Der Landesbeauftragte für den
DATENSCHUTZ und die
INFORMATIONSFREIHEIT
Rheinland-Pfalz

Schmiermittel -Anonymisierung und Pseudonymisierung
Kommunikationsmittel - Messengerdienste

Helmut Eiermann
Stellv. Landesbeauftragter / Leiter Bereich Technik

Anonymisierung / Pseudonymisierung

Anonymisierung / Pseudonymisierung

Ausgangspunkt: personenbezogene Daten

nicht personenbezogen

nicht (mehr) personenbeziehbar

Anonymisierung

Anonymisierung/Pseudonymisierung - Genese

Datenschutzrichtline 95/46 (EG)

Erwägungsgrund 26:

„*Die Schutzprinzipien finden keine Anwendung auf Daten, die derart **anonymisiert** sind, daß die betroffene Person **nicht** mehr identifizierbar ist.“*

Anonymisierung/Pseudonymisierung - Genese

Art. 4 Nr. 5 DSGVO:

*„**Pseudonymisierung** die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung **zusätzlicher Informationen** nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen **gesondert aufbewahrt** werden und **technischen und organisatorischen Maßnahmen** unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.“*

Erwägungsgründe 26, 28, [...]

Ausgangspunkt: personenbezogene Daten

nicht personenbezogen

nicht (mehr) personenbeziehbar

Pseudonymisierung

Pseudonymisierung - Funktionen

Artikel 11

Verarbeitung, für die eine Identifizierung der betroffenen Person nicht erforderlich ist

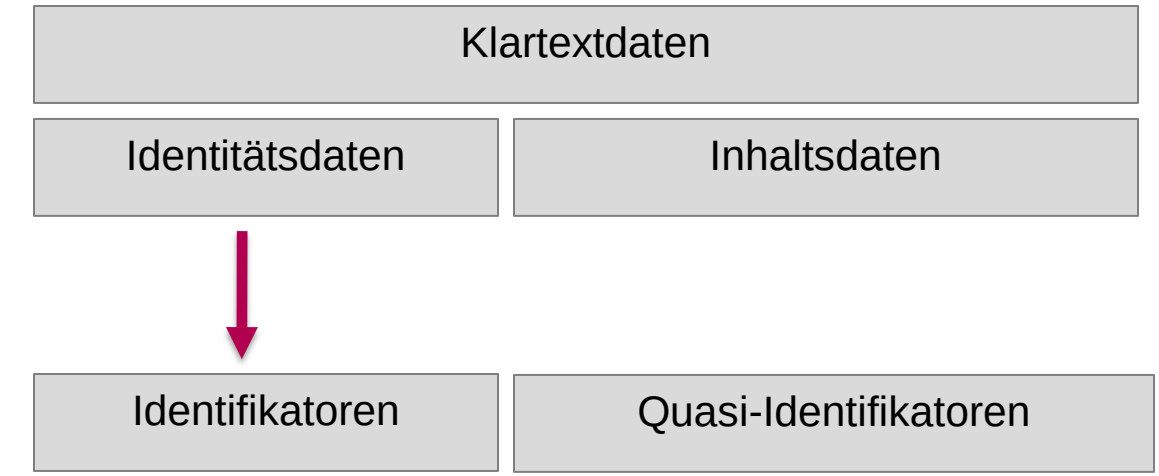
(1) Ist für die Zwecke, für die ein Verantwortlicher personenbezogene Daten verarbeitet, die Identifizierung der betroffenen Person durch den Verantwortlichen nicht oder nicht mehr erforderlich, so ist dieser nicht verpflichtet, zur bloßen Einhaltung dieser Verordnung zusätzliche Informationen aufzubewahren, einzuholen oder zu verarbeiten, um die betroffene Person zu identifizieren.

(2) Kann der Verantwortliche in Fällen gemäß Absatz 1 des vorliegenden Artikels nachweisen, dass er nicht in der Lage ist, die betroffene Person zu identifizieren, so unterrichtet er die betroffene Person hierüber, sofern möglich. In diesen Fällen finden die Artikel 15 bis 20 keine Anwendung, es sei denn, die betroffene Person stellt zur Ausübung ihrer in diesen Artikeln niedergelegten Rechte zusätzliche Informationen bereit, die ihre Identifizierung ermöglichen.

Pseudonymisierung - Funktionen

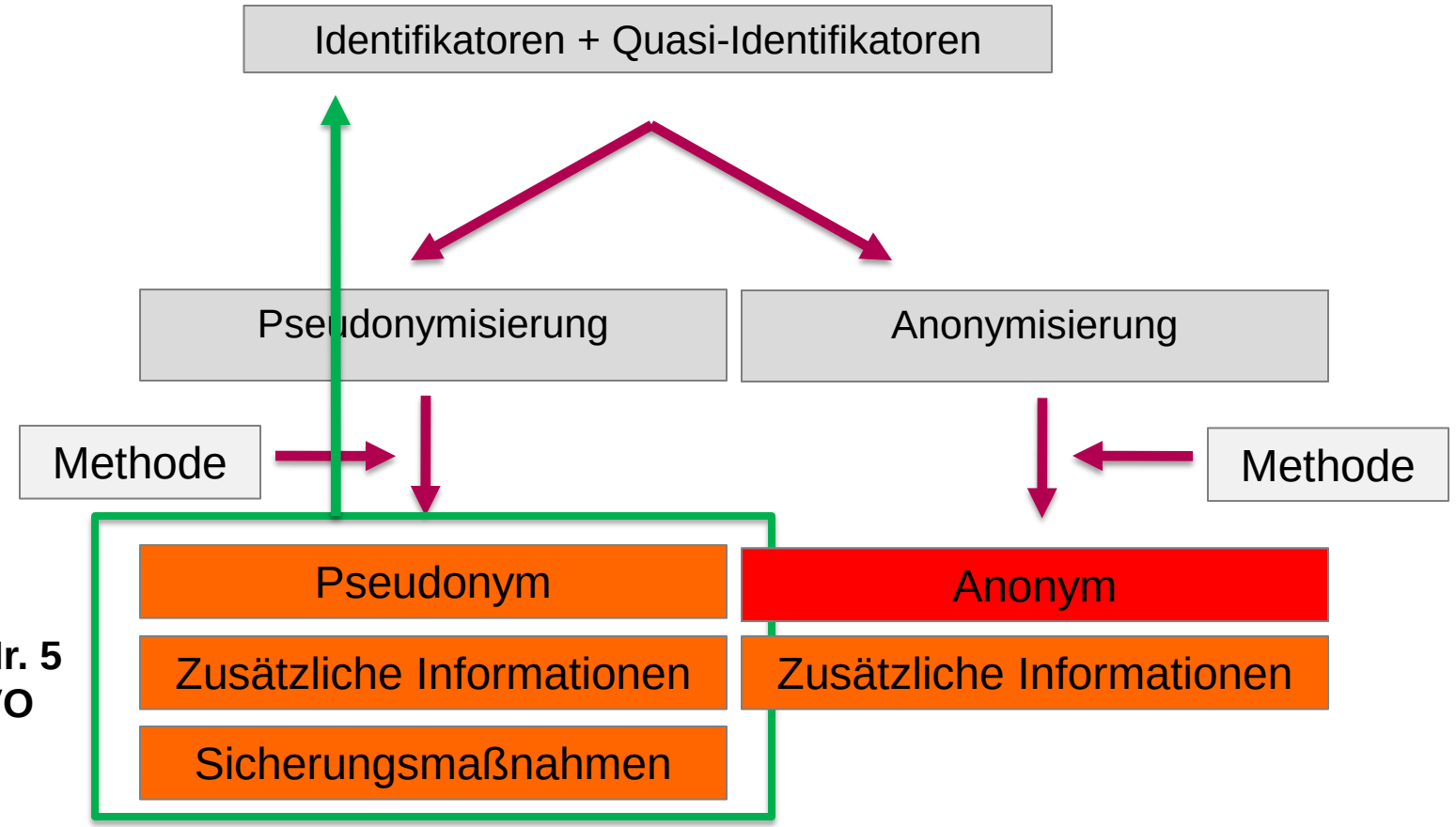
- Technologiefunktion (Privacy by Design), Art.25
- Datenminimierungsfunktion, Art. 5 (1) lit. c
- Schutzfunktion, Art. 32
- Risikominimierungsfunktion, ErwGr. 28, Art. 6 (1) f, Art. 34 (3)
- Befreiungsfunktion (Erfüllung Betroffenenrechte), Art. 11(1)+(2)
- Erleichterungsfunktion (Zweckänderung, Geeignete Garantien), Art. 6 (4) e, 28, 89 (1)

Pseudonymisierung – Anonymisierung



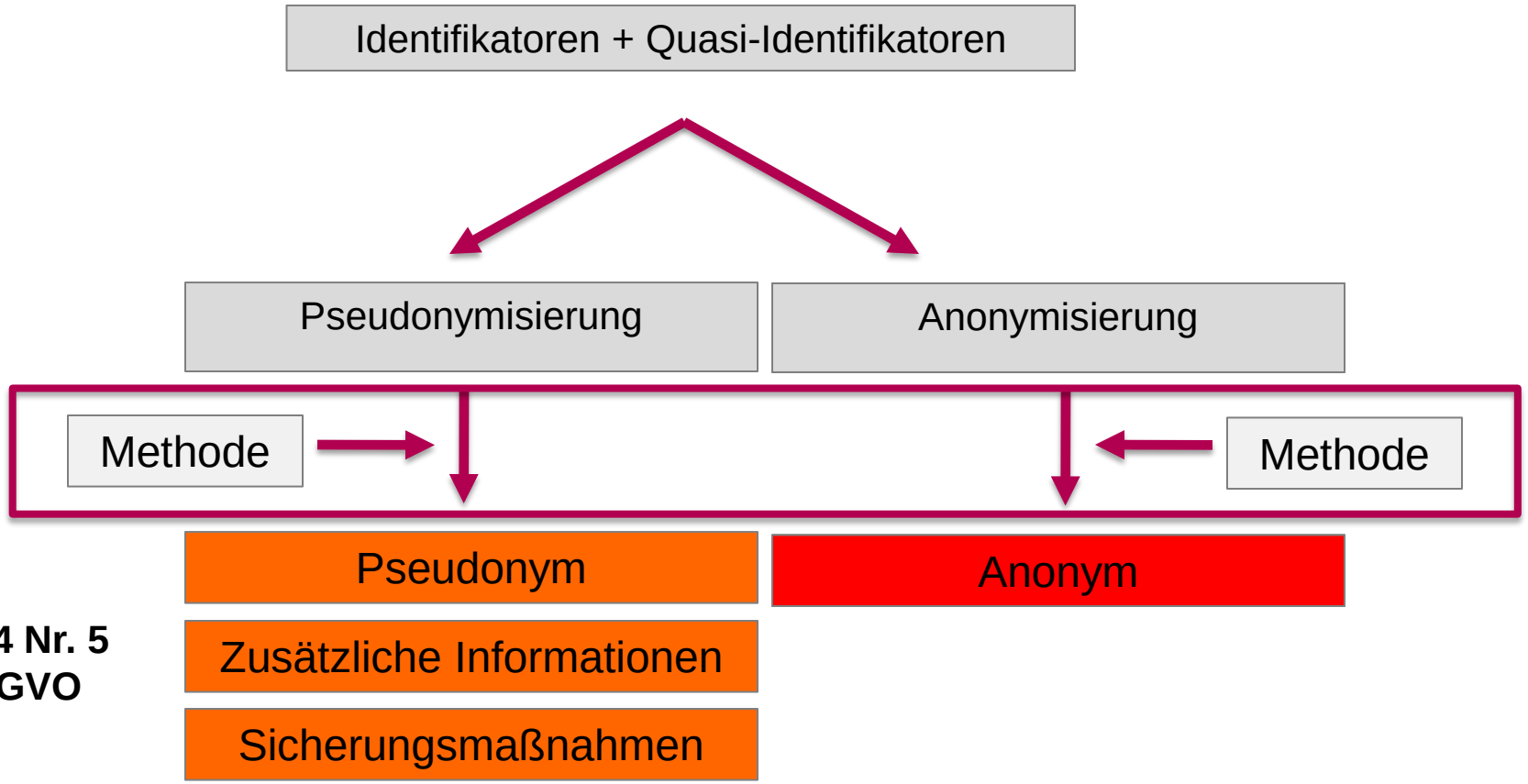
Helmut Eiermann + Adresse Stellv. LfDI RP 2020

Pseudonymisierung – Anonymisierung

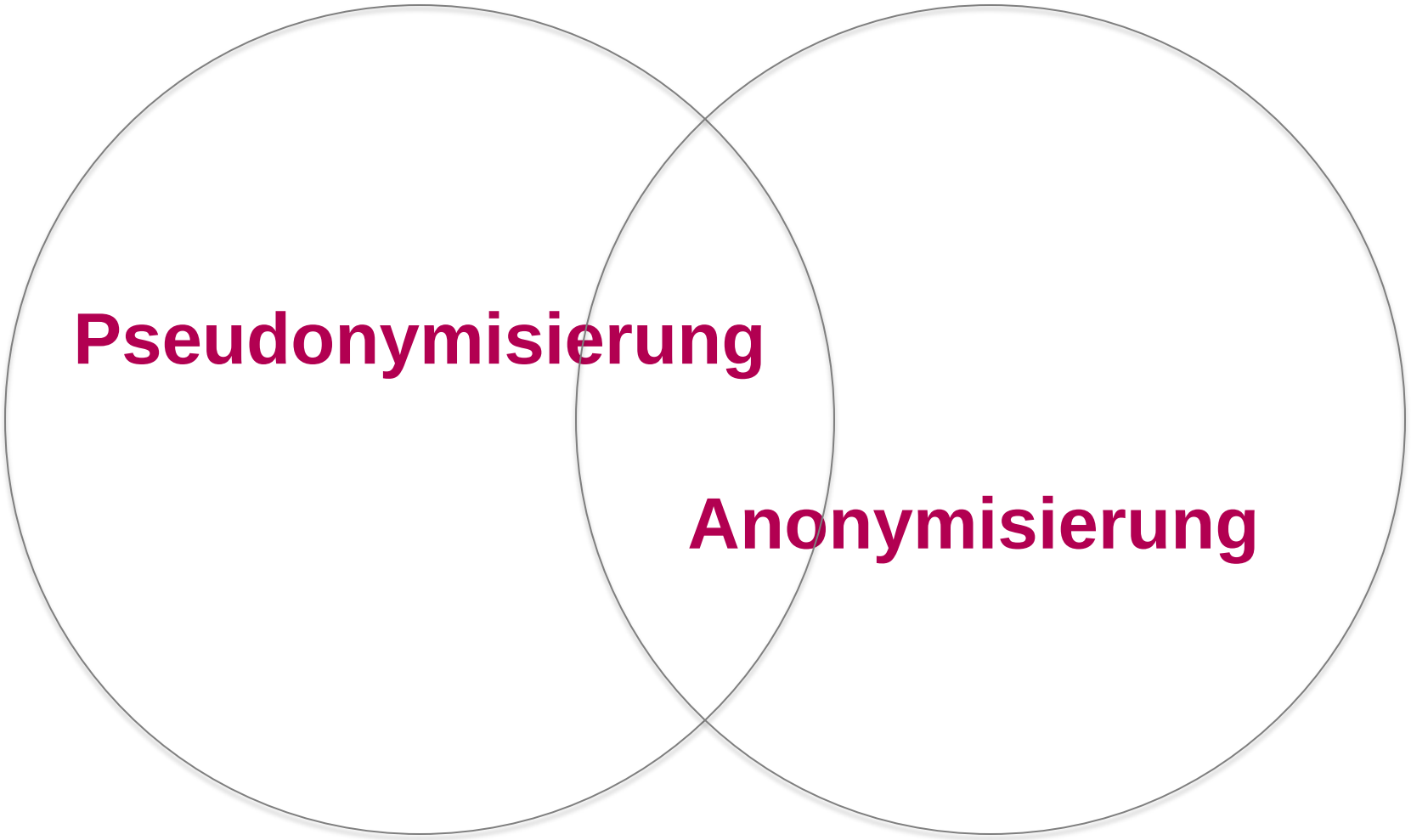


Art. 4 Nr. 5 DSGVO

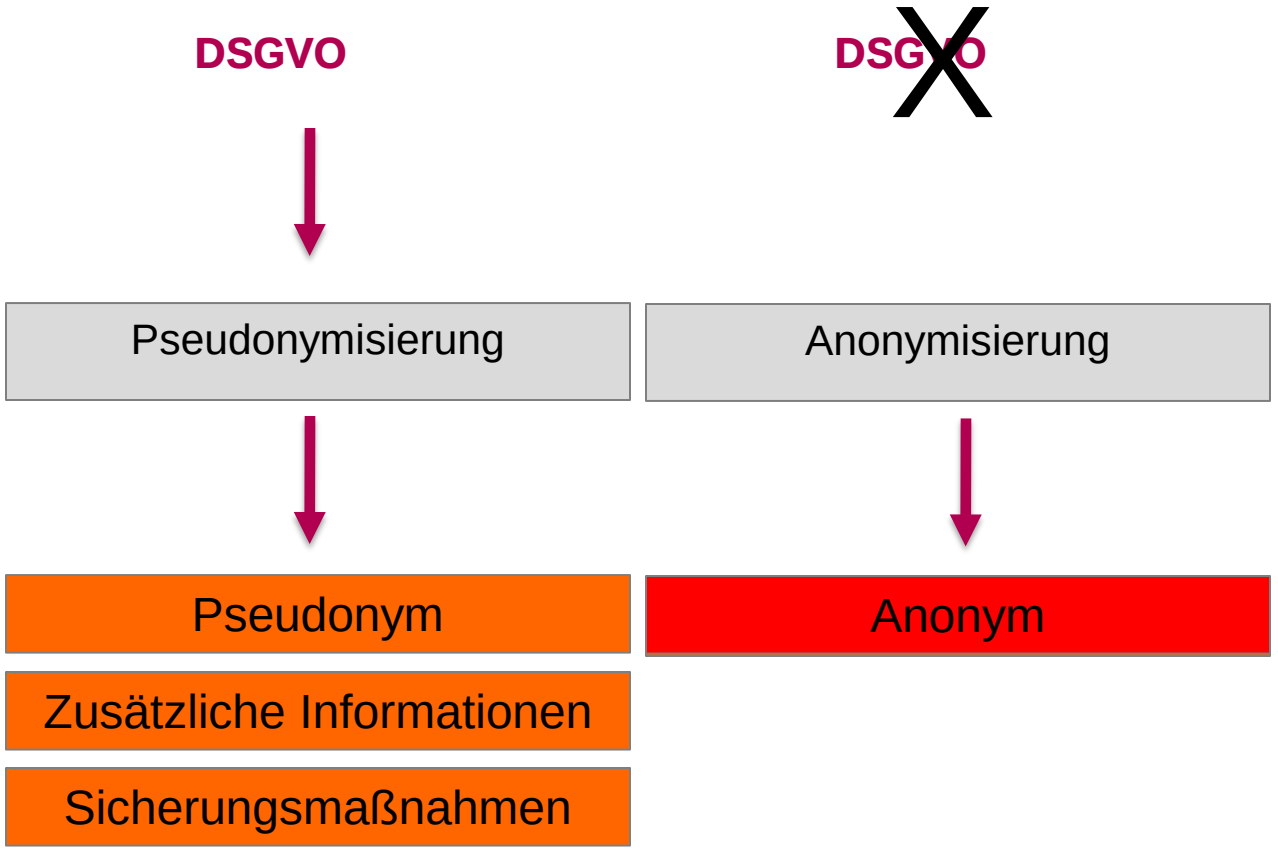
Pseudonymisierung – Anonymisierung



Art. 4 Nr. 5 DSGVO


Pseudonymisierung
Anonymisierung

Pseudonymisierung – Anonymisierung



Pseudonymisierung - Anonymisierung

ErwGr. 26:
*„... **nicht oder nicht mehr** identifiziert werden kann.“*

absolut oder **relativ**?

ErwGr. 26:
*„Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten **alle Mittel** berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person **nach allgemeinem Ermessen wahrscheinlich** genutzt werden. [...]*
*Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten **alle objektiven Faktoren** herangezogen werden.“*

Pseudonymisierung - Anonymisierung

ErwGr. 26:
*„... **nicht oder nicht mehr** identifiziert werden kann.“*

absolut oder **relativ**?

Kriterien (ErwGr 26)**:**

- Kosten
- Zeitaufwand
- Verfügbare Technologien
- Technologische Entwicklung
- Sonstige objektive Faktoren

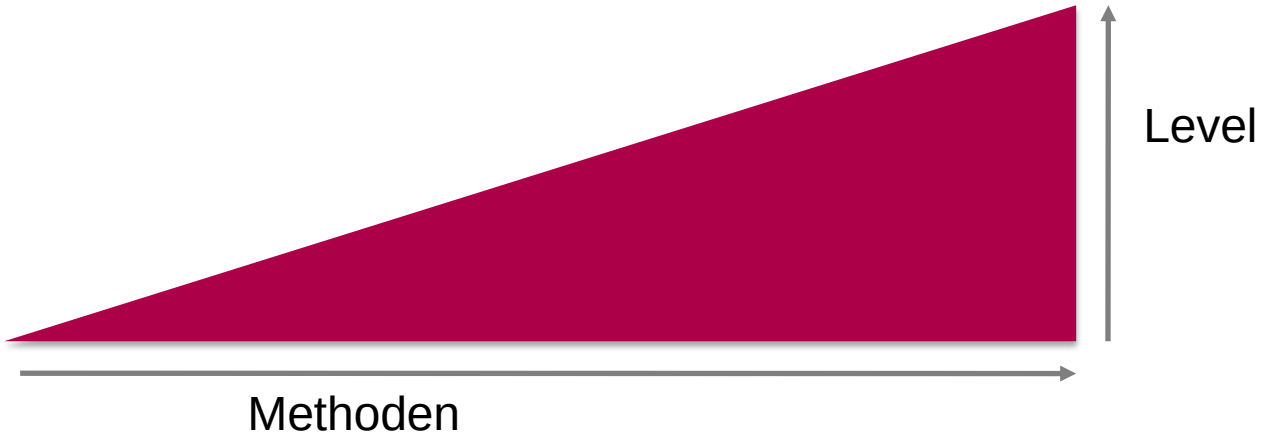
Risikobewertung
(u.a. Art. 24 (1), 32 (1)

Datenschutzfolgenabschätzung
(Art. 35)

Pseudonymisierung
Anonymisierung

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

Anonymisierung/Pseudonymisierung - Güte



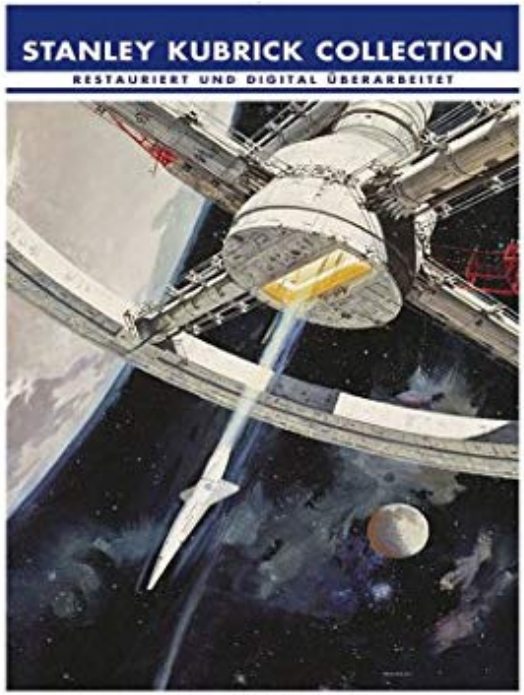
Designkriterien

- D1 keine (realistische) Re-Identifizierungsmöglichkeit
- D2 Kein Herausgreifen einzelner Personen (Singling out)
- D3 Keine Verknüpfbarkeit von Datensätzen (Linkability)
- D4 Keine Ableitbarkeit weiterer Informationen (Inference)

Pseudonymisierung - Designkriterien

- D1 – keine (realistische) Re-Identifizierungsmöglichkeit

Methode



+1

IBM

Designkriterien

- D2 Kein Herausgreifen einzelner Personen (Singling out)

männlich	10.1.59	PLZ 55262	Kaufmann
männlich	15.3.60	PLZ 55262	Bäcker
weiblich	15.3.60	PLZ 55116	Polizistin
männlich	16.12.32	PLZ 55124	Lehrer
weiblich	21.8.89	PLZ 25869	Logopädin
weiblich	26.7.62	PLZ 55xxx	Lehrerin

Gröde, SH, 7 Einwohner

Designkriterien

- D3 Keine Verknüpfbarkeit von Datensätzen (Linkability)

4711	Ford PKW	PLZ 55262	15.6.2015
4711	BASF	PLZ 55262	1.10.1995

Pseudonym

4711	10.1.59	PLZ 55262	Kaufmann
0815	15.3.60	PLZ 55262	Bäcker
2324	15.3.60	PLZ 55116	Polizistin
5793	16.12.32	PLZ 55124	Lehrer
1672	21.8.89	PLZ 25869	Logopädin
9062	26.7.62	PLZ 55124	Lehrerin

Verkettbarkeit ➔ Re-Identifizierungs-Risiko

Designkriterien

- D4 Keine Ableitbarkeit weiterer Informationen (Inference)

männlich	60 - 69	PLZ 55xxx	Kaufmann	Grippe
männlich	50 - 59	PLZ 55xxx	Bäcker	Glaukom
weiblich	50 - 59	PLZ 55xxx	Polizistin	HIV
männlich	80 - 89	PLZ 55xxx	Lehrer	Beinbruch
weiblich	30 - 39	PLZ 25xxx	Logopädin	Blutspende
weiblich	50 - 59	PLZ 55xxx	Lehrerin	Grippe

Kontext/Zusatzwissen:
Meine Nachbarin wurde ins Krankenhaus eingeliefert.
Sie ist 57 Jahre alt. Sie ist Polizistin.

Pseudonymisierung - Güte

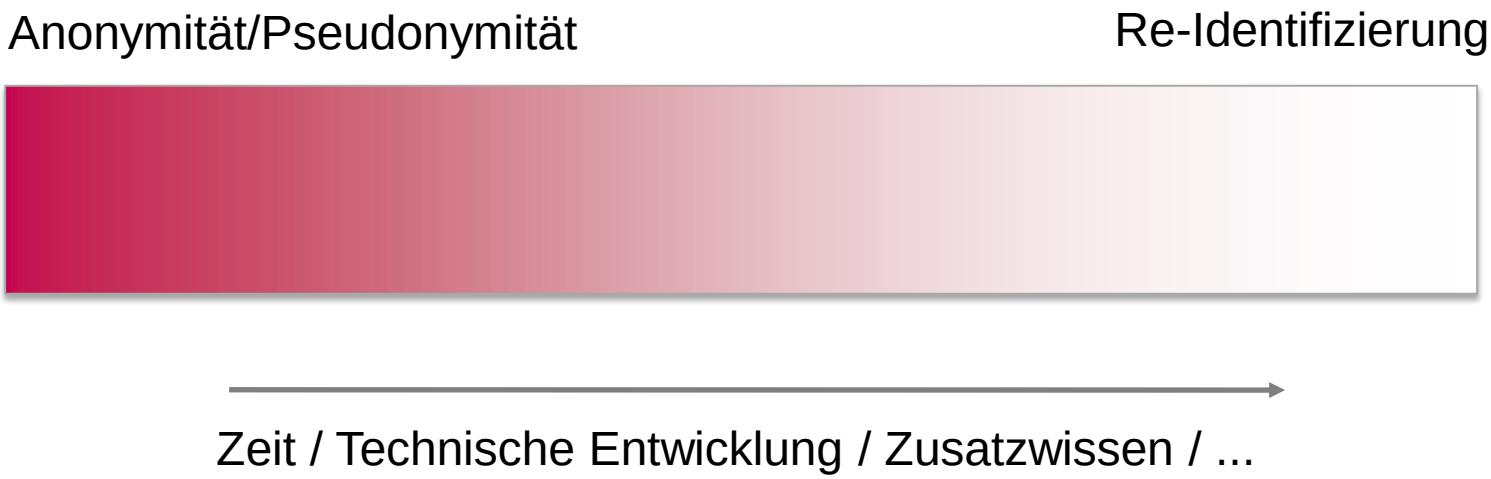
Zeit / Technische Entwicklung / Zusatzwissen / ...

Zustand

pseudonym
anonym

pseudonym
anonym

Pseudonymisierung - Güte

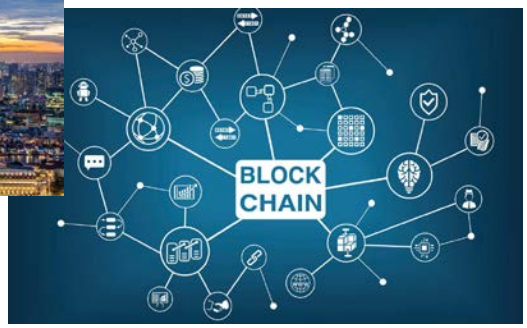


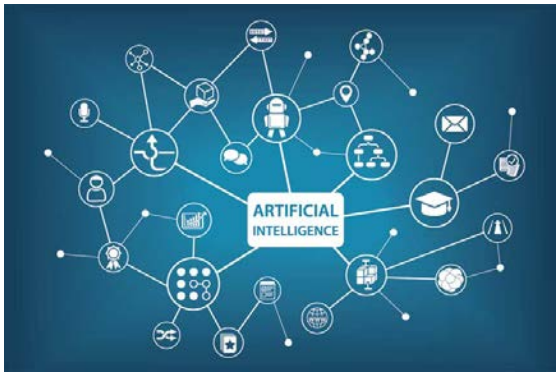
- Annahme eines „sicheren **Zeitraums**“ (vgl. BSI-Kryptoempfehlungen)
- Turnusmäßige **Neubewertung** / Audits
- **Re-Anonymisierung/Re-Pseudonymisierung**

Funktionen

- Technologiefunktion (Privacy by Design), Art.25
- Datenminimierungsfunktion, Art. 5 (1) lit. c
- Schutzfunktion, Art. 32
- Risikominimierungsfunktion, ErwGr. 28, Art. 6 (1) f, Art. 34 (3)
- Befreiungsfunktion (Erfüllung Betroffenenrechte), Art. 11(1)+(2)
- Erleichterungsfunktion (Zweckänderung, Geeignete Garantien), Art. 6 (4) e, 28, 89 (1)

Pseudonymisierung – der Enabler



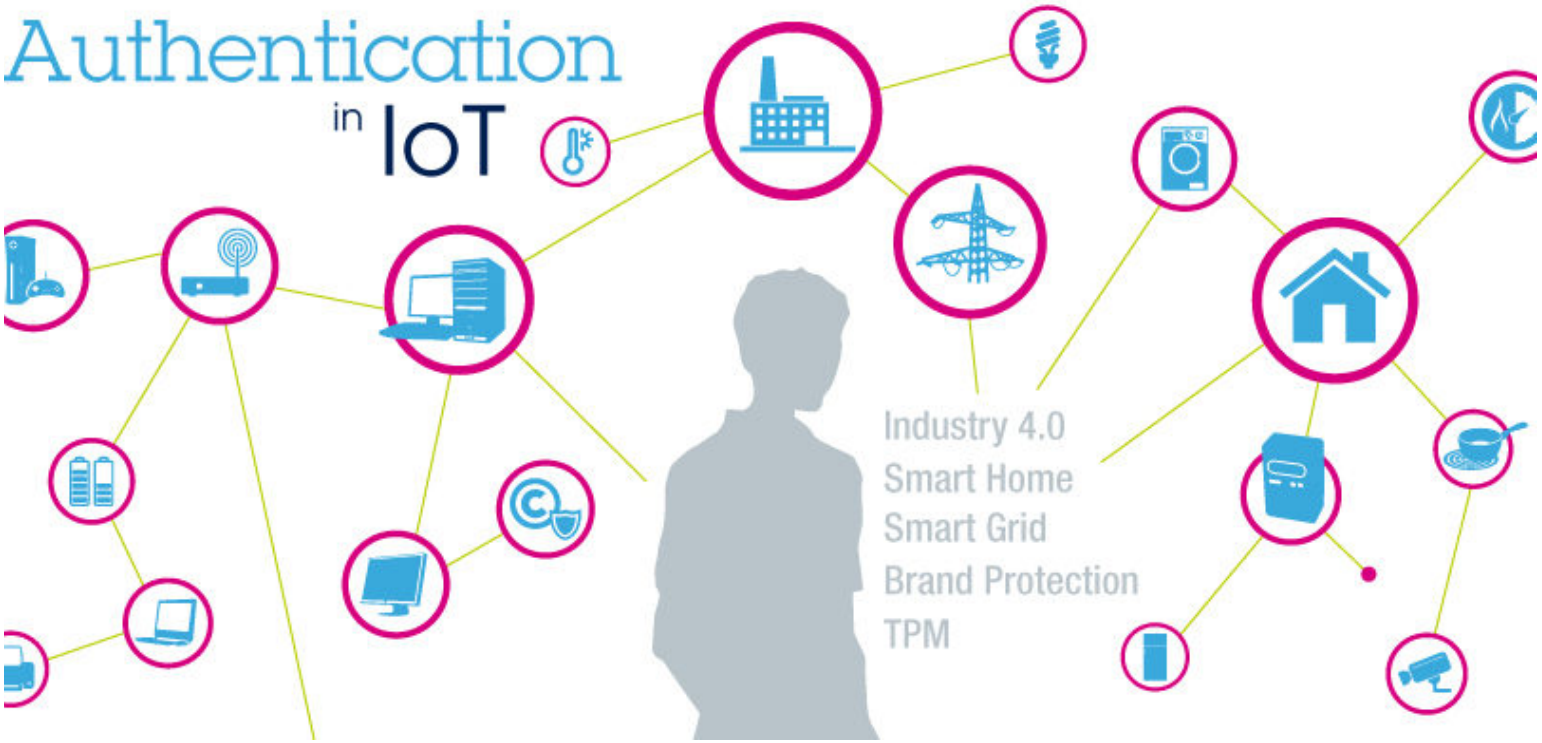


Pseudonymisierung


SMART
CITY


SMART ENERGY


Smart
Industry


Authentication
in IoT
Industry 4.0
Smart Home
Smart Grid
Brand Protection
TPM

Datenschätze

- Standortdaten
- Datum/Uhrzeit
- Ereignisdaten
- Verbrauchsdaten
- Kommunikationsdaten
- Nutzungsdaten
- Korrelationsdaten
- Umgebungsdaten
- Metadaten
- Historische Daten
- …

Datenschätze

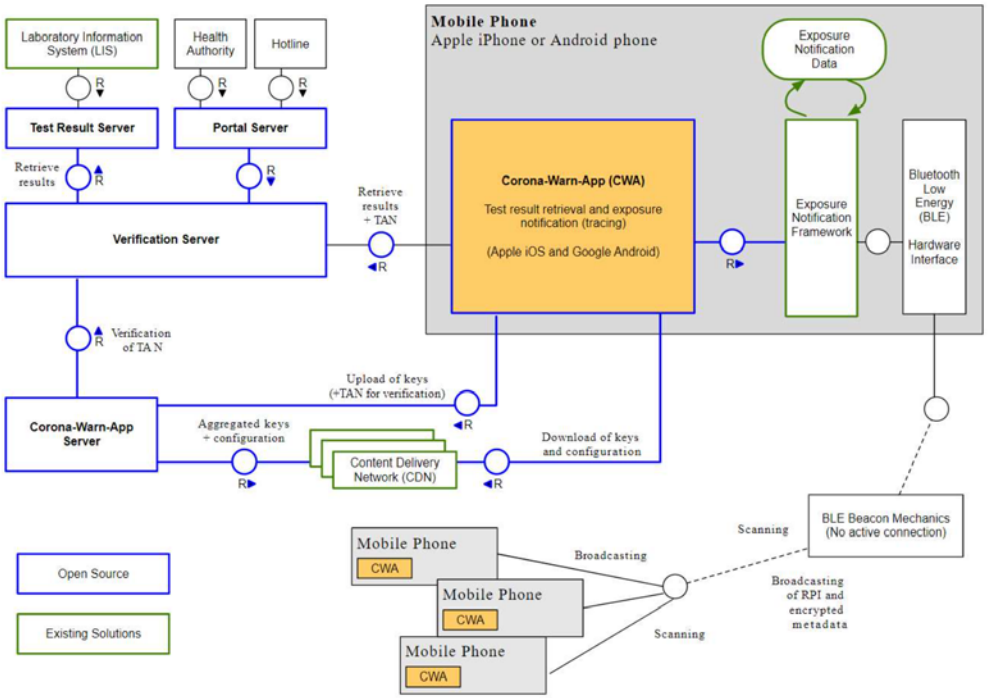
Analyse
und
Vorhersage


MEDICAL
MEDICAL
MEDICAL
MEDICAL
MEDICAL
HEALTHCARE'S
SMART FUTURE

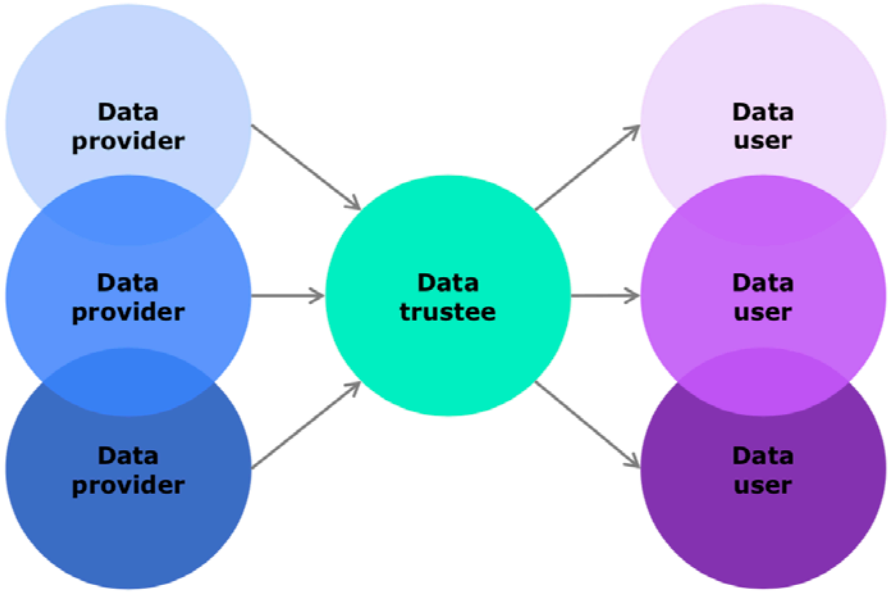
2 Architecture Outline

2.1 Big Picture

To reduce the spread of COVID-19, it is necessary to inform people about their close proximity to positively tested individuals. So far, health departments and affected individuals have identified possibly infected individuals in personal conversations based on each individuals' memory. This has led to a high number of unknown connections, e.g. when using public transport.



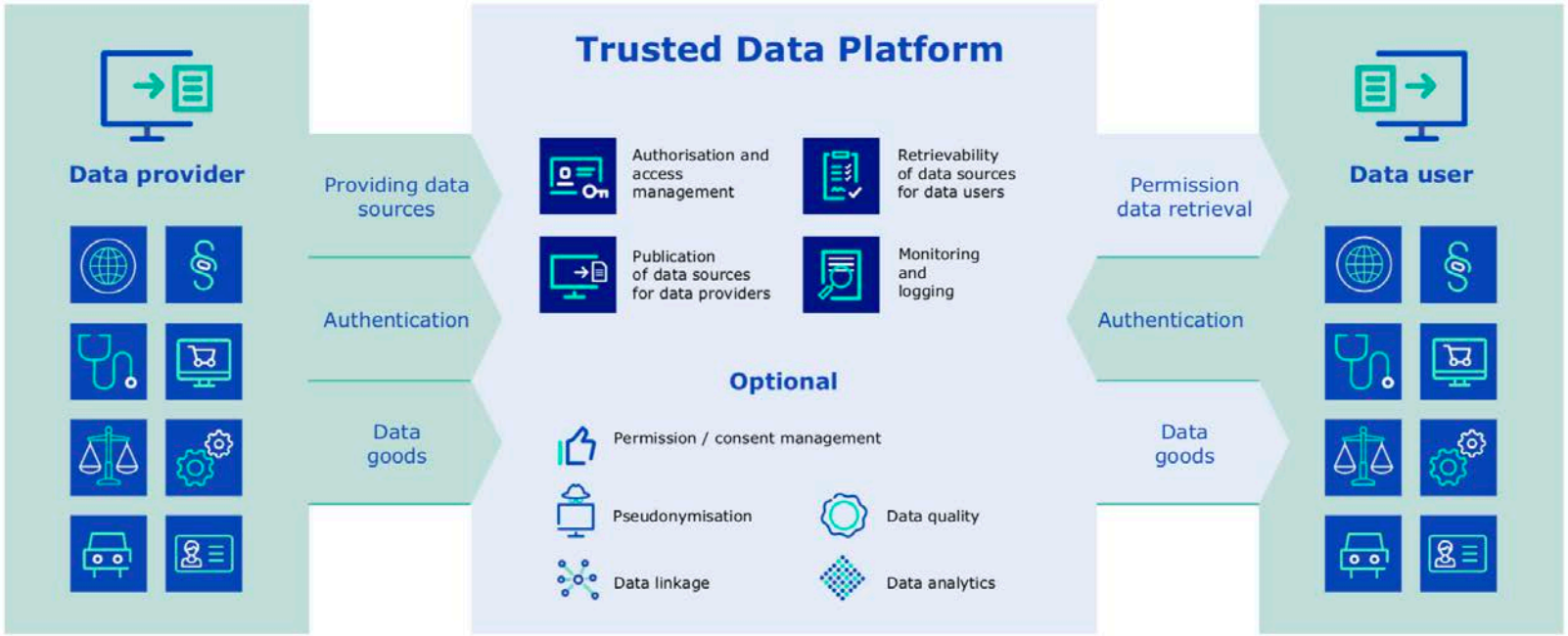
The data trustee is an independent trust authority that mediates data between the data provider and the data user.



- Identity and authorisation management
- Consent and access management
- Transparency and sovereignty
- Data security
- Logging and protocol
- Pseudonymisation and anonymisation

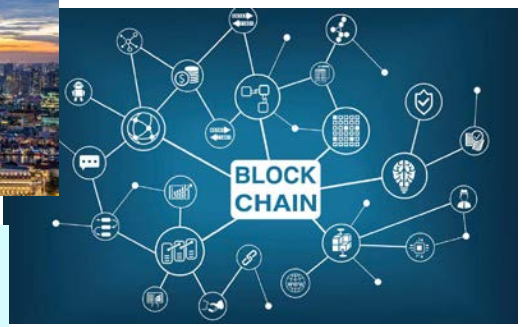
Quelle: Bundesdruckerei

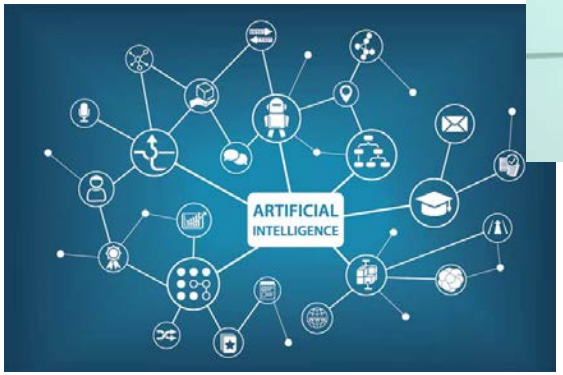
Bundesdruckerei as **data trustee** or **trust office** ensures the necessary data governance



Quelle: Bundesdruckerei

Pseudonymisierung – der Enabler





Pseudonymisierung

Literatur:

- Working Paper 216 Art. 29-Gruppe
  https://www.bfdi.bund.de/SharedDocs/Publikationen/DokumenteArt29Gruppe_EDSA/Stellungnahmen/WP216_Opinion52014AnonymisationTechniques.html
- Guidelines 4/2019 on Article 25 Data Protection by Design and by Default; EDPB
  https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf
- Whitepaper „Pseudonymisierung“ der Fokusgruppe Datenschutz; Digitalgipfel 2017
  https://www.projekt29.de/pseudonymisierung-nach-der-dsgvo-fokusgruppe-datenschutz-veroeffentlicht-whitepaper/
- Arbeitspapier „Anforderungen an den datenschutzkonformen Einsatz von Pseudonymisierungslösungen“ der Fokusgruppe Datenschutz; BMI; Digitalgipfel 2018
  https://www.gdd.de/downloads/anforderungen-an-datenschutzkonforme-pseudonymisierung
- ENISA Working Paper 218 „Recommendations on shaping technology according to GDPR provisions

  https://www.enisa.europa.eu/publications/recommendations-on-shaping-technology-according-to-gdpr-provisions-part-2/at_download/fullReport

Technische Anforderungen an Messengerdienste im Krankenhaus

Messenger-Einsatzbereiche

Krankenhausinterne Nutzung

Konsil

Bereitschafts-dienst

Sozialdienste

Apotheken

Leistungserbringer

Patient

Rettungsdienste

Arztpraxen

Gesundheitsnetze

Telemedizin

Nachsorgeeinrichtungen

„Whitepaper“ der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder – 07.11.2019

Technische Datenschutzanforderungen an Messenger-Dienste im Krankenhausbereich (Whitepaper der Datenschutzkonferenz)

➔ Verabschiedung „Whitepaper“ auf der 98. DSK

➔ Kommentierungsverfahren mit den Verbänden (DKG, bvitg, VKD, BÄK etc.)

https://www.datenschutzkonferenz-online.de/media/oh/20191106_whitepaper_messenger_krankenhaus_dsk.pdf

Technisch-organisatorische Maßnahmen

- Verordnungskonformität
- Einhaltung der Datenschutzgrundsätze nach Art. 5
  - Datenminimierung
  - Speicherbegrenzung
  - Zweckbindung
  - Verarbeitung nach Treu und Glauben
- Vertraulichkeit, Integrität, Verfügbarkeit
- Belastbarkeit
- Wahrung der Betroffenenrechte
- Informationspflichten

Messenger-Einsatzbereiche

Krankenhausinterne Nutzung

Konsil

Bereitschafts-dienst

Rettungsdienste

Arztpraxen

Gesundheitsnetze

Telemedizin

Sozialdienste

Apotheken

Leistungserbringer

Patient

Nachsorgeeinrichtungen

Anforderungen der Datenschutz-Aufsichtsbehörden an Messenger-Dienste im Krankenhausbereich*

** https://www.datenschutzkonferenz-online.de/media/oh/20191106_whitepaper_messenger_krankenhaus_dsk.pdf*

- Applikation
- Endgerät
- Kommunikation
- Plattform/Betrieb

Applikation

- Unterrichtung nach Art. 13 DS-GVO
- Authentifizierungs-Mechanismen
- Eigene zugriffsgeschützte Speicherbereiche
- Verlässliche Identifizierung und Authentifizierung der Kommunikationspartner
- Schnittstellen (z.B. KIS)
- Löschfunktionen
- Bearbeitungsfunktionen (Schwärzung)
- Privacy by Default

Endgerät

- Zugriffsschutz (PIN/Passphrase)
- Device Management (Ortung, Löschung/Sperre)

Kommunikation

- Ende-zu-Ende-Verschlüsselung nach dem Stand der Technik
- Integritätsschutz (Elektronische Signatur)
- Begrenzung der Speicherung von Verbindungsdaten
- Verzicht auf proprietäre Kommunikationsprotokolle

Plattform / Betrieb

- Nur zugelassene Nutzer (Registrierung/Autorisierung)
- Rollen-/Berechtigungskonzept
- Datenschutzfolgenabschätzung
- On premise / Dienstleister

Problembereich: Nutzung privater Geräte

- Sicherheitsrisiken / Sicherheitsniveau
- gemischte Nutzungsszenarien (privat/dienstlich)
- Einwilligungsproblematik im Arbeitsverhältnis
- begrenzte Einwirkungsmöglichkeiten des Arbeitgebers auf Gerätekonfiguration und Nutzung
- ...

Problembereich: Nutzung privater Geräte

Speiseplan

Schichtplan

Behandlungsplan

Grundsatz: Keine Nutzung privater Geräte.

Der Landesbeauftragte für den
DATENSCHUTZ und die
INFORMATIONSFREIHEIT
Rheinland-Pfalz

Helmut Eiermann

Stellvertretender Landesbeauftragter für den Datenschutz
und die Informationsfreiheit Rheinland-Pfalz /
Leiter Bereich Technik

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