CHARITÉ
UNIVERSITÄTSMEDIZIN BERLIN

Grundlagen des Datenschutzes in medizinischen Forschungsvorhaben

GB Governance, Compliance
und Datenschutz

Abteilung behördl. Datenschutzbeauftragte | 27.03.2025
Dr. Grit Zimmermann

Ziel der Veranstaltung

- Erlangen eines **Grundverständnisses** für die in medizinischen Forschungsvorhabens relevanten Fragen des Datenschutzes
- **Sensibilisierung** für datenschutzkritische Verarbeitungen und Aufzeigen erforderlicher Maßnahmen durch den Verantwortlichen bzw. Folgen bei Unterlassen
- Hilfe zur **Selbsthilfe**
- Überblick über die von dem Verantwortlichen **zu treffenden datenschutzrechtliche Maßnahmen** vor Beginn, während und nach Ende des Forschungsprojektes
- Möglichkeit für **Ihre Fragen**

Agenda

1. Einführung und Verantwortlichkeit für die Verarbeitung personenbezogener Daten
2. Personenbezogene, pseudonymisierte und anonyme Daten
3. Grundsätze des Datenschutzes – Gewährleistungsziele
4. Zulässigkeit der Datenverarbeitung: Rechtsgrundlagen und informierte Einwilligung
5. Rechte der von der Verarbeitung betroffenen Personen
6. Vorliegen und Umgang mit Datenschutzverletzungen („Datenpannen“/“Databreaches“)
7. Datenschutzrechtliche Dokumentation
8. Zusammenfassung

1

Einführung und Verantwortlichkeit für die Verarbeitung personenbezogener Daten

Datenschutz in medizinischen Forschungsvorhaben

Sicht der Betroffenen

Gesundheitsdaten sind sensibel und wecken Begehrlichkeiten bei vielen Akteuren.

- Mögliche **Gefahr bei der Verarbeitung**: unbefugte Weitergabe und Verarbeitung bzw. Verlust der sensiblen Daten
- Mögliche **Folgen** für Betroffene:
  - → Irreversible Schädigungen in gesellschaftlichem Ansehen und Fortkommen
  - → Existentiell bedrohliche Schädigungen durch Erpressung, Ausschluss bei Arbeitsverträgen oder Versicherungsverträgen
  - → Finanzielle Schäden
  - → Probleme für die gesamte Familie (z. B. in Bezug auf Daten zu genetischen Anlagen oder privaten Informationen)
  - → Psychische Schädigungen, Mobbing, Scham
  - → KI: Diskriminierung oder falsche Ergebnisse/Schlussfolgerungen insbesondere bei der Behandlung

- **Betroffene** sollen möglichst **Kontrolle über ihre Daten haben**, insbesondere durch:
  - → Transparenz vor und während der Datenverarbeitung (Information, Auskunftsrecht), auch über Art der Generierung von Ergebnissen (“KI”)
  - → Intervenierbarkeit (Widerruf und Widerspruch, Löschen/Sperren)
  - → Kenntnis zu Ansprechpartnern und Rechtsmitteln

Verantwortlichkeit - Studienleitung/Kooperationspartner

Definition

Grundsatz (Art. 4 DS-GVO):

Jede:r der:die allein oder gemeinsam mit anderen über die Verarbeitung der Daten entscheidet:

- Forscher, Forscherteam, gemeinsam mit Sponsor oder Kooperationspartnern, ←→ nicht: Weisungsgebundene Auftragsverarbeitung Diensleister

In Kooperationen Art. 26 DS-GVO "gemeinsame Verarbeitung":

→ Klären: gemeinsam oder getrennt (nacheinander unabhängige Verarbeitung)

→ Abgrenzung der Verantwortungssphären über Verträge

→ Wahrung der Rechte der Betroffenen: Prüf-Team/Studienleitung in Team haben die IDAT und sind alleiniger Ansprechpartner für Teilnehmende auch dann, wenn nicht direkt an der Beforschung der Gesundheitsdaten beteiligt

→ Gesamtschuldnerische Haftung bei Datenpannen oder nicht rechtmäßiger Verarbeitung gegenüber Allgemeinheit (DS-Behörde) und Betroffenen (Wahlrecht des Gläubigers), nach innen Regressansprüche nach Grad des Verschuldens (Absicht, grobe Fahrlässigkeit) Ausgleich im Innenverhältnis vertraglich regeln

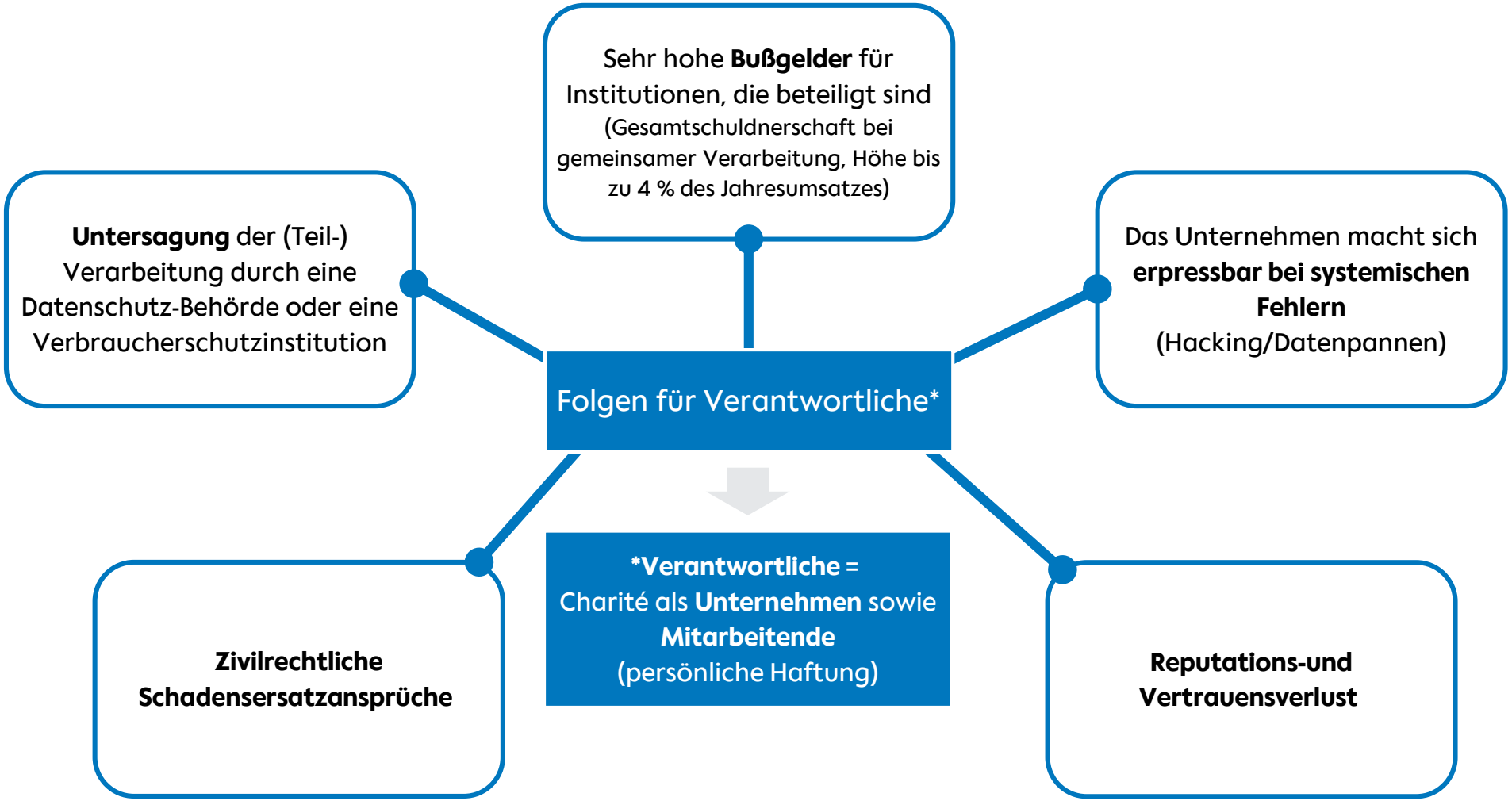
Wie weit reicht die Verantwortlichkeit der Studienleitung?

Beispiel Einsatz von durch Anbieter bereitgestellter Technologie (Apps, Wearables, KI-Algorithmen, Clouds):

- **Irrtum:** das geht den Studienleiter nichts an
- **Richtig**: die Studienleitung ist **(mit)verantwortlich**, vor allem
  - → für die Aufklärung über den vollständigen Datenfluss, ggf. auch über besondere Risiken (KI, Ausleitung von Daten)
  - → die darauf basierende Einwilligung und
  - → für die rechtmäßige Erhebung und Verarbeitung der Daten auch durch den Anbieter der Technologie (vgl. Jahresbericht Berliner BDI 2017, Bl. 99 ff, https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/jahresbericht/BlnBDI-Jahresbericht-2017-Web.pdf)
- Folgendes sollte für **alle** klargestellt sein:
  - → Datenfluss und Zugriffe aller Beteiligten, damit das Prüfteam den Teilnehmenden aufklären kann
  - → Bestimmtheit/Zweckbindung – möchte Anbieter Daten zu weiteren Zwecken, klare Abgrenzung in der Information/Einwilligung und konsistente Klarstellung in dem Vertrag, vor allem Umsetzung der Betroffenenrechte
  - → Nutzung private Endgeräte, Wearables: soweit Handeln des Teilnehmers zu spezifischen Risiken führt, ist das im DSK zu berücksichtigen und dem Teilnehmer kenntlich zu machen, Hinweis zu Voreinstellungen im Endgerät (Musterberufsordnung Ärzte, Deklaration von Helsinki, Transparenz – und Fairnessgebot Art. 5 DS-GVO)

Welche Folgen kann die Verletzung der datenschutzrechtlichen Regeln haben?

Sicht der Verantwortlichen/Unternehmen



2

Personenbezogene, pseudonymisierte und anonyme Daten

Personenbezogene Daten Allgemein

Definition

Daten sind personenbezogen, wenn:

1. ein direkter Bezug zu einer lebenden Person herstellbar ist.

   Hinweis: berufsrechtliche Schweigepflicht gilt über den Tod hinaus.

   → identifizierenden Daten: z.B. Name, Telefonnummer, Geburtsdatum, E-Mail-Adresse

   → Auch der Bezug zu einer identifizierbaren Gruppe kann personenbezogen sein, z. B. seltene Erkrankungen.

2. Indirekter Bezug, wenn mithilfe weiterer Informationen Rückschluss auf eine Person möglich ist.

   → Man spricht von pseudonymisierten Daten.

Daten sind nicht (mehr) personenbezogen wenn sie anonym sind, das heißt:

- ein Bezug zu einer Person(-engruppe) überhaupt nicht oder nur mit unverhältnismäßig hohem Aufwand erfolgt.
- Die Abgrenzung ist nicht immer einfach.
- Aufgrund der sich rasch entwickelnden Technologien in Biometrie und Genforschung **können sich die Bewertungen zur Anonymität oder ausreichender Pseudonymisierung ändern**.

Personenbezogene Daten in der med. Forschung - Teilnehmende

Identifizierende Daten (IDAT) – in der Regel nicht sensibel, erst in Kombination

- Name
- Geburtsdatum
- Anschrift
- Telefonnummer, E-Mail
- Patientennummer…

Forschungsdaten = i. d. R. sensibel (Art. 9 DS-GVO):

- Gesundheitsdaten, psychisch und physisch
- Weltanschauung, politische Überzeugung, Sexualität, ethnische Herkunft
- Sozioökonomische Daten wie z. B. Ausbildung oder Familie
- Genetische Daten und Biomaterial
- Biometrische Daten
- Bildgebendes Material, z. B. MRT und Röntgenbilder, Videos zum Gangbild, Bilder von Gesicht und Körperteilen
- Audiodaten bei Aufnahme der Stimme

Quellen/Erhebung:

- Klinisches Dokumentationssystem der Routinebehandlung
- Patient*in, Proband*in, Kooperationspartner, Verwandte, Wearables, Apps

Personenbezogene Daten in der med. Forschung - Mitarbeitende

- Name
- berufliche Kontaktdaten
- beruflicher Lebenslauf
- Ggf. Bilder

Diese Daten sind grundsätzlich **nicht** sensibel.

Aber: Sensibel ist die Verarbeitung und Weitergabe von/Zugriff auf **biometrische Daten** zum Beispiel zur 2-Faktor-Authentifizierung an Geräten bzw. zum Zugang zu Daten per Fingerprint oder Gesichtserkennung.

Biometrische Daten sind sensibel, Art. 9 Abs. 1 DS-GVO: Eine Einwilligung ist erforderlich.

- Ist diese Einwilligung im Arbeitsverhältnis freiwillig?
- Welche technisch-organisatorischen Maßnahmen sind zum Schutz der Mitarbeitenden erforderlich?
- Antwort: i.d.R. nicht freiwillig, daher Verarbeitung nur wenn erforderlich und verhältnismäßig, z. B. keine dauerhafte Speicherung, Weitergabe und Veröffentlichung, auch auf den Geräten, auf denen die Datenerhebung erfolgt

Personenbezogene Daten – Pseudonymisierung

Definition

Grundsatz Art. 4 Abs. 5 DS-GVO (zzgl. div. Erwägungsgründe)

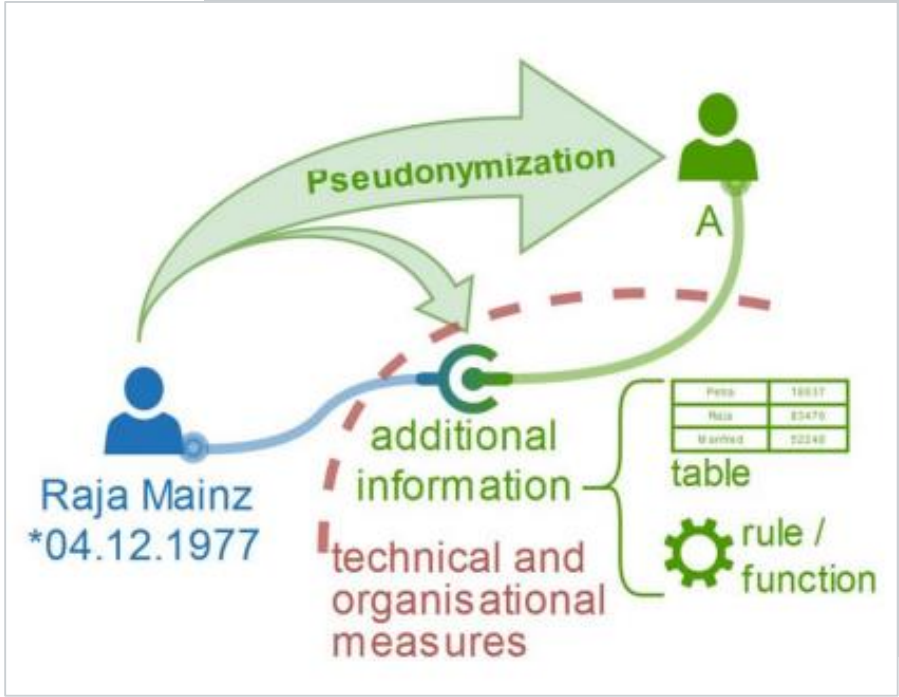
- personenbezogenen Daten können ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person oder Gruppe zugeordnet werden (Stichwort seltene Erkrankungen)

  → sofern diese zusätzlichen Informationen/Zuordnungsregel (Re-Identifizierungsliste) gesondert aufbewahrt werden

  UND

  → technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.

- **Fazit:** Pseudonymisierte Forschungsdaten sind personenbezogen, der Bezug wird lediglich erschwert (=TOM).



Quelle: https://www.datenschutzzentrum.de/uploads/vortraege/20190910_DiWoKi_Pseudonymisierung_Walczak.pdf

Personenbezogene Daten – Pseudonymisierung

Anforderungen

- Anforderungen an ein **wirksames Pseudonym**

  → kein Rückschluss auf Person/spezifische Gruppe ermöglichen: z. B. über Geburtsdatum, Initialen, Krankheitsgruppe.

  → Standard: randomisierte Pseudonymisierung, z. B. per Software

  → Pseudonym zusammen mit identifizierenden Daten auf einer getrennten Liste/Datei, die besonders sicher mit starken Zugriffsbeschränkungen zu verwahren ist (Need-to-know-Prinzip, i. d. R. Studienleitung und im DSK benannte Personen).

  → Die Pseudonymisierung darf nicht durch falsche Handhabung der Betroffenenanfragen aufgeweicht werden. → Nur wer identifizieren darf, sollte Kontakt mit den Betroffenen haben.

- Das **Verfahren** des Pseudonymisierung **ist im DSK/DSFA zu beschreiben**. Je sensibler die Daten, desto höher die Anforderungen an den Pseudonymisierungsgrad.

ID	Pseudonym (self-chosen)	Pseudonym (numbered)	Pseudonym (random)
Petra Agridou *13.11.1972	MickeyMouse	56483	18637
Raja Mainz *04.12.1977	Tux_0412	56484	83476
Ramos Petrov *09.12.1981	Ramos_Petrov	56485	52248

Quelle: https://www.datenschutzzentrum.de/uploads/vortraege/20190910_DiWoKi_Pseudonymisierung_Walczak.pdf

Personenbezogene Daten – Anonym DS-GVO

Erwägungsgrund 26 DS-GVO

- anonym sind Informationen, „die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass **die betroffene Person nicht oder nicht mehr identifiziert werden kann**“.
- Das **Anonymisieren** stellt **eine Weiterverarbeitung** im Sinne von Art. 4 DS-GVO dar, da ein Löschen der identifizierenden Daten und z.B. ein Aggregieren von Daten (z.B. Bildung von Altersgruppen) erfolgt.
- Für die Anonymisierung **gelten die Erfordernisse der DS-GVO**, d. h. es ist ein Erlaubnistatbestand erforderlich: eine Rechtsgrundlage
- Hintergrund der Ansicht:

  → nach herrschender Meinung **sollen Betroffene auch darüber entscheiden, wer aus der Verarbeitung ihrer Daten Nutzen zieht**, z. B. relevant bei späterer kommerzieller Verwendung anonymer Daten.

  → Folge der Anonymisierung: Betroffene können ihre Rechte auf Löschung etc. nicht mehr geltend machen.

Personenbezogene Daten – Anonym international

Unterschiedliches Verständnis zu dem Begriff anonym im globalen Kontext:

Angloamerikanisch Empfängersicht: relativ anonym

- Anonymität ist bereits gegeben, wenn der Empfänger von Daten keinen Rückschluss auf die Person ziehen kann.

Europa Betroffenensicht: absolut anonym

- Daten sind erst anonym, wenn nach dem Stand der Technik (so gut wie) ausgeschlossen ist, dass weder Empfänger noch Dritte Rückschlüsse auf die Person oder eine identifizierbare Personengruppe ziehen kann.
- medizinische Forschung:
  - → i. d. R. wenn Re-Identifizierungsliste vernichtet wird, starkes Aggregieren der Daten vor Weitergabe zur Veröffentlichung, anders oft bei genetischen Daten und Bildgebung
  - → herrschende Ansicht: Biomaterialproben und Bilddaten lassen sich nicht zuverlässig anonymisieren, evtl. Bilder zerkleinern „ohne Rand“, verpixeln
  - → **erlaubter Mittelweg,** um die Forschung weniger zu blockieren: faktische Anonymisierung vor Weitergabe, Einbindung Datentreuhandstelle und Datenintegrationszentrum

Personenbezogene Daten – Pseudonymisierung vs. Anonymisierung

Warum keine Anonymisierung? Dann bestünden keine datenschutzrechtlichen Probleme (?)

- Eine zuverlässige Anonymisierung ist **oft nicht zu gewährleisten**, da genetische Daten oder bestimmte Datensätze ***verhältnismäßig*** **einfach zu re-identifizieren** und verknüpfbar sind (Stand der Technik).
- **Fortschritt der Technik**: Bewertungen zur Anonymität oder ausreichender Pseudonymisierung kann sich ändern
- Nach den **Regeln guter wissenschaftlicher Praxis** sind Originaldaten (IDAT) 10 Jahre nach Veröffentlichung der Daten aufzubewahren. Zuordnung zu Personen muss über Re-Identifizierungsliste = Personenbezug herstellbar bleiben.
- Arzneimittelrecht: **unerwünschte Nebenwirkungen** erfordern einen längerfristigen Personenbezug.

Ausblick:

- evtl. rechtssichere neue juristische Bewertung durch EuG - Urteil vom 26.4.2023 (Az: T-557/20), das erst durch EuGH zu bestätigen ist: Empfängersicht, wenn dieser keine legalen Mittel hat die Personen zu identifizieren
- NEU: §§ 7, 9 Gesundheitsdatennutzungsgesetz vom 26.3.2024: unerlaubtes Re-Identifizieren von Forschungsdaten strafbar

3

Grundsätze des Datenschutzes – Gewährleistungsziele

Grundsätze zum Schutz (personenbezogener) Daten

Datensparsamkeit/ Datenminimierung

Transparenz

Zweckbindung und Bestimmtheit

Spezialfall der Zweckbindung: Nichtverkettbarkeit

Richtigkeit der Daten

Speicherbegrenzung

Integrität und Vertraulichkeit

Verfügbarkeit

Rechenschaftspflicht: Der Verantwortliche muss nachweisen, dass er den Anforderungen der DS-GVO genügt. Hierzu ist eine entsprechende Dokumentation aller entsprechenden Vorgänge erforderlich.

Verantwortliche haben zu dokumentieren:

- Datenschutzkonzept gemäß Studiendesign
- Rechtsgrundlage, die jede Verarbeitungstätigkeit umfasst
- Information der Betroffenen **vor** Verarbeitung
- Einwilligung der Betroffenen **vor** Verarbeitung (nicht bei gesetzlicher Grundlage)
- Ggf. Verträge mit Partnern und Dienstleistern
- Eintrag in ein Verzeichnis von Verarbeitungstätigkeiten und ggf. in Vertragskataster (AVV)

4

Zulässigkeit der Datenverarbeitung: Rechtsgrundlagen und informierte Einwilligung

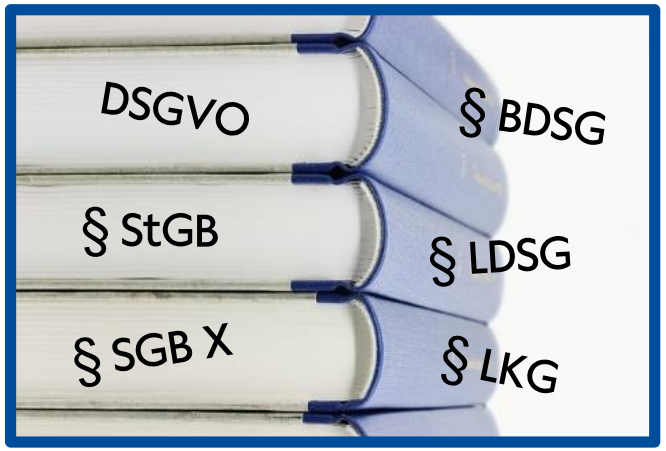
Zulässigkeit der Datenverarbeitung

Verbot mit Erlaubnisvorbehalt
Alles, was nicht ausdrücklich erlaubt ist, ist verboten.

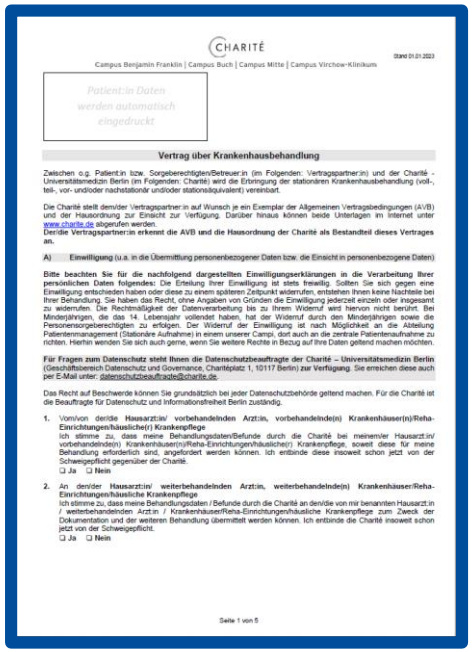
Grundlagen für die zulässige Datenverarbeitung:

Informations-pflichten bestehen immer!

Gesetzliche Grundlage



Einwilligung



CHARITÉ

Campus Benjamin Franklin | Campus Buch | Campus Mitte | Campus Virchow-Klinikum

Stand 01.01.2023

Patient:in Daten werden automatisch eingedruckt

Vertrag über Krankenhausbehandlung

Zwischen o.g. Patient:in bzw. Sorgeberechtigten/Betreuer:in (im Folgenden: Vertragspartner:in) und der Charité - Universitätsmedizin Berlin (im Folgenden: Charité) wird die Erbringung der stationären Krankenhausbehandlung (voll-, teil-, vor- und/oder nachstationär und/oder stationsäquivalent) vereinbart.

Die Charité stellt dem/der Vertragspartner:in auf Wunsch je ein Exemplar der Allgemeinen Vertragsbedingungen (AVB) und der Hausordnung zur Einsicht zur Verfügung. Darüber hinaus können beide Unterlagen im Internet unter www.charite.de abgerufen werden.
Der/die Vertragspartner:in erkennt die AVB und die Hausordnung der Charité als Bestandteil dieses Vertrages an.

A) **Einwilligung** (u.a. in die Übermittlung personenbezogener Daten bzw. die Einsicht in personenbezogene Daten)

Bitte beachten Sie für die nachfolgend dargestellten Einwilligungserklärungen in die Verarbeitung Ihrer persönlichen Daten folgendes: Die Erteilung Ihrer Einwilligung ist stets freiwillig. Sollten Sie sich gegen eine Einwilligung entschieden haben oder diese zu einem späteren Zeitpunkt widerrufen, entstehen Ihnen keine Nachteile bei Ihrer Behandlung. Sie haben das Recht, ohne Angaben von Gründen die Einwilligung jederzeit einzeln oder insgesamt zu widerrufen. Die Rechtmäßigkeit der Datenverarbeitung bis zu Ihrem Widerruf wird hiervon nicht berührt. Bei Minderjährigen, die das 14. Lebensjahr vollendet haben, hat der Widerruf durch den Minderjährigen sowie die Personensorgeberechtigten zu erfolgen. Der Widerruf der Einwilligung ist nach Möglichkeit an die Abteilung Patientenmanagement (Stationäre Aufnahme) in einem unserer Campi, dort auch an die zentrale Patientenaufnahme zu richten. Hierhin wenden Sie sich auch gerne, wenn Sie weitere Rechte in Bezug auf Ihre Daten geltend machen möchten.

Für Fragen zum Datenschutz steht Ihnen die Datenschutzbeauftragte der Charité – Universitätsmedizin Berlin (Geschäftsbereich Datenschutz und Governance, Charitéplatz 1, 10117 Berlin) **zur Verfügung.** Sie erreichen diese auch per E-Mail unter: datenschutzbeauftragte@charite.de.

Das Recht auf Beschwerde können Sie grundsätzlich bei jeder Datenschutzbehörde geltend machen. Für die Charité ist die Beauftragte für Datenschutz und Informationsfreiheit Berlin zuständig.

1. Vom/von der/die **Hausarzt:in/ vorbehandelnden Arzt:in, vorbehandelnde(n) Krankenhäuser(n)/Reha-Einrichtungen/häusliche(r) Krankenpflege**
   Ich stimme zu, dass meine Behandlungsdaten/Befunde durch die Charité bei meinem/er Hausarzt:in/ vorbehandelnden(n) Krankenhäuser(n)/Reha-Einrichtungen/häusliche(r) Krankenpflege, soweit diese für meine Behandlung erforderlich sind, angefordert werden können. Ich entbinde diese insoweit schon jetzt von der Schweigepflicht gegenüber der Charité.
   ❑ Ja ❑ Nein

2. An den/der **Hausarzt:in/ weiterbehandelnden Arzt:in, weiterbehandelnde(n) Krankenhäuser/Reha-Einrichtungen/häusliche Krankenpflege**
   Ich stimme zu, dass meine Behandlungsdaten / Befunde durch die Charité an den/die von mir benannten Hausarzt:in / weiterbehandelnden Arzt:in / Krankenhäuser/Reha-Einrichtungen/häusliche Krankenpflege zum Zweck der Dokumentation und der weiteren Behandlung übermittelt werden können. Ich entbinde die Charité insoweit schon jetzt von der Schweigepflicht.
   ❑ Ja ❑ Nein

Seite 1 von 5

Gesetzliche Zulässigkeit der Datenverarbeitung – retrospektiv ohne Einwilligung

Rechtsgrundlagen

Direkt: (nicht abschließend)

- Seit April 2024 § 6 Gesundheitsdatennutzungsgesetz (retrospektive Studien)
- Berlin: § 25 Bln. Krankenhausgesetz
- Bundesdatenschutzgesetz
- Landesdatenschutzgesetz
- Strahlenschutzverordnung (bes. Aufbewahrungsfrist, Einwilligung und Widerruf-Folgen)
- Arzneimittelverordnung und Medizinprodukte-Recht (MDR) (besondere Aufbewahrungsfrist, Einwilligung und Widerruf-Folgen)
- § 287 a SGB V
- Art. 9 Absatz 2, 89 Datenschutz-Grundverordnung (DS-GVO) = Rahmenwerk

Indirekt (eher allgemeine Vorgaben):

- Deklaration von Helsinki
- Berufsordnung der Ärzte (Musterberufsordnung)
- Verordnungen und ggf. Satzungen o. ä. zur guten wissenschaftlichen Praxis (GWP)

Wichtig: Eine **Information** über die Datenverarbeitung und die Rechte der Betroffenen ist auch dann **erforderlich, wenn keine Einwilligung notwendig ist**. In der Praxis erfolgt dies z.B. über den Behandlungsvertrag oder einen gut wahrnehmbaren Aushang.

Zulässigkeit der Datenverarbeitung

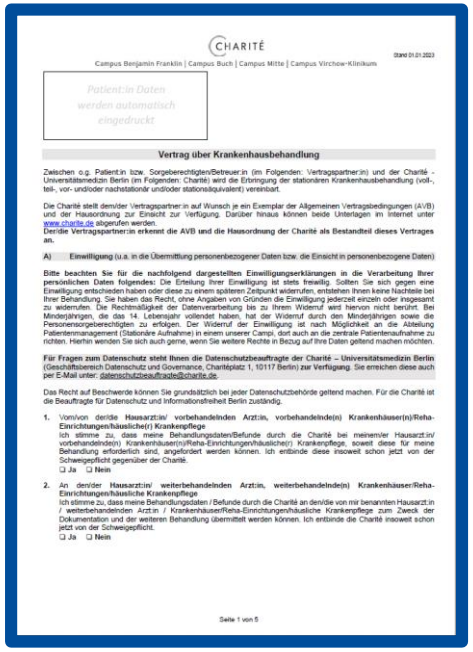
Die informierte Einwilligung

Verbot mit Erlaubnisvorbehalt
Alles, was nicht ausdrücklich erlaubt ist, ist verboten.

Grundlagen für die zulässige Datenverarbeitung:

Gesetzliche Grundlage

Einwilligung



CHARITÉ

Campus Benjamin Franklin | Campus Buch | Campus Mitte | Campus Virchow-Klinikum

Stand 01.01.2023

Patient:in Daten werden automatisch eingedruckt

Vertrag über Krankenhausbehandlung

Zwischen o.g. Patient:in bzw. Sorgeberechtigten/Betreuer:in (im Folgenden: Vertragspartner:in) und der Charité - Universitätsmedizin Berlin (im Folgenden: Charité) wird die Erbringung der stationären Krankenhausbehandlung (voll-, teil-, vor- und/oder nachstationär und/oder stationsäquivalent) vereinbart.

Die Charité stellt dem/der Vertragspartner:in auf Wunsch je ein Exemplar der Allgemeinen Vertragsbedingungen (AVB) und der Hausordnung zur Einsicht zur Verfügung. Darüber hinaus können beide Unterlagen im Internet unter www.charite.de abgerufen werden.
Der/die Vertragspartner:in erkennt die AVB und die Hausordnung der Charité als Bestandteil dieses Vertrages an.

A) Einwilligung (u.a. in die Übermittlung personenbezogener Daten bzw. die Einsicht in personenbezogene Daten)

Bitte beachten Sie für die nachfolgend dargestellten Einwilligungserklärungen in die Verarbeitung Ihrer persönlichen Daten folgendes: Die Erteilung Ihrer Einwilligung ist stets freiwillig. Sollten Sie sich gegen eine Einwilligung entschieden haben oder diese zu einem späteren Zeitpunkt widerrufen, entstehen Ihnen keine Nachteile bei Ihrer Behandlung. Sie haben das Recht, ohne Angaben von Gründen die Einwilligung jederzeit einzeln oder insgesamt zu widerrufen. Die Rechtmäßigkeit der Datenverarbeitung bis zu Ihrem Widerruf wird hiervon nicht berührt. Bei Minderjährigen, die das 14. Lebensjahr vollendet haben, hat der Widerruf durch den Minderjährigen sowie die Personensorgeberechtigten zu erfolgen. Der Widerruf der Einwilligung ist nach Möglichkeit an die Abteilung Patientenmanagement (Stationäre Aufnahme) in einem unserer Campi, dort auch an die zentrale Patientenaufnahme zu richten. Hierhin wenden Sie sich auch gerne, wenn Sie weitere Rechte in Bezug auf Ihre Daten geltend machen möchten.

Für Fragen zum Datenschutz steht Ihnen die Datenschutzbeauftragte der Charité – Universitätsmedizin Berlin (Geschäftsbereich Datenschutz und Governance, Charitéplatz 1, 10117 Berlin) **zur Verfügung.** Sie erreichen diese auch per E-Mail unter: datenschutzbeauftragte@charite.de.

Das Recht auf Beschwerde können Sie grundsätzlich bei jeder Datenschutzbehörde geltend machen. Für die Charité ist die Beauftragte für Datenschutz und Informationsfreiheit Berlin zuständig.

1. Vom/von der/die **Hausarzt:in/ vorbehandelnden Arzt:in, vorbehandelnde(n) Krankenhäuser(n)/Reha-Einrichtungen/häusliche(r) Krankenpflege**
   Ich stimme zu, dass meine Behandlungsdaten/Befunde durch die Charité bei meinem/er Hausarzt:in/ vorbehandelnden(n) Krankenhäuser(n)/Reha-Einrichtungen/häusliche(r) Krankenpflege, soweit diese für meine Behandlung erforderlich sind, angefordert werden können. Ich entbinde diese insoweit schon jetzt von der Schweigepflicht gegenüber der Charité.
   ❑ Ja ❑ Nein

2. An den/der **Hausarzt:in/ weiterbehandelnden Arzt:in, weiterbehandelnde(n) Krankenhäuser/Reha-Einrichtungen/häusliche Krankenpflege**
   Ich stimme zu, dass meine Behandlungsdaten / Befunde durch die Charité an den/die von mir benannten Hausarzt:in / weiterbehandelnden Arzt:in / Krankenhäuser/Reha-Einrichtungen/häusliche Krankenpflege zum Zweck der Dokumentation und der weiteren Behandlung übermittelt werden können. Ich entbinde die Charité insoweit schon jetzt von der Schweigepflicht.
   ❑ Ja ❑ Nein

Seite 1 von 5

Zulässigkeit der Datenverarbeitung

Informierte Einwilligung - **Informationserfordernisse**

- Damit die Einwilligung wirksam ist, sind die Betroffenen **VOR** der Verarbeitung ihrer Daten in **transparenter einfacher laienverständlicher** Weise zu **informieren** (Art. 5,13 ff. 26 DS-GVO) über:

die **gesamte geplante Verarbeitung** ihrer Daten und ggf. Proben inklusive Technologie

die **Zwecke, Rechtsgrundlagen**, die **Empfänger** der Daten sowie die Angabe, ob diese einem **angemessenen Datenschutzniveau** unterliegen oder nicht (bei nein sind die Risiken und mögl. Folgen zu benennen) – gern kurz und prägnant

Risiken, die bei der Verarbeitung der Daten bestehen (z.B. genetische Daten, Bilddaten etc.)

Ansprechpartner, Verantwortlicher, ggf. Datenschutzbeauftragte (Briefkopf)

die **Form der Zusammenarbeit der Verantwortlichen** z. B. gemeinsame oder getrennte Verarbeitung, ggf. Auftragsverarbeitung

die **Aufbewahrungsfrist** bzw. Kriterien, nach denen sich die Aufbewahrung richtet

die **Rechte der Betroffenen** einschließlich Beschwerderecht

Andere Zwecke als für die Erhebung z. B. beabsichtigte Nutzung für **zukünftige Forschung**: genauere Angaben, unter welchen Bedingungen Daten weitergebeben werden, Informationsmöglichkeit für die Betroffenen

Zulässigkeit der Datenverarbeitung

Informierte Einwilligung – Umfang und Art

- Die Einwilligung sollte sich bezüglich allgemeiner Verarbeitung ausdrücklich auf die Information beziehen („Wie in der Studieninformation angegeben“).
- Spiegelung der Rechte der Betroffenen durch Bestätigung der Kenntnis
- Eine **gesonderte** Einwilligung (Opt-in) **für verschiedene Zwecke** ist erforderlich, bei **besonders risikoträchtigen Verarbeitungen** oder **solchen, die über die eigentliche Studie hinausgehen** wie z. B:
  - → Weitergabe in ein Drittland ohne angemessenes Datenschutzniveau
  - → Weitergabe von Daten oder Biomaterial an Biobanken oder Register (diese sind in der Information näher zu beschreiben)
  - → Nutzung der Daten zu Zwecken zukünftiger Forschung
  - → Weitergabe der Daten an behandelnde Ärzte oder Einbeziehung der Informationen von dort (Entbindung von der Schweigepflicht, Widerruflichkeit)
- Spiegelung der Risiken und Folgen bei risikoreichen Verarbeitungen durch Bestätigung der Kenntnis

Ich willige ein in **Zweck 1 ….**
☐ Ja ☐ Nein

Ich willige ein in **Zweck 2 ….**
☐ Ja ☐ Nein

…

Ich willige ein in **Zweck X …. Mir ist bekannt, dass…**
☐ Ja ☐ Nein

Zulässigkeit der Datenverarbeitung

Informierte Einwilligung - **Leicht zu vermeidende Fehler bei der Information und der Einwilligung:**

- Die **Information** zur Datenverarbeitung ist **zu lang**, evident überflüssige Inhalte, **lückenhaft oder unverständlich** und gibt nicht bzw. **nicht transparent** die geplante Datenverarbeitung wieder, insbesondere bei Weitergaben an Externe und Verarbeitung mit IT-Technologie.
- Die **Reihenfolge** der Darstellung ist **unlogisch bzw. verwirrend**.
- Es sind **fernliegende oder nicht zutreffende Informationen** enthalten, wie z. B. zu Rechtsgrundlagen oder bestimmte **Zusicherunge**n, die nicht objektiv nachprüfbar sind.
- Die **Angaben zu den Betroffenenrechten** bzw. deren Einschränkungen oder zu den Ansprechpartnern **fehlen**.
- Wesentliche Datenverarbeitungen sind in der Einwilligung **nicht** als **Opt-in** („Ja“) ausgestaltet.
- Für die Wahrnehmung der Rechte der Betroffenen ist allein ein **unberechtigter Ansprechpartner** benannt, also eine Person, die **kein Recht hat identifizierende Daten einzusehen** bzw. eine Verknüpfung mit den identifizierenden Daten vorzunehmen.

5

Rechte der betroffenen Personen

Rechte von der Verarbeitung betroffene Personen

Ansprechpartner sollte stets die Institution sein, die identifizieren darf. Das ist bei dem Design, in den Verträgen und DS-Konzepte/SOP von Beginn an spiegelbildlich sicherzustellen.

Recht auf Information Art. 5, 13, 14 DS-GVO (Angehörige, Erbkrankheiten)

→ auch bei nicht erforderlichen Einwilligung bei retrospektiver Forschung

Recht auf Widerruf der Einwilligung z.B. Art. 7 DS-GVO

→ Hinweis: auch bei AMG-Studien, dann eingeschränkte Weiterverarbeitung aus den in § 40b Abs. 6 Nr. 2 AMG .F. angegebenen Gründen. Es ist zu prüfen, welche Daten für die Zwecke erforderlich sind, der Rest ist zu löschen.

Recht auf Widerspruch Art. 21 DS-GVO

→ anstelle des Rechts auf Widerruf, wenn die Verarbeitung ohne Einwilligung aufgrund öffentlichen Interesses oder berechtigtem Interesse erfolgt

Recht auf Auskunft und kostenlose Kopie Art. 15 DSGVO

→ restriktive Ausnahme: zu hoher Aufwand

Recht auf Berichtigung Art. 16 DSGVO

Recht auf Löschen/Anonymisierung Art. 17 DSGVO

→ wenn rechtswidrige Verarbeitung (unwirksame Einwilligung), im Fall eines Widerrufs wenn keine anderweitige Rechtgrundlage gegeben oder wenn die Daten sind nicht mehr erforderlich zu dem Zweck, zu dem sie erhoben worden sind

→ Ausnahme möglich, wenn durch Löschen das Forschungsvorhaben vereitelt oder ernsthaft beeinträchtigt wird (Art. 17 Abs. 3 DS-GVO)

Recht auf Einschränkung der Verarbeitung Art. 18 DSGVO

Recht auf Datenübertragbarkeit Art. 20 DSGVO

→ = Datenübertragbarkeit im maschinenlesbaren Format

→ ermöglicht die Mitnahme von Daten, die aufgrund aktiven Handelns erteilt wurden (auf Basis der Einwilligung, Ausfüllen von Fragebögen, Eingabe von Daten auf Apps und mobile device), relevant z.B. bei gewünschter Mitnahme der Daten mit zum behandelnden Arzt

Recht auf Information bei „Data Breaches“ mit vss. hoher Gefährdung (Art. 34 DS-GVO)

→ Pflicht des Verantwortlichen zur Meldung von Pannen gegenüber der DS-Behörde für alle Verantwortlichen innerhalb von 72 Stunden, wenn Gefährdung Betroffener nicht auszuschließen ist

6

Datenschutzverletzungen („Datenpannen“/“Data-Breaches“)

Datenschutzverletzungen – wann liegt die vor?

Eine Datenpanne kann in jeder Verletzung der Gewährleistungsziele bestehen!

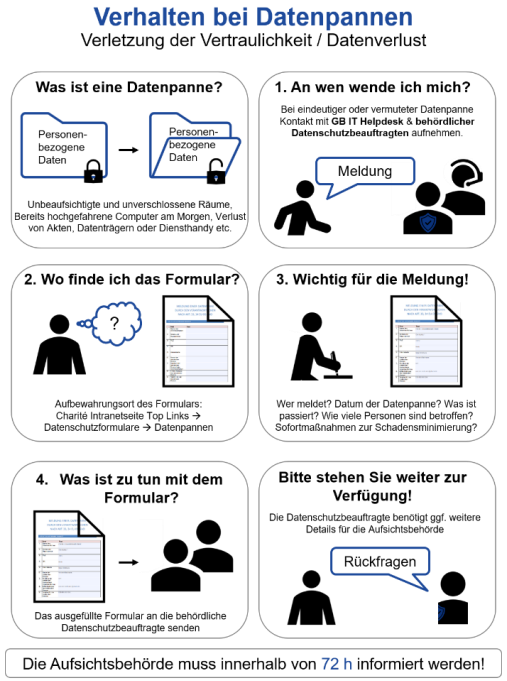
Typische Praxisbeispiele:

- Diebstahl Verlust von Datenträgern – betrifft Verfügbarkeit, Vertraulichkeit, ggf. Nichtverkettbarkeit – Unerlaubte Re-Identifizierung von Personen
- Hacking von PC oder Endgeräten - betrifft Vertraulichkeit, Integrität, Nichtverkettbarkeit, Authentizität, Transparenz, Zweckbindung, Transparenz
- Unkontrollierte oder unverschlüsselte Weiterleitung oder Manipulation von Daten – betrifft Schutzziele Vertraulichkeit, Integrität, Zweckbindung, Rechtmäßigkeit und Transparenz
- Papierbasiert: Versehentlich falscher Adressat mit Gesundheitsdaten – betrifft Zweckbindung, Rechtmäßigkeit, Vertraulichkeit

Datenschutzverletzungen – Regelungen im Unternehmen (Beispiel)

Datenschutzvorfall

Meldung an Zentrale Stelle und Vorgesetzte
(je nach Richtlinie oder Unternehmensregeln)



Charité:
Datenschutzbeauftragte
(ggf. IT Helpdesk)

Rechtliche Prüfung –
Meldung an

- Berliner Datenschutz-behörde (72 h Frist)[1]
- Verantwortlicher
- Betroffener[2]

Unverzüglich zu ergreifende Maßnahmen zur Schadens- und Risikominimierung
wie z. B. neues Schloss, neues Passwort, Auffordern des falschen Empfängers, elektronisch erhaltene Daten zu löschen (frankierter Rückumschlag für die Zusicherung), Fernsperrung von Endgeräten, ferner Ursachenforschung und Behebung wenn möglich, Rechte- und Rollen-Konzept prüfen.

[1]**Meldepflicht** gegenüber der **Datenschutzaufsichtsbehörde** innerhalb von 72 Stunden i. d. R. über Datenschutzbeauftragten

[2]**Informationspflicht** gegenüber dem **Betroffenen** wenn Gefährdung wahrscheinlich, kann von Behörde ggf. verlangt werden, wenn abweichende Einschätzung

7

Datenschutzrechtliche Dokumentation

Datenschutzrechtliche Dokumentation

Verzeichnis von Verarbeitungstätigkeiten
VVT
(Art. 30 DSGVO)

Datenschutzkonzept/
Datenschutzfolgenabschätzung

Datenschutzrechtliche Dokumentation

Verzeichnis über Verarbeitungstätigkeiten VVT (Art. 30 DSGVO)

Verzeichnis von Verarbeitungstätigkeiten
VVT
(Art. 30 DSGVO)

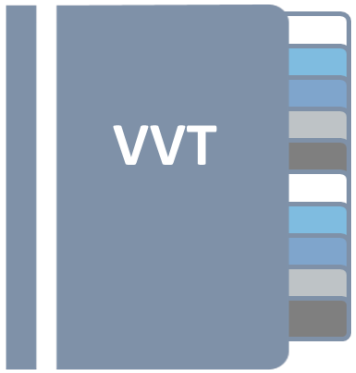
- **Jeder Verantwortliche** hat Datenverarbeitungen in ein Verfahrensverzeichnis einzutragen.
- VVT dient der
  - → **Selbstkontrolle** des Unternehmens,
  - → der **Dokumentation** der Datenverarbeitung sowie
  - → der **Kontrolle durch die Datenschutzbehörde**.
- In Auftragsverarbeitungsverhältnissen und in Kooperationen mit gemeinsamer Verantwortung muss jeder Partner in sein Verzeichnis eintragen.

Mindestinhalte gemäß Art. 30 DS-GVO

- Namen und Kontakt des Verantwortlichen
- Zwecke der Verarbeitung
- Kategorien der betroffenen Personen und verarbeiteten Daten
- Kategorien der Empfänger einschließlich in Drittländern oder internationalen Organisationen, hierbei Dokumentation der geeigneten Garantien
- Löschfristen der verschiedenen Datenkategorien
- Beschreibung der technisch - organisatorischen Maßnahmen (TOM)

Datenschutzrechtliche Dokumentation

Verzeichnis von Verarbeitungstätigkeiten
VVT
(Art. 30 DSGVO)



Datenschutzkonzept/
Datenschutzfolgenabschätzung

Datenschutzrechtliche Dokumentation

Datenschutzkonzept/Datenschutzfolgenabschätzung

Datenschutzkonzept/
Datenschutzfolgenabschätzung

- DSK begründet die **Erforderlichkeit** und **Angemessenheit** der Vorgehensweise des med. Forschungsvorhabens und beschreibt **alle Maßnahmen**, die zum wirksamen Schutz der Persönlichkeitsrechte beitragen
- **Verantwortlichkeit** zur Erstellung und Aktualität liegt bei den **Projekt-/Studienleitenden**
- Die DS-GVO bzw. Datenschutzgesetze sehen keine Formatvorlage vor, Anlehnung an DSFA Klinische Verfahren, werden auf Studien angepasst
  - → wichtig: Darstellung muss übersichtlich und logisch sein, Sicherstellung der Transparenz
- **Unterschied zwischen Datenschutzkonzept und DSFA**: Inhaltlich gering, in beiden ist die Datenverarbeitung zu beschreiben. DSFA sieht Einbindung der:s DSB vor (Art. 35 DS-GVO) - daher Stellungnahme Prozess sichern, zeitlich einplanen für besonders risikoreiche Prozesse oder Einsatz neuer Technologien

Datenschutzkonzept/ Datenschutzfolgenabschätzung (DSFA)

Inhalte aus der Praxis

Begründung der **Erforderlichkeit/Zweck**: welches Forschungsziel soll erreicht werden und welche Datensammlungen sind dazu notwendig.

Beschreibung der **Angemessenheit:** warum kann das Forschungsziel nur auf diese Weise und nicht mit geringeren Eingriffen in Persönlichkeitsrechte erreicht werden kann. Eine **Abwägung** der Angemessenheit der Schutzmaßnahmen ist vorzunehmen: u.a. Begründung, an welchen Stellen Daten personenbezogen vorliegen müssen, wo Pseudonymisierung angemessen ist und wo anonymisierte Daten ausreichen.

Beschreibung der **Verantwortlichkeit und Zuständigkeiten** im Projekt inkl. **Verträge** sowie der **Rechtsgrundlagen**

Beschreibung der **betroffenen Personen** (sind Minderjährige, Personen mit eingeschränkter Willensbildung betroffen?)

Beschreibung der **Daten und Datenkategorien** sowie der **Empfänger/Weitergabe** (intern, extern)

Beschreibung des **Datenflusses** und der **Prozesse** einschließlich der Verarbeitung über Technologie und Weitergabe an Empfänger (bestimmter Datenkategorien), Einsichtsrechte, **von der Erhebungsquelle bis zum Löschen/Anonymisieren**

Beschreibung der **eingesetzten Systeme**

Beschreibung der **Speicher- und Aufbewahrungsorte** während der Projektlaufzeit und nach Beendigung des Projekts sowie die **Dauer** und deren Rechtsgrundlagen

Evaluierung von **Risiken** für die Freiheiten sowie Rechte der Betroffenen

Beschreibung der **Maßnahmen** zum Nachweis der Wirksamkeit des Schutzes von Persönlichkeitsrechten: umfasst **organisatorische Regelungen und technische Maßnahmen zur IT-Sicherheit**.

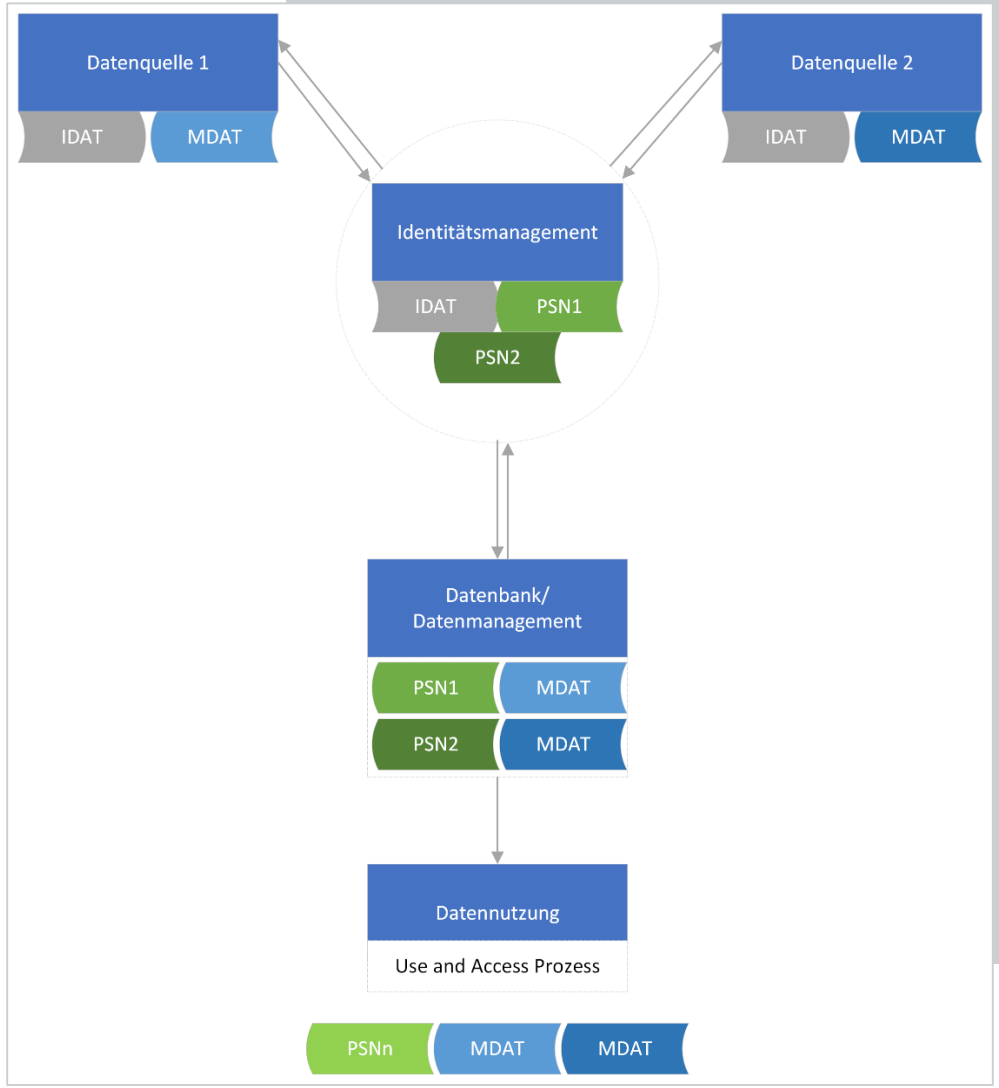
Typische TOM I

Informationelle Gewaltenteilung

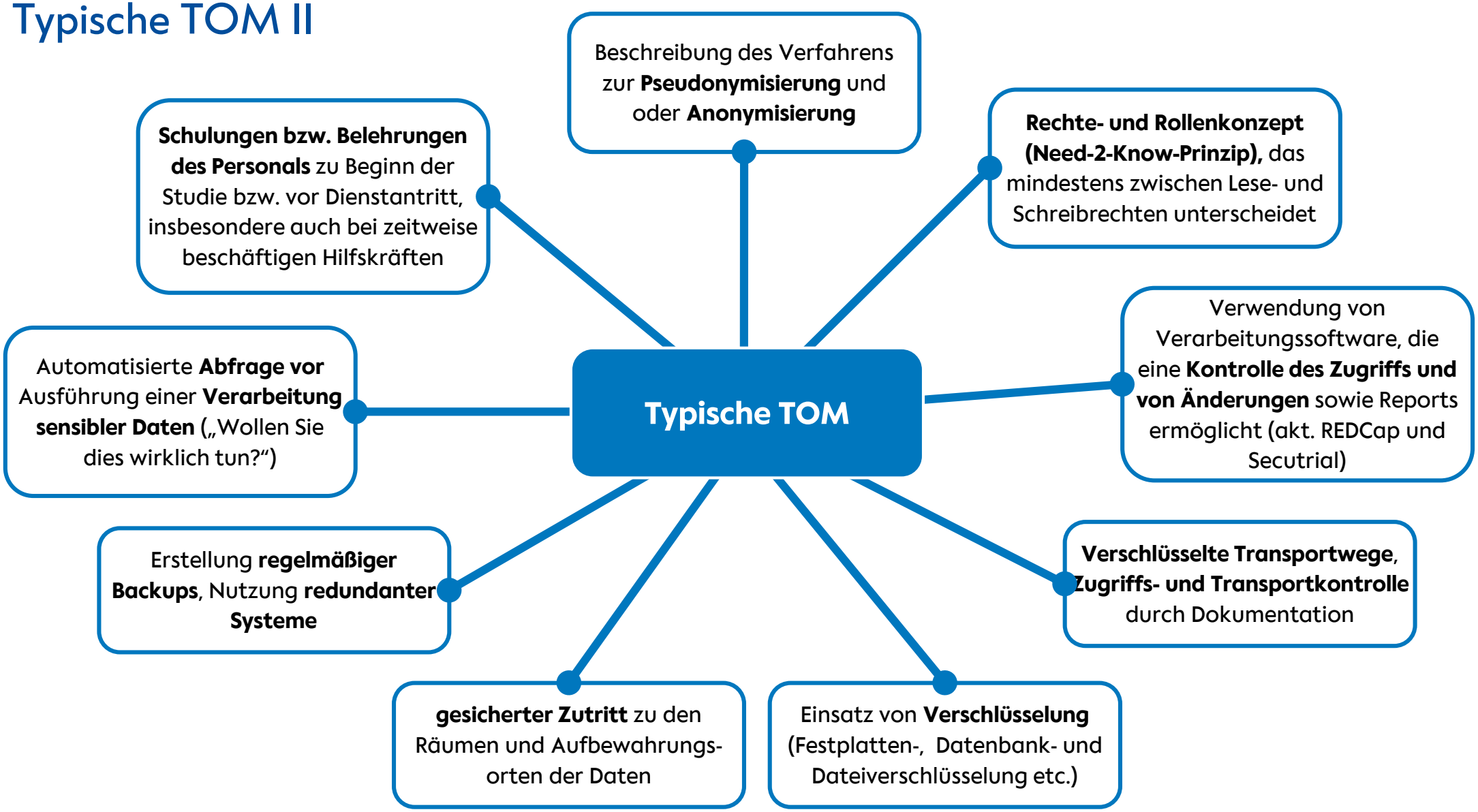
- Informationelle Gewaltenteilung = Getrennte Aufbewahrung von identifizierenden Daten und pseudonymisierten Forschungsdaten sowie der Re-Identifizierungsliste,

  → Dezentral: nur der Verantwortliche und von diesem autorisierte Personen haben Zugriff auf Re-Identifizierungsliste

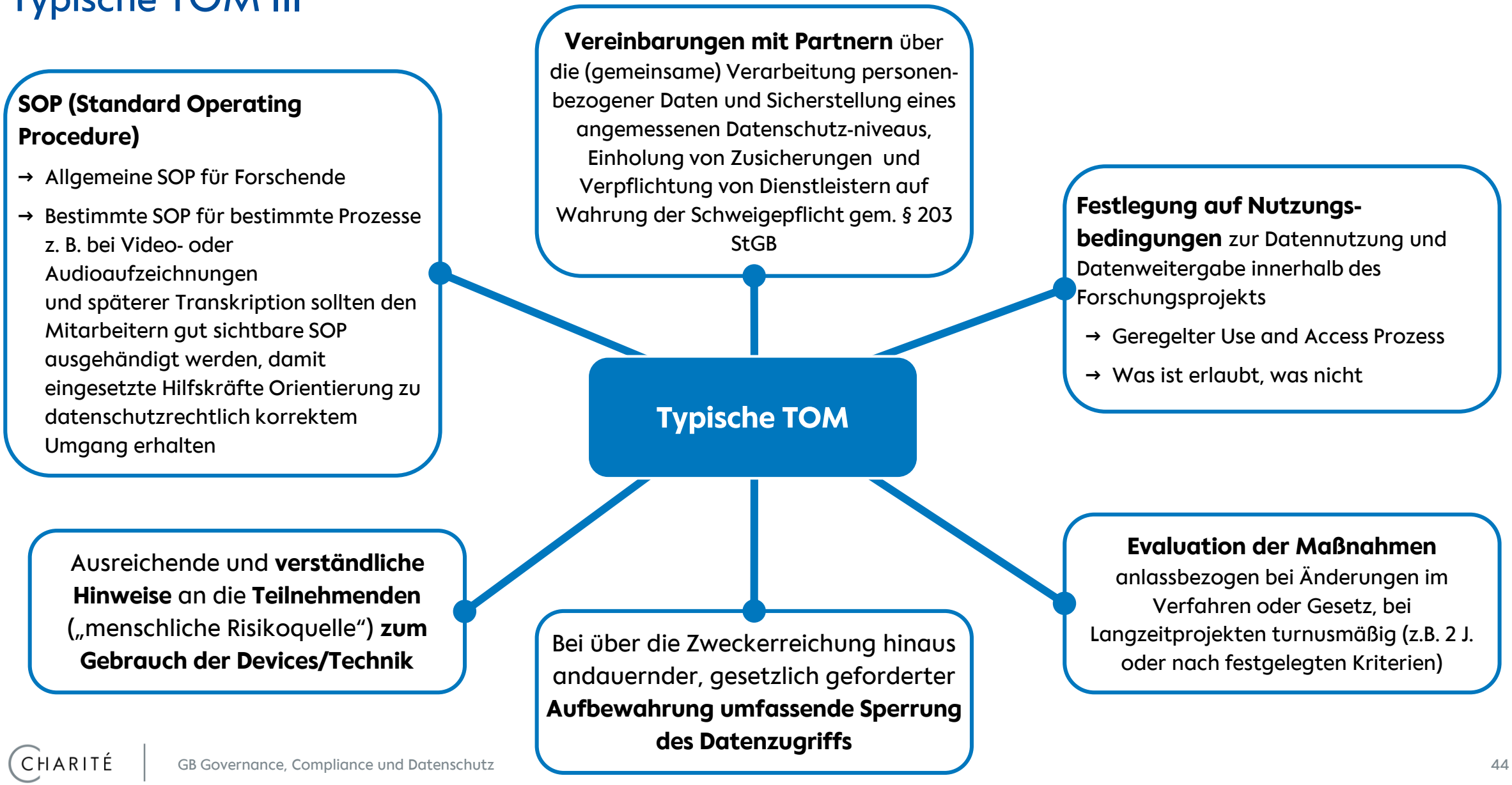
  → Zentral: unabhängige Stelle verwaltet Re-Identifizierungsliste



Typische TOM II



Typische TOM III



8

Zusammenfassung

Zusammenfassung

- Medizinische Forschungsvorhaben beinhalten i. d. R eine **umfangreiche Verarbeitung sensibler Daten** mit sehr **hohen Risiken** für die Betroffenen.
- Die sensiblen personenbezogenen Daten sind die nicht wegzudenkende Arbeitsgrundlage für Forschungsvorhaben.
- Daher ist **Datenschutz von Beginn an mit zu planen**.
- Wenn nötig oder vorgeschrieben, sollte frühzeitig eine Beratung der Datenschutzbeauftragten eingeholt werden und eine Abstimmung mit den Forschungspartnern erfolgen.

© Copyright 2024 – Alle Inhalte, insbesondere Texte, Fotografien und Grafiken sind urheberrechtlich geschützt.
Alle Rechte, einschließlich der Vervielfältigung, Veröffentlichung, Bearbeitung und Übersetzung, bleiben vorbehalten.

Zusammenfassung

Die (Durchführungs-) Verantwortlichen unterliegen vor der Verarbeitung personenbezogener Daten folgenden **datenschutzrechtlichen Pflichten**:

Sicherstellen der rechtmäßigen Verarbeitung pb Daten – ggf. Fragen bei Partnern/Beratung DSB

Transparenz gegenüber Betroffenen herstellen und beibehalten durch Information und Einwilligung sowie Internetpräsenz oder Rückfragemöglichkeit

Datenschutzkonzept bzw. DSFA

Eintrag in das **Verzeichnis von Verarbeitungstätigkeiten** bei eigener Institution und **Vertragskataster** (AVV, Kooperationsverträge)

Vereinbarungen mit Partnern über die (gemeinsame) Verarbeitung personenbezogener Daten und **Sicherstellung eines angemessenen Datenschutzniveaus**

© Copyright 2025 – Alle Inhalte, insbesondere Texte, Fotografien und Grafiken sind urheberrechtlich geschützt.
Alle Rechte, einschließlich der Vervielfältigung, Veröffentlichung, Bearbeitung und Übersetzung, bleiben vorbehalten.