

# ***Datenschutzrecht***

## **Gesundheitsdatenschutz & Schutz von Forschungsdaten**

29. Juni 2026  
Harald Zwingelberg

Ansprechpartner Vorlesungsreihe: Benjamin Bremert

Vertretene Auffassungen sind solche des Referenten und geben nicht die  
Rechtsauffassung des ULD oder der Forschungsprojekte bzw. der deren  
Konsortialpartner wieder.

Mit Ergebnisse der  
Forschungsprojekte:



# *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, beziehen sich alle genannten Artikel auf die DSGVO.

## ***Agenda***

- Wiederholung
- Gesundheitsdatenschutz  
mit Exkurs Berufsgeheimnis
- Forschungsdatenschutz

**Wiederholung:**

**Grundlagen**  
**&**  
**Auftragsdatenverarbeitung**

# ***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 Vertraulichkeit**
  - Technische und organisatorische Maßnahmen, Integrität und Vertraulichkeit
- **Kontrolle**
  - Interner / externer Datenschutzbeauftragter

\*) Zum ganzen siehe Vorlesungsfolien von B. Bremert „Einführung Datenschutzrecht I und 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>



# ***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  
Behandlung und Forschung

**Gesundheitsdaten!**

**Gesundheitsdatenschutz  
&  
Recht der Berufsgeheimnisträger**

# ***Medizin- und Sozialdatenschutz***

1. Geheimnisschutz
2. Gesetzesgrundlagen, Datenerhebung
3. Einwilligung + Schweigepflichtentbindung
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 kennen Sie?
- Welche Gründe kann es geben Daten bei Sozialversicherungsträgern besonders zu schützen?

# ***Rechtsgrundlagen für u.a. Ärzte***

## **Ausdrückliche Einwilligung, Art 9**

- Ausdrücklich: Eindeutiger Bezug, dass Gesundheitsdaten als besondere Arten persbez. Daten verarbeitet werden
- Freiwillig ohne Zwang
- Bestimmt: Konkretisierte Zwecke
- Informiert über Daten, Empfänger Zwecke
- Unmissverständliche bestätigende Handlung

## **Gesetzliche Grundlagen**

- Gesetzliche Erlaubnis (Art. 9 Abs. 2 lit. h DSGVO): Verarbeitung für Diagnostik, Therapie & Versorgung
- Dokumentationspflicht: Gesetzliche und berufsrechtliche Pflicht zur Aktenführung (§ 630f BGB, § 10 MBOÄ)
- Behandlungsvertrag: Erfüllung von Haupt- und Nebenpflichten (§§ 630a ff. BGB)

# ***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.***

# ***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 möglich durch:
    - Einwilligung
    - Mutmaßliche Einwilligung (z.B. bei Bewusstlosen in Notaufnahme)
    - Gesetzliche Offenbarungspflichten (z.B. § 138 StGB)
    - Rechtfertigender Notstand (u.a. § 34 StGB)

## § 203 StGB Verletzung von Privatgeheimnissen

## Gesetzestext

(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.
- Merke: Bei einem spezifischen Verbot braucht es eine spezifische Ausnahme.



## ***Grenzen der Schweigepflicht: einleitende Fallbeispiele***

- Bankräuber kündigt Tat beim Arzt / Psychotherapeuten 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 erlaubt / geboten / Pflicht?: § 34 StGB
- Einschaltung externer Inkassounternehmen bei der Behandlungsabrechnung als Auftragsverarbeiter: (siehe unten)
- Arzthaftungsprozess: Mitteilung von Patientendaten zur rechtlichen Verteidigung? Nach § 34 StGB zulässig im erforderlichen Umfang
- Polizei fahndet nach einem Bankräuber und befragt den Arztpraxen, ob dieser dort in Behandlung war: Schweigepflicht!

## § 138 StGB Nichtanzeige geplanter Straftaten

## Gesetzestext

(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.

# ***Grenzen der Schweigepflicht Sonderregelungen für Ärzte***

Es gibt Spezialgesetzliche Sonderregelungen etwa

- Infektionsschutzgesetz (Nicht-namentliche & namentliche Meldungen)
  - Für Meldungen zum Krebsregister
  - Meldung einer Kindeswohlgefährdung<sup>1</sup> durch Mediziner, Psychologen, Familienberatung, Sozialarbeiter, Lehrkräfte in abgestuften Vorgehen § 4 KKG<sup>2</sup>:
    - 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!“

<sup>1</sup> KKG: Gesetz zur Kooperation und Information im Kinderschutz

<sup>2</sup> Dazu TB 2019 des ULD: [https://www.datenschutzzentrum.de/tb/tb37/kap04\\_5.html#451](https://www.datenschutzzentrum.de/tb/tb37/kap04_5.html#451)

# ***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: InfektionsschG, KrebsregisterG, PersonenstandsG
- 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

## ***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: Eine 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

# ***Auftragsverarbeitung***

- Auftragsverarbeitung für Berufsgeheimnisträger möglich

- 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 Erlaubnisgrundlage
- Rechtsgrundlage z.B. Auftragsverarbeitung 28 DSGVO
- Pflicht: dem Risiko angemessene tech.-org. Maßnahmen, Sorgfalt bei Auswahl der Dienstleister  
Wünschenswert: Wahlmöglichkeit für Patienten

# ***Auftragsverarbeitung IT- Dienstleistung***

- IT-Dienstleistung ist als Auftragsverarbeitung möglich
- Keine Strafbarkeit nach § 203 StGB, da IT-Dienstleister keine „Dritten“ mehr sind, sondern „Mitwirkende“.
- Pflicht: Formelle Verpflichtung zur Verschwiegenheit durch den Arzt/Klinikleitung.
- Strafandrohung: IT-Dienstleister haften bei Geheimnisbruch wie Ärzte (§ 203 Abs. 4 StGB).



# ***Betroffenenrechte im Medizinbereich***

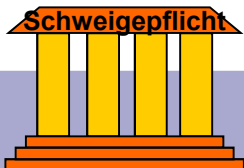
## medizinrechtliche Ansprüche

- 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 objektiven Befunde unterliegen  
dem Einsichtsrecht. Arzt darf aber  
persönliche Notizen schwärzen.

## datenschutzrechtliche Ansprüche

- 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                              Aufbewahrungspflichten

# ***Data Breach – Verletzung des Schutzes personenbezog. Daten, Art 33, 34 DSGVO***

- **Meldung an die Aufsichtsbehörde, Art. 33 DSGVO**
  - Unverzüglich (i.d.R. binnen 72 h)
  - *Ausnahme:* Kein Risiko für die Rechte und Freiheiten der Betroffenen.
- **Benachrichtigung der betr. Personen, Art. 34 DSGVO**
  - Nur bei einem **hohen Risiko** für die persönlichen Rechte.
  - Bei Gesundheitsdaten (Art. 9) wird oft „hohes Risiko“ durch die Sensibilität der Daten anzunehmen sein.
- **Typische medizinische Fallbeispiele:**
  - Ransomware-Verschlüss. der Patientenakten (Verfügbarkeit).
  - Fehlversand von Laborbefunden per unverschlüsselter E-Mail.
- **Saubere Dokumentation, Art. 33 Abs. 5 DSGVO**

# ***Wiederholung / Kurzübersicht Betroffenenrechte***

Welche Betroffenenrechte nach DSGVO kennen Sie?

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

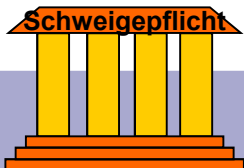


Warum genügt folgende Antwort auf ein umfassendes Auskunftersuchen nicht: „Wir speichern über Sie: Name, Adresse, Loginname, Passwort („gehasht“) & Kundennummer“?

- Eine umfassende Auskunft ist Vorbedingung zur Wahrnehmung der Rechte auf Berichtigung, Löschung und Einschränkung der Verarbeitung. 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.

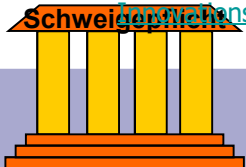
# ***Kontrolle im Gesundheitsbereich***

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



# ***Weiterführende Quellen: Gesundheitsdatenschutz***

- EuGH, Urteil vom 04.10.2024, C-21/23 (Lindenapotheke), Bestelldaten für nicht-verschreibungspflichtige Medikamente sind Gesundheitsdaten sein, wenn sie den Gesundheitszustand offenbaren können <https://eur-lex.europa.eu/eli/C/2025/689/oj/eng>
- Europäischer Datenschutzausschuss, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679 (u. a. Anforderungen an die ausdrückliche Einwilligung), 2020, [https://www.edpb.europa.eu/documents/guideline/guidelines-052020-on-consent-under-regulation-2016679\\_de](https://www.edpb.europa.eu/documents/guideline/guidelines-052020-on-consent-under-regulation-2016679_de)
- Europäischer Datenschutzausschuss (Legacy: Art. 29 WP), Leitlinien für Transparenz gemäß der Verordnung 2016/679 (WP 260 rev.01), 2018, Link zur EU-Kommission <https://ec.europa.eu/newsroom/article29/items/622227/en>
- Datenschutzkonferenz (DSK), EntschlieÙung kostenlose Kopie Patientenakte, 2024, [https://www.datenschutzkonferenz-online.de/media/en/2024-09-11\\_Entschliessung\\_DSK\\_Patientenakte.pdf](https://www.datenschutzkonferenz-online.de/media/en/2024-09-11_Entschliessung_DSK_Patientenakte.pdf)
- Datenschutzkonferenz (DSK), Stellungnahme zum GeDIG-Entwurf], 2026, [https://www.datenschutzkonferenz-online.de/media/st/20260518\\_Stellungnahme\\_Datenschutzbehoerden-der-Laender\\_Gesundheitsdaten-und-Genomik-Gesetz.pdf](https://www.datenschutzkonferenz-online.de/media/st/20260518_Stellungnahme_Datenschutzbehoerden-der-Laender_Gesundheitsdaten-und-Genomik-Gesetz.pdf)



# **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<sup>[1]</sup> Schutz des Privat- und Familienlebens
- EU: Art 8 GrCh Schutz personenbezogener Daten

[1] [https://www.europarl.europa.eu/charter/pdf/text\\_de.pdf](https://www.europarl.europa.eu/charter/pdf/text_de.pdf)

## **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.“





# ***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 berücksichtigt
  - Nationale Gesetzgeber haben Erlaubnisnormen geschaffen
  - Aber: Es bleibt beim Grundsatz, dass spezielle Verbote auch spezielle Erlaubnisnormen brauchen (siehe Abschnitt zu Medizindatenschutz). Diese Normen müssen Ausgleich herstellen z.B. durch TOMs, Zweckbindung, ...

# ***Einwilligung im Forschungskontext***

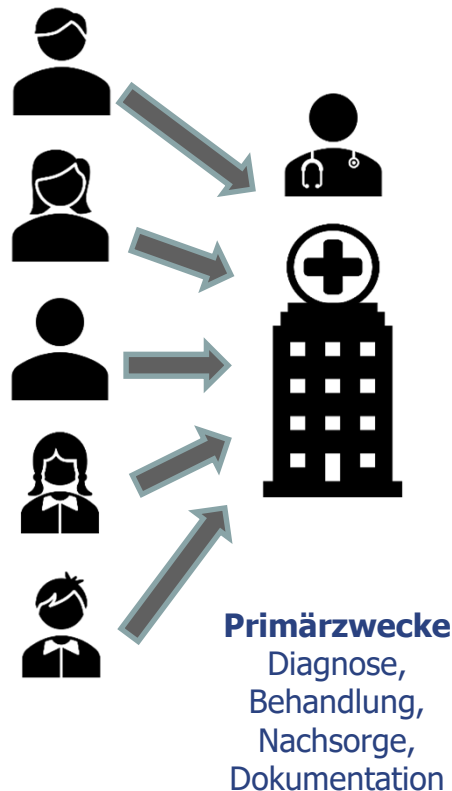
- Einwilligung ist auch im Forschungskontext erforderlich. Zu trennen:
    - Medizinisch bezüglich aller Untersuchungen, Eingriffe
    - Ethik (teilweise weitergehende Aspekte umfasst auch Datenschutz)
    - Datenschutz nach Datenschutzrecht
  - Rechtsgrundlagen im Datenschutz
    - Einwilligung nach Art. 6 I a DSGVO (iVm Art 9 DSGVO)
    - Überwiegendes Interesse an der Forschung
      - Universitäten, öffentl.-rechtl. Institute: Art. 6 I e DSGVO in Verbindung mit Normen des Landesdatenschutzrechts, Hochschulrechts, LKranhG
      - Private Stellen: Teilweise Landesrecht, ggf. Art. 6 I f DSGVO
  - Immer erforderlich für Ethik und Datenschutz: Umfassende Aufklärung und Unterrichtung
  - Anforderungen kommen u.a. von: Hochschulinternen Regelungen aber auch durch Fördergeber (BMBF, Horizon-Programme der EU)
- => Rat für Forschende: Datenschutzbeauftragte und Ethik-Kommission einbinden.

# ***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*



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

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

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

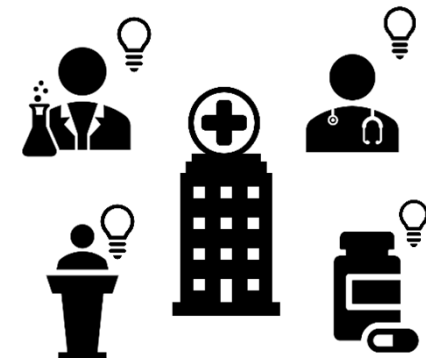
# ***Sekundärnutzung von Daten***

## ***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

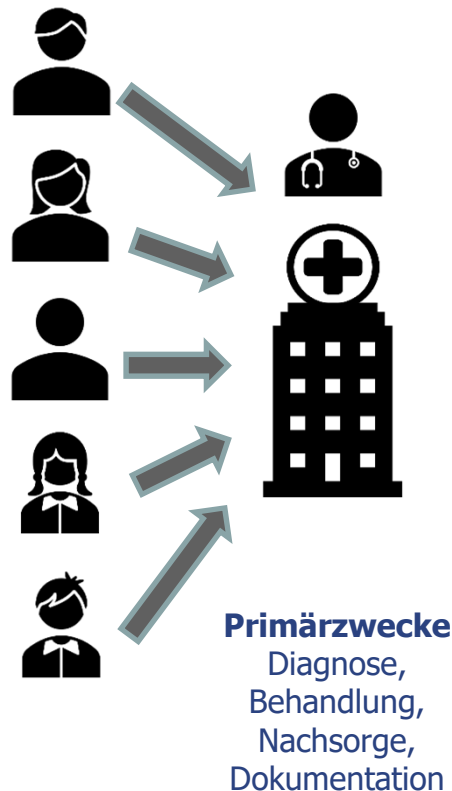


### **Sekundärzwecke**

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

# Sekundärnutzung von Daten

*primäre  
Datenverarbeitung*



*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 via Einwilligung – der klassische Weg***

- Konzept: Selbstbestimmung durch explizite Entscheidung
  - „Ausdrückliche“ Einwilligung, Art. 9 Abs. 2 lit. a DSGVO
- Herausforderung: Hoher Aufwand bei Langzeitstudien und großen Datenmengen; „Informed Consent“ stößt bei unklaren künftigen Forschungsfragen an Grenzen.
- Lösung: Der „Broad Consent“ (Medizininformatik-Initiative):
  - Proaktive Einholung einer Einwilligung für bestimmte Bereiche wissenschaftlicher Forschung (statt nur für ein Projekt).
  - Akzeptiert durch die DSK (2020), sofern kompensierende Garantien (Ethik-Votum, Transparenz) vorliegen.
- Technische Unterstützung:
  - Dynamic Consent: Patienten steuern Freigaben modular.
  - Dashboards: Transparente Kontrolle über Datennutzungen.

# Sekundärnutzung von Daten

*primäre  
Datenverarbeitung*

*sekundäre  
Datenverarbeitung*





# Sekundärnutzung von Daten



# ***Paradigmenwechsel von Einwilligung zum Gesetz***

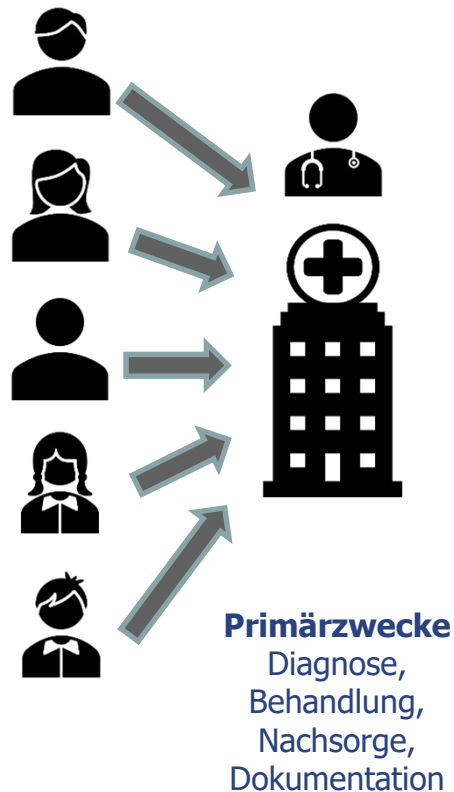
- Kerngedanke: Zugunsten des Gemeinwohlinteresses Ersatz der einwilligungsbasierten Forschung durch gesetzliche Erlaubnistatbestände
- Die Lösung (EHDS & GDNG): Datennutzung kraft Gesetzes als neue Regelsäule.
- Zentrale Merkmale:
  - Datenbereitstellungspflicht: Krankenhäuser und Kassen müssen Daten für die Sekundärnutzung vorhalten.
  - Opt-out statt Opt-in: Daten (z. B. aus der ePA) dürfen für gemeinwohlorientierte Forschung genutzt werden, sofern der Patient nicht aktiv widerspricht.
  - Zweckbindung: Nutzung strikt begrenzt auf Forschung, Statistik und öffentliche Gesundheit.

# ***Paradigmenwechsel Widerspruchsrecht (Opt-Out)***

- Daten fließen kraft Gesetzes (GDNG/EHDS), aber Patienten behalten teilweise die Kontrolle durch Widerspruchslösung.
- Anforderung (DSK, Petersberger Erklärung): Der Widerspruch muss einfach und ohne Begründung möglich sein („voraussetzungslose Widerspruchsmöglichkeit“).
- Mögliche Informationstechnische Umsetzungen:
  - Integration von Widerspruchs-Schnittstellen in Patientenportale/ePA-Apps.
  - Sicherstellung der Intervenierbarkeit: Ein Widerspruch muss systemübergreifend den Stopp der Sekundärnutzung auslösen.
  - Transparenz: Patienten müssen über Dashboards sehen können, welche Stellen ihre Daten nutzen, um ihr Opt-out gezielt ausüben zu können

# Gesamtbild Sekundärnutzung von Daten

*primäre  
Datenverarbeitung*



Informierte Einwilligung

Gesetzliche Rechtsgrundlagen



*sekundäre  
Datenverarbeitung*



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

# Sekundärnutzung von Daten Anonymisierung?

## Identity-Reduction: The Technical Perspective

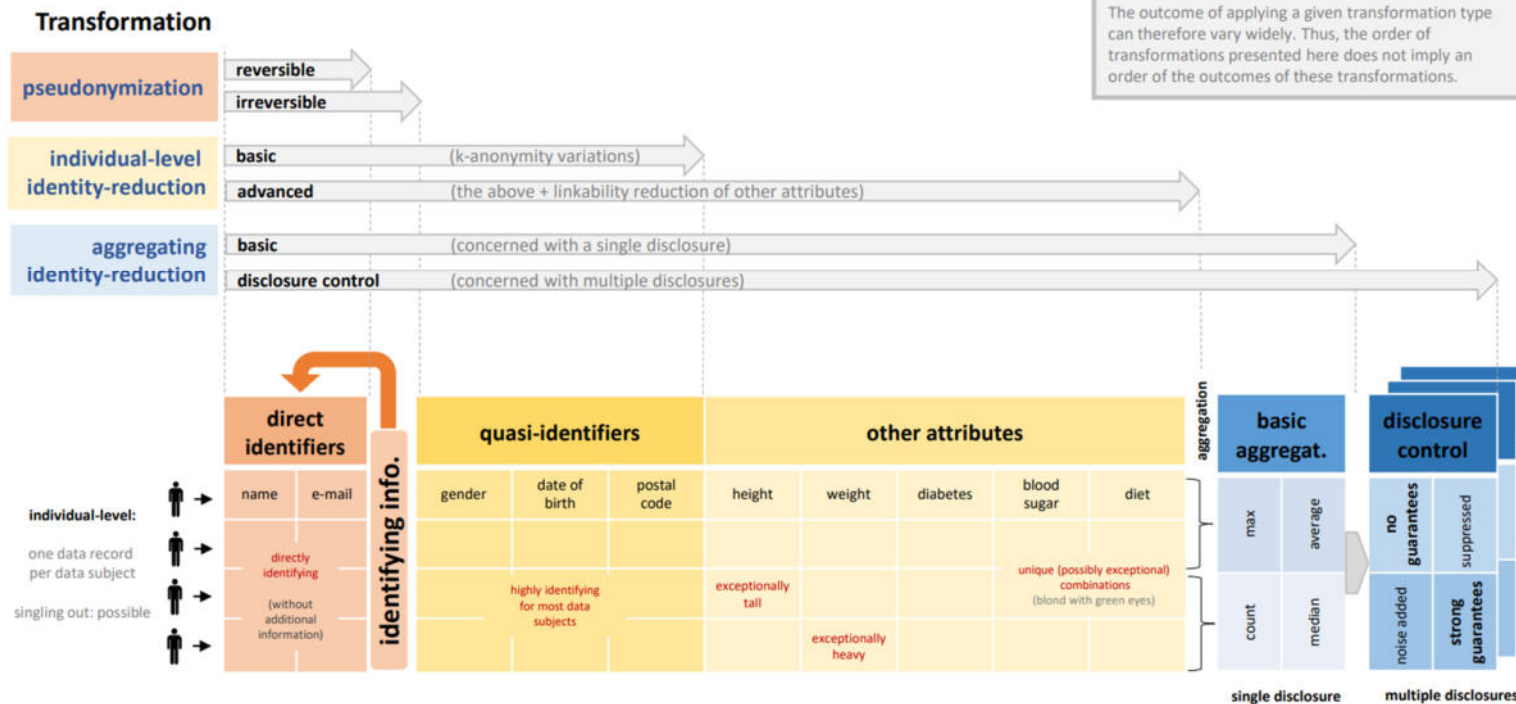
### 1 The Scope of Identity-Reduction Transformations

#### Disclaimer:

This taxonomy cannot attempt to answer the question of when data can be considered to be anonymous.

This depends on the data, on the parameters of the transformations, on the available additional information, the state of the art of re-identification, the motivation and resources of possible attackers, ...

The outcome of applying a given transformation type can therefore vary widely. Thus, the order of transformations presented here does not imply an order of the outcomes of these transformations.



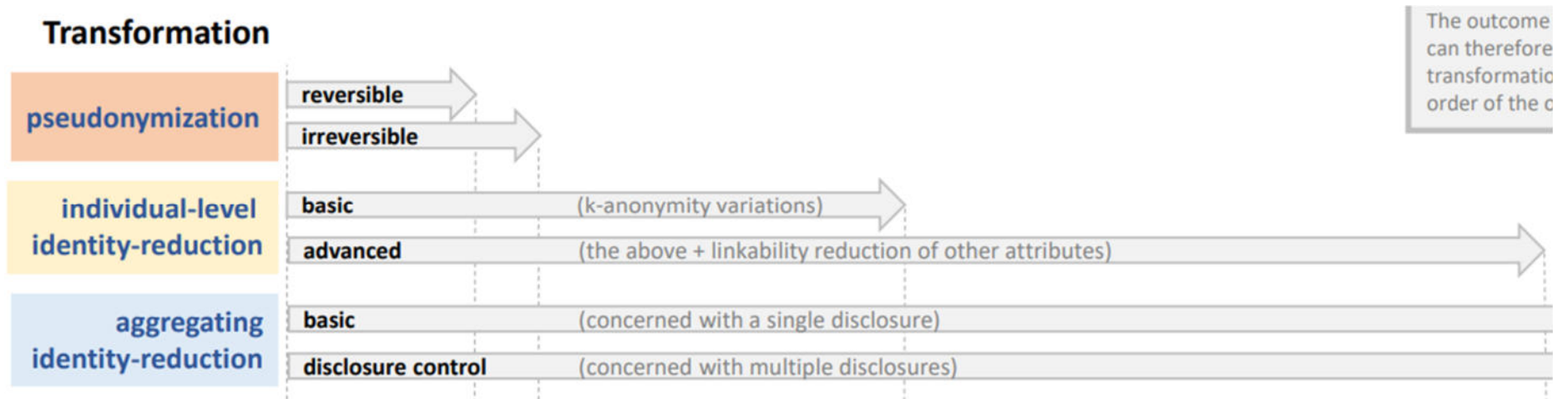
# ***Sekundärnutzung von Daten***

## ***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                                                                                                                                                                                    |
|-------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Fully Identified Personal Data</b>                                                                                         | <ul style="list-style-type: none"><li>• <b>direct identification</b> is possible (since data is unchanged)</li></ul>                                                                                                    |
| <b>(Basic) Pseudonymous Data</b><br><i>personal data</i> (Recital 26 GDPR)                                                    | <ul style="list-style-type: none"><li>• direct identification is no longer possible</li><li>• <b>only indirect identification</b> using <b>additional information</b> is possible</li></ul>                             |
| <b>Advanced Pseudonymous Data</b><br><i>likely still personal data</i>                                                        | <ul style="list-style-type: none"><li>• direct identification is no longer possible</li><li>• <b>even indirect identification</b> is rendered <b>difficult</b> or <b>prevented</b> (but with unknown success)</li></ul> |
| <b>Supposedly Anonymous Data</b><br><i>likely anonymous</i><br><i>but future re-identification cannot be excluded</i>         | <ul style="list-style-type: none"><li>• <b>all relevant known re-identification attacks are excluded</b></li><li>• <b>thorough assessment of re-identification risk</b> results in low risk</li></ul>                   |
| <b>Successfully Anonymous Data</b><br><i>certainly anonymous</i><br><i>future practical re-identification can be excluded</i> | <ul style="list-style-type: none"><li>• <b>re-identification can be practically<sup>[1]</sup> excluded</b></li><li>• strong guarantees or thorough assessment of re-identification risk</li></ul>                       |

[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                                                                                                                                                              |
|-------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Fully Identified Personal Data</b>                                                                                         | <ul style="list-style-type: none"><li>• <b>direct identification</b> is possible (since data is unchanged)</li></ul>                                                                              |
| <b>(Basic) Pseudonymous Data</b><br><i>personal data</i> (Recital 26 GDPR)                                                    | <ul style="list-style-type: none"><li>• direct identification is no longer possible</li><li>• <b>only indirect identification</b> using <b>additional information</b> is possible</li></ul>       |
| <b>Advanced Pseudonymous Data</b><br><i>likely still personal data</i>                                                        | <ul style="list-style-type: none"><li>• direct identification is no longer possible</li><li>• <b>even indirect identification</b> is possible (but with additional information)</li></ul>         |
| <b>Supposedly Anonymous Data</b><br><i>likely anonymous</i><br><i>but future re-identification cannot be excluded</i>         | <ul style="list-style-type: none"><li>• <b>thorough assessment</b> of re-identification risk is required</li></ul>                                                                                |
| <b>Successfully Anonymous Data</b><br><i>certainly anonymous</i><br><i>future practical re-identification can be excluded</i> | <ul style="list-style-type: none"><li>• <b>re-identification can be practically<sup>[1]</sup> excluded</b></li><li>• strong guarantees or thorough assessment of re-identification risk</li></ul> |

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

[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.

Quelle: [https://www.datenschutzzentrum.de/uploads/projekte/anomed/Identity-Reduction\\_v0\\_9\\_2.pdf](https://www.datenschutzzentrum.de/uploads/projekte/anomed/Identity-Reduction_v0_9_2.pdf)



## ***Wiederholung***

Wer ist zuständig und haftet im Forschungsverbund wenn mehrere Institute beteiligt sind und ggf. leicht unterschiedliche Forschungsschwerpunkte setzen?

**Gemeinsame Verantwortlichkeit**, wenn zwei oder mehr Stellen die Zwecke und Mittel der festlegen.

- Typisch für moderne Verbundforschung
- „Joint Controller Agreement“ ist notwendig, das bestimmt:
  - Wer erfüllt welche Pflichten der DSGVO
  - Wer informiert die Patienten? Wer bearbeitet Auskunftersuchen? Wer meldet Datenpannen?
  - Transparenz: Die wesentlichen Punkte dieser Vereinbarung müssen den Patienten zur Verfügung gestellt werden (z. B. via Website oder Infoblatt).

Vergl. zur Abgrenzung Auftragsverarbeitung und Gemeins. Verantwortlichkeit Folien der Veranstaltung „Auftragsdatenverarbeitung“

# ***Wiederholungsfall***

## **Romanhandlung:**

In der Notaufnahme legt der Arzt das OP-Besteck beiseite, blickt kurz auf die Wunden und sagt zum OP-Pfleger: *„Das sind Messerstiche und die Kugel ist vermutlich Kaliber .22. Bereiten Sie bitte das Meldeformular für die Polizei vor.“* In welchem Klinikum spielt dieser Fall?

- **Antwort: Jedenfalls nicht in Deutschland**

In den meisten US-Bundesstaaten ist eine Meldung solcher Verletzungen an die Polizei gesetzlich vorgeschrieben. Ein Unterlassen kann dort sogar strafbar sein.

- In Deutschland gilt dagegen:

- **§ 203 StGB**, Offenbarungsbefugnis fehlt
- **DSGVO Art. 9**, keine Grundlage für die Übermittlung
- Erforderliche **spezialgesetzliche** Ermächtigung fehlt

- Klinik darf zur Anzeige raten und anbieten, die Polizei zwecks Aufnahme der Anzeige zu rufen.

# ***Weiterführende Quellen Forschungsdatenschutz***

- Europäischer Datenschutzausschuss (EDSA), „Guidelines 1/2026 on processing of personal data for scientific research purposes“, 2026, [https://www.edpb.europa.eu/public-consultations/guidelines-12026-on-processing-of-personal-data-for-scientific-research\\_en](https://www.edpb.europa.eu/public-consultations/guidelines-12026-on-processing-of-personal-data-for-scientific-research_en)
- Datenschutzkonferenz (DSK), „Petersberger Erklärung zu datenschutzkonformen Verarbeitung von Gesundheitsdaten in der wissenschaftlichen Forschung“, November 2022  
[https://www.datenschutzkonferenz-online.de/media/en/20221124\\_en\\_06\\_Entschliessung\\_Petersberger\\_Erklaerung.pdf](https://www.datenschutzkonferenz-online.de/media/en/20221124_en_06_Entschliessung_Petersberger_Erklaerung.pdf)
- 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/>



# Herzlichen Dank für die gemeinsame Diskussion



Kontakt:

Harald Zwingelberg

uld6@datenschutzzentrum.de

[www.datenschutzzentrum.de](http://www.datenschutzzentrum.de)

0431/988-1222



AnoMed

PRiMA



Gefördert durch:



Bundesministerium  
für Forschung, Technologie  
und Raumfahrt



Funded by  
the European Union