Rechtsgrundlage zur Datenverarbeitung von Gesundheitsdaten

Version 0.1.1

anonymisierte Daten

Die Verarbeitung personenbezogenen Gesundheitsdaten benötigt...

eine **zweckbezogene Rechtsgrundlage**

Welche mögliche **zweckbezogene Rechtsgrundlagen** gibt es?

Behandlungszweck

Art. 6 Abs. 1b DSGVO "Vertrag"
und ggf. LKHG: Behandlungsvertrag;
Datenverarbeitung steht in direktem Bezug zur Patientenbehandlung

Zweck **"nur" Forschung**; Patient:innen hat keinen direkten Nutzen

§ 1 GDNG: gemeinwohlorientierte Forschungszwecke;
§ 6 Abs. 1 GDNG: Weiterverarbeitung;
§ 6 Abs. 3 GDNG: Weitergabe an Dritte

§ 46 LKHG (u.a.)
Forschung als Krankenhaus im Interesse des Krankenhauses

Art. 6 Abs. 1f DSGVO "Wahrung berechtigter Interessen" des Verantwortlichen oder eines Dritten;
§ 27 BDSG "Ausnahme vom Verbot" des Art. 9 Abs. 1 DSGVO

Art. 6 Abs. 1a DSGVO "Einwilligung"; zweckbezogen, zutreffend, nicht widerrufen; eingeholt "von wem auch immer"

Auftragsverarbeitung oder **Kooperation**

Sie sind beauftragter Dienstleister (Auftragsverarbeiter): es gilt Art. 28 DSGVO; Sie verarbeiten Daten "im Auftrag" für einen Verantwortlichen, der eine Rechtsgrundlage bereits erfüllt

Sie sind Teil einer Kooperation, Kooperationspartner sind berechtigt zu forschen und Sie haben über "gemeinsame Verantwortung nach Art. 26 DSGVO daran teil

Um Gesundheitsdaten verarbeiten zu dürfen, bedarf es einer **zweckbezogenen Rechtsgrundlage** oder die Daten müssen **vollständig** (= unwiederbringlich) **anonymisierte** Daten sein.

Die Anonymisierung müsste 100% gesichert sein, was praktisch schwer zu erreichen ist. Die Rückbeziehbarkeit müsste ausgeschlossen sein.

Wahl der zweckbezogene Rechtsgrundlage:
Die folgenden Fragen helfen zu entscheiden, auf welche Rechtsgrundlage zurückgegriffen werden kann.

1. Welche Zwecksetzung verfolgt Ihre Organisation damit?

2. In welcher Beziehung stehen Sie zu den Patienten?

3. Forschen Sie, weil Sie beauftragt sind und forschen formal für eine andere Organisation?

Das **Reallabor ROUTINE** wird im Zeitraum zwischen 12/2022 und 12/2024 durch Landesmittel des Ministerium für Soziales, Gesundheit und Integration Baden-Württemberg gefördert.

Gesetzliche Vorgaben zum "Wie" der Datenverarbeitung

Jeder

Oberbegriffe für zu erreichende Schutzziele - Umsetzung der Datenschutzgrundsätze aus Art. 5 DSGVO:
- Rechtsgrundlage nachweisbar
- transparente Information der betroffenen Patienten, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung/Löschkonzept, Integrität und Vertraulichkeit - Nachweis, was Sie jeweils konkret und effektiv tun (Rechenschaftspflicht - jeweils schriftlicher Nachwies zu den konkreten Maßnahmen)

Verantwortliche Organisation

Anforderungen an DS-Konzept/DS-Management, Art. 24 DSGVO:
Sie berücksichtigen Art, Umfangs, Umstände und Zwecke der Verarbeitung sowie Eintrittswahrscheinlichkeit und Schwere der Risiken für die Patienten und ergreifen geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß der DSGVO erfolgt und überprüfen und aktualisieren diese bei Bedarf.

Maßstab für IT-Maßnahmen, Art. 25 DSGVO:
Beim Einsatz von Technik (z.B. Software/KI) machen Sie möglichst viel Datenschutz durch entsprechende Technikgestaltung und datenschutzfreundliche Voreinstellungen.

Ausdrückliche Maßnahmen für die Sicherheit der Verarbeitung nach Art. 32 DSGVO (Auswahl insb. nach Angemessenheit, Geeignetheit, "Machbarkeit"):
a) Pseudonymisierung und Verschlüsselung
b) Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit
c) Wiederherstellung
d) Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Maßnahmen

Jeder

Zusätzliche "Maximalmaßnahme" Anonymisierung:
(kein Datenbezug mehr, streng genommen greift dann Datenschutzrecht nicht mehr)

- **Rechtsunsicherheit (Risiko)** (gefestigte Rechtsprechung für **Definition** fehlt (noch):
  *Anonymisieren ist das Verändern von Daten derart, dass Einzelangaben über persönliche oder sachliche Verhältnisse (gar) nicht mehr / **oder** "nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft" einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.*

- bei kleinen Kohorten gelingt wirksame Anonymisierung ggf. nicht.
- **Praktisches Problem:** nach Anonymisierung ist keine Rückbeziehbarkeit der Daten auf Patienten mehr möglich; wenn doch ist es keine Anonymisierung (zumindest im strengeren Sinne).

Aktuelle Informationen: https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2025/guidelines-012025-pseudonymisation_en

Nach Klärung der Rechtsgrundlage (= auf welcher Grundlage darf ich Datenverarbeiten?), müssen **zusätzliche Anforderungen** an den Datenschutz beachtet werden (= welche gesetzlichen Vorgaben gibt es wie die Datenverarbeitung auszusehen hat?).

Können Sie/der Verantwortliche das **hohe Schutzniveau** für Gesundheitsdaten **nachweisen** (Art. 24, 25, 32 DSGVO)?

Die Festlegung geschieht in **eigener Verantwortung**: Ein angemessener Schutz ist durch geeignete, effektive Maßnahmen zu treffen.

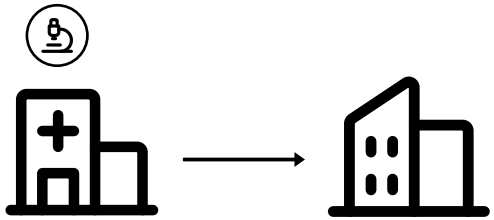
Eine Datenschutzverletzung ist ein Indiz, dass die Maßnahmen nicht ausreichend gewählt haben. Es besteht eine Meldepflicht zu Datenschutz-verletzungen.

Das **Reallabor ROUTINE** wird im Zeitraum zwischen 12/2022 und 12/2024 durch Landesmittel des Ministerium für Soziales, Gesundheit und Integration Baden-Württemberg gefördert.

Die 3 ROUTINE Use Cases: Beispiele für Rechtskonstellationen

Version 0.1.1

Für die drei in ROUTINE betrachteten Use Cases (Beispiele A-C) wurden die jeweils möglichen Rechtsgrundlagen zur Datenweitergabe und -verarbeitung betrachtet. Um diese Beispiele zur Orientierung nutzen zu können, ordnen Sie Ihr Forschungsvorhaben einer der drei Beispielen zu. Sie passen zu einem der drei Beispiele, wenn Sie **alle** der Fragen jeweils mit **"Ja" beantworten**.



A **Forschung** eines **Krankenhaus**; Weitergabe an **öffentliche und private Forschung**

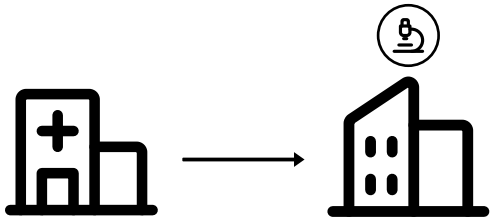
Forschung eines Krankenhauses mit Weitergabe der Daten an öffentliche oder private Einrichtung

1. Sie sind ein Krankenhaus (Gesundheitseinrichtung) und beforschen Daten "Ihrer Patienten", auch um ggf. diese Patienten entsprechend modifiziert zu behandeln?

2. Sie benötigen für die Erreichung der Forschungszwecke Zuarbeit/Unterstützung Dritter, ins. als Dienstleistung / Inanspruchnahme für Software, Know-How, Infrastruktur?

3. Die datenempfangende Organisation haben kein "eigenes" Interesse an den Daten?

4. Die datenempfangende Organisation hat kein Interesse an den Forschungsergebnissen?



B **Forschung Dritter** (öffentlich/ privat) mit **Daten aus Krankenhaus**

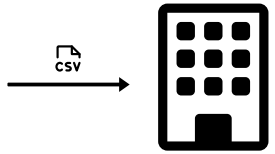
Forschung Dritter (öffentl./privat) mit Daten eines Krankenhauses

1. Sie sind in eine Forschungskooperation formal eingebunden, wenn auch ggf. in einer unklaren oder doppelten Rolle?

2. Ihnen werden Daten für die Forschung kostenfrei und (auch) im eigenen Interesse von Kooperationspartnern zur Verfügung gestellt, oder Sie bringen in solch einer Konstellation fragen ein?

3. Ein KI-Reallabor (oder Kooperationspartner mit vergleichbarem Profil) ist als wichtiger Akteur eingebunden/beteiligt?

4. Gemeinsame Zielerreichung ist wesentlicher Teil des Gesamtkonzeptes der Kooperation, ggf. i.S.v. "Gemeinsame Verantwortung" Art. 26 DSGVO?



C **KI-Reallabor** als **Auftragsverarbeiter**

KI-Reallabor als Auftragsverarbeiter zur Validierung von KI Algorithmen

1. Sie haben keinen eigenen (ausreichenden) Datenbestand für Ihren Forschungszweck?

2. Sie sind (in Bezug auf die Forschung) kein/e Krankenhaus / Gesundheitseinrichtung, sondern Forschungseinrichtung / Privatunternehmen; Ihre handelnden Personen sind (eher) keine Berufsgeheimnisträger i.S.v. § 203 StGB?

3. Die konkrete Erfüllung bestehender Behandlungsverträge kein primäres Handlungsinteresse Ihrer Forschung; Rückbeziehung der Daten ist nicht in Ihrem Interesse?

4. Sie haben vor allem die Entwicklung eines "Produktes" als Ziel, sie könnten mit anonymen Daten, oder mit einem anderen Datensatz (der vergleichbar valide ist) ebensogut Ihre Forschung durchführen?

Das **Reallabor ROUTINE** wird im Zeitraum zwischen 12/2022 und 12/2024 durch Landesmittel des Ministerium für Soziales, Gesundheit und Integration Baden-Württemberg gefördert.

A Forschung eines Krankenhaus; Weitergabe an öffentliche und private Forschung; Verarbeitung dort

Die Verarbeitung personenbezogenen Gesundheitsdaten benötigt...

- **anonymisierte** Daten
- eine **zweckbezogene Rechtsgrundlage**

Welche mögliche **zweckbezogene Rechtsgrundlagen** gibt es?

Behandlungszweck

Art. 6 Abs. 1b DSGVO "Vertrag" und ggf. LKHG: Behandlungsvertrag; Datenverarbeitung steht in direktem Bezug zur Patientenbehandlung

Zweck **"nur" Forschung**; Patient:innen hat keinen direkten Nutzen

§ 1 GDNG: gemeinwohlorientierte Forschungszwecke;
§ 6 Abs. 1 GDNG: Weiterverarbeitung;
§ 6 Abs. 3 GDNG: Weitergabe an Dritte

§ 46 LKHG (u.a.)
Forschung als Krankenhaus im Interesse des Krankenhauses

Art. 6 Abs. 1f DSGVO "Wahrung berechtigter Interessen" des Verantwortlichen oder eines Dritten;
§ 27 BDSG "Ausnahme vom Verbot" des Art. 9 Abs. 1 DSGVO

Art. 6 Abs. 1a DSGVO "Einwilligung"; zweckbezogen, zutreffend, nicht widerrufen; eingeholt "von wem auch immer"

Auftragsverarbeitung oder **Kooperation**

Sie sind beauftragter Dienstleister (Auftragsverarbeiter): es gilt Art. 28 DSGVO; Sie verarbeiten Daten "im Auftrag" für einen Verantwortlichen, der eine Rechtsgrundlage bereits erfüllt

Sie sind Teil einer Kooperation, Kooperationspartner sind berechtigt zu forschen und Sie haben über "gemeinsame Verantwortung nach Art. 26 DSGVO daran teil

Fall A: Ein **Krankenhaus** gibt im **Forschungsinteresse** des Krankenhauses **pseudonymisierte Daten** an **öffentliche/ private Einrichtungen** weiter. Die Verarbeitung der Daten geschieht dort.

Daten**weitergabe**:

- **Anonymisierte Daten**: Abgrenzung pseudonym vs. anonym aktuell in Klärung bei EUGH. Bei Anonymität greift Datenschutzrecht nicht (mehr).
- **§ 46 LKHG Abs. 1 Nr. 2a LKHG** erlaubt Weitergabe von Patientendaten an Dritte bei Forschung *des Krankenhaus.*
- **§ 6 Abs. 1 GDNG** erlaubt "Weiterverarbeitung" zur Forschung. Unklar ist insb. der Anwendungsbereich "Gemeinwohlorientierung". Auch Einschränkungen durch § 6 Abs. 3 "Einwilligungserfordernis" möglich.

Daten**verarbeitung**:

- **Art. 6 Abs. 1f DSGVO** erlaubt die Datenverarbeitung als Ausnahme positiver Interessensabwägung.
- **Art. 9 Abs. 2 Bst. j DSGVO** erlaubt die Verarbeitung personenbezogener Daten im öffentlichen Interesse für wissenschaftliche Zwecke (= Öffnungsklausel). Umsetzung durch § 27 BDSG, bzw. § 13 LDSG-BW.
- **Auftragsdatenverarbeitung**, dann ist es keine Weitergabe an Dritte, da Auftragnehmer i.S.d. Art. 28 DSGVO kein "Dritter" ist.
- **Art. 6 Abs. 1a DSGVO** erlaubt Weitergabe und Verarbeitung, liegt jedoch häufig nicht vor.

Das **Reallabor ROUTINE** wird im Zeitraum zwischen 12/2022 und 12/2024 durch Landesmittel des Ministerium für Soziales, Gesundheit und Integration Baden-Württemberg gefördert.

B **Forschung** Dritter (öffentlich/privat); mit Daten aus dem Krankenhaus

anonymisierte Daten

Die Verarbeitung personenbezogenen Gesundheitsdaten benötigt...

eine **zweckbezogene Rechtsgrundlage**

Welche mögliche **zweckbezogene Rechtsgrundlagen** gibt es?

Behandlungszweck

Art. 6 Abs. 1b DSGVO "Vertrag" und ggf. LKHG: Behandlungsvertrag; Datenverarbeitung steht in direktem Bezug zur Patientenbehandlung

Zweck **"nur" Forschung**; Patient:innen hat keinen direkten Nutzen

§ 1 GDNG: gemeinwohlorientierte Forschungszwecke;
§ 6 Abs. 1 GDNG: Weiterverarbeitung;
§ 6 Abs. 3 GDNG: Weitergabe an Dritte

§ 46 LKHG (u.a.)
Forschung als Krankenhaus im Interesse des Krankenhauses

Art. 6 Abs. 1f DSGVO "Wahrung berechtigter Interessen" des Verantwortlichen oder eines Dritten;
§ 27 BDSG "Ausnahme vom Verbot" des Art. 9 Abs. 1 DSGVO

Art. 6 Abs. 1a DSGVO "Einwilligung"; zweckbezogen, zutreffend, nicht widerrufen; eingeholt "von wem auch immer"

Auftragsverarbeitung oder **Kooperation**

Sie sind beauftragter Dienstleister (Auftragsverarbeiter): es gilt Art. 28 DSGVO; Sie verarbeiten Daten "im Auftrag" für einen Verantwortlichen, der eine Rechtsgrundlage bereits erfüllt

Sie sind Teil einer Kooperation, Kooperationspartner sind berechtigt zu forschen und Sie haben über "gemeinsame Verantwortung nach Art. 26 DSGVO daran teil

Fall B: Ein **Krankenhaus** gibt **pseudonymisierte Daten** an **öffentliche/ private Einrichtungen** zu deren **Forschungsinteresse** weiter.

Daten**weitergabe**:

- **Anonymisierte Daten:** Weitergabe anonymisierter Daten i.S.d. Sekundärdatennutzung möglich (Art. 9 Abs. 2f DSGVO i.V.m. § 27 BDSG)

  Achtung: geringe Kohortengröße darf keine Re-identifizierung ermöglichen.
- **Pseudonymisierte Daten**: Nach aktueller Rechtssprechung ist die Weitergabe pseudonymisierter Daten derzeit nur mit Rechtsgrundlage möglich.
- **§ 6 Abs. 1 GDNG** erlaubt "Weiterverarbeitung" zur Forschung. Unklar ist insb. der Anwendungsbereich "Gemeinwohlorientierung". Auch Einschränkungen durch § 6 Abs. 3 "Einwilligungserfordernis" möglich.
- **Auftragsdatenverarbeitung**: Auftragsdatenverarbeitung als mögliche rechtssichere Alternative.

  Prinzipiell Doppelrolle als Konsortialpartner im einem Forschungskonsortium und Auftragsdatenverarbeiter möglich
- **§ 46 LKHG** beschränkt Forschung auf Forschung des Krankenhauses und sperrt vermutlich **§ 27 BDSG**.
- **Art. 6 Abs. 1a DSGVO** erlaubt die Datenweitergabe, liegt oft nicht vor.

Das **Reallabor ROUTINE** wird im Zeitraum zwischen 12/2022 und 12/2024 durch Landesmittel des Ministerium für Soziales, Gesundheit und Integration Baden-Württemberg gefördert.

C KI-Reallabor als Auftragsverarbeiter; zur Validierung von KI-Algorithmen

anonymisierte Daten

Die Verarbeitung personenbezogenen Gesundheitsdaten benötigt...

eine **zweckbezogene Rechtsgrundlage**

Welche mögliche **zweckbezogene Rechtsgrundlagen** gibt es?

Behandlungszweck

Art. 6 Abs. 1b DSGVO "Vertrag" und ggf. LKHG: Behandlungsvertrag; Datenverarbeitung steht in direktem Bezug zur Patientenbehandlung

Zweck **"nur" Forschung**; Patient:innen hat keinen direkten Nutzen

§ 1 GDNG: gemeinwohlorientierte Forschungszwecke;
§ 6 Abs. 1 GDNG: Weiterverarbeitung;
§ 6 Abs. 3 GDNG: Weitergabe an Dritte

§ 46 LKHG (u.a.)
Forschung als Krankenhaus im Interesse des Krankenhauses

Art. 6 Abs. 1f DSGVO "Wahrung berechtigter Interessen" des Verantwortlichen oder eines Dritten;
§ 27 BDSG "Ausnahme vom Verbot" des Art. 9 Abs. 1 DSGVO

Art. 6 Abs. 1a DSGVO "Einwilligung"; zweckbezogen, zutreffend, nicht widerrufen; eingeholt "von wem auch immer"

Auftragsverarbeitung oder **Kooperation**

Sie sind beauftragter Dienstleister (Auftragsverarbeiter): es gilt Art. 28 DSGVO; Sie verarbeiten Daten "im Auftrag" für einen Verantwortlichen, der eine Rechtsgrundlage bereits erfüllt

Sie sind Teil einer Kooperation, Kooperationspartner sind berechtigt zu forschen und Sie haben über "gemeinsame Verantwortung nach Art. 26 DSGVO daran teil

Fall C: Ein **Reallabor** ist **Auftragsverarbeiter** zur Validierung von KI-Algorithmen.

Das Reallabor als Auftragsempfänger in Analogie zu einem kl.-chemischen Labor.

Validierung ist an der Grenze **zwischen Forschung und Produktentwicklung**. Aktuell wird der Forschungsbegriff eng ausgelegt. Die Abgrenzung soll im **EU AI Act** zukünftig geregelt werden.

Daten**verarbeitung**:

- **Anonymisierte Daten:** Nutzung anonymisierter Daten zur Validierung ist unproblematisch, solange Anonymisierung gewährleistet ist.
- **Auftragsdatenverarbeitung**: möglich, wenn das Ergebnis dem Patienten zurückgespielt wird. Rechtsgrundlage ist Art. 6 Abs. 1b DSGVO i.V.m. Behandlungsvertrag oder Einwilligung gem. Art. 6 Abs. 1a DSGVO.

  Achtung: Standesregelung, ärztliche Schweigepflicht.

Das **Reallabor ROUTINE** wird im Zeitraum zwischen 12/2022 und 12/2024 durch Landesmittel des Ministerium für Soziales, Gesundheit und Integration Baden-Württemberg gefördert.