Datenschutzrecht

Medizindatenschutz,
Schutz von Forschungsdaten

1. Juli 2024

Harald Zwingelberg

Ansprechpartner Vorlesungsreihe: Benjamin Bremert

Vertretene Auffassungen sind solche des Referenten bzw. teilweise Ergebnisse aus dem Projektbereicht und nicht zwingend eine aufsichtsbehördliche Positionierung.

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:
  - Grundprinzipien
  - personenbezogene Daten
  - besondere Kategorien personenbezogener Daten
  - Auftragsverarbeitung
- Gesundheitsdatenschutz
- Datenschutz und Forschung
- Aktuelles aus der Datenschutz-Forschung

Wiederholung

Grundlagen

Wiederholung

- Wo sind die Grundprinzipien des Datenschutzes geregelt?
  - Art. 5 DSGVO

- Nennen sie die Grundprinzipien und deren Kerninhalt
  1. Rechtmäßigkeit, Art. 5 I a
  2. Zweckbindung, Art. 5. I b
  3. Erforderlichkeit, Art. 5 I b, c (u.a. Datenminimierung)
  4. Transparenz, Art. 5 I a (Auskunft, …)
  5. Integrität und Vertraulichkeit (Datensicherheit), Art. 5 I f
  6. Rechenschaftspflicht, Art. 5 II

*Wiederholung *)*
Sechs Goldene Regeln des Datenschutzes

Welche Grundsätze des Datenschutzes kennen Sie?

- Rechtmäßigkeit
  - Gesetz, Einwilligung, Vertrag, Dienst- oder Betriebsvereinbarung
- Zweckbindung
  - Weiterverarbeitung nur für einem mit Erhebungszweck vereinbaren Zweck
- Datenminimierung und Speicherbegrenzung
  - Verarbeitung nur soweit für Erhebungszweck erforderlich
- Transparenz und Betroffenenrechte
  - Unterrichtung über Verwendung, Auskunfts-/Berichtigungs-/Löschrechte
- Integrität und Vertrautlichkeit
  - Technische und organisatorische Maßnahmen, Integrität und Vertraulichkeit
- Kontrolle
  - Interner / externer Datenschutzbeauftragter

*) Zum ganzen siehe Einführung von B. Bremert „Einführung II"
Ausführlich zu Data Protection Principles, B. Bruegger, http://guidelines.panelfit.eu/the-gdpr/main-principles/
und als Vortragsfolien (CC-by-Lizenz) https://www.datenschutzzentrum.de/uploads/projekte/anomed/GDPR-Principles.pdf

AnoMed
PANELFIT

Wiederholung
Art. 6 DSGVO: Zentrale Befugnisnorm

- Datenverarbeitung ist (nur!) rechtmäßig, wenn:
  - **Einwilligung**
  - **Vertragserfüllung**
  - **Erfüllung rechtlicher Verpflichtung**
  - Lebenswichtige Interessen
  - Ausübung öffentliche Gewalt
  - **Wahrung berechtigter Interessen, sofern Interessen des Betroffenen nicht überwiegen *)**

*) Ausführlich zur Verarbeitung für berechtigte Interessen nach Art. 6 I f DSGVO:
Robrahn/Bremert, Interessenskonflikte im Datenschutzrecht, ZD 2018, 291ff.
Autorenversion frei verfügbar :
https://www.datenschutzzentrum.de/uploads/projekte/itesa/Robrahn-Bremert-Artikel6abs1fDSGVO.pdf

SeDaFa
Selbstdatenschutz im vernetzten Fahrzeug

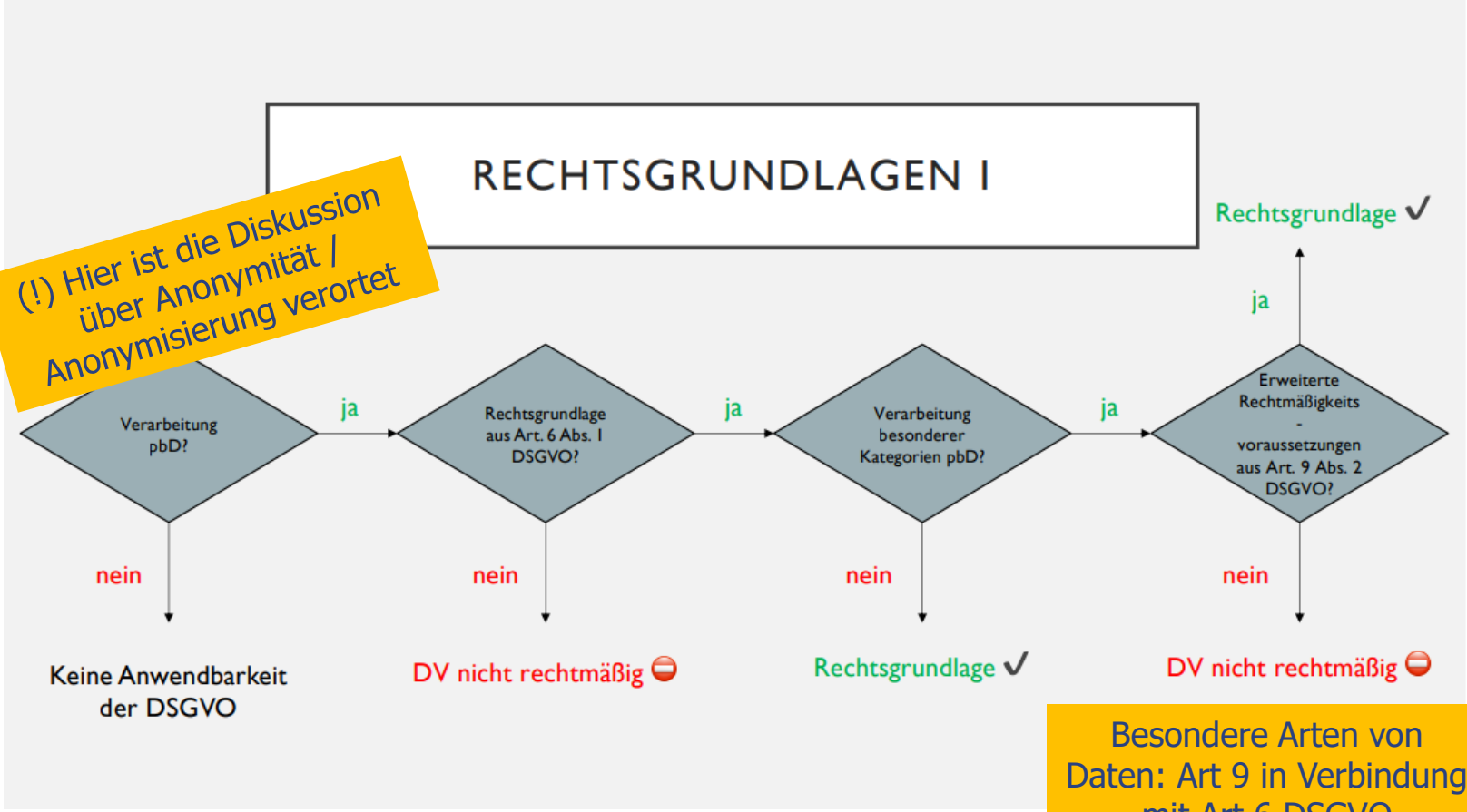
iTESA

Wiederholung
Besondere Kategorien personenbez. Daten

- Art. 9 (1) DSGVO:
  Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer nat. Person ist untersagt.

- Art 9 (2) DSGVO: Ausnahmen vom Verbot u.a. für Behanldung und Forschung

Rechtsgrundlagen Wiedergholung



Quelle der Folie: Benjamin Bremert, zur wiederholung siehe Veranstaltung „Einfühung II" vom

Wiederholung Auftragsverarbeitung

- Sind mehrere an der Datenverarbeitung beteiligt ist deren Verhältnis zueinander zu klären.

- Gemeinsame Verantwortlichkeit lässt die Notwendigkeit einer RGL nicht entfallen! Das Recht, die Daten zu verarbeiten / übermitteln, / auszutauschen, muss schon vorher vorhanden sein.

- Anders bei rechtmäßiger Auftragsverarbeitung. Diese ist für die Datenflüsse vom Verantwortlichen zum Auftragnehmer zugleich Rechtsgrundlage. Anforderungen, Rechte und Pflichten sowie Haftung sind in Art 28 DSGVO geregelt.

Gesundheitsdatenschutz

&

Recht der Berufsgeheimnisträger

Medizin- und Sozialdatenschutz

1. Geheimnisschutz
2. Gesetzesgrundlagen, Datenerhebung
3. Einwilligung – Schweigepflichtsentbindungserklärung
4. Zweckbindung und Erforderlichkeit
5. Datenübermittlung
6. Betroffenenrechte, insbesondere Akteneinsichtsrechte
7. Datensicherheit
8. Kontrolle

Fragen

- Patientendaten beim Arzt unterliegen einem besonderen Schutz. Welche Gründe könnte es dafür geben? Wer hat ein Interesse an diesem Schutz?

- Welche weiteren Berufsgeheimnisträger kennen sie?

- Welche Sozialversicherungsträger (‚Sozialversicherungen') kennen Sie?

- Welche Gründe kann es geben Daten bei Sozialversicherungsträgern besonders zu schützen?

Gründe für Schweigepflicht und Sozialgeheimnis

Ärztliche Schweigepflicht

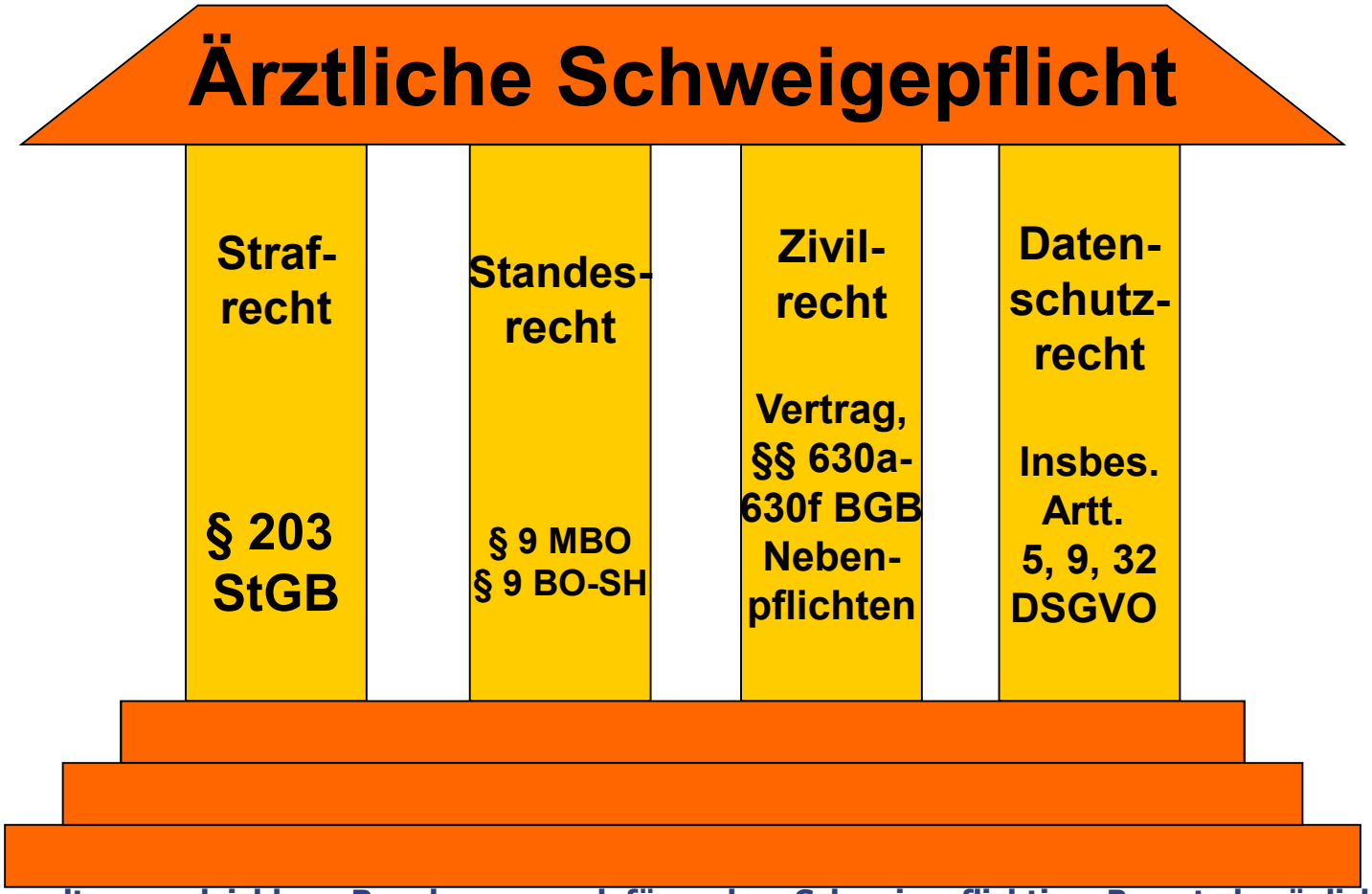
- Persönlichkeitsrecht des Patienten
- staatliches Interesse an gesunden Bürgern und Vertrauen in die Vertraulichkeit der Arzt-Patientenbeziehung
- Eigeninteresse der Ärzte – Vertrauen der Patienten (therapeutisch und wirtschaftlich – siehe Erläuterungen zum Hippokratischen Eid)
- besonders schutzbedürftige Daten

Sozialgeheimnis

- Persönlichkeitsrecht des Betroffenen
- staatliches Interesse an der Vermeidung sozialer Notlagen
- Angehörige einer Sozialversicherung (ob zwangsweise oder freiwillig) sollen nicht mehr staatlichen Eingriffen ausgesetzt sein als andere
- besonders schutzbedürftige Daten (insbes. Gesundheit, Vermögen, soziale Verhältnisse)

Beachte: Auch Datenschutzrechtlich unterliegen Gesundheitsdaten als besondere Arten von Daten nach § 9 DSGVO besonderen datenschutzrechtlichen Anforderungen. Im Sozialrecht finden sich diese im SGB X.

*Grundlagen der ärztlichen Schweigepflicht**



*** im Kern gelten vergleichbare Regelungen auch für andere Schweigepflichtige: Beamte bezüglich Amtsgeheimnissen, Rechtsanwälte, Steuerberater, Ehe-, Familien- oder Suchtberater, Sozialarbeiter, Mitarbeiter bei Krankenkassen… Unterschiede bestehen bezüglich der anwendbaren Rechtsgrundlagen.**

Umfang und Adressatenkreis der ärztlichen Schweigepflicht

§ 203 StGB: Verletzung von Privatgeheimnissen

- Adressatenkreis: u.a. Ärzte, Zahnärzte, Tierärzte, Heilberufe mit staatl. Prüfung, Psychologen, Rechtsanwälte, Notare, Steuerberater, Ehe-, Familien- & Jugendberater, MA von Beratungsstellen, Sozialarbeiter, Mitarbeiter privater Krankenkassen bzw. Unfall- oder Lebensversicherungen, Amtsträger, Personalvertretung, Forschende…
- Umfang: Bereits die Tatsache, dass jemand Patient ist
- „unbefugte" Offenbarung eines fremden Geheimnisses
  - Keine Mitteilung an Familienmitglieder der Patienten
  - Schweigepflicht gilt idR über den Tod des Patienten hinaus
  - Rechtfertigung der Geheimnisoffenbarung durch
    - Einwilligung
    - Mutmaßliche Einwilligung (z.B. bei Bewusstlosen)
    - Gesetzliche Offenbarungspflichten (z.B. § 138 StGB)
    - Rechtfertigender Notstand (z.B. § 34 StGB)

§ 203 StGB Verletzung von Privatgeheimnissen **! spare slide !**

(1) Wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als
1. Arzt, Zahnarzt, Tierarzt, Apotheker oder Angehörigen eines anderen Heilberufs, der für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung erfordert,
2. Berufspsychologen mit staatlich anerkannter wissenschaftlicher Abschlußprüfung,
3. Rechtsanwalt, Kammerrechtsbeistand, Patentanwalt, Notar, Verteidiger in einem gesetzlich geordneten Verfahren, Wirtschaftsprüfer, vereidigtem Buchprüfer, Steuerberater, Steuerbevollmächtigten,
3a. Organ oder Mitglied eines Organs einer Wirtschaftsprüfungs-, Buchprüfungs- oder einer Berufsausübungsgesellschaft von Steuerberatern und Steuerbevollmächtigten, einer Berufsausübungsgesellschaft von Rechtsanwälten oder europäischen niedergelassenen Rechtsanwälten oder einer Berufsausübungsgesellschaft von Patentanwälten oder niedergelassenen europäischen Patentanwälten im Zusammenhang mit der Beratung und Vertretung der Wirtschaftsprüfungs-, Buchprüfungs- oder Berufsausübungsgesellschaft im Bereich der Wirtschaftsprüfung, Buchprüfung oder Hilfeleistung in Steuersachen oder ihrer rechtsanwaltlichen oder patentanwaltlichen Tätigkeit,
4. Ehe-, Familien-, Erziehungs- oder Jugendberater sowie Berater für Suchtfragen in einer Beratungsstelle, die von einer Behörde oder Körperschaft, Anstalt oder Stiftung des öffentlichen Rechts anerkannt ist,
5. Mitglied oder Beauftragten einer anerkannten Beratungsstelle nach den §§ 3 und 8 des Schwangerschaftskonfliktgesetzes,
6. staatlich anerkanntem Sozialarbeiter oder staatlich anerkanntem Sozialpädagogen oder
7. Angehörigen eines Unternehmens der privaten Kranken-, Unfall- oder Lebensversicherung oder einer privatärztlichen, steuerberaterlichen oder anwaltlichen Verrechnungsstelle
anvertraut worden oder sonst bekanntgeworden ist, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als
1. Amtsträger oder Europäischer Amtsträger,
2. für den öffentlichen Dienst besonders Verpflichteten,
3. Person, die Aufgaben oder Befugnisse nach dem Personalvertretungsrecht wahrnimmt,
4. Mitglied eines für ein Gesetzgebungsorgan des Bundes oder eines Landes tätigen Untersuchungsausschusses, sonstigen Ausschusses oder Rates, das nicht selbst Mitglied des Gesetzgebungsorgans ist, oder als Hilfskraft eines solchen Ausschusses oder Rates,
5. öffentlich bestelltem Sachverständigen, der auf die gewissenhafte Erfüllung seiner Obliegenheiten auf Grund eines Gesetzes förmlich verpflichtet worden ist, oder
6. Person, die auf die gewissenhafte Erfüllung ihrer Geheimhaltungspflicht bei der Durchführung wissenschaftlicher Forschungsvorhaben auf Grund eines Gesetzes förmlich verpflichtet worden ist,
anvertraut worden oder sonst bekanntgeworden ist. Einem Geheimnis im Sinne des Satzes 1 stehen Einzelangaben über persönliche oder sachliche Verhältnisse eines anderen gleich, die für Aufgaben der öffentlichen Verwaltung erfaßt worden sind; Satz 1 ist jedoch nicht anzuwenden, soweit solche Einzelangaben anderen Behörden oder sonstigen Stellen für Aufgaben der öffentlichen Verwaltung bekanntgegeben werden und das Gesetz dies nicht untersagt.
(2a) (weggefallen)
(3) Kein Offenbaren im Sinne dieser Vorschrift liegt vor, wenn die in den Absätzen 1 und 2 genannten Personen Geheimnisse den bei ihnen berufsmäßig tätigen Gehilfen oder den bei ihnen zur Vorbereitung auf den Beruf tätigen Personen zugänglich machen. Die in den Absätzen 1 und 2 Genannten dürfen fremde Geheimnisse gegenüber sonstigen Personen offenbaren, die an ihrer beruflichen oder dienstlichen Tätigkeit mitwirken, soweit dies für die Inanspruchnahme der Tätigkeit der sonstigen mitwirkenden Personen erforderlich ist; das Gleiche gilt für sonstige mitwirkende Personen, wenn diese sich weiterer Personen bedienen, die an der beruflichen oder dienstlichen Tätigkeit der in den Absätzen 1 und 2 Genannten mitwirken.

Rechtliche Bedeutung der Schweigepflicht

- Verfassungsrechtliche Ausgangslage: Dem Bürger ist alles erlaubt, was nicht verboten ist (Art. 2 Abs. 1 GG: Recht auf freie Entfaltung der Persönlichkeit, insb. allgemeine Handlungsfreiheit).
- Im Datenschutz gilt aber auch für Private: Alles ist verboten, was nicht erlaubt ist (Art. 6 (1) und Art. 5 (1) (a) DSGVO). – Jeder Umgang mit personenbezogenen Daten bedarf einer rechtlichen Grundlage. [Stichwort: Rechtmäßigkeit]

- In Bereichen, die einem besonderen Geheimnisschutz unterstellt sind (neben der ärztlichen Schweigepflicht und dem Sozialgeheimnis etwa auch das Steuergeheimnis) werden an die rechtlichen Grundlagen besondere Anforderungen gestellt: Daten dürfen nur dann erhoben, verarbeitet und übermittelt werden, wenn ***bereichsspezifische*** Regelungen dies erlauben.
  Also bei speziellem Verbot braucht es eine spezielle Ausnahme.

Grenzen der Schweigepflicht: Beispiele

- Bankräuber kündigt Tat beim Arzt an: Pflicht zur Anzeige nur bei bestimmten geplanten (künftigen!) Straftaten (vgl. § 138 StGB). Im Übrigen gilt Schweigepflicht
- Patient fährt regelmäßig unter Alkoholeinfluss Auto: Mitteilung an Register oder Führerscheinbehörde möglich / geboten / Pflicht?: § 34 StGB
- Einschaltung externer Inkassounternehmen bei der Behandlungsabrechnung als Auftragsverarbeiter denkbar (siehe unten)
- HIV-Patient beim Arzt: Mitteilung der HIV-Infektion an den/die Sexualpartner(in)? § 34 StGB bei Anhaltspunkten für eine *konkrete* Ansteckungsgefahr vertretbar. Ggf. jetzt anders denkbar bei Virostatika (OLG Frankfurt sah Pflicht(!) zur Warnung bei erklärter Absicht des Patienten zu ungeschütztem Geschlechtsverkehr mit einer bestimmten Person, die ebenfalls Patient desselben Arztes war. Sehr umstr. Urteil)
- Arzthaftungsprozess: Mitteilung von Patientendaten zur rechtlichen Verteidigung? Nach § 34 StGB zulässig, aber nur im erforderlichen Umfang
- Polizei fahndet nach einem Bankräuber und befragt den Arztpraxen, ob dieser dort in Behandlung war: Schweigepflicht

§ 138 StGB Nichtanzeige geplanter Straftaten **! spare slide !**

(1) Wer von dem Vorhaben oder der Ausführung
1. (weggefallen)

2. eines Hochverrats in den Fällen der §§ 81 bis 83 Abs. 1,

3. eines Landesverrats oder einer Gefährdung der äußeren Sicherheit in den Fällen der §§ 94 bis 96, 97a oder 100,

4. einer Geld- oder Wertpapierfälschung in den Fällen der §§ 146, 151, 152 oder einer Fälschung von Zahlungskarten mit Garantiefunktion in den Fällen des § 152b Abs. 1 bis 3,

5. eines Mordes (§ 211) oder Totschlags (§ 212) oder eines Völkermordes (§ 6 des Völkerstrafgesetzbuches) oder eines Verbrechens gegen die Menschlichkeit (§ 7 des Völkerstrafgesetzbuches) oder eines Kriegsverbrechens (§§ 8, 9, 10, 11 oder 12 des Völkerstrafgesetzbuches) oder eines Verbrechens der Aggression (§ 13 des Völkerstrafgesetzbuches),

6. einer Straftat gegen die persönliche Freiheit in den Fällen des § 232 Absatz 3 Satz 2, des § 232a Absatz 3, 4 oder 5, des § 232b Absatz 3 oder 4, des § 233a Absatz 3 oder 4, jeweils soweit es sich um Verbrechen handelt, der §§ 234, 234a, 239a oder 239b,

7. eines Raubes oder einer räuberischen Erpressung (§§ 249 bis 251 oder 255) oder

8. einer gemeingefährlichen Straftat in den Fällen der §§ 306 bis 306c oder 307 Abs. 1 bis 3, des § 308 Abs. 1 bis 4, des § 309 Abs. 1 bis 5, der §§ 310, 313, 314 oder 315 Abs. 3, des § 315b Abs. 3 oder der §§ 316a oder 316c
zu einer Zeit, zu der die Ausführung oder der Erfolg noch abgewendet werden kann, glaubhaft erfährt und es unterläßt, der Behörde oder dem Bedrohten rechtzeitig Anzeige zu machen, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer
1. von der Ausführung einer Straftat nach § 89a oder
2. von dem Vorhaben oder der Ausführung einer Straftat nach § 129a, auch in Verbindung mit § 129b Abs. 1 Satz 1 und 2,
zu einer Zeit, zu der die Ausführung noch abgewendet werden kann, glaubhaft erfährt und es unterlässt, der Behörde unverzüglich Anzeige zu erstatten. § 129b Abs. 1 Satz 3 bis 5 gilt im Fall der Nummer 2 entsprechend.

(3) Wer die Anzeige leichtfertig unterläßt, obwohl er von dem Vorhaben oder der Ausführung der rechtswidrigen Tat glaubhaft erfahren hat, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

ärztliche Schweigepflicht Sonderregelungen

Es gibt Spezialgesetzliche Sonderregelungen etwa

- Infektionsschutzgesetz (Nicht-/ und namentliche Meldungen)
- Für Meldungen zum Krebsregister
- Meldung einer Kindeswohlgefährdung[1] durch Mediziner, Psychologen, Familienberatung, Sozialarbeiter, Lehrkräfte in abgestuftem Vorgehen § 4 KKG[2]:
  - Erörterung der Situation mit Kind oder Sorgeberechtigten und auf Inanspruchnahme von Hilfe hinwirken
  - Rücksprachemöglichkeit und Beratung durch die Jugendhilfe für die Normadressaten (Ärzte,…) zur Beurteilung der Kindeswohlgefährdung mit Einbeziehung von Kind / Eltern
  - Gestattung, das Jugendamt einzuschalten (keine Pflicht)

  ⇒ „Datenschutz verhindert keinen Kinderschutz!"

[1] KKG: Gesetz zur Kooperation und Information im Kinderschutz

[2] Dazu TB 2019 des ULD: https://www.datenschutzzentrum.de/tb/tb37/kap04_5.html#451

Sozialgeheimnis

- § 35 Abs. 1 Satz 1 SGB I – Sozialgeheimnis:
- Berechtigter: „Jeder" (über den Sozialdaten erhoben werden) Leistungsempfänger, Vermieter, Arbeitgeber,...
- Adressat: alle Leistungsträger (nicht Leistungserbringer wie z.B. Ärzte)

  => Institutionenbezogenes Spezialrecht für Leistungsträger
- Klarstellung: Auch innerhalb eines Leistungsträgers dürfen Daten nur Befugten zugänglich sein, § 35 I SGB I

- Gegenstand: Sozialdaten nach § 67 Abs. 1 SGB X

  „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person (Betroffener)"
- Normbefehl:
  - Verbot „unbefugter" Datenverarbeitung
  - § 35 II SGB I: nur nach den Voraussetzungen der §§ 67 ff. SGB X

Erhebung von Sozialdaten, § 67a SGB X

- Grundsatz: Sozialdaten dürfen erhoben werden, wenn sie zur Aufgabenerfüllung erforderlich sind
  - Keine Datenerhebung auf Vorrat
  - Nur entscheidungserhebliche Tatsachen
  - Daten müssen auch tatsächlich Verwendung finden
  - Kontoauszüge: Vorlagepflicht für Auszüge der vergangenen 3 Monate, Schwärzung bei bes. Arten personenbezogenen Daten statthaft. § 67a I 2, i.V.m. § 67 XII SGB X

Zu Kontoauszügen siehe: BSG, Urteil vom 19. 9. 2008 - B 14 AS 45/ 07 R ; und unter: https://www.datenschutzzentrum.de/artikel/1109-.html (Stand 2017)

Erhebung von Sozialdaten, § 67a SGB X

- Es gilt der Grundsatz der Datenerhebung beim Betroffenen

- Transparenz: Betroffener muss bei Erhebung über den Zweck der Erhebung und Verarbeitung, die verantwortliche Stelle und die relevanten Rechtsvorschriften informiert werden.

- Hinweis auf Rechtsfolgen: Soweit eine Auskunftspflicht besteht oder bei Nichtauskunft Nachteile drohen, ist darauf hinzuweisen.
  (Auskunftspflicht z.B. in § 60 SGB I, Folgen § 66 SGB I)

Exkurs: Einwilligung in eine medizinische Untersuchung

Medizinrechtliche Einwilligung

- Einwilligung in den Eingriff, andernfalls ist Behandlung eine Körperverletzung
- Informed consent = Aufklärung und freie Einwilligung
- Aufklärung über
  - 1. Diagnose und Diagnosesicherheit
  - 2. Verlaufsprognose
  - 3. Wesen der Maßnahme, Mitwirkungspflichten
  - 4. Erfolgsquote, Nutzen
  - 5. Komplikationen und Komplikationswahrscheinlichkeit
  - 6. Handlungsalternativen
  - 7. Wirtschaftliche Aufklärung
- Schwerpunkt: Einwilligung in körperlichen Eingriff
- Aber auch: Einwilligung in Informationsgewinnung und übermittlung (Recht auf informationelle Selbstbestimmung und Recht auf Nichtwissen)

-

Datenschutzrechtliche Einwilligung:

- Informierte Einwilligung, Art. 13 DSGVO
- Anforderungen nach Art. 7 DSGVO, insb.:
  - freie Entscheidung, Art. 7 (4)
  - Aufklärung über den Zweck der Datenerhebung oder -verarbeitung Art. 13 (1) (c)
  - Keine Formpflicht aber Nachweisobliegenheit, Art. 7 (1)
  - ggf. besondere Hervorhebung der datenschutzrechtlichen Einwilligungserklärung Art. 7 (2)
  - ausdrücklicher Hinweis auf die Verwendung von Gesundheitsdaten, Art. 8 (2) (a) DSGVO
- Schwerpunkt: Schutz des Rechts auf informationelle Selbstbestimmung
- beachte z.B. § 9 Abs. 3 MBO: Hinweis auf die Daten, die aufgrund einer vermuteten Einwilligung übermittelt werden dürfen

Einwilligung - Beispielsfälle

- Heimlicher HIV-Test – unzulässig, da keine zu erwartende Routineuntersuchung.

- Forschung: Forschung mit anonymisierten Daten ist zulässig, Untersuchungen an personenbezogenen Proben ohne Einwilligung sind i.d.R. unzulässig (Recht auf informationelle Selbstbestimmung und Recht auf Nichtwissen).
  Aber: „erfolgreiche" Anonymisierung ist schwer umzusetzen.

- Betriebsarzt: Proband muss über die Untersuchung im Vorwege aufgeklärt werden, insbesondere wenn Untersuchung nicht üblich oder erkennbare Voraussetzung für die angestrebte Tätigkeit ist.

Zweckbindung und Erforderlichkeit

- Der Zweck der Erhebung und Verarbeitung muss hinreichend bestimmt sein. Rahmen ist in der Regel das konkrete Behandlungsverhältnis
- Der Umfang der Erhebung und Verarbeitung der Daten muss erforderlich sein. (Die Erforderlichkeit wird häufig durch die gesetzgeberische Wertung sichergestellt. In diesem Fall ist sie nur gesondert zu prüfen, wenn ausdrücklich gefordert, z.B. § 27 Abs. 1 BDSG nF. für Forschung mit Daten)
- Arzthaftungsprozess: Es dürfen nur Patientendaten dem RA offengelegt werden, deren Kenntnis für den Prozess erforderlich ist, Art. 9 (2) (f) DSGVO. Schwierige Bestimmung der Erforderlichkeit, weil Vor- oder Miterkrankungen u.a. für die Bestimmung der Schadenshöhe relevant sind und diese Bewertung oft nur im Dialog mit dem RA erfolgen kann.
- Forschung, Archive, Statistik: Art. 9 (2) (j) DSGVO i.V.m. nationalen Gesetzen wie § 27 BDSG-neu, §§ 13, 26 LDSG-SH

Typische Übermittlungsbefugnisse im ärztlichen Beruf

- Abrechnung mit der Kassenärztlichen Vereinigung
- Bei Privatliquidation ist bisher Einwilligung für Übermittlung an eine Einzugsstelle notwendig – Transparenzpflicht bleibt aber!
  StGB ist kein Hindernis, § 203 III 2 StGB (2017)
- §§ 284 ff, 294 ff SGB V (Vertragsarztrecht)
  - Wirtschaftlichkeitsprüfungen
  - Qualitätsprüfungen z.B. Sonografie (Stichproben)
- Meldepflichten: InfektionsschutzG, KrebsregisterG
- Bei vor-, mit und nachbehandelnden Ärzten wird konkludente Einwilligung unterstellt - d.h. Widerspruch ist möglich, § 9 MBO
- Praxisinterne Übermittlung, gegenseitige Einsicht in Patientenakten:
  (+) Gemeinschaftspraxis (Partner, Gesellschaft), MVZ,
  (-) Praxisgemeinschaft (gemeinsam genutzte Räume und Mitarbeiter), angegliederte Kosmetikerin beim Dermatologen
- Kliniken: Meldeschein zur Einsicht der Polizei, wie in einem Hotel

Auftragsverarbeitung

- Bis 2017 war Auftragsverarbeitung für Berufsgeheimnisträger nur in Ausnahmefällen (Ländergesetze) möglich oder auf Grund einer Einwilligung.
- Seit 2017: § 203 Abs. 3 StGB:

  Die in den Absätzen 1 und 2 Genannten dürfen fremde Geheimnisse gegenüber sonstigen Personen offenbaren, die an ihrer beruflichen oder dienstlichen Tätigkeit mitwirken, soweit dies für die Inanspruchnahme der Tätigkeit der sonstigen mitwirkenden Personen erforderlich ist; das Gleiche gilt für sonstige mitwirkende Personen, wenn diese sich weiterer Personen bedienen, die an der beruflichen oder dienstlichen Tätigkeit der in den Absätzen 1 und 2 Genannten mitwirken.
- Damit entfällt die Strafbarkeit
- Das ist für sich allein aber keine Erlaubnis.
- Rechtsgrundlage z.B. Auftragsverarbeitung 28 DSGVO
- Pflicht: dem Risiko angemessene tech.-org. Maßnahmen

Auftragsverarbeitung

- Besondere Anforderungen an die Auftragsverarbeitung im Gesundheitsbereich:
  - Bekanntgabe der Identitäten der Auftragsverarbeiter, Zwecke, Umfang der Verarbeitung vor Beginn der Behandlung.
  - Besonders sorgfältige Auswahl aller Auftragsverarbeiter.
  - Klare Verpflichtung auf die Verschwiegenheit zwingend – Auftragnehmer muss alle eingesetzten Mitarbeiter verpflichten.
  - Soweit möglich sollen Betroffene einzelnen Verarbeitungen widersprechen können – Praktisch nicht möglich beim Haupt-IT-Dienstleister eine Klinik, denkbar aber durchaus bei der Auswahl eines externen Medizin- oder Dentallabors.

Übermittlung von Sozialdaten, §§ 67d ff SGB X

- Übermittlung Grundsatz: Es bedarf einer **gesonderten Übermittlungsbefugnis**, die von der übermittelnden Stelle zu prüfen ist. Soweit eine andere Stelle anfragt, trägt diese die Verantwortung für die Richtigkeit der Anfrage, §_67d II SGB X

- diverse Übermittlungsbefugnisse in §§ 68-77 SGB X und anderen Sonderregelungen, z.B. für den Datenabgleich gegen Sozialleistungsmissbrauch und Schwarzarbeit

- Bei erhobenen medizinischen Daten Weitergabe nur, wenn sie dem Arzt selbst gestattet gewesen wäre, § 76 I SGB X

Betroffenenrechte im Medizinbereich

<u>medizinrechtliche Ansprüche</u>

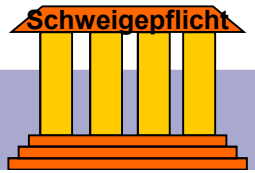
- Medizinrechtlicher Auskunftsanspruch aus Art. 2 I i.V.m. Art. 1 I GG
  - Patientenautonomie als Ausprägung des Rechts auf freie Entfaltung der Persönlichkeit
- Einsicht in Patientenakte:
  - § 630g BGB als Teil des Behandlungsvertrags
  - § 10 II Berufsordnung Ärzte
- Alle objektive Befunde unterliegen dem Einsichtsrecht. Arzt darf aber persönliche Notizen schwärzen.

<u>datenschutzrechtliche Ansprüche</u>

- Art. 13, 14 DSGVO Benachrichtigung
- Art. 15 DSGVO Auskunft
- Art. 17 DSGVO Löschung
- Art. 18 DSGVO Sperrung

- Zusätzlich: Schadensersatzansprüche nach DSGVO und BGB

Für den Sozialdatenschutz finden sich entsprechende Regelungen in den §§ 84 ff. SGB X

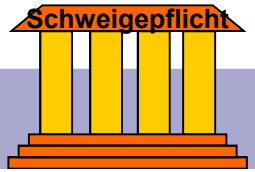


Datensicherheit im Gesundheitsbereich

- Gesundheitsdaten sind besondere Arten von Daten und unterliegen je nach datenverarbeitender Stelle besonderer Berufsgeheimnisse.
- Es sind die **geeigneten** Maßnahmen zu treffen mit Rücksicht u.a. auf das **Risiko für die Betroffenen**.
- Umfang hängt von Quantität und Qualität der Daten ab, insbesondere welche Einschnitte Betroffene bei einem Datenverlust erleiden würden.
- Arzt hat dabei sicherzustellen:
  - Vertraulichkeit — Keine Einsicht durch Dritte
  - Verfügbarkeit — Dokumentation, Folgebehandlungen
  - Integrität — Aufbewahrungsfirsten

Kontrolle im Gesundheitsbereich

- Interne Kontrolle erfolgt durch betrieblichen / behördlichen Datenschutzbeauftragten.
- Externe Kontrolle je nach rechtlicher „Säule“
  - DSGVO einschl. OWi: Datenschutzaufsichtsbehörden
  - Berufsrecht: Kammern (Ärztekammer, Anwaltskammer, Notarkammer, etc.)
  - Strafrecht: Staatsanwaltschaft. Aufsichtsbehörden geben solche Vorgänge an die zuständige StA ab. § 203 StGB ist ein Antragsdelikt so Strafantrag von Geschädigten erforderlich ist, § 205 StGB.
  - BGB: Patient verfolgt seine Ansprüche selbst auf dem Zivilrechtsweg.



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.

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

Einwilligung in eine medizinische Untersuchung

- Einwilligung in Behandlung in Datenverarbeitung können Teil desselben Dokument sein. Es muss aber klar werden, dass es sich um unterschiedliche Erklärungen handelt und auch die Möglichkeit geben diese einzeln abzulehnen.

- Frage: Einwilligungen sind kompliziert und für Patienten oft schwer verständlich, teilweise mit erheblicher Sprachbarriere. Umgekehrt sind diese Gespräche Zeitaufwendig für das ärztliche Personal – Patienten sind sich dessen bewusst und trauen sich womöglich nicht alle Frage zu stellen. Was wäre bei einer Aufklärung und Einwilligung mittels einer KI zu Bedenken?
  - Art 5 (2) DSGVO Rechenschaftspflicht – Es muss belegbar sein, dass und worüber aufgeklärt wurde und dass korrekt und verständlich (Art 12 (1) DSGVO) informiert wurde.
  - Medizinische Aufklärung: Alles korrekt dargestellt? Möglichkeit zur Rücksprache mit ärztlichem Personal?
  - => ein KI-Dialog, ggf. auch Videos können eine sehr hilfreiche Idee sein, auch die direkte Übersetzung in die bevorzugte Sprache des Patienten
    ABER jeder Verantwortliche (für Behandlung und für Datenschutz) sollte Nachweis einer vollständigen, korrekten Informationen führen können.

Aus der Arbeit des BMBF-geförderten Projekts PRIMA

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:
  - Medizinisch bezüglich aller Untersuchungen, Eingriffe
  - 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, LKranhenhG
    - Private Stellen: Teilweise Landesrecht, ggf. Art. 6 I f DSGVO
- Immer erforderlich für Ethik und Datenschutz: Umfassende Aufklärung und Unterrichtung (Herausforderung etwa für „Legende" bei psychol. Studien)
- Anforderungen kommen u.a. von: Hochschulinternen Regelungen aber auch durch Fördergeber (BMBF, Horizon-Programme der EU)

=> Rat für Forschende: Datenschutzbeauftragte und Ethik-Kommission kontaktieren

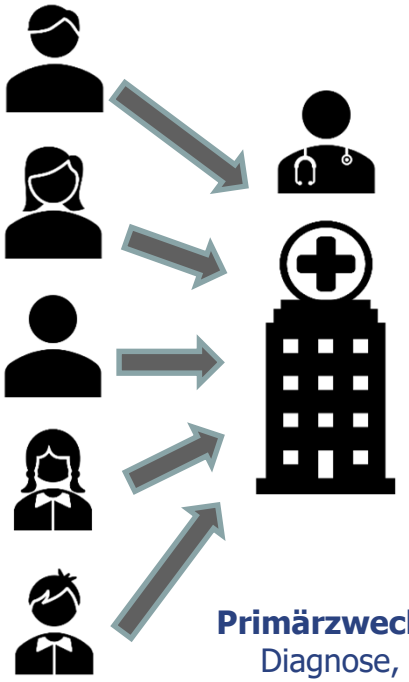
Sekundärnutzung von Daten

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

- Herausforderungen
  - 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.

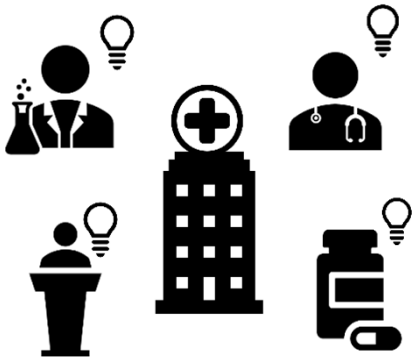
Sekundärnutzung von Daten

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



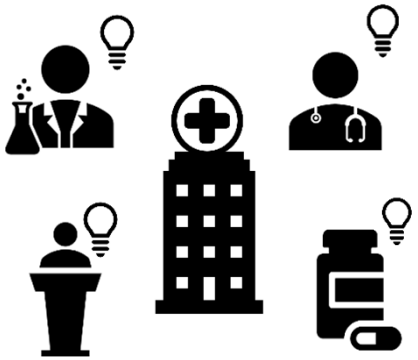
Sekundärzwecke
Wissenschaft, Forschung, Lehre, Entwicklung von Arznei- und Medizinprodukten

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

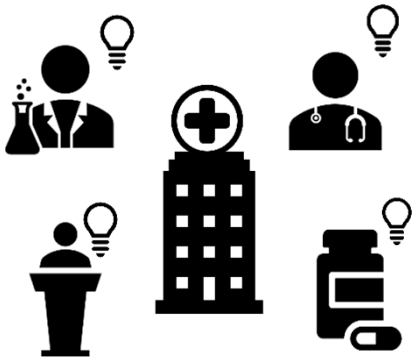
[1] DSK, Petersberger Erklärung vom November 2022

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

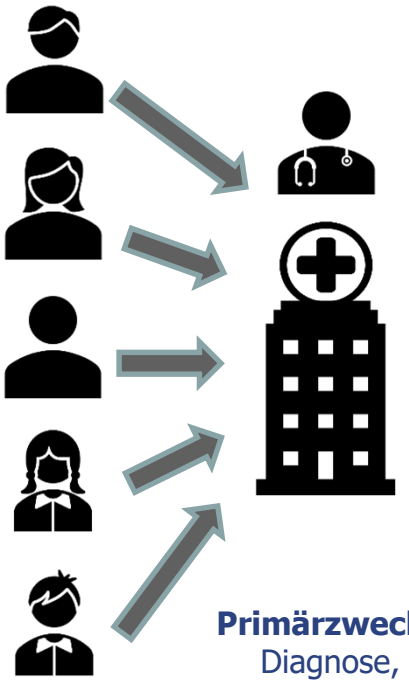


Sekundärzwecke
Wissenschaft, Forschung, Lehre, Entwicklung von Arznei- und Medizinprodukten

[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.

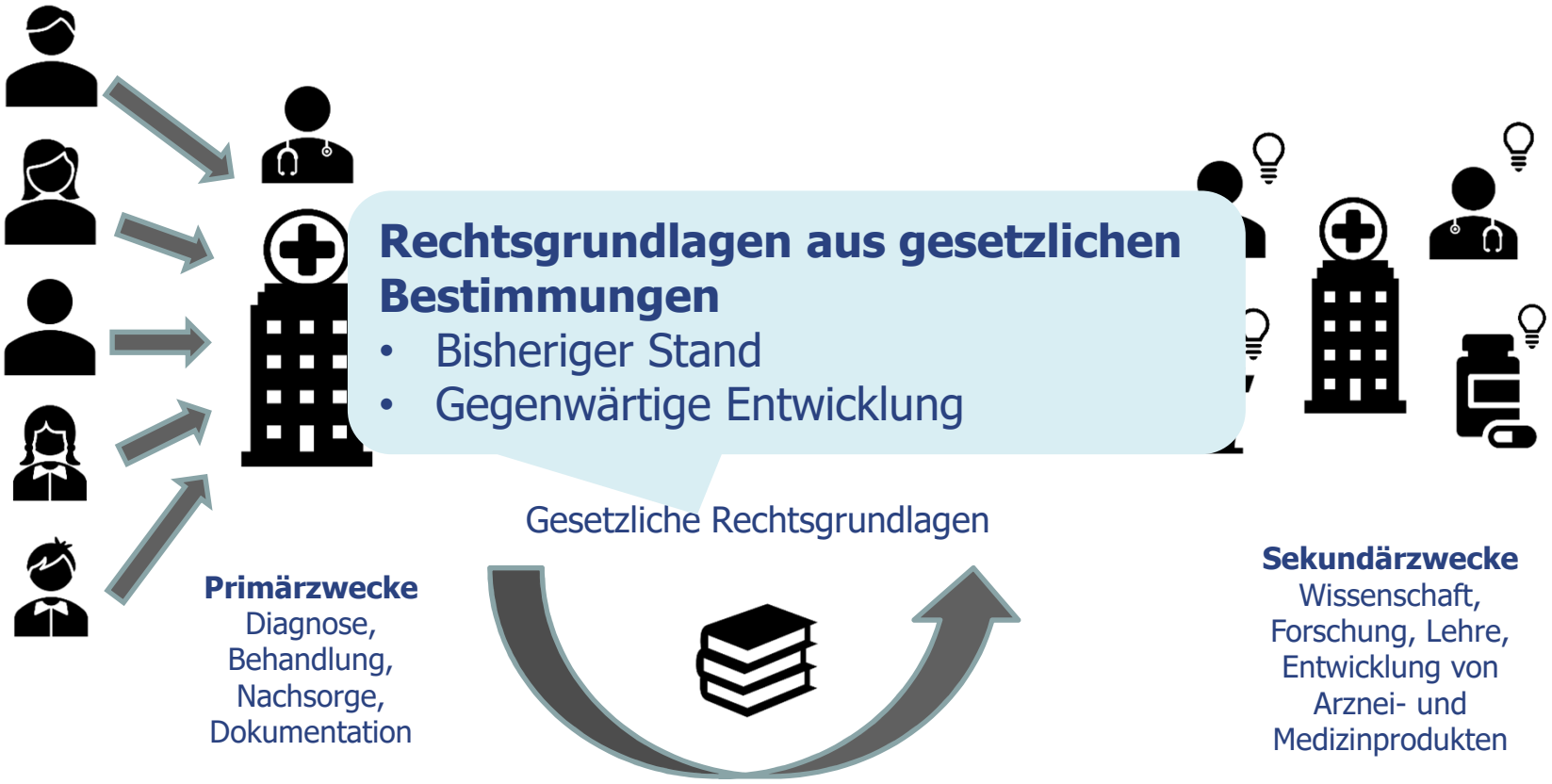
Ideen zur technischen Verbesserung:

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

Sekundärnutzung von Daten

primäre Datenverarbeitung

sekundäre Datenverarbeitung



Rechtsgrundlagen aus gesetzlichen Bestimmungen

- Bisheriger Stand
- Gegenwärtige Entwicklung

Gesetzliche Rechtsgrundlagen

Primärzwecke
Diagnose, Behandlung, Nachsorge, Dokumentation

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

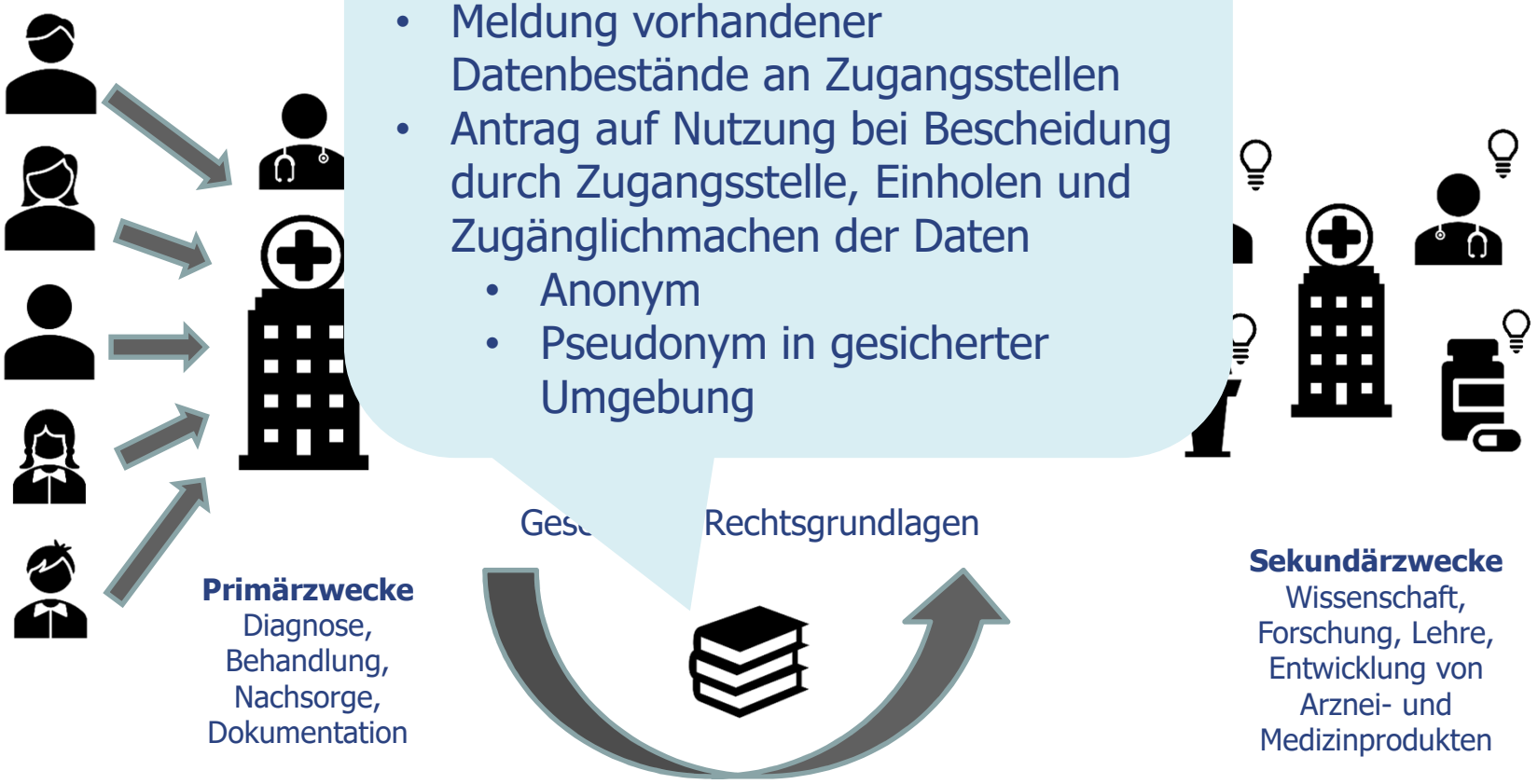
Sekundärnutzung von Daten

primäre Datenverarbeitu

sekundäre Datenverarbeitung

European Health Data Space (EHDS)
Gesundheitsdatennutzungsgesetz

- Meldung vorhandener Datenbestände an Zugangsstellen
- Antrag auf Nutzung bei Bescheidung durch Zugangsstelle, Einholen und Zugänglichmachen der Daten
  - Anonym
  - Pseudonym in gesicherter Umgebung

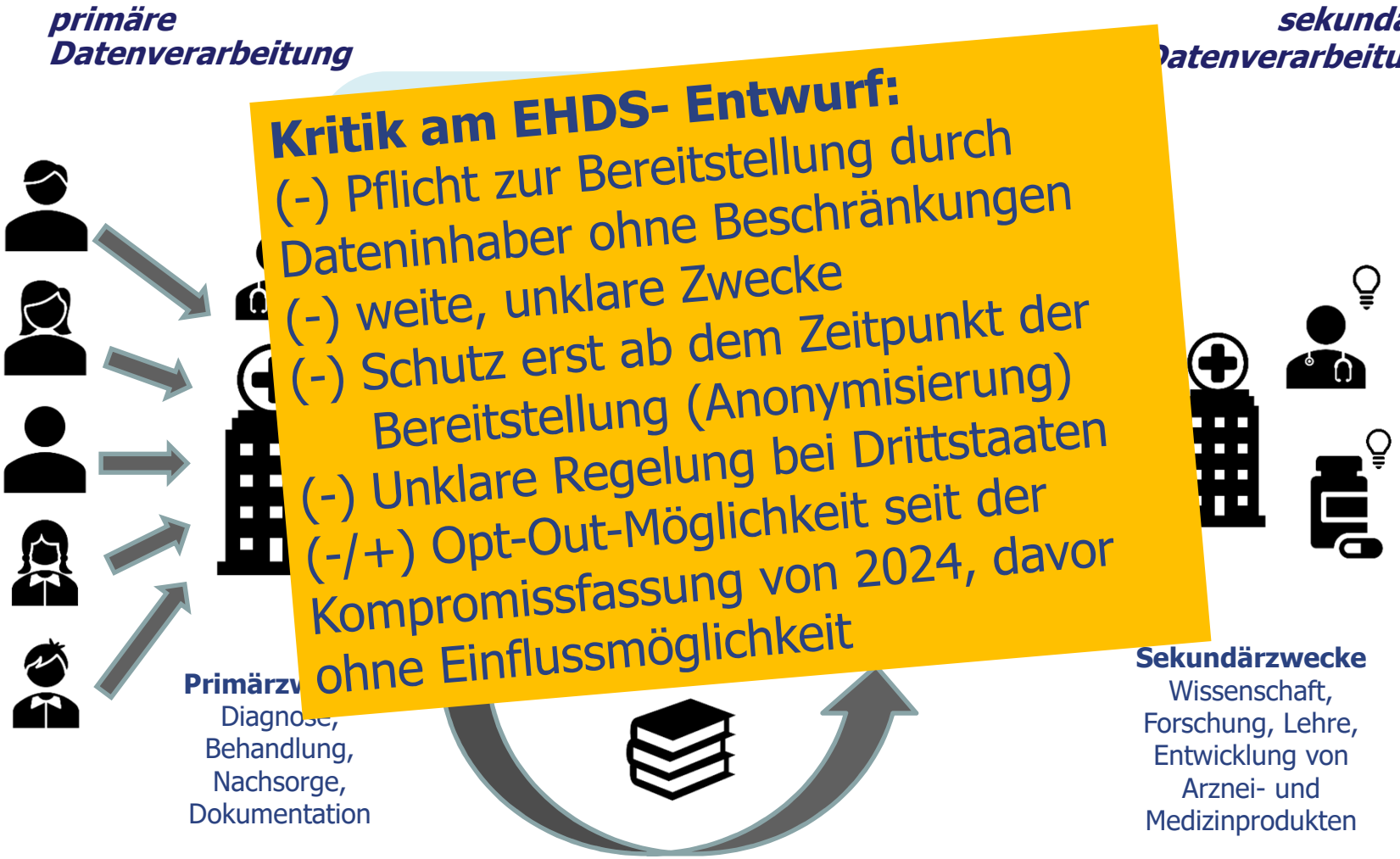


Ges Rechtsgrundlagen

Primärzwecke
Diagnose, Behandlung, Nachsorge, Dokumentation

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

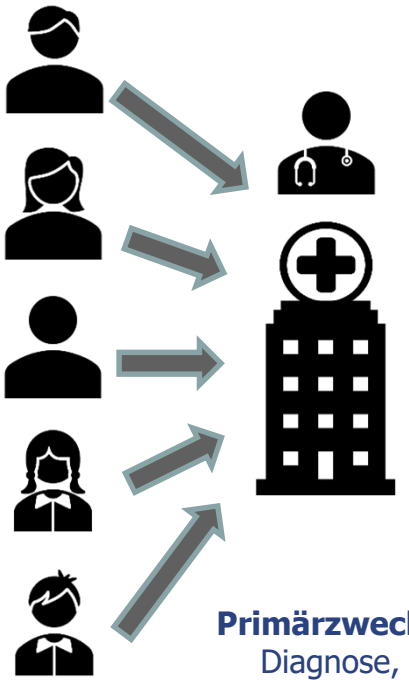
Sekundärnutzung von Daten



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

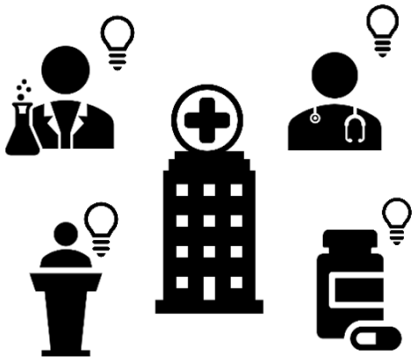


Primärzwecke
Diagnose, Behandlung, Nachsorge, Dokumentation

Informierte Einwilligung

Gesetzliche Rechtsgrundlagen

sekundäre Datenverarbeitung



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

Sekundärnutzung von Daten
Technisch Organisatorische Maßnahmen

- Anonymisierung / Pseudonymisierung
  (siehe nächste Folie)

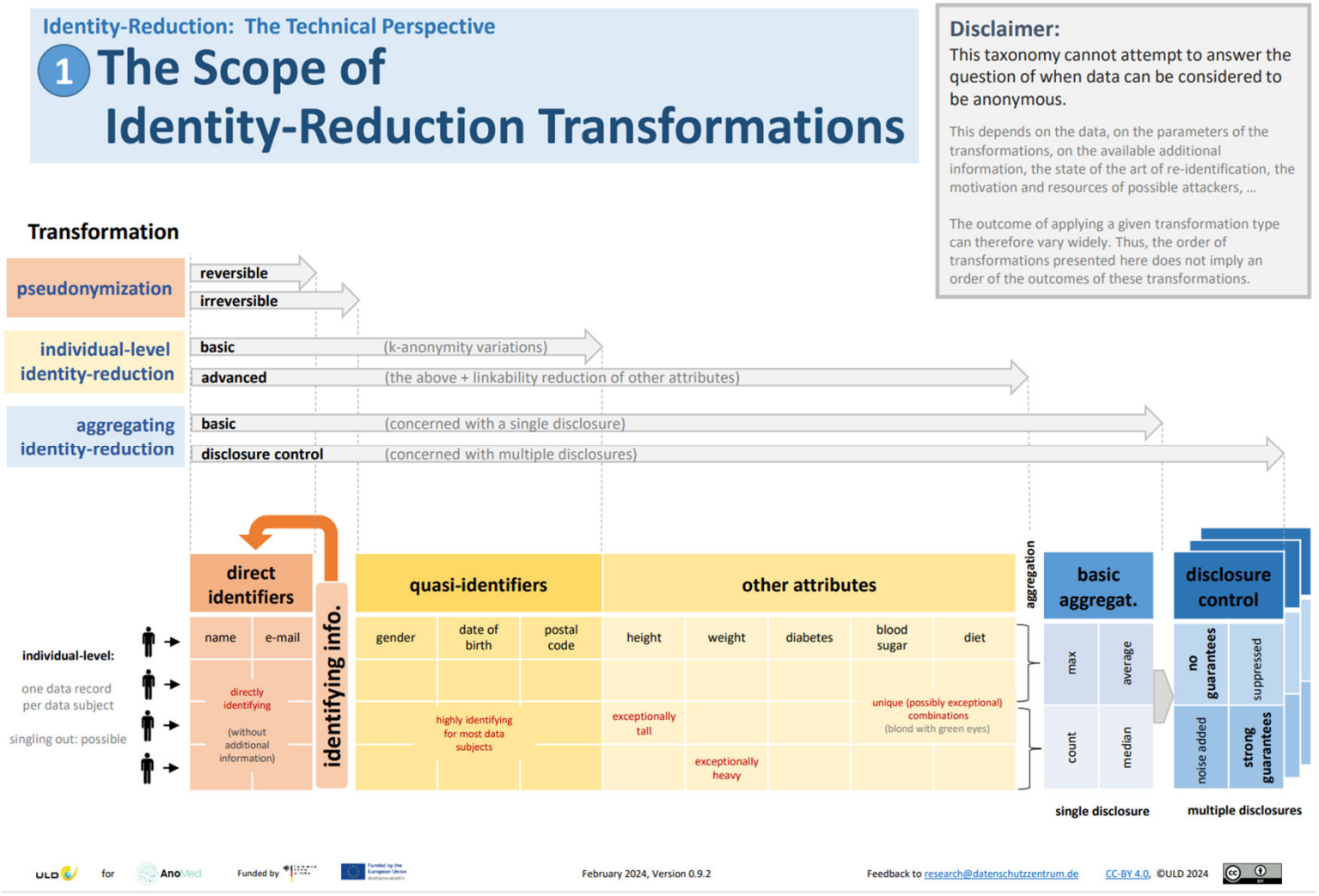
- Dezentrale Verarbeitung:
  Übermittlung der Daten vermeiden durch dezentrale Auswertung bei den Quellen denkbar z.B. KI-Training oder statistische Auswertungen.
  Eingesetzte Verfahren könnten zumindest sukzessiven Umstieg auf dezentrale Verfahren vorsehen.

- Datenschutz-Folgenabschätzung (DFSA) für alle Verfahren der Zugangsstelle.

Aktuelles aus

der Datenschutzforschung

Sekundärnutzung von Daten
Anonymisierung?



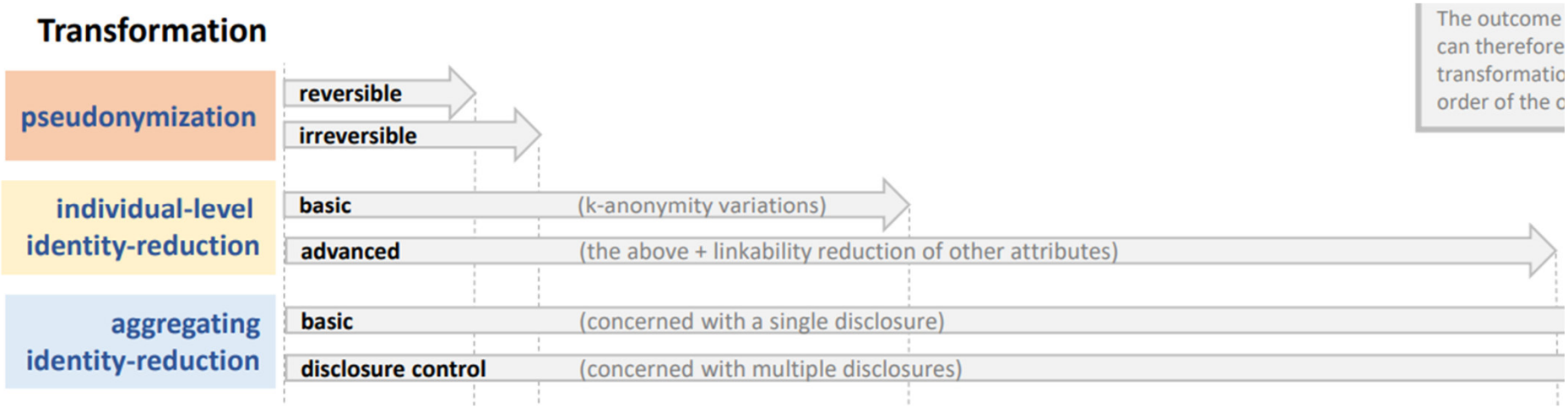
Quelle: https://www.datenschutzzentrum.de/uploads/projekte/anomed/Identity-Reduction_v0_9_2.pdf

Sekundärnutzung von Daten
Anonymisierung?

Personenbezug zu reduzieren ist komplex.

Verfahren haben sehr unterschiedliche Ergebnisse.

Ausgehend von der Definition personenbezogener Daten ist entscheidend, ob die Daten sich auf Einzelpersonen beziehen oder bezogen werden können.



Sekundärnutzung von Daten
Anonymisierung?

Kategorien möglichen Outputs

Data Category	Possibilities of (Re-)Identification
Fully Identified Personal Data	• **direct identification** is possible (since data is unchanged)
(Basic) ***Pseudonymous Data*** *personal data* (Recital 26 GDPR)	• direct identification is no longer possible • **only indirect identification** using **additional information** is possible
Advanced Pseudonymous Data *likely still personal data*	• direct identification is no longer possible • **even indirect identification** is rendered **difficult** or **prevented** (but with unknown success)
Supposedly Anonymous Data *likely anonymous* *but future re-identification cannot be excluded*	• **all relevant known re-identification attacks are excluded** • **thorough assessment of re-identification risk** results in low risk
Successfully Anonymous Data certainly anonymous *future practical re-identification can be excluded*	• **re-identification can be practically**[1] **excluded** • strong guarantees or thorough assessment of re-identification risk

[1] *practically* here means considering any party who can reasonably likely gain access to the data, its reasonably likely means, and taking into account technological developments.

Sekundärnutzung von Daten
Anonymisierung?

Personenbezug beseitigen ist komplex.

Verfahren haben sehr unterschiedliche Outputs.

Data Category	Possibilities of (Re-)Identification
Fully Identified Personal Data	• **direct identification** is possible (since data is unchanged)
(Basic) ***Pseudonymous Data*** *personal data* (Recital 26 GDPR)	• direct identification is no longer possible • **only indirect identification** using **additional information** is possible
Advanced Pseudonymous Data *likely still personal data*	• direct id • **even ind** (but with
Supposedly Anonymous Data *likely anonymous* *but future re-identification cannot be excluded*	• **thorough**
Successfully Anonymous Data certainly anonymous *future practical re-identification can be excluded*	• **re-identification can be practically**[1] **excluded** • strong guarantees or thorough assessment of re-identification risk

[1] *practically* here means considering any party who can reasonably likely gain access to the data, its reasonably likely means, and taking into account technological developments.

Wurde das Risiko von Fehlern bei der Einschätzung des Erfolgs der Anonymisierungsmaßnahmen bedacht?

Quelle: https://www.datenschutzzentrum.de/uploads/projekte/anomed/Identity-Reduction_v0_9_2.pdf

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

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.

Förderhinweise

Unboxing.IoT.Privacy

https://www.anomed.de/

https://panelfit.eu/

trapeze-project.eu

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

GEFÖRDERT VOM

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

TRAPEZE

EMPRI-DEVOPS