Datenräume ohne Desaster – oder Datenpannen by Design?

Dr. h.c. Marit Hansen
Landesbeauftragte für Datenschutz Schleswig-Holstein

Sommerakademie 2024 in Kiel, 09.09.2024

Plattform Privatheit

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Überblick

1. Startpunkt: Europäische Datenstrategie
2. Datenräume
3. Risiken und Maßnahmen … und Maßnahmen
4. … und Risiken?
5. Fazit

1. Daten teilen, Daten nutzen

Europäische Datenstrategie

Die EU zum Vorbild für eine digitale Gesellschaft machen

Die Europäische Datenstrategie soll die EU an die Spitze einer datengesteuerten Gesellschaft bringen. Ein Binnenmarkt für Daten ermöglicht eine EU-weite und branchenübergreifende Datenweitergabe zum Nutzen von Unternehmen, Forschenden und öffentlichen Verwaltungen.

https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_de

Überblick

2. Datenräume

Diese Datenräume werden Folgendes umfassen:

i) die Einführung von Werkzeugen und Plattformen für die gemeinsame Datennutzung;

ii) die Schaffung von Rahmenbedingungen für die Daten-Governance;

iii) die Verbesserung der Verfügbarkeit, Qualität und Interoperabilität der Daten – sowohl in sektorspezifischen Zusammenhängen als auch sektorenübergreifend.

Die Unterstützung von Datenräumen wird sich auch auf Datenverarbeitungs- und Rechenkapazitäten erstrecken, die den grundlegenden Anforderungen in Bezug auf Umweltleistung, Sicherheit, Datenschutz, Interoperabilität und Skalierbarkeit genügen.

Überblick

2. Datenräume

- Also: pro Sektor ein „Datenhaufen" mit ein paar Regeln?
- Nicht unbedingt:

So wohl nicht.

Mit Datentreuhänder

Dezentral

Icon: Risk Assessment Icons erstellt von Freepik - Flaticon

Bilder: StableDiffusion

Überblick

3. Risiken und Maßnahmen

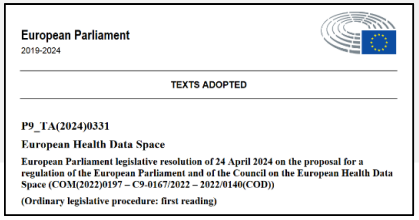
- Risiko: Mangelnde oder unklare Datenqualität
- Maßnahme: Kuratierung und Beschreibung

?

Icon: Risk Assessment Icons erstellt von Freepik - Flaticon

Bilder: Elena Leya via Unsplash (links)
Ella C via Unsplash (rechts)

Überblick


European Parliament
2019-2024

TEXTS ADOPTED

P9_TA(2024)0331

European Health Data Space

European Parliament legislative resolution of 24 April 2024 on the proposal for a regulation of the European Parliament and of the Council on the European Health Data Space (COM(2022)0197 – C9-0167/2022 – 2022/0140(COD))

(Ordinary legislative procedure: first reading)

3. Risiken und Maßnahmen

- Risiko: Unerlaubte Zugriffe
- Maßnahme: Absicherung, z.B. über eine sichere Verarbeitungsumgebung

EHDS

Article 50

Secure processing environment

The health data access bodies shall provide access to electronic health data ***pursuant to a data permit*** only through a secure processing environment, with technical and organisational measures and security and interoperability requirements. In particular, ***the secure processing environment*** shall ***comply with*** the following security measures:

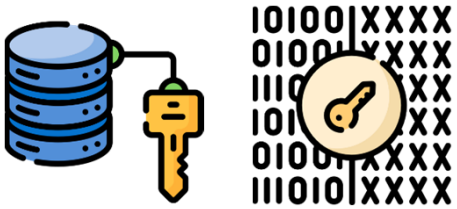
https://www.europarl.europa.eu/doceo/document/TA-9-2024-0331_EN.pdf

3. Risiken und Maßnahmen

- Secure Processing Environment für Zugriffschutz

Autorisierung

Authentisierung



Verschlüsselung

Protokollierung

ISMS / DSMS

Regelmäßige Audits

- Aber Risiko der Anhäufung und des Kontrollverlusts

Icons: Risk Assessment, Authorization, Password, Key Value database, Encrypt, Data Table, Control Room und Audit Icons erstellt von Freepik - Flaticon

Überblick

3. Risiken und Maßnahmen

- Weitere Maßnahmen gegen unberechtigten Zugriff

Dezentrale Verarbeitung (z.B. Federated Learning)

Statt Zugriff auf Daten: Ausführung von Analysen

Policies mit Restriktionen

- Risiko Identifizierbarkeit – Anforderung Anonymisierung, Pseudonymisierung, …

Reduzieren der Identifizierbarkeit

Trennung von Datenbeständen

Icons: Risk Assessment, Software Development, Research and Development, Proposal, Anonymous und Health Icons erstellt von Freepik - Flaticon

Überblick

3. Risiken und Maßnahmen

EHDS, Erwägungsgrund 43

development of common standards. They should apply tested ***state-of-the-art*** techniques that ensure electronic health data is processed in a manner that preserves the privacy of the information contained in the data for which secondary use is allowed, including techniques for pseudonymisation, anonymisation, generalisation, suppression and randomisation of personal data. Health data access bodies can prepare datasets to the data user requirement linked to the issued data permit. ***In that regard, health data access bodies should cooperate across borders to develop and exchange best practices and techniques.*** This includes rules for ***anonymisation*** of microdata sets. ***When relevant, the Commission should set out the procedures and requirements, and provide technical tools, for a unified procedure for anonymising and pseudonymising the electronic health data.***

Überblick

3. Risiken und Maßnahmen

- … und weitere Maßnahmen, z.B. mit Hilfe des Instrumentenkastens der Privacy-Enhancing Technologies
  - Besondere Arten der Verschlüsselung oder Umschlüsselung für eine genauere Zugriffssteuerung [z.B. Attribute Based Encryption, Proxy-Re-Encryption, Polymorphic Encryption]
  - Möglichkeiten der Berechnungen auf verschlüsselten Daten [z.B. Homomorphic Encryption]
  - Besondere Pseudonymisierungsverfahren [z.B. Oblivious Pseudonymization-as-a-Service: der Service (über einen Intermediär) erhält weder Kenntnis über Daten noch über Pseudonyme]
  - Dezentrale Verarbeitungen [z.B. Federated Learning]

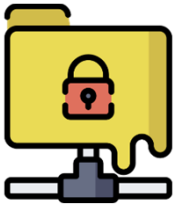
Icon: Risk Assessment Icons erstellt von Freepik - Flaticon

4. … und Risiken?

- Risiko: Fehleinschätzung und Unwissen bzgl. des beim Nutzer mobilisierbaren Zusatzwissens → Identifizierbarkeit [Roßnagel, DuD 2024, 513 (520)]

- Risiko: Noch mehr Zusatzwissen durch weiteres Datenteilen (Einzel-Risiken tragbar, Gesamtschau nicht) → Identifizierbarkeit

- Risiko: Single-Point-of-Data → Hacking, staatliche Zugriffe, faktische Macht der Verarbeiter



- Risiko: Verzicht auf bessere Lösungen

Icons: Risk Assessment, Collaboration, Data Leak und Spy Icons erstellt von Freepik - Flaticon

5. Fazit

- Datenteilen unter Wahrung der Rechte anderer ist kein triviales Problem
- Aus Datenschutzsicht zahlreiche Risiken

- Für Datenräume ohne Desaster:
  - Zunächst Fortschritte beim „State of the Art“ ~~erwartet~~ nötig
  - Professionalität und Sorgfalt vor Eile
  - Folgenabschätzungen im Vorfeld, beim Aufbau und im Betrieb

Bild: Jeremy Yap via Unsplash

Überblick

1. Startpunkt: Europäische Datenstrategie
2. Datenräume
3. Risiken und Maßnahmen … und Maßnahmen
4. … und Risiken?
5. Fazit

Material

- DSK: Nutzung von Gesundheitsdaten braucht Vertrauen – Der Europäische Gesundheitsdatenraum darf das Datenschutzniveau der Datenschutz-Grundverordnung nicht aushöhlen, Stellungnahme vom 27.03.2023, https://www.datenschutzkonferenz-online.de/media/st/2023-03-27_DSK-Stellungnahme_EHDS.pdf
- EDPB: EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space, 2022, https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-032022-proposal_en
- ENISA: Data Protection Engineering, Januar 2022, https://www.enisa.europa.eu/publications/data-protection-engineering
- ENISA: Deploying Pseudonymisation Techniques, März 2022, https://www.enisa.europa.eu/publications/deploying-pseudonymisation-techniques
- ENISA: Engineering Personal Data Sharing, Januar 2023, https://www.enisa.europa.eu/publications/engineering-personal-data-sharing
- ENISA: Engineering Personal Data Protection in EU Data Spaces, Januar 2024, https://www.enisa.europa.eu/publications/engineering-personal-data-protection-in-eu-data-spaces