Datenschutzrecht

Forschungsdaten und aktuelle Forschungsfragen zum Datenschutz

(Personenbezug & Anonymität, Internet of Things)

15. Januar 2024

Harald Zwingelberg

Ansprechpartner Vorlesungsreihe: Benjamin Bremert

Vertretene Auffassungen sind solche des Referenten bzw. teilweise Ergebnisse aus dem Forschungs- und Projektbereich und kann von den Auffassungen der Datenschutz-Aufsichtsbehörde(n) abweichen.

Ankündigungen

- Gesetzestexte für Vorbereitung und Klausur:
  - DSGVO (insbesondere Art. 1-40)
  - https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A32016R0679
  - Druckfassung bereitgestellt: https://www.datenschutzzentrum.de/uploads/vorlesungen/cau/Gesetzessammlung.pdf

- Soweit nicht anders gekennzeichnet, sind alle genannten Artikel solche der DSGVO.

Agenda

- Wiederholung
- Personenbezug und Anonymität
- Datenschutz im Internet of Things
- Datenschutz in der Forschung

Wiederholung

Betroffenenrechte

Berufsgeheimnis,
Gesundheitsdaten

Auftragsverarbeitung

Wiederholung / Kurzübersicht Betroffenenrechte

Welche Betroffenenrechte nach DSGVO kennen Sie?

- Auskunft, Art. 15 DSGVO
- Berichtigung, Art. 16 DSGGVO
- Löschung, ‚right to be forgotten', Art. 17 DSGVO
- Einschränkung der Verarbeitung, Art. 18 DSGVO

Warum genügt folgende Antwort auf ein umfassendes Auskunftsersuchen nicht: „Wir speichern über Sie: Name, Adresse, Loginname, Passwort („gehasht") & Kundennummer"?

- Eine umfassende Auskunft ist Vorbedingung zur Wahrnehmung der Rechte auf Berichtigung, Löschung und Sperrung. Es müssen die konkreten Daten („Werte" in der Datenbank) mitgeteilt werden, nicht nur die Kategorien. DSGVO regelt Recht auf Datenkopie ausdrücklich in Art. 15 (2) DSGVO.

Auftragsverarbeitung

- Wie kommt die Auftragsverarbeitung in der Praxis zum Einsatz?

- Welche Rechtsfolge ergibt sich, wenn die Voraussetzungen für eine Auftragsverarbeitung erfüllt sind

Antworten: nächste Folie

Auftragsdatenverarbeitung Rechtsfolgen

Rechtsfolgen

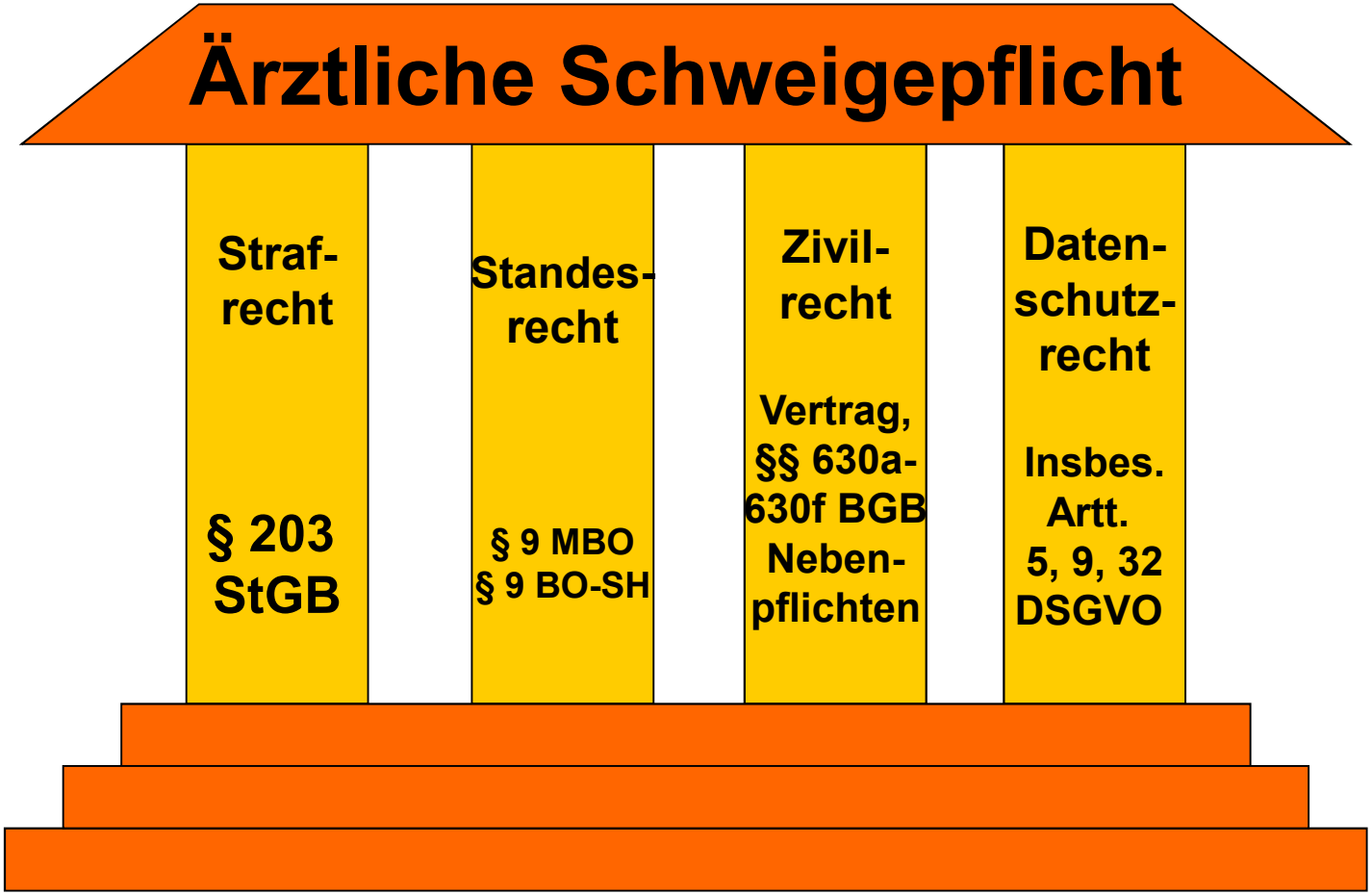
- Datentransfer zum und Verarbeitung beim Auftragsverarbeiter ist privilegiert, d.h. sie bedarf keiner gesonderten Rechtsgrundlage neben dem Auftrag.

- Geldbußen wegen Verstoß gegen die eigenen Pflichten können gegen den Auftragsverarbeiter direkt verhängt werden.

- Ein fehlender Vertrag über die Auftragsverarbeitung ist für beide Parteien bußgeldbewährt, so dass Auftragnehmer einen solchen aus Eigeninteresse anbieten sollten.
  Hinweis: Der Vertrag lässt sich bei einigen Hosting- und Mailprovidern als PDF herunterladen, unterzeichnen und zur Dokumentation nehmen.

Gesundheitsdatenschutz

- Auf welchen „4 Säulen“ beruht das Berufsgeheimnis



Personenbezug, Identifizierbarkeit, Pseudonymität, Anonymität

(ausgewählten Aspekte aus der Datenschutzforschung)

Personenbezug Begriff

PERSONENBEZOGENE DATEN

- Sind alle Informationen, die sich auf eine identifizierte oder identifizierbare Person beziehen, Art. 4 Nr. 1 DSGVO.
  - Identifiziert ist eine Person, wenn sich ihre Identität **unmittelbar aus den Informationen** ergibt.
  - Identifizierbar ist eine Person, wenn die Informationen durch Verknüpfung mit weiteren Informationen einer Person zugeordnet werden können.
    - Dabei sind alle Möglichkeiten (Mittel und Wissen) zur berücksichtigen, die nach allgemeinen Ermessen (objektiver Maßstab) wahrscheinlich genutzt werden können.
    - Dabei ist auch Wissen und Mittel anderer Personen zu berücksichtigen (etwa Internet-Veröffentlichungen oder wenn der Verantwortliche einen rechtlichen Anspruch auf Herausgabe dieser Informationen hat).

Wiederholung aus Vorlesung „Einführung I" von B. Bremert am 23.10.2023

Personenbezug Relevanz

- Hohe Bedeutung in der Praxis:
- Personenbezug entscheidet über die allgemeine Anwendbarkeit datenschutzrechtliche Vorschriften auf die Verarbeitung eben dieser Informationen
- Unterscheidung ist zentral für alle datenschutzrechtlichen Normen und deren Adressaten (DSGVO, Bundesrecht, Landesrecht, Justiz-Richtlinie, Data Spaces etc.)
- **Identifizierbarkeit** ist zentrale Weichenstellung

Personenbezug
Reduktion der Identifzierbarkeit

Wiederholung aus Vorlesung „Datenschutz durch Technik IV" von M. Hansen am 18.12.2023

Folie für Diskussion und Interaktion in der Vorlesung, nicht Teil der Druckfassung

Personenbezug Reduktion der Identifzierbarkeit

Anmerkung: Die in der Vorlesung gemeinsam erörterten Folien 13-15 stammen aus der laufenden Projekttätigkeit.

Die Grafiken zur Reduktion der Identifizierbarkeit werden in der finalen Version veröffentlicht unter:

https://www.datenschutzzentrum.de/projekte/anomed/

Eine Zusammenfassung der Eckpunkte finden Sie auf den nächsten Folien

AnoMed

Quelle: Laufende Arbeit aus dem ULD-Projekt „AnoMed". Veröffentlichung folgt

Personenbezug
Reduktion der Identifizierbarkeit

- Identifizierbarkeit kann reduziert werden
  - Pseudonymisierung, Ersetzen / löschen direkt identifizierender Informationen

  Auf Ebene einzelner Daten
  - Löschen identifizierender Informationen
  - Verallgemeinern von sonstigen Attributen, die zusammengenommen eine Identifikation erlauben

  Aggregation
  - Durch Aggregation der Daten in Statistiken, AI-Modelle, künstliche Daten
  - Kontinuierliche Kontrolle der Veröffentlichung von Informationen aus dem Datenpool

Personenbezug Ergebnisse von Pseudo- und Anonymisierung

- Voll identifizierte Daten
  - Direkt identifiziert
- Pseudonymisierte Daten
  - indirekte Identifizierung möglich mit „zusätzlichen Informationen" [additional data]
- Mutmaßliche Anonymität [supposedly anonymous]
  - Alle bekannten Re-Identifikationsmöglichkeiten ausgeschlossen
  - Risikobewertung kann künftige Risiken nicht ausschließen
- Vollständige Anonymisierung [certainly anonymous]
  - Re-Identifikation ist praktisch ausgeschlossen auch gegenüber erwartbaren künftigen Attacken
  - Zusätzliche Garantien u.a. durch Abstreitbarkeit

Quellen: B. Bruegger Projekte Panelfit und Forum Privatheit, https://uld-sh.de/pseudoanon. Laufende Arbeit aus dem ULD-Projekt „AnoMed".

Personenbezug Ergebnisse von Pseudo- und Anonymisierung

- Voll identifizierte Daten
  - Direkt identifiziert
- Pseudonymisierte Daten
  - indirekte Identifizierung möglich mit „zusätzlichen Informationen" [additional data]
- Mutmaßliche Anonymität [supposedly
  - Alle bekannten Re-Identifikationsmöglich
  - Risikobewertung kann künftige Risiken n
- Vollständige Anonymisierung [certainly anonymous]
  - Re-Identifikation ist praktisch ausgeschlo
    erwartbaren künftigen Attacken
  - Zusätzliche Garantien u.a. durch Abstreitbarkeit

Personenbezogen

Geringeres Risiko, Art 32
Bedingung einiger RGL (Forschung)

- Geringes Restrisiko
-Maßnahmen zur Risikokontrolle und Schadensbegrenzung
- Empfehlung: Wenn möglich wie personenbezogene Daten behandeln, gesetzliche RGL zur Verarbeitung

DSGVO nicht anwendbar
Veröffentlichung möglich

Quellen: B. Bruegger Projekte Panelfit und Forum Privatheit, https://uld-sh.de/pseudoanon. Laufende Arbeit aus dem ULD-Projekt „AnoMed".

Personenbezug
EuG: Relativer und absoluter Begriff

- Urteil des Europäischen Gerichts erster Instanz April 2023
  - EU-Behörde übermittelt Stellungnahme von Bürgern und Gläubigern eine spanischen Bank an Consulting-Unternehmen.
  - Die Daten sind Pseudonymisiert. Namen etc wurden durch eine Kennziffer ersetzt.
  - Das Consulting-Unternehmen war nicht transparent als Empfänger benannt.
  - Auf Beschwerde von Betroffenen hat der europäische Datenschutzbeauftragte (EDPS) das Vorgehen gerügt.
  - Die EU-Behörde brachte den Fall vor den EuG. Dieser argumentierte, dass der EDPS hätte prüfen müssen, ob dem Consulting-Unternehmen ein Identifizieren möglich sei. Dafür käme es darauf an, was der Empfänger könne und welche Informationen diesem zur Verfügung stünden.

Personenbezug
EuG: Relativer und absoluter Begriff

- Auffassung des Referenten:
  - (Re-)Identifizierbarkeit sollte objektiv bewertet werden und nicht aus Sicht der Empfänger.
  - Jedenfalls ist zu berücksichtigen: Exponentielles Wachstum verfügbarer Daten + Datenverfügbarkeit (z.B. Data Spaces statt Daten Silos) + universelle Verkettung von Datenbeständen (AI)
  - Umkehrschluss aus Art 11 DSGVO. Der sieht vor, dass Verantwortliche, die ohne zusätzliche Informationen nicht identifizieren können, zwar von einzelnen Pflichten der Art 15-20 ausgenommen werden, die DSGVO bleibt aber anwendbar. Ohne Personenbezug hätte Art 11 keinen Anwendungsbereich.
  - Good practice Empfehlung: Transparenzanforderungen vorsorglich einhalten. Auftragsverarbeitung oder gemeinsame Verantwortung mit entsprechenden Vereinbarungen zum Schutz Betroffener.

Datenschutz für das Internet of Things (IoT)

Transparenz und das Internet of Things

- Problemstellung: Wie kann im Internet of Things die erforderliche Transparenz für alle hergestellt werden?

- Lösungsidee: Privacy Label
- Bewertungsmetrik für Datenschutzeigenschaften u.a. für Kaufentscheidungen
- Verständliche und bildliche Darstellung

- Folgeproblem: Beschaffung der Informationen?
  - Produktbeschreibungen
  - Hersteller / Importeure
  - Dokumentation der Einstellungsoptionen
  - Webtraffic-Analyse, Funktionen und Verhalten des Geräts
  - Firmware-Analyse

Befassung am ULD wird erfolgen im BMBF-geförderten Projekt Unboxing.IoT.Privacy
Bildquelle: A. Railean, Privacy&Us-Projekt

Figure 1: "Privacy facts" label for IoT devices.

Schutz von Forschungsdaten

(mit ausgewählten Fragen aus der Datenschutzforschung)

Verfassungsrechtliche Grundlagen Datenschutz und Forschung I

Datenschutz

- D: Informationelle Selbstbestimmung, Art 2 I iVm Art 1 I GG (Volkszählung, 1983)
- EU: Art 7 GrCh[1] Schutz des Privat- und Familienlebens
- EU: Art 8 GrCh Schutz personenbezogener Daten

Wissenschaftsfreiheit

- D: Art 5 III GG: „Kunst und Wissenschaft, Forschung und Lehre sind frei. Die Freiheit der Lehre entbindet nicht von der Treue zur Verfassung. ...“
- EU: Art 13 GrCh, „Kunst und Forschung sind frei. Die akademische Freiheit wird geachtet.“

[1] https://www.europarl.europa.eu/charter/pdf/text_de.pdf

Verfassungsrechtliche Grundlagen Datenschutz und Forschung II

- Wissenschaftsfreiheit umfasst auch Freiheit zur Forschung und Lehre als Ausprägungen des Grundrechts.
- Konflikt zwischen Wissenschaftsfreiheit und Datenschutz
- Rechtsgüter sind in Ausgleich zu bringen im Rahmen der praktischen Konkordanz, so dass beiden gerecht wird

  - EU-Gesetzgeber hat Forschung bei DSGVO teilweise beachtet
  - Nationale Gesetzgeber haben Erlaubnisnormen geschaffen
  - Aber: Es bleibt beim Grundsatz, dass spezielle Verbote aus spezielle Erlaubnisnormen brauchen (siehe Abschnitt zu Medizindatenschutz). Diese Normen müssen Ausgleich herstellen z.B. durch TOMs, Zweckbindung, …

Einwilligung im Forschungskontext

- Einwilligung ist auch im Forschungskontext erforderlich. Zu trennen:
  - Ethik (teilweise weitergehende Aspekte umfasst auch Datenschutz)
  - Datenschutz nach Datenschutzrecht
- Rechtsgrundlagen im Datenschutz
  - Einwilligung nach Art. 6 I a DSGVO (iVm Art 9 DSGVO)
  - Überwiegendes Interesse an der Forschung
    - Universitäten, öffent.-rechtl. Institute: Art. 6 I e DSGVO in Verbindung mit Normen des Landesdatenschutzrechts, Hochschulrechts
    - Private Stellen: Teilweise Landesrecht, ggf. Art. 6 I f DSGVO
- Immer erforderlich für Ethik und Datenschutz: Umfassende Aufklärung und Unterrichtung (Problem etwa „Legende" bei psychol. Studien)
- Anforderungen kommen u.a. von: Hochschulinternen Regelungen aber auch durch Fördergeber (BMBF, Horizon-Programme der EU)

=> Rat für Forschende: Datenschutzstelle und Ethik-Kommission fragen

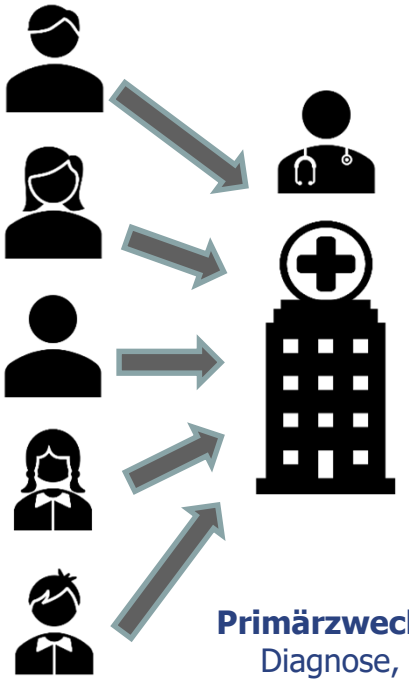
Sekundärnutzung von Daten

- Sollen vorhandene Daten für Forschungszwecke herangezogen werden spricht man von Sekundärnutzung.

- Probleme:
  - Bei Behandlung ist künftige Forschung ggf. weder bekannt noch absehbar
  - Fehlende Transparenz für Betroffene über Schicksal der Daten
  - Nachträglich Einholung von Einwilligungen ist komplex und Rücklaufquote von Anfragen gering
  - „Broad Consent" eine Universaleinwilligung für künftige Forschung bedarf weiterer Rahmenbedingungen (DSK-Beschluss zu „broad consent", 2019)
  - Weitergehende Konkretisierung durch gesetzliche RGL nötig

Sekundärnutzung von Daten

primäre Datenverarbeitung



Primärzwecke
Diagnose,
Behandlung,
Nachsorge,
Dokumentation

Grundsatz der Rechtmäßigkeit: Für jede Verarbeitung ist eine RGL erforderlich.

Für Diagnose und Behanlung etwa Behandlungsvertrag und Art. 9 (2) (h) iVm Art. 6 DSGVO.

IdR sind gesetzliche RGL für Behandlung, Abrechnung, Archivierung vorhanden.

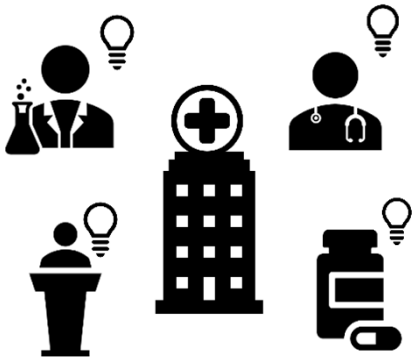
Sekundärnutzung von Daten

sekundäre Datenverarbeitung

Grundsatz der Rechtmäßigkeit: Für Erhebung, Analyse und weitere Schritte ist eine RGL erforderlich, soweit Daten personenbezogen sind.

Bei Gesundheitsdaten besteht oft Risiko einer Re-Identifikation, so dass Anonymisierung oft nicht zuverlässig gelingt oder Daten danach für Forschungszweck unbrauchbar sind

⇒ Entweder ist Einwilligung oder eine spezifische gesetzliche RGL erforderlich



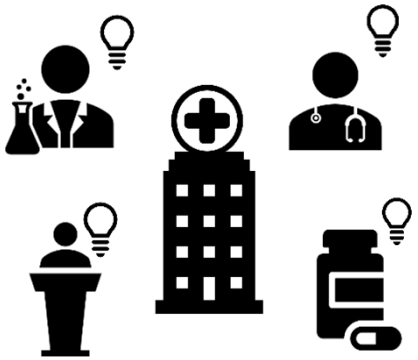
Sekundärzwecke
Wissenschaft, Forschung, Lehre, Entwicklung von Arznei- und Medizinprodukten

Sekundärnutzung von Daten

sekundäre Datenverarbeitung

Anforderungen an gesetzliche Regelung[1]

- Betroffener darf nicht Objekt der Datenverarbeitung werden
- Voraussetzungslose Widerspruchsmöglichkeit
- Betroffene einbinden, informieren und Mitwirkung ermöglichen (Daten-Dashboard)
- Einwilligung idR Vorrang – Gesetz also u.a. wenn Einwilligung nicht einholbar ist
- Normenklarer wirksamer Schutz
- Geeignete Garantien für Freiheiten und Rechte
- Grundlegende Maßnahmen zur Risikominimierung gesetzlich geregelt
- Verpflichtende Datenschutzfolgenabschätzung
- Forschungsgeheimnis inkl. Beschlagnahmeschutz



Sekundärzwecke
Wissenschaft, Forschung, Lehre, Entwicklung von Arznei- und Medizinprodukten

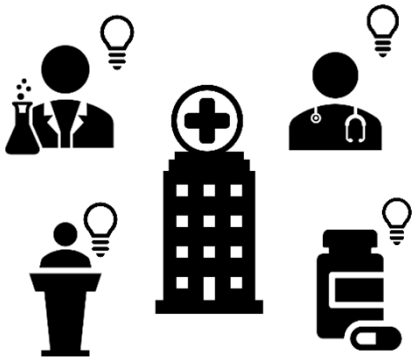
[1] DSK, Petersberger Erklärung vom November 2022

Sekundärnutzung von Daten

sekundäre Datenverarbeitung

Denkbare Anforderungen an eine gesetzlich privilegierte Datennutzung [1]

- Ergebnisbezogne Aspekte
  - Veröffentlichung der Ergebnisse
  - Ggf. Art und Umfang einer Lizensierung
  - Verfügbarkeit der Daten für Validierung?
- Forschungs- und Einrichtungsbezogene Aspekte
  - Gemeinwohlinteresse
  - Öffentliche Einrichtung oder öff. Förderung
  - Potentieller Nutzen der Ergebnisse
- Datenschutzbezogene Aspekte
  - Datenschutz durch Technikgestaltung
  - Frühe Anonymisierung oder Pseudonymis.
  - DSFA erfolgt und veröffentlicht

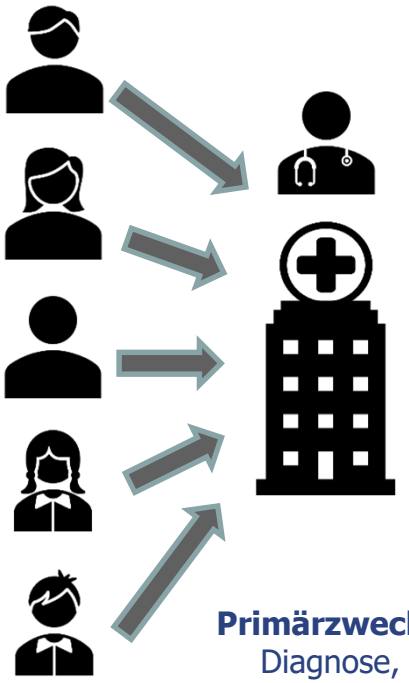


Sekundärzwecke
Wissenschaft, Forschung, Lehre, Entwicklung von Arznei- und Medizinprodukten

[1] Teilweise so auch die DSK in der Petersberger Erklärung vom November 2022, teilweise Erwägungen des Referenten

Sekundärnutzung von Daten

primäre Datenverarbeitung



Primärzwecke
Diagnose,
Behandlung,
Nachsorge,
Dokumentation

sekundäre Datenverarbeitung

Informierte Einwilligung

„Ausdrückliche" (Art 9) und informierte Einwilligung.

Ideen zur technischen Verbesserung:

- Dynamic consent mit Möglichkeit zur Rückfrage
- Dashboard-Lösungen für Kontrolle
- Einfache Widerrufsmöglichkeit

TRAPEZE

AnoMed

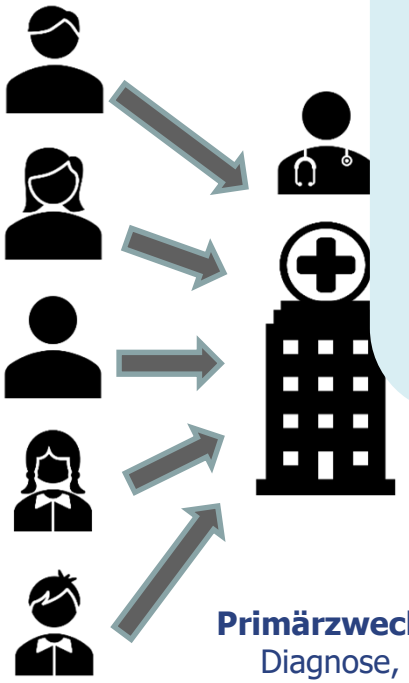
Sekundärnutzung von Daten

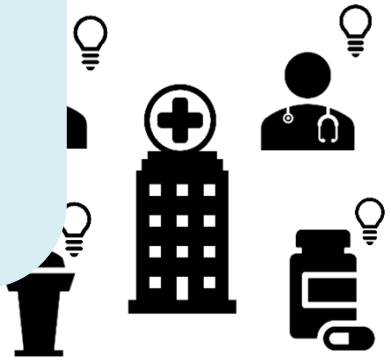
primäre Datenverarbeitung

sekundäre Datenverarbeitung

Ideen aus dem Entwurf für EHDS:

- Plan: nationale Zugangsstellen
- Meldung vorhandener Datenbestände (nicht der Daten selbst)
- Antrag Einholen Bewilligung durch Zugangsstelle, Einholen und Weitergabe der Daten



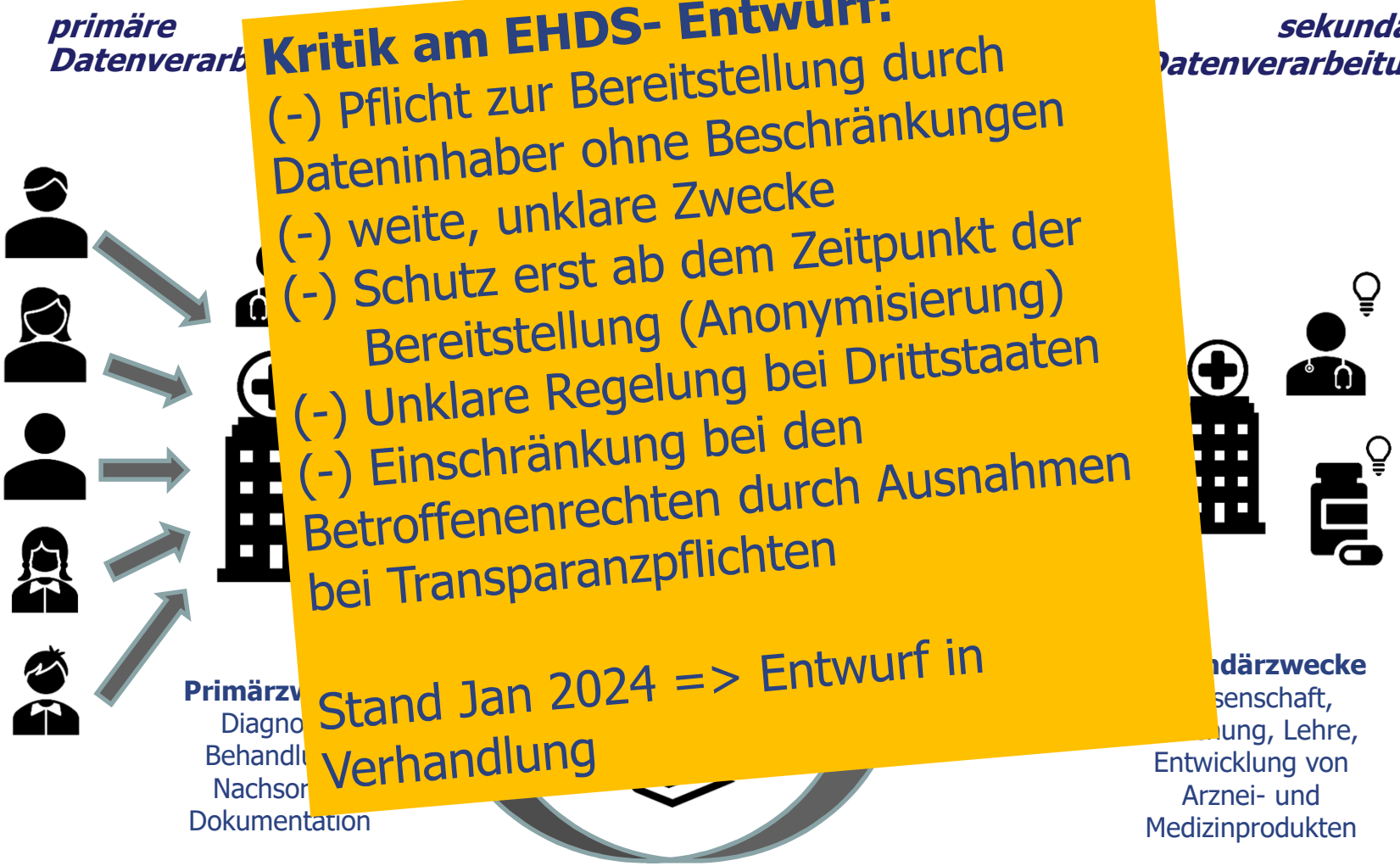


Gesetzliche Rechtsgrundlagen

Primärzwecke
Diagnose, Behandlung, Nachsorge, Dokumentation

Sekundärzwecke
Wissenschaft, Forschung, Lehre, Entwicklung von Arznei- und Medizinprodukten

Sekundärnutzung von Daten



Kritik am EHDS- Entwurf:

(-) Pflicht zur Bereitstellung durch Dateninhaber ohne Beschränkungen

(-) weite, unklare Zwecke

(-) Schutz erst ab dem Zeitpunkt der Bereitstellung (Anonymisierung)

(-) Unklare Regelung bei Drittstaaten

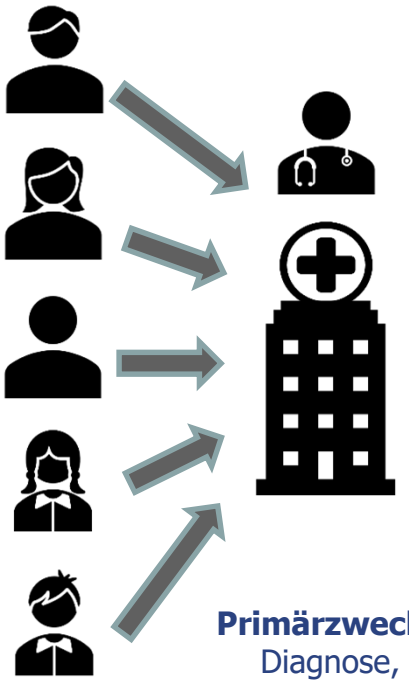
(-) Einschränkung bei den Betroffenenrechten durch Ausnahmen bei Transparanzpflichten

Stand Jan 2024 => Entwurf in Verhandlung

Quelle u.a.: EDPB-EDPS Joint Opinion 03/3022 on Proposal for a Regulation on the EHDS, 2022, p. 22 et seq.

Sekundärnutzung von Daten

primäre Datenverarbeitung

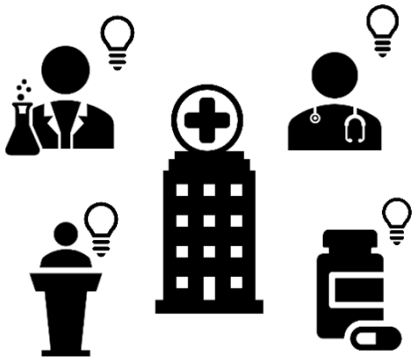


Primärzwecke
Diagnose,
Behandlung,
Nachsorge,
Dokumentation

Informierte Einwilligung

Gesetzliche Rechtsgrundlagen

sekundäre Datenverarbeitung



Sekundärzwecke
Wissenschaft,
Forschung, Lehre,
Entwicklung von
Arznei- und
Medizinprodukten

Datenerhebung und Verwendung Rechtsgrundlagen Sekundärnutzung

- Rechtsgrundlagen sind verstreut:
- DSGVO
  - Einwillgiung Art 6 i.V.m. Art 9 (2) (a) DSGVO
  - Die DSGVO ist „forschungsfreundlich" hat aber keine eigne ausdrücklichke Forschungserlaubnis
  - Art. 9 (2) (f) DSGVO: DV zu Forschungszwecken möglich auf Grundlage von Gemeinschaftsrecht (EHDS in Planung) oder nationalen Rechts sofern angemessen und Maßnahmen zum Schutz der Rechte und Interessen vorgesehen sind
  - Bund: § 27 DSGVO, SGB X
  - Landesrechte: u.a. in LDSG, § 15 BOÄ, KlinikG, HochschulG

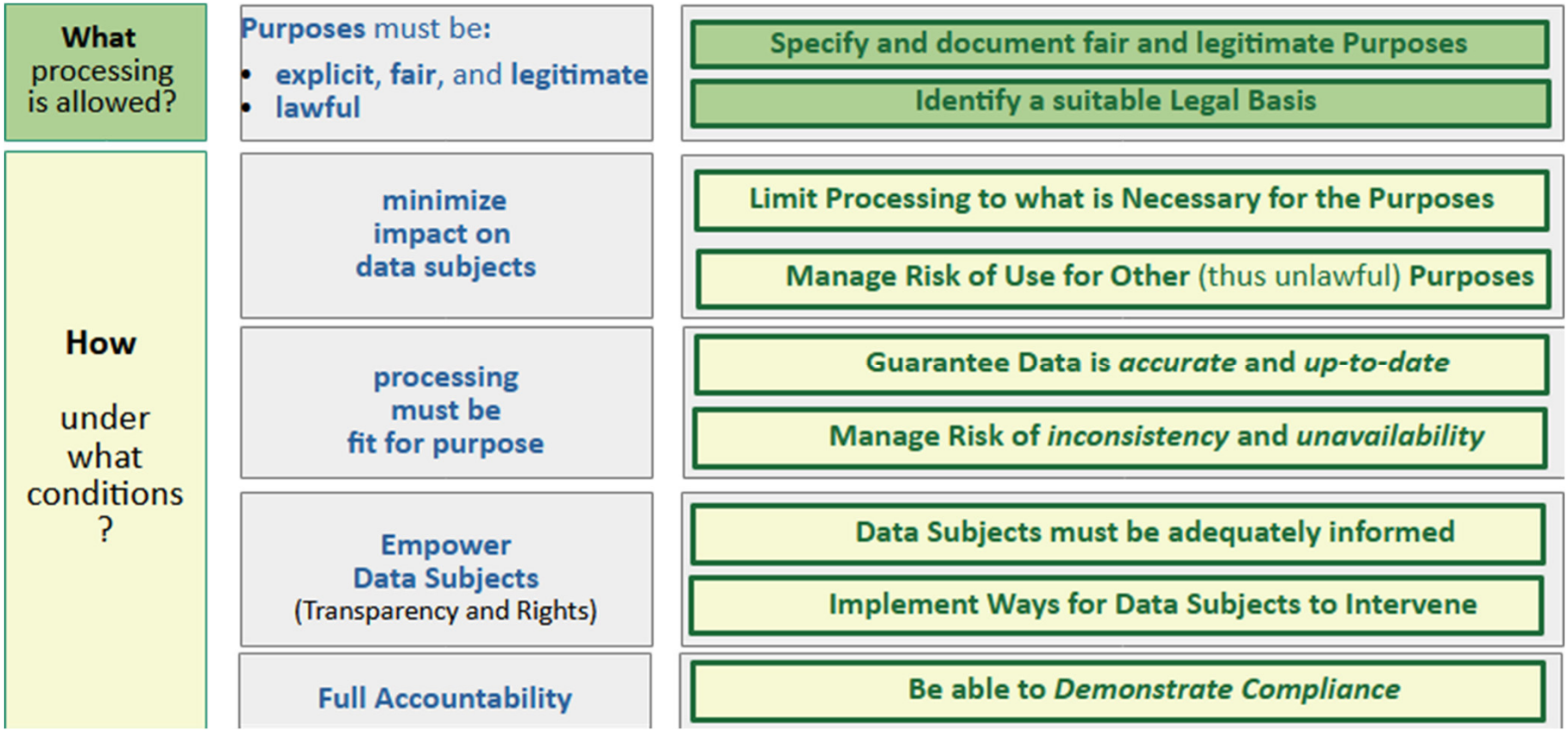
Sekundärnuzung nach Landesdatenschutzgesetzen (Quelle, Weichert, Rahmenbedingunge, 2022 S. 38):
§ 13 LDSG BW, Art. 25 BayDSG, §§ 17, 35 BlnDSG, § 25 BbgDSG, § 13 BremDSGVOAG,
§§ 24, 45 HDSIG, § 9 DSG MV, § 13 NDSG, § 17 DSG NRW, §§ 22, 31 LDSG RP, § 23 SDSG, § 12 SächsDSG, § 27 DSG LSA, §§ 13, 26 LDSG SH, § 28 ThürDSG.

Siehe auch übersicht bei Dierks, „Lösungsvorschläge", 2019, S. 37 f

Weiterführende Quellen Forschungsdatenschutz

- T. Weichert, „Datenschutzrechtliche Rahmenbedingungen medizinischer Forschung“, TMF-Schriftenreihe, 2022
  Open Access: https://www.mwv-open.de/site/books/m/10.32745/9783954667000/
- PANELFIT: B. Bruegger, GDPR-Principles,
  https://guidelines.panelfit.eu/the-gdpr/main-principles/
- Datenschutzkonferenz (DSK), Petersberger Erklärung zu datenschutzkonformen Verarbeitung von Gesundheitsdaten in der wissenschaftlichen Forschung, November 2022
- EDPB-EDPS Joint Opinion 03/3022 on Proposal for a Regulation on the EHDS, 2022,
  https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-032022-proposal_en

Wiederholung: Datenschutzprinzipien aus Perspektive von Verantwortlichen



Quelle: Projekt AnoMed, www.anomed.de

Förderhinweise

Unboxing.IoT.Privacy

https://www.anomed.de/

Beide Projekte werden gefördert durch das Bundesministerium für Bildung und Forschung (BMBF). Der Forschungscluster AnoMed ist zudem finanziert von der Europäischen Union – NextGenerationEU.

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

Finanziert von der Europäischen Union
NextGenerationEU

https://panelfit.eu/

trapeze-project.eu

Gefördert durch die Europäische Kommission im H2020 Rahmenprogrammn

Links: https://www.datenschutzzentrum.de/projekte/

Herzlichen Dank für die gemeinsame Diskussion zum Thema

Harald Zwingelberg
vorlesung@zwingelberg.de
0431 / 988-1222 (dienstl.)

AnoMed

PANELFIT

EMPRI-DEVOPS

TRAPEZE