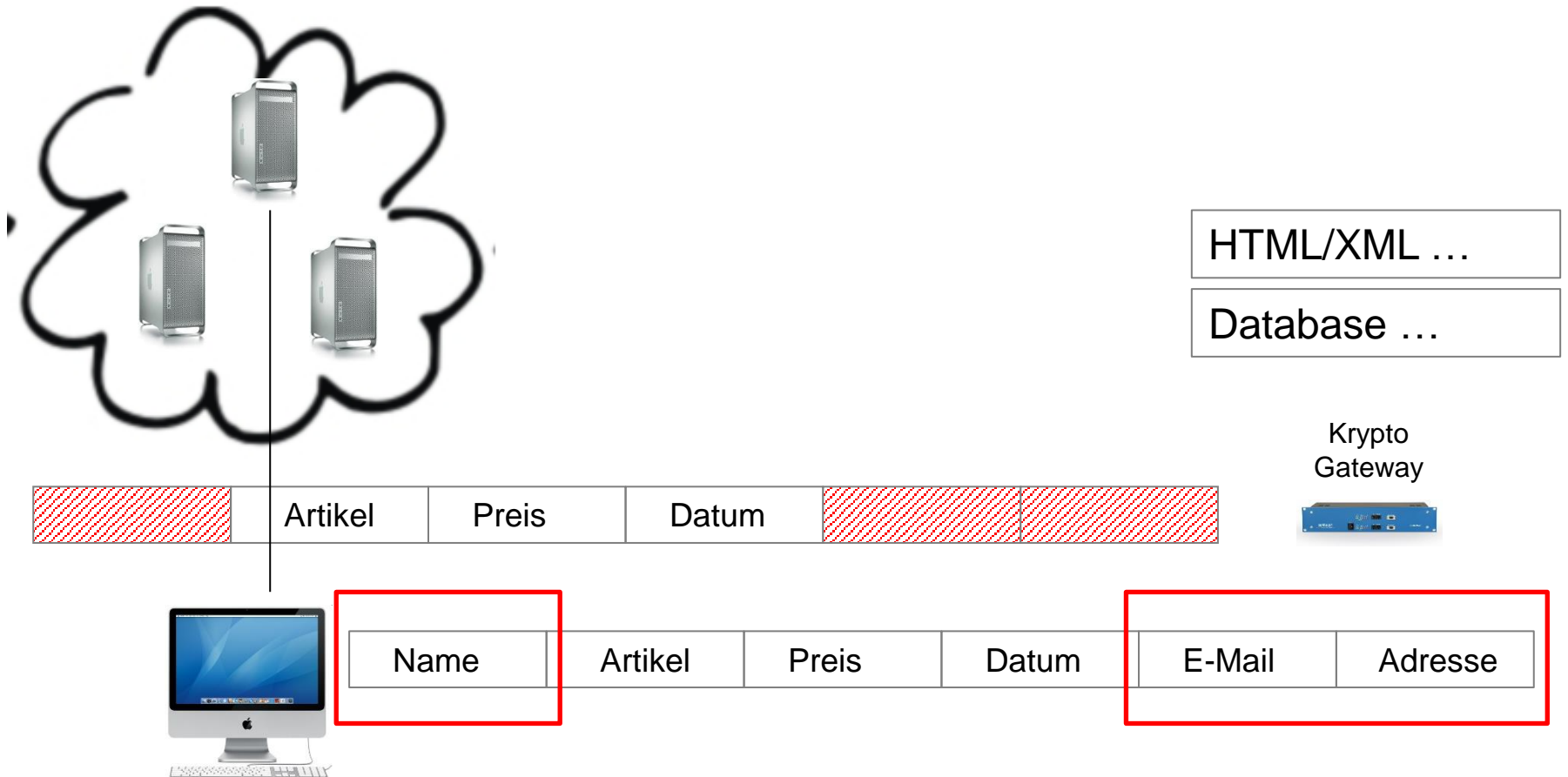


use, whether they be individual consumers or business customers. We offer AWS clients strong encryption as one of many standard security features, and we provide them the option to manage their own encryption keys. We publish security best practices documents on our website and

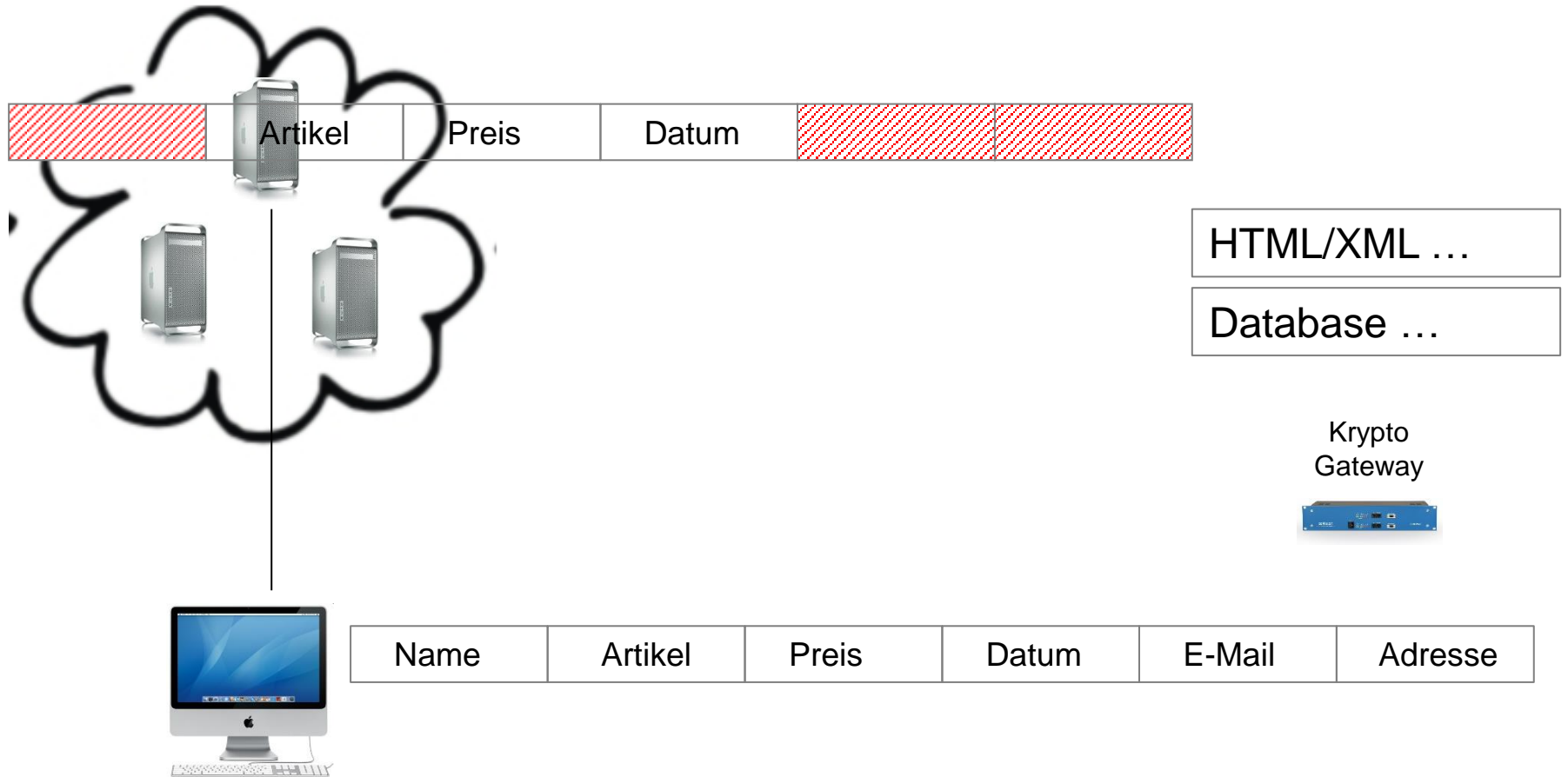
Lösungsansatz Verschlüsselung (IaaS)



Lösungsansatz Verschlüsselung (IaaS, PaaS)



Lösungsansatz Verschlüsselung (IaaS, PaaS)



4.2. Empfehlungen des LfDI RP

- ▶ Bausteine für eine grundrechtskonforme Datenübermittlung:
 - ▶ Anonymisierung/Pseudonymisierung

Ausgangspunkt: personenbezogene Daten



nicht
personenbezogen
nicht (**mehr**)
personenbeziehbar



Anonymisierung

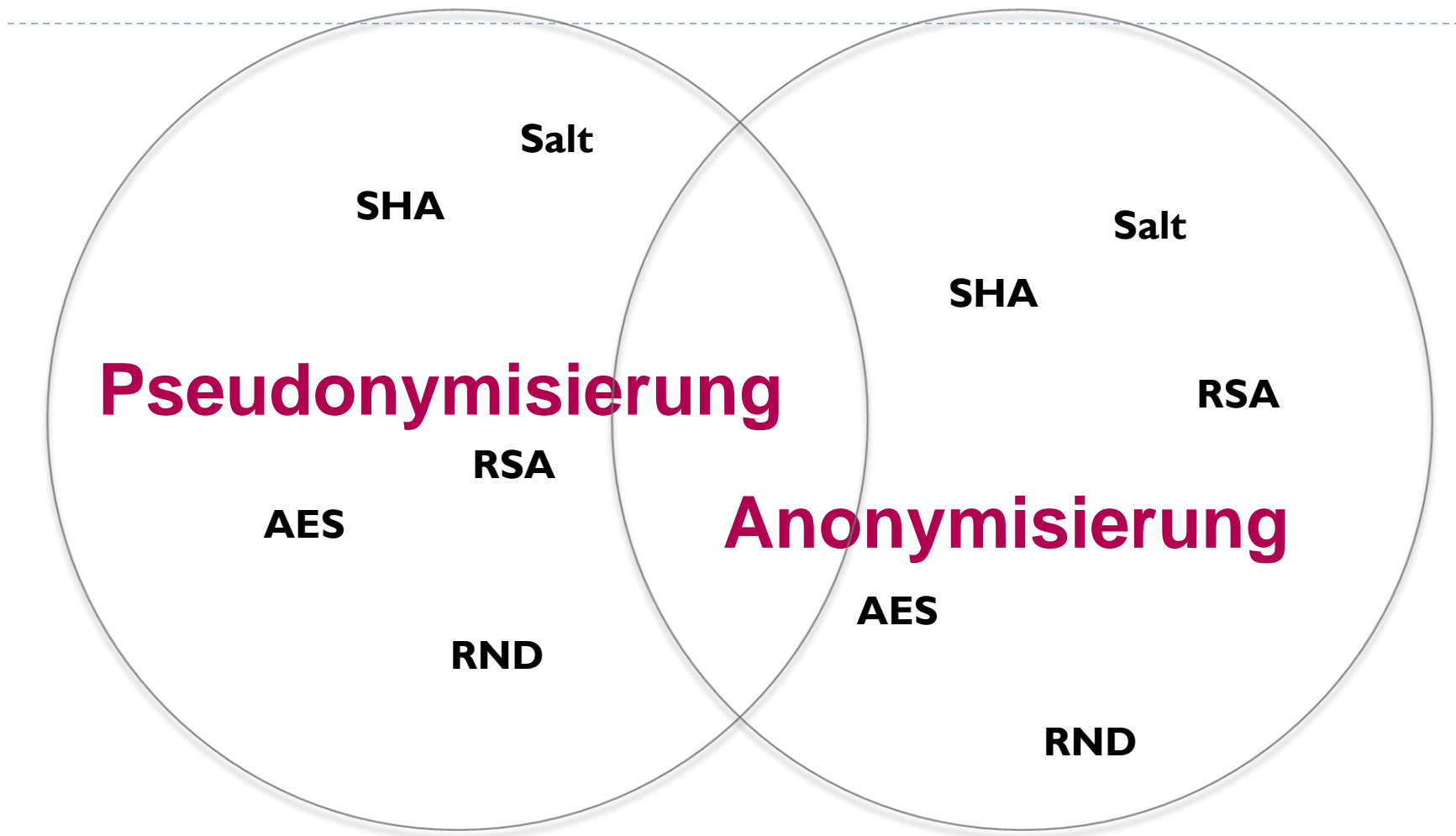
Ausgangspunkt: personenbezogene Daten



~~nicht
personenbezogen
nicht (mehr)
personenbeziehbar~~



Pseudonymisierung



Anonymisierung

Pseudonymisierung

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

Pseudonymisierung - Güte

Anonymität/Pseudonymität

Re-Identifizierung



—————>
Zeit / Technische Entwicklung / Zusatzwissen / ...

- ▶ 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

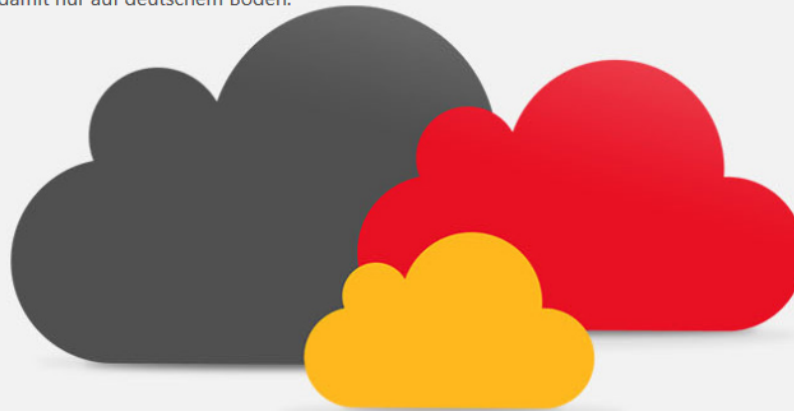
5. Ausblick

- ▶ 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**

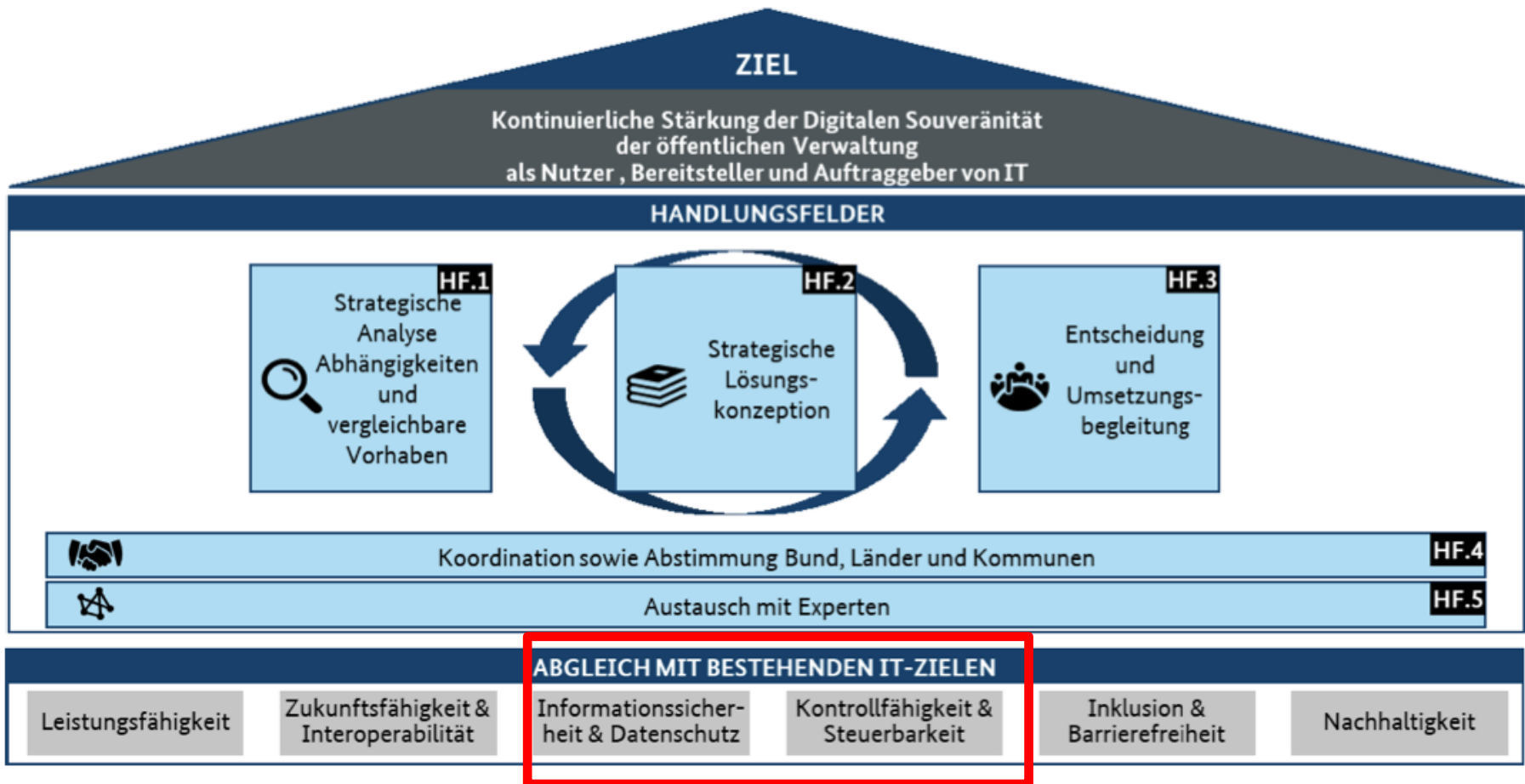
Stärkung der Digitalen Souveränität der Öffentlichen Verwaltung

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





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