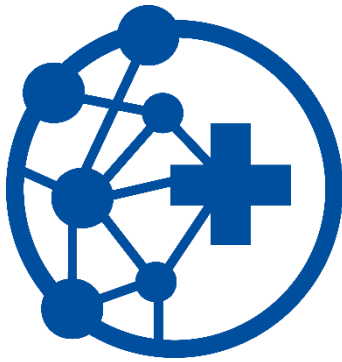




DIM.RUHR

DATENKOMPETENZZENTRUM FÜR DIE INTERPROFESSIONELLE
NUTZUNG VON GESUNDHEITSDATEN IN DER METROPOLE RUHR

Rechtliche Aspekte der Gesundheitsda- tennutzung

Autor	Marius Brinkmann
Mitwirkende	Konsortialmitglieder des Projekts DIM.RUHR
Datum	31.10.2025 – Version 1.0 („Erstveröffentlichung“)
Kontakt	Konsortialführung des Projekts DIM.RUHR Universität Witten/Herdecke dimruhr@uni-wh.de
Lizenz	Dieses Werk ist lizenziert unter einer Creative Commons Namensnennung - Weitergabe unter gleichen Bedingungen 4.0 International Lizenz: CC BY-SA 4.0. Von dieser Lizenz ausgenommen sind Organisationslogos sowie – falls gekennzeichnet – einzelne Bilder und Visualisierungen. 
Quellen	Dieses Werk basiert in einzelnen – insbesondere rechtlichen – Teilen auf der OER „Einführung in das Forschungsdatenmanagement“ aus dem Verbund HeFDI (Autor:innen: <i>Krähwinkel/Langner/Lipp/Pietsch</i> u. a.). Wesentliche Bearbeitungen, Aktualisierungen und Erweiterungen durch Marius Brinkmann (2025).

Das Projekt DIM.RUHR wird unter dem Förderkennzeichen 16DKZ2008A-F durch das BMBF gefördert und von der Europäischen Union – NextGenerationEU finanziert. Die geäußerten Ansichten und Meinungen sind ausschließlich die des Konsortiums und spiegeln nicht unbedingt die Ansichten der Europäischen Union oder der Europäischen Kommission wider. Weder die Europäische Union noch die Europäische Kommission können für sie verantwortlich gemacht werden.



Inhaltsverzeichnis

A. Einführung & Lernziele	6
I. Relevante Rechtskreise	6
II. Grundlagen	8
1. Personenbezogene Daten	8
2. Daten ohne Personenbezug	9
3. Überblick Forschungsdatenzyklus	10
4. Begriffsbestimmungen	10
a) Gesundheitsdaten	10
b) Sozialdaten	11
c) Versorgungsnahe Daten (VeDa)	11
d) Anonymisierung	11
e) Pseudonymisierung	11
5. Beispiel: Klinische Studie zur Wirksamkeit eines neuen Medikaments	12
a) Gesundheitsdaten:	12
b) Sozialdaten:	12
c) Versorgungsnahe Daten:	13
d) Pseudonymisierung:	13
e) Anonymisierung:	13
III. Sektorale Spezialgesetze zur Gesundheitsdatennutzung	14
1. Gesetz zur Beschleunigung der Digitalisierung des Gesundheitswesens (DigiG)	14
2. Gesundheitsdatennutzungsgesetz (GDNG)	15
3. Bezug zu versorgungsnahen Daten	16
B. Anforderungen an die Einwilligung	17
I. Herleitung / ethische Bezüge	18
II. Voraussetzungen der informierten Einwilligung	19
1. Freiwilligkeit	19
2. Ausdrücklichkeit	19
3. Bestimmtheit	19
4. Informiertheit	19

5. Widerrufbarkeit	20
6. Hinweise und Rechtsgrundlagen	20
III. Zwischenfazit.....	21
IV. Voraussetzungen der weiten Einwilligung.....	21
1. Freiwilligkeit.....	22
2. Ausdrücklichkeit.....	22
3. Zweckrahmen.....	22
4. Informiertheit	22
5. Schutz- und Transparenzmaßnahmen	22
6. Widerrufbarkeit	23
7. Hinweise und Rechtsgrundlagen	23
VI. Spannungsfeld der Einwilligungsarten.....	24
1. Regelungshorizont	24
2. Rechtliche Fundamente für Schutzmaßnahmen beim broad consent	25
a) Datenschutzrechtliche Grundprinzipien.....	25
b) Rechenschaftspflicht und „Privacy by Design“	25
c) Ausnahmen und Kompensationsrechte nach Art. 89 DSGVO	26
d) Nationale Konkretisierung durch § 27 BDSG.....	26
e) Spezielle Regelungen des Gesundheitsdatennutzungsgesetzes (GDNG)	26
f) Forschungsethische Leitlinien	27
3. Praktische Ausgestaltung der Nachweis- und Schutzpflicht	28
4. Spannungsfeld / Zusammenfassung	28
B. Datenschutzerfordernisse	30
I. Datenschutzrechtliche Grundlagen bei der Verarbeitung von Forschungsdaten	30
II. Mittel zur Entfernung identifizierender Merkmale	31
I. Geheimhaltungspflicht	33
1. Begriff und Funktion	33
2. Rechtsgrundlagen	33
a) Berufsrechtliche Schweigepflichten	33
b) Weitere Rechtsgrundlagen für die Geheimhaltungspflicht.....	34
3. Rechtmäßigkeit / Rechtfertigung	34

C. Entscheidungsbefugnis.....	36
I. Urheberrechte und Leistungsschutzrechte	36
II. Nutzungsrechtseinräumungen im Rahmen von Dienst- und Arbeitsverträgen	38
D. Veröffentlichung und Lizenzierung von Forschungsdaten	40
I. Was sind geeignete Lizenzierungsmodelle?	42
II. Was kann einer Veröffentlichung entgegenstehen?	43
III. Schutz vertraulicher Informationen in Forschungsdatenzentren.....	44
F. Bedeutung für die Forschungspraxis.....	45
I. Publikationsfreiheit vs. Rechte Dritter	45
II. Erlaubnisfreie Nachnutzung fremder Werke.....	47

A. Einführung & Lernziele

Aus rechtlicher Perspektive geht es dir um die Gewährleistung ethischer Prinzipien im Umgang mit Gesundheitsdaten. Ethik und Recht bilden die Vertrauensgrundlage zwischen Patient:innen, Ärzt:innen und dir als Forschende:r. Rechtssicherheit stellt ethische Standards sicher, und Ethik bildet die Grundlage für jede Rechtssetzung.

Die Rechtsgrundlagen für die Datenverarbeitung sind vielfältig und werden dir hier überblicksartig vorgestellt. Sie sollen dich für den Bereich sensibilisieren, in dem Gesundheits- und Versorgungsdaten als schutzwürdige Rechtsgüter aus unterschiedlichen Motiven erhoben und verarbeitet werden.

Allgemeingültig ist die Unterscheidung der Rechtsgüter nach *Roscoe Pound* in den drei Kategorien der individuellen, öffentlichen und gesellschaftlichen Interessenlage. Die Erfordernisse an die Datenerhebung und Datenverarbeitung können folglich interessenabhängig unterschiedlich sein. Ebenso sei erwähnt, dass sich rechtliche Fragen im Umgang mit Forschungsdaten in jeder Phase des sog. Forschungsdatenlebenszyklus stellen (vgl. hierzu A. II. 3.).

Ziel dieser OERs ist es, ein Gespür für rechtlich sensible Themen im Zusammenhang mit Daten zu entwickeln und ein Grundverständnis für die Umsetzung der Forschungsethik im Recht zu erlangen. Nach Abschluss dieses Kapitels kannst du:

- die wichtigsten Rechtsgebiete im Umgang mit Forschungsdaten benennen,
- konkrete Schritte zur rechtskonformen Umsetzung deines Forschungsvorhabens durchführen,
- entscheiden, ob und wie du deine Daten veröffentlichen kannst,
- zentrale Fachbegriffe im Datenschutz verstehen,
- dich bei rechtlichen Fragen an die passenden Stellen wenden,

I. Relevante Rechtskreise

Zum einschlägigen Regelungskreis zählen insbesondere das Datenschutzrecht, das Urheberrecht, die Leistungsschutzrechte und das Vertragsrecht. Je nach Forschungsprojekt können weitere Rechtsgebiete relevant werden. Wenn mit deiner Forschung beispielsweise Erfindungen verbunden sind, musst du das Patentrecht und ggf. auch das Arbeitnehmererfindungsgesetz beachten. Bei Kooperationen mit Unternehmen oder in der Auftragsforschung gelten zudem häufig vertragliche Vereinbarungen wie Geheimhaltungserklärungen oder Nutzungsrechtsvereinbarungen.

Hinweis:

Um in einem Forschungsvorhaben den relevanten Regelungskreis frühzeitig zu erfassen, empfiehlt es sich (bzw. ist teils auch verpflichtend vorgesehen), die zuständigen Abteilungen zu kontaktieren. Außerdem kann das Votum einer Ethikkommission verpflichtend sein, die sich häufig auch mit rechtlichen Fragen befasst. Hochschulen unterhalten in der Regel solche Kommissionen für bestimmte

Fachdisziplinen zur Beurteilung ethischer Grundsatzfragen sowie ethischer Aspekte wissenschaftlicher Untersuchungen. Auch das Projekt DIM.RUHR hat ein ELSA-Konzept (Ethical, Legal and Social Aspects) entwickelt.

Konkrete Schritte zur rechtskonformen Umsetzung deines Forschungsvorhabens:

Um dein Forschungsvorhaben rechtssicher zu gestalten, solltest du folgende Schritte durchlaufen:

1. Klärung des Personenbezugs

Prüfe, ob du mit personenbezogenen Daten arbeitest. Falls ja, gelten die Vorgaben der DSGVO und weiterer datenschutzrechtlicher Vorschriften.

2. Zweckbeschreibung

Beschreibe den Forschungszweck konkret und detailliert. Dies ist Grundlage für die datenschutzrechtliche Bewertung und die Wahl der Rechtsgrundlage.

3. Festlegung der Verantwortlichkeiten

Kläre, wer im Projekt verantwortlich ist (z. B. Projektleitung, beteiligte Institutionen). Bei Kooperationen: Gibt es gemeinsame Verantwortlichkeiten (sog. Joint Controllership)?

4. Datenerhebung und -kategorien

Bestimme, welche Daten erhoben werden, ob sensible Kategorien (z. B. Gesundheitsdaten) betroffen sind und welche Metadaten anfallen.

5. Rechtsgrundlage wählen

Lege fest, auf welcher Rechtsgrundlage du die Daten verarbeitest (z. B. Einwilligung, öffentliches Interesse, berechtigtes Interesse). Bei Gesundheitsdaten ist meist eine Einwilligung erforderlich.

6. Einwilligung einholen

Sofern erforderlich: Erstelle Informationsschreiben und Einwilligungserklärungen, die den Anforderungen der DSGVO entsprechen (informiert, freiwillig, widerrufbar).

7. Datenschutzmaßnahmen umsetzen

Anonymisierung oder Pseudonymisierung planen, technische und organisatorische Maßnahmen (TOM) festlegen, sichere Speicherung und Zugriffskontrolle gewährleisten.

8. Drittbeteiligung regeln

Bei Einbindung externer Dienstleister (z. B. Cloud-Anbieter, Umfrage-Tools): Auftragsverarbeitungsverträge (AVV) abschließen. Bei Kooperationen mit anderen Forschungseinrichtungen: Vereinbarungen zu gemeinsamer Verantwortlichkeit treffen.

9. Informationspflichten erfüllen

Informiere die betroffenen Personen transparent über die Datenverarbeitung (Art. 13/14 DSGVO).

10. Datenmanagementplan (DMP) erstellen

Dokumentiere alle Schritte in einem Datenmanagementplan. Dieser sollte Angaben zu Datenerhebung, -speicherung, -sicherung, -archivierung und -veröffentlichung enthalten.

11. Ethikkommission konsultieren

Falls erforderlich: Hole das Votum der zuständigen Ethikkommission ein, bevor du mit der Datenerhebung beginnst.

12. Regelmäßige Überprüfung

Überprüfe während des Projektverlaufs regelmäßig, ob alle rechtlichen und ethischen Anforderungen eingehalten werden.

II. Grundlagen

Bei der Erhebung, Speicherung, Verarbeitung und Weitergabe von Forschungsdaten mit Personenbezug sind Datenschutzrechte zu beachten. Wenn du als Wissenschaftler:in oder Forscher:in an einer Hochschule oder einem Institut mit entsprechenden Daten arbeitest, empfiehlt es sich, die Grundzüge der aktuellen Gesetze zum Datenschutz zu kennen. Hierzu gehören die Datenschutz-Grundverordnung (DSGVO), das Bundesdatenschutzgesetz (BDSG), das Gesundheitsdatennutzungsgesetz (GDNG) sowie das jeweilige Landesdatenschutzgesetz (in Nordrhein-Westfalen das DSG NRW).

Für den fachgerechten Umgang mit Gesundheitsdaten werden die wichtigsten Begriffe im Folgenden erläutert.

1. Personenbezogene Daten

Personenbezogene Daten sind gemäß Art. 4 Abs. 1 DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare lebende Person beziehen. Typischerweise sind dies: Name, Anschrift, Geburtsdatum, Fingerabdrücke, Online-Kennungen wie IP-Adressen oder Cookies. Beispiele für personenbezogene Forschungsdaten sind Umfragedaten in den Sozialwissenschaften oder Gesundheitsdaten in der medizinischen Forschung.

Dabei ist es irrelevant, ob die verarbeitende Person selbst oder ein Dritter in der Lage ist, den Personenbezug herzustellen. Entscheidend ist, ob die Identifizierung unter Berücksichtigung aller Mittel (Kosten, Zeit, verfügbare Technologie) wahrscheinlich ist.

Als **identifizierbar** wird eine Person angesehen, die direkt oder indirekt mittels Zuordnung identifiziert werden kann:

- **insbesondere zu einer Kennung** wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung *oder*
- **zu einem oder mehreren besonderen Merkmalen**, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind. Bei der Prüfung, ob eine Person identifizierbar ist, sind alle Mittel zu berücksichtigen, die von dem Verantwortlichen oder einer anderen Person unter normalen Umständen (hinsichtlich Kosten und Zeitaufwand) wahrscheinlich genutzt werden, um die Person zu identifizieren (Erwägungsgrund 26 DSGVO).

In der **Rechtsprechung** sind insbesondere folgende Fälle entschieden worden:

- Bildnisse, Film- und Tonaufnahmen, wenn ein Personenbezug besteht
- IP-Adressen
- schriftliche Antworten eines Prüflings in einer berufsbezogenen Prüfung
- Anmerkungen der Prüferin/des Prüfers zur Bewertung dieser Antworten

Praxishinweis:

Personenbezogene Daten werden in der Forschung beispielsweise bei Interviews, Befragungen, Evaluationen, Beobachtungen oder Experimenten erhoben. In allen diesen Fällen sind die datenschutzrechtlichen Vorgaben zu beachten. Falls Unsicherheiten in Bezug auf die Einordnung von Daten als personenbezogene Daten bestehen, sollte vorsorglich davon ausgegangen werden, dass es solche sind.

Hinweis:

Vor allem in der epidemiologischen Forschung mit personenbezogenen Daten und bei Forschung mit therapeutischer Zielsetzung sollten im Vorfeld auch ethische Überlegungen erfolgen. Diese sind oft bereits in disziplinspezifischen Richtlinien zusammengefasst, z. B.:

- I. Ethik-Kodex der Deutschen Vereinigung für Politikwissenschaft (DVPW) [[pdf](#)]
- II. Ethische Richtlinien der Deutschen Gesellschaft für Psychologie (DGP) und des Berufsverbands Deutscher Psychologinnen und Psychologen (BDP) [[pdf](#)]
- III. Ethik-Kodex der Deutschen Gesellschaft für Soziologie (DGS) und des Berufsverbandes Deutscher Soziologinnen und Soziologen (BDS) [[pdf](#)]
- IV. [World Medical Association \(WMA\)](#).

2. Daten ohne Personenbezug

Daten ohne Personenbezug – etwa anonymisierte oder aggregierte Datensätze – fallen nicht unter die Datenschutz-Grundverordnung. Sie können jedoch unter Berücksichtigung sonstiger Rechte (z. B. Urheberrechte) weiterverwendet werden.

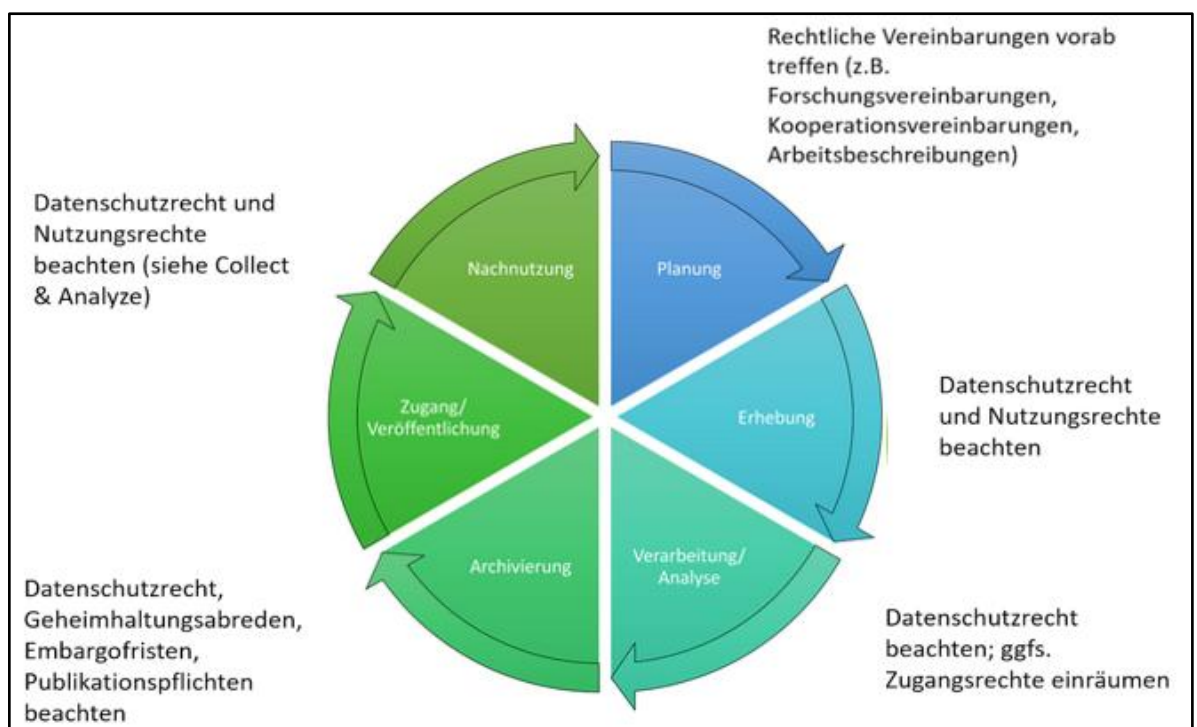
Praxishinweis:

Wenn nicht eindeutig klar ist, ob ein Personenbezug vorliegt, solltest du im Zweifelsfall unterstellen, dass es sich um personenbezogene Daten handelt, um rechtliche Risiken zu vermeiden.

3. Überblick Forschungsdatenzyklus

Rechtliche Fragen im Umgang mit Forschungsdaten stellen sich in jeder Phase des sog. Forschungsdatenlebenszyklus. Hervorzuheben sind:

- **Planung und Erhebung** (z. B. Einholung von Einwilligungen, Prüfungen durch Ethikkommission)
- **Speicherung und Dokumentation** (z. B. technische und organisatorische Maßnahmen)
- **Auswertung und Weitergabe** (z. B. Pseudonymisierung, Auftragsverarbeitung)
- **Archivierung und Langzeitarchivierung** (z. B. Datenmanagementpläne)
- **Veröffentlichung und Nachnutzung** (z. B. Open Data, Lizenzierung)



Bearbeitung angelehnt an: Paul Baumann/Philipp Krahn, [Rechtliche Rahmenbedingungen des FDM - Grundlagen und Praxisbeispiele](#), Dresden 2020, Folie 4

4. Begriffsbestimmungen

a) Gesundheitsdaten

Gemäß der Legaldefinition des Art. 4 Nr. 15 der DSGVO sind Gesundheitsdaten personenbezogene Daten, „die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der

Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen“.

Beispiele: Diagnosen, Laborbefunde, Medikationsdaten, ärztliche Berichte.

b) Sozialdaten

§ 67 Abs. 2 SGB X definiert Sozialdaten als personenbezogene Daten, „die von einer in § 35 SGB I genannten Stelle im Hinblick auf ihre Aufgaben nach diesem Gesetzbuch erhoben, verarbeitet oder genutzt werden.“ Dazu gehören auch Gesundheitsdaten, soweit sie im Rahmen sozialrechtlicher Aufgaben verarbeitet werden. Sozialdaten unterliegen einem besonderen Schutz.

Beispiele: Angaben zu Rentenansprüchen, Krankenkassenleistungen, Pflegebedürftigkeit.

c) Versorgungsnahe Daten (VeDa)

Versorgungsnahe Daten (VeDa) sind Daten aus der medizinischen Routineversorgung, die ohne spezifische Studienvorgaben erhoben werden und regelmäßig aus der Anwendung zugelassener Arzneimittel im Rahmen ihrer jeweiligen Indikation resultieren.

Wichtige Datenquellen sind GKV-Routinedaten (§ 303a – 303e SGB V) und Registerdaten (z. B. § 65c SGB V – Klinische Krebsregister).

Hinweis: Weitere Regelungen zu VeDa findest du in Kapitel III („DigiG und GDNG“).

d) Anonymisierung

Die Anonymisierung ist nicht legaldefiniert, aber anerkannt (z. B. durch Erwägungsgrund 26 der DSGVO): Anonymisierung bezeichnet die Verarbeitung personenbezogener Daten in einer Weise, dass die betroffene Person **nicht mehr identifizierbar ist**, weder direkt noch indirekt, auch nicht durch Rückgriff auf zusätzliche Informationen. Nach der Anonymisierung handelt es sich **nicht mehr um personenbezogene Daten**, die DSGVO ist dann **nicht mehr anwendbar**.

Wichtig: Die Anonymisierung muss irreversibel sein – auch unter Berücksichtigung realistischer Mittel eines Dritten.

Anonymisierung
Eine derartige Veränderung der Daten, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr (sog. absolute Anonymisierung) oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft (sog. faktische Anonymisierung) einer bestimmten oder bestimmbar natürlichen Person zugeordnet werden können.

e) Pseudonymisierung

Gem. Art. 4 Nr. 5 DSGVO ist die Pseudonymisierung die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten **ohne Hinzuziehung zusätzlicher Informationen** nicht mehr einer

spezifischen betroffenen Person zugeordnet werden können, wobei diese zusätzlichen Informationen **gesondert aufbewahrt** werden, und **technischen und organisatorischen Maßnahmen** unterliegen.

Beispiel 1: Liste der Matrikelnummern ohne den jeweiligen Namen der Studierenden. Die zusätzlichen Informationen (z.B. Verknüpfungstabelle) werden getrennt und geschützt aufbewahrt.

Beispiel 2: Ein Datenmanagementzentrum ersetzt Name und Geburtsdatum durch einen Studiencode. Die Zuordnungstabelle wird sicher verwahrt, sodass nur befugte Stellen eine Re-Identifizierung vornehmen können.

Pseudonymisierung
Die Trennung der personenbezogenen Merkmale unmittelbar nach der Erhebung von den restlichen Daten, so dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen Person zugeordnet werden können.

5. Beispiel: Klinische Studie zur Wirksamkeit eines neuen Medikaments

Ein Universitätsklinikum führt eine multizentrische klinische Studie durch, um die Wirksamkeit eines neuen Medikaments zur Behandlung von Diabetes mellitus Typ 2 zu untersuchen. Dabei werden Daten von Patientinnen und Patienten an mehreren Studienzentren erhoben und zentral ausgewertet.

a) Gesundheitsdaten:

Im Rahmen der Studie werden erhoben:

- Blutzuckerwerte
- HbA1c-Werte
- Medikamentengabe und Nebenwirkungen
- Diagnosen (Diabetes, Komorbiditäten)
- Körpergewicht, Blutdruck

Diese Daten sind gemäß **Art. 4 Nr. 15 DSGVO** als **Gesundheitsdaten** einzustufen, da sie Rückschlüsse auf den Gesundheitszustand der betroffenen Personen ermöglichen.

b) Sozialdaten:

Falls die Studie von einer **gesetzlichen Krankenkasse** unterstützt oder mit Sozialleistungsdaten (z. B. Abrechnungsdaten, Versichertenstatus) verknüpft wird, handelt es sich bei diesen Daten zusätzlich um **Sozialdaten** i. S. d. **§ 67 Abs. 1 SGB X**.

Beispiel: Abrechnungsdaten der medikamentösen Versorgung durch die GKV.

c) Versorgungsnahe Daten:

Zusätzlich zu den primär erhobenen Studiendaten können Daten aus der realen Versorgung („Routine-daten“) genutzt werden. Dazu zählen insbesondere:

- Abrechnungsdaten der Krankenkassen (§ 303b SGB V),
- Arzneimittelverschreibungsdaten (§ 300 SGB V),
- Daten aus klinischen Registern (z. B. Krebsregister, § 65c SGB V),
- Daten aus der elektronischen Patientenakte (§ 341 SGB V).

Diese Daten werden gemäß den Vorgaben der §§ 303a–303e SGB V über die Datensammelstelle, die Vertrauensstelle und das Forschungsdatenzentrum Gesundheit aufbereitet und für die wissenschaftliche Forschung bereitgestellt. Sie ermöglichen es, die Wirksamkeit und Sicherheit des Medikaments im Versorgungsalltag („Real-World-Effectiveness“) zu prüfen, Langzeitfolgen zu analysieren und gesundheitsökonomische Fragestellungen (z. B. Hospitalisierungsraten, Kosten) zu untersuchen.

d) Pseudonymisierung:

Vor der Weiterleitung an das zentrale Studienzentrum ersetzt ein Datenmanagementzentrum personenbezogene Identifikatoren (Name, Geburtsdatum, Versichertennummer) durch einen **Studiencode**.

- Die Zuordnungstabelle (Pseudonym → reale Identität) wird **getrennt und sicher verwahrt**.
- Nur das lokale Studienzentrum kann diese Rückführung vornehmen, etwa bei schwerwiegenden Nebenwirkungen.

Die Daten sind somit **pseudonymisiert** i. S. v. **Art. 4 Nr. 5 DSGVO**. Sie sind personenbezogen, aber ohne direkten Personenbezug für den zentralen Auswerter.

e) Anonymisierung:

Nach Abschluss der Studie werden alle personenbezogenen Merkmale entfernt oder dauerhaft unkenntlich gemacht (z. B. auch Kombinationen, die Rückschlüsse erlauben wie Alter und seltene Diagnose).

- Auch mit Zusatzwissen kann keine Re-Identifizierung mehr erfolgen.
- Die Daten dienen nun etwa der Sekundäranalyse oder Publikation.

Diese Daten gelten als **anonymisiert**. Sie unterliegen **nicht mehr der DSGVO**.

Hinweis: Derartige Fälle können sich weitaus komplizierter gestalten und es ist teils umstritten, ab wann eine Anonymisierung tatsächlich gelungen ist. Wende dich im Zweifel an die Rechtsabteilung und/oder die/den Datenschutzbeauftragte:n.

III. Sektorale Spezialgesetze zur Gesundheitsdatennutzung

Zur Nutzung von Gesundheitsdaten existieren spezialgesetzliche Regelungen auf Bundesebene, die sich aus den folgenden Gesetzen ergeben.

1. Gesetz zur Beschleunigung der Digitalisierung des Gesundheitswesens (DigiG)

Das DigiG wurde am 22. März 2024 als sog. Artikelgesetz, d.h., das mehrere andere Gesetze zugleich dadurch (neu) geregelt wurden (hier relevante Änderungen befinden sich vorwiegend im SGB V), beschlossen und trat am 26. März 2024 in Kraft. Es verfolgt das Ziel, die digitale Transformation des Gesundheitswesens zu beschleunigen und die Potenziale digitaler Anwendungen für die Versorgung zu nutzen.

Im Folgenden werden einige zentrale Regelungen des DigiG kurz erläutert.

Elektronische Patientenakte (ePA) im Opt-out-Verfahren:

Seit dem 15. Januar 2025 stellen die Krankenkassen allen Versicherten automatisch eine ePA zur Verfügung, sofern diese nicht innerhalb von sechs Wochen nach vorheriger Information widersprochen (§ 342 Abs. 1 Satz 2 SGB V). Die ePA bleibt eine freiwillige Anwendung, deren Nutzung du jederzeit widersprechen oder einschränken kannst.

Automatisierte Befüllung der ePA:

Ziel ist die vollumfängliche, weitestgehend automatisiert laufende Befüllung der ePA mit strukturierten Daten, die die Versorgung gezielt unterstützen. Der erste Anwendungsfall ist der digital gestützte Medikationsprozess. Weitere Anwendungsfälle wie die elektronische Patientenkurzakte (ePKA) und Labordaten-Befunde folgen.

E-Rezept:

Das E-Rezept wird weiterentwickelt und verbindlich eingeführt. Die E-Rezept-App der Gesellschaft für Telematik kann künftig auch mittels der ePA-Apps genutzt werden. Die Krankenkassen werden verpflichtet, ihre Versicherten über das E-Rezept zu informieren (§ 361b SGB V).

Digitale Gesundheitsanwendungen (DiGA):

Der Leistungsanspruch wird auf Medizinprodukte höherer Risikoklassen (Risikoklasse IIb nach Art. 51 der Verordnung (EU) 2017/745) ausgeweitet. Die Preisgestaltung wird stärker an Erfolgskriterien ausgerichtet, und es wird eine anwendungsbegleitende Erfolgsmessung obligatorisch vorgegeben (§ 139e Abs. 13 SGB V).

Videosprechstunden und Telekonsilien:

Die bisher geltende Begrenzung der Videosprechstunden wird aufgehoben. Die ärztliche Vergütung wird künftig stärker an Qualitätsmerkmalen orientiert (§ 87 Abs. 2n SGB V).

Verbesserung der Interoperabilität:

Die Verbindlichkeit von Standards, Profilen und Leitfäden wird erhöht, um den Informationsaustausch im Gesundheitswesen zu verbessern.

Erhöhung der Cybersicherheit:

Bei der Verarbeitung von gesundheits- und personenbezogenen Daten mithilfe cloudbasierter Informationssysteme müssen künftig die Mindestanforderungen des C5-Kriterienkatalogs (Cloud Computing Compliance Criteria Catalogue) des Bundesamts für Sicherheit in der Informationstechnik erfüllt werden (§ 393 SGB V).

2. Gesundheitsdatennutzungsgesetz (GDNG)

Das GDNG wurde ebenfalls am 22. März 2024 beschlossen und trat am 26. März 2024 in Kraft. Es dient der Regelung der Nutzung von Gesundheitsdaten zu gemeinwohlorientierten Forschungszwecken und zur datenbasierten Weiterentwicklung des Gesundheitswesens (§ 1 Abs. 1 GDNG). Die zentralen Regelungen des GDNG sind:

Datenzugangs- und Koordinierungsstelle für Gesundheitsdaten:

Beim Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) wird eine zentrale Datenzugangs- und Koordinierungsstelle eingerichtet (§ 3 Abs. 1 GDNG). Sie unterstützt und berät Datennutzende beim Zugang zu Gesundheitsdaten, führt einen öffentlichen Metadaten-Katalog und nimmt Anträge auf Zugang zu Gesundheitsdaten entgegen (§ 3 Abs. 2 GDNG).

Erleichterung der Sekundärnutzung von Gesundheitsdaten:

Das GDNG ermöglicht die Nutzung von Gesundheitsdaten zu gemeinwohlorientierten Forschungszwecken ohne Einwilligung der betroffenen Personen, sofern die Daten pseudonymisiert sind und die Forschung im öffentlichen Interesse liegt (§ 1 Abs. 2 GDNG).

Unter **Sekundärdatennutzung** versteht man die Verwendung bereits erhobener Gesundheitsdaten zu anderen, meist wissenschaftlichen oder gemeinwohlorientierten Zwecken als dem ursprünglichen Erhebungszweck. Sie ermöglicht damit eine weitergehende Auswertung vorhandener Versorgungs- oder Forschungsdaten, ohne dass erneut Daten erhoben oder individuelle Einwilligungen eingeholt werden müssen – soweit die gesetzlichen Voraussetzungen, insbesondere Pseudonymisierung und öffentliches Interesse, erfüllt sind.

Opt-out-Verfahren für ePA-Daten zu Forschungszwecken:

Die Freigabe von Daten aus der elektronischen Patientenakte an das Forschungsdatenzentrum Gesundheit erfolgt im Opt-out-Verfahren. Versicherte können der Übermittlung ihrer ePA-Daten an das Forschungsdatenzentrum widersprechen (§ 303e Abs. 1 SGB V i. d. F. des GDNG).

Verknüpfung von Daten des Forschungsdatenzentrums Gesundheit mit Krebsregisterdaten:

Es wird ein Verfahren vorgesehen, mit dem Daten des Forschungsdatenzentrums Gesundheit und Daten der klinischen Krebsregister der Länder nach § 65c SGB V datenschutzkonform und rechtssicher verknüpft werden können (§ 4 GDNG). Die Verknüpfung erfolgt anhand einer anlassbezogen erstellten Forschungskennziffer unter Mitwirkung der Vertrauensstelle nach § 303c SGB V.

Stärkung des Gesundheitsdatenschutzes:

Es wird eine Geheimhaltungspflicht für mit Gesundheitsdaten Forschende samt Strafnorm eingeführt

(§§ 7, 9 GDNG). Die unbefugte Weitergabe von Gesundheitsdaten oder deren Verarbeitung zum Zweck der Re-Identifizierung wird mit Freiheitsstrafe bis zu einem Jahr oder Geldstrafe bestraft (§ 9 Abs. 1 GDNG). Bei Handeln gegen Entgelt oder in Bereicherungsabsicht erhöht sich die Strafandrohung auf bis zu drei Jahre Freiheitsstrafe (§ 9 Abs. 2 GDNG).

Registrierungs- und Publikationspflicht:

Forschungsvorhaben, bei denen Gesundheitsdaten ohne Einwilligung der betroffenen Personen verarbeitet werden, müssen in einem von der Weltgesundheitsorganisation anerkannten Primärregister registriert werden (§ 8 Satz 1 GDNG). Die Forschungsergebnisse sind innerhalb von 24 Monaten nach Abschluss des Forschungsvorhabens zu veröffentlichen (§ 8 S. 3 GDNG).

Weiterverarbeitung von Versorgungsdaten:

Datenverarbeitende Gesundheitseinrichtungen dürfen rechtmäßig gespeicherte Daten zur Qualitätssicherung, Patientensicherheit, medizinischen/pflegerischen Forschung und zu statistischen Zwecken weiterverarbeiten (§ 6 Abs. 1 GDNG). Die Daten sind zu pseudonymisieren und sobald möglich zu anonymisieren (§ 6 Abs. 1 Satz 2 GDNG).

Querverweis: Weitere Details zu den praktischen Auswirkungen von DigiG und GDNG auf deine Forschungspraxis findest du in Kapitel F („Bedeutung für die Forschungspraxis“).

Mit diesem Überblick verstehst du, welche spezialgesetzlichen Anforderungen DigiG und GDNG für deine Forschung im Gesundheitsbereich stellen und wie diese Gesetze die Nutzung von Gesundheitsdaten erleichtern und gleichzeitig den Datenschutz stärken.

3. Bezug zu versorgungsnahen Daten

Das OER-Ziel, bei dir ein Gespür für rechtlich sensible Themen im Umgang mit Gesundheits- und Versorgungsdaten zu entwickeln und ein Grundverständnis für die Forschungsethik im Recht zu vermitteln, spiegelt sich in den spezialgesetzlichen Regelungen.

Versorgungsnahen Daten, die in der Routineversorgung entstehen und in Registern oder bei gesetzlichen Krankenkassen gespeichert werden, gewinnen durch das DigiG und das GDNG erheblich an Bedeutung. Deine Forschung profitiert von der erweiterten Zugänglichkeit und Standardisierung dieser Daten, während gleichzeitig strenge Datenschutz- und Sicherheitsanforderungen greifen.

- Das DigiG stellt mit den erweiterten C5-Cybersicherheitsanforderungen (§ 393 Abs. 6 SGB V) sicher, dass Cloudsysteme, über die Versorgungsdaten bereitgestellt werden, höchsten Schutz bieten. Damit kannst du versorgungsnahen Daten sicher abrufen und verarbeiten, ohne Ethik- und Datenschutzstandards zu gefährden.
- Das GDNG ermöglicht die pseudonymisierte Nutzung von GKV-Routinedaten (§ 6 Abs. 1–2 GDNG) und die Verknüpfung mit Registerdaten wie klinischen Krebsregistern (§ 4 Abs. 1–2 GDNG). So kannst du Real-World-Effekte analysieren und gesundheitsökonomische Fragestellungen bearbeiten, während das Opt-out-Verfahren für ePA-Sekundärnutzung (§ 303e Abs. 1 SGB V) die datenschutzrechtliche Freigabe deiner Daten sicherstellt.

Durch diese Regelungen werden deine Forschungsaktivitäten nicht nur erleichtert, sondern zugleich durch strenge technische und rechtliche Vorgaben abgesichert. Damit stehst du im Einklang mit dem OER-Ziel, rechtlich sensible Themen praxisnah und ethikorientiert umzusetzen.

Das Forschungsdatenzentrum Gesundheit (FDZ-G) beim BfArM nahm im ersten Quartal 2025 seinen Betrieb auf und bearbeitet seitdem Anfragen zur pseudonymisierten Nutzung von GKV-Routinedaten und Registerdaten (z. B. Krebsregister) im Opt-out-Verfahren. Auch die Einrichtung eines öffentlichen Metadatenkatalogs (§ 3 Abs. 2 GDNG) ist abgeschlossen; erste Datensätze (Abrechnungs- und Krebsregisterdaten) sind seit Mai 2025 verfügbar.

B. Anforderungen an die Einwilligung

Nachdem du nun die verschiedenen Arten von Daten sowie deren Verarbeitungsschritte kennengelernt hast, stellt sich in der Forschungspraxis die zentrale Frage, auf welcher **rechtlichen Grundlage** diese Daten überhaupt erhoben und genutzt werden dürfen.

Neben speziellen gesetzlichen Erlaubnistatbeständen – etwa den §§ 303a bis 303e SGB V für versorgungsnahe Daten – kommt in der Forschungspraxis insbesondere **die Einwilligung der betroffenen Personen** in Betracht. Sie ist damit ein zentrales Instrument, um die Nutzung von Gesundheits- und Sozialdaten rechtmäßig zu gestalten.

Bei der Einholung einer Einwilligung gilt es mehrere **Prüfungspunkte** zu beachten. Grundsätzlich dürfen personenbezogene Forschungsdaten nur mit einer **informierten Einwilligung** („informed consent“) der betroffenen Person oder auf Grundlage einer **gesetzlichen Erlaubnisnorm** erhoben und verarbeitet werden – sog. **Grundsatz des Verbots mit Erlaubnisvorbehalt** (Art. 9 Abs. 2 lit. a DSGVO).

Die informierte Einwilligung beschreibt die **freiwillige, auf hinreichender Aufklärung beruhende Zustimmung** zu einer Maßnahme – etwa einer medizinischen Behandlung, der Teilnahme an einer Studie oder der Verarbeitung personenbezogener Daten – nach umfassender Information über Zweck, Inhalt, Risiken und mögliche Alternativen. Näheres zu den **Voraussetzungen der informierten Einwilligung** findest du im folgenden Abschnitt II.

Mit dem **Gesundheitsdatennutzungsgesetz (GDNG)** ist daneben auch eine **weite („broad“) Einwilligung** zulässig. Dabei handelt es sich um eine pauschale Zustimmung zur Nutzung von Daten für mehrere, bei Abgabe der Einwilligung noch nicht konkret benannte Forschungszwecke. Beide Einwilligungsarten – der „informed consent“ und der „broad consent“ – werden im Folgenden gegenübergestellt und ihre Spannungsfelder erläutert.

Zur Ausnahme nach **Art. 9 Abs. 2 lit. h–j DSGVO** → siehe Abschnitt V. („Spannungsfeld der Einwilligungsarten“).

Hinweis:

Auch wenn das GDNG und die §§ 303a bis 303e SGB V spezifische Rechtsgrundlagen zur Datenverarbeitung schaffen, bleibt die **Einwilligung für Forschende regelmäßig der sicherste Weg**. Die genannten

Vorschriften sind kein allgemeiner Freibrief, sondern etablieren ein „Regime der Datentransparenz“ mit klar verteilten Rollen – Datensammelstelle (§ 303b SGB V), Vertrauensstelle (§ 303c SGB V) und Forschungsdatenzentrum Gesundheit (§ 303d SGB V) – sowie zweckgebundenen Befugnissen.

Die Erlaubnistatbestände wirken nur für die dort genannten Stellen, Zwecke und Verfahren.

I. Herleitung / ethische Bezüge

Der ethische Ursprung des „Informed Consent“ liegt in den Prinzipien der medizinischen Ethik und Menschenrechte. Wesentliche Bezugspunkte sind:

- **Autonomie:** Jeder Mensch hat das Recht, selbstbestimmt über seinen Körper und seine Daten zu entscheiden. Der informierte Entscheidungsprozess sichert diese Autonomie.
- **Nicht-Schädigung (non-maleficence):** Die Einwilligenden sollen vor Risiken geschützt werden, über die sie nicht aufgeklärt wurden.
- **Transparenz und Vertrauen:** Eine informierte Einwilligung fördert das Vertrauen in Forschung und Versorgung.
- **Vermeidung von Machtungleichgewichten:** Besonders bei vulnerablen Gruppen – etwa Patient:innen oder älteren Menschen – muss sichergestellt sein, dass eine Einwilligung nicht auf Abhängigkeiten oder unvollständiger Information beruht.

Auch der „**broad consent**“ lässt sich trotz seiner pauschalen Struktur ethisch begründen, wenn bestimmte normative Bedingungen erfüllt sind. Er soll Forschung erleichtern, ohne das Selbstbestimmungsrecht der betroffenen Person aufzugeben. Seine ethische Fundierung folgt in der Regel drei zentralen Argumentationslinien:

- **Gemeinwohlorientierung:** Gesundheitsforschung dient häufig überindividuellen Zielen – etwa der Verbesserung von Prävention, Diagnostik oder Versorgung. In dieser Perspektive ist der broad consent Ausdruck eines Solidaritätsprinzips. Er betont das utilitaristische Argument des Nutzens für viele (z. B. durch neue Therapien), das durch eine pauschale Datennutzung effizienter erreicht werden kann. Zugleich wird auf die **Public-Health-Ethik** verwiesen: Eine einzel-fallbezogene Zustimmungspflicht könnte viele Forschungsprojekte faktisch verhindern oder verzögern – was dem Prinzip der **Gerechtigkeit im Zugang zu Innovationen** widersprechen würde.
- **Autonomiekompatibilität:** Der broad consent ist kein Verzicht auf Autonomie, sondern ein **informierter Vertrauensvorschuss**. Wird die betroffene Person angemessen über Rahmenbedingungen, Zwecke, Rückzugsmöglichkeiten, Datenverantwortliche und Risiken aufgeklärt, bleibt ihre Autonomie gewahrt – auch wenn nicht jeder Einzelfall bekannt ist (**prozedurale Autonomie**). Da in komplexen Forschungssystemen vollständige Informationen über jede künftige Datennutzung kaum möglich sind, kommt es auf eine **transparente, überprüfbare Governance-Struktur** an („kontextuelle Autonomie“).

- **Institutionelle Verantwortung – Trust-Framework:** Ein ethisch vertretbarer broad consent setzt Vertrauen in eine verlässliche institutionelle Rahmung voraus. Ethikkommissionen prüfen daher projektbezogen Zweckbindung und Risikominimierung. Transparenzpflichten, Audit-Mechanismen sowie digitale Rückzugs- und Widerspruchsmöglichkeiten (Opt-out, Tracking) sind unerlässlich.
- **Vergleich mit analogen / etablierten Bereichen:** In der Biobank-Forschung, in Genomdatenbanken und in großen Kohortenstudien ist der broad consent international anerkannt – etwa in den **OECD-Guidelines on Human Biobanks and Genetic Research Databases**, der **WMA Declaration of Taipei** sowie im **EU Data Governance Act** (Erwägungsgrund 60).

II. Voraussetzungen der informierten Einwilligung

Gemäß [Erwägungsgrund 32 S.2 DSGVO](#) lassen sich für die informierte Einwilligung folgende Vorgaben festhalten:

1. Freiwilligkeit

Die Einwilligung muss **aus freien Stücken**, also ohne physischen oder psychischen Druck, erfolgen (vgl. Art. 4 Nr. 11 DSGVO). Eine Einwilligung, die unter Zwang, Abhängigkeit oder unzulässigem Druck erfolgt, ist unwirksam.

2. Ausdrücklichkeit

Die Einwilligung muss durch eine **aktive Handlung** und eine **eindeutige Willensbekundung** erfolgen. Bei minderjährigen oder nicht einwilligungsfähigen Personen erfolgt sie durch Sorgeberechtigte oder Betreuende (§ 630d Abs. 1 S. 2 BGB). Bei sensiblen personenbezogenen Daten (Art. 9 und 10 DSGVO) empfiehlt sich eine **schriftliche Dokumentation** der Einwilligung. Eine elektronische Form ist zulässig (z. B. digitale Signatur oder Bestätigungsfeld). Eine stillschweigende oder mutmaßliche Einwilligung ist ausgeschlossen (Erwägungsgrund 32 DSGVO). Der **Nachweis der Einwilligung** obliegt dem Verantwortlichen (Art. 7 Abs. 1 DSGVO; § 51 BDSG).

3. Bestimmtheit

Die Einwilligung muss **spezifisch und zweckgebunden** formuliert sein; eine pauschale oder unbestimmte Zustimmung ist unzulässig. Der Einwilligungstext muss klar erkennen lassen, **für welche Zwecke und durch wen** die Daten verarbeitet werden. Zum bereits erwähnten „broad consent“ vgl. unten Abschnitt B. IV. 5 (hier: Schutzmaßnahmen und Zweckbindung).

4. Informiertheit

Die betroffene Person muss in klarer, verständlicher Sprache über die wesentlichen Punkte der Datennutzung **informiert** werden. Die Einwilligenden müssen durch entsprechende Vorabinformationen

konkret nachvollziehen können, welche ihrer persönlichen Daten **wie, für was, von wem und wie lange** verwendet werden sollen. D. h. die Personen sollen in die Lage versetzt werden, die Konsequenzen der eigenen Einwilligung genau einschätzen zu können.

5. Widerrufbarkeit

Die Einwilligung ist **jederzeit und ohne Angabe von Gründen widerrufbar** (Art. 7 Abs. 3 DSGVO). Über dieses Recht ist vor Abgabe der Einwilligung zu informieren. Der Widerruf darf keine Nachteile zur Folge haben und wirkt **nur für die Zukunft**. Bereits erfolgte Verarbeitungen bleiben rechtmäßig.

6. Hinweise und Rechtsgrundlagen

Ergänzt werden muss die Einwilligungserklärung um Informationen über die Verarbeitung der Daten. Darunter fallen die Rechtsgrundlagen und Zwecke der Verarbeitung (soweit diese über die Verarbeitung hinausgehen), eine eventuelle Datenübermittlung in Länder außerhalb der EU, die Speicher- bzw. Löschfristen der personenbezogenen Daten und das Beschwerderecht bei einer Datenschutzaufsichtsbehörde (vgl. *Watteler/Ebel* in, Forschungsdatenmanagement sozialwissenschaftlicher Umfragedaten Grundlagen und praktische Lösungen für den Umgang mit quantitativen Forschungsdaten 2019, S. 60).

Hinweis für die Praxis:

Zentrale Voraussetzung der informierten Einwilligung ist die **Freiwilligkeit**. Das bedeutet, dass die Einwilligung ohne Zwang oder unzulässigen Druck erfolgen muss. Sie basiert auf **Aufklärung und Verständnis**. Es muss erkenntlich sein, auf welche (klar bestimmte) Maßnahme sich die Einwilligung bezieht. Daneben muss die betroffene Person in einer verständlichen Sprache über Art, Umfang und mögliche Folgen der Maßnahme informiert werden. Zur Aufklärung gehört auch, dass die Einwilligung verweigert werden kann und, wenn sie erteilt, die Einwilligung mit Wirkung für die Zukunft jederzeit widerrufen kann, bisherige Nutzungen aber nicht rückgängig gemacht werden können (vgl. <https://www.forschungsdaten-bildung.de/einwilligung>).

Relevante Rechtsgrundlagen sind:

- **Art. 4 Nr. 11 DSGVO** definiert die Einwilligung als „jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung [...]“.
- Für besondere Kategorien personenbezogener Daten, wie Gesundheitsdaten (Art. 9 Abs. 2 lit. a DSGVO), ist eine ausdrückliche Einwilligung erforderlich.
- Weitere Konkretisierungen finden sich z. B. im **§ 27 BDSG** (für Forschungszwecke) und in sektoralen Gesetzen wie der **DiGAV** oder dem **GDNG**.
- Flankierende Vorschriften sind Art. 6 Abs. 1 lit. a, Art. 7 DSGVO, § 51 BDSG (spezielle Anforderungen an Einwilligung bei besonderer Datenverarbeitung), § 630d, 630e BGB (Einwilligung in

medizinische Maßnahmen – z. B. für Behandlungsdaten), §§ 67 ff. SGB X (Verarbeitung durch Sozialleistungsträger), § 27 BDSG (für Forschung, insb. i.V.m. § 75 SGB X)

III. Zwischenfazit

Der „informed consent“ bildet die rechtliche und ethische Grundlage für eine verantwortungsvolle Nutzung von Gesundheitsdaten sowie für medizinische Maßnahmen. Er ist Ausdruck des Respekts vor der Autonomie und Selbstbestimmung der betroffenen Person und gewährleistet, dass Entscheidungen über die Nutzung personenbezogener Daten bewusst, informiert und freiwillig getroffen werden.

Damit verbindet der informed consent rechtliche Verbindlichkeit mit ethischer Legitimation und schafft Vertrauen in Forschung, Versorgung und Datenpraxis.

Im nächsten Abschnitt werden die Voraussetzungen und ethisch-rechtlichen Grenzen der **weiten Einwilligung („broad consent“)** mit Bezug zu § 6 Abs. 3 S. 4 GDNG dargestellt.

IV. Voraussetzungen der weiten Einwilligung

Für wissenschaftliche Zwecke kann eine Einwilligung auch **abstrakt** für Forschungsnutzungen erteilt werden, deren konkrete Zwecke zum Zeitpunkt der Datenerhebung noch **nicht bekannt** sind (sog. „**broad consent**“). Je präziser jedoch die Beschreibung des Forschungsrahmens erfolgt, desto eher kann sich der **Geltungsbereich der Einwilligung** auch auf weitergehende Nutzungen erstrecken, die über den ursprünglichen Erhebungszweck hinausgehen.

Wird eine **Veröffentlichung von Daten im Rahmen des Forschungsdatenmanagements (FDM)** angestrebt, sollte die Einwilligung ausdrücklich auch die **Speicherung, Verarbeitung und Veröffentlichung** dieser Daten umfassen. Ein praktikabler Ansatz ist eine **abgestufte Einwilligung**, die zwischen allgemeinen Forschungszwecken und konkreteren Datennutzungen unterscheidet.

Die weite Einwilligung muss – ebenso wie der *informed consent* – bestimmte **Mindestanforderungen** erfüllen. Sie richtet sich nach den Vorgaben der **DSGVO** und den **nationalen Regelungen**, insbesondere dem **Gesundheitsdatennutzungsgesetz (GDNG)**.

Der wesentliche Unterschied zur informierten Einwilligung besteht darin, dass der *broad consent* eine **pauschale Zustimmung** zu einer Vielzahl potenzieller, zum Zeitpunkt der Einwilligung noch nicht konkret bestimmbarer **Forschungsvorhaben** umfasst.

Die betroffene Person wird dabei über den **allgemeinen Zweck- und Rahmenkontext** informiert, nicht jedoch über jeden spezifischen künftigen Nutzungszweck. Sie verzichtet also auf eine vollständige Detailkenntnis vorab, behält jedoch ihr **Recht auf Widerruf und Transparenz** nach Art. 7 und 13 DSGVO.

Für die **Weitergabe an Dritte** gelten die engen Voraussetzungen des **§ 6 GDNG**, insbesondere die Anforderungen an **Zweckbindung, Pseudonymisierung und sichere Verarbeitungsumgebungen** (vgl. unten B. IV. 7).

Rechtlich stützt sich der *broad consent* auf **Art. 9 Abs. 2 lit. j DSGVO** in Verbindung mit **Art. 89 Abs. 1 DSGVO** sowie auf **§ 6 Abs. 3 S. 4 GDNG**, wonach eine Forschungsaufnahme im Sinne des Art. 89 DSGVO zulässig ist, sofern geeignete Garantien wie **Pseudonymisierung, Anonymisierung und sichere Verarbeitungsumgebungen** gewährleistet sind.

Im nächsten Abschnitt werden u.a. die ethischen und rechtlichen Safeguards behandelt, die eine weite Einwilligung flankieren und Missbrauch verhindern sollen.

1. Freiwilligkeit

Die Einwilligung muss **freiwillig** erfolgen (vgl. oben B. II. 1). Sie darf nicht unter Druck, Zwang oder aufgrund von Abhängigkeitsverhältnissen erteilt werden.

2. Ausdrücklichkeit

Die Einwilligung ist **schriftlich oder elektronisch** zu dokumentieren (vgl. oben B. II. 2). Eine stillschweigende oder konkludente Einwilligung ist unzulässig.

3. Zweckrahmen

Die Einwilligung darf sich auf mehrere Zwecke innerhalb eines definierten Forschungsbereichs oder -felds erstrecken (z. B. „medizinische Forschung“, „Epidemiologie“). Eine unbeschränkte, vollkommen unbestimmte Einwilligung ist unzulässig. Der Zweckrahmen muss möglichst klar beschrieben sein. Er sollte in der Regel durch die positive Begutachtung einer Ethikkommission oder einer vergleichbaren Prüfinstanz erstellt werden. Die Datenverwendung muss tatsächlich und ausschließlich zu wissenschaftlichen oder statistischen Zwecken erfolgen, Art. 89 DSGVO.

4. Informiertheit

Die betroffene Person ist **über Umfang, Zweck und Rahmenbedingungen** der beabsichtigten Datennutzung aufzuklären. Da bei einer weiten Einwilligung die Detailtiefe zwangsläufig begrenzt ist, sollte ein **wahrscheinlicher Verwendungsumfang** (ggf. exemplarisch) beschrieben werden. Die **Transparenzpflichten** nach **Art. 13 und 14 DSGVO** sind dabei **so weit wie möglich zu erfüllen**.

5. Schutz- und Transparenzmaßnahmen

Es müssen **geeignete Schutzmaßnahmen** implementiert sein, um Rechte der Betroffenen effektiv zu schützen. Dazu zählen insbesondere die Pseudonymisierung (und möglichst Anonymisierung) der Daten gem. Art. 89 Abs. 1 S. 3 DSGVO und das **Vorhalten technischer und organisatorischer Sicherheitsmaßnahmen** gem. Art. 32 DSGVO. Hier gilt es insbesondere klar definierte Zugriffsrechte und Kontrollmechanismen einzuhalten. Diese gehen ebenfalls mit der Begutachtung einer Ethikkommission einher.

Hinsichtlich der Datenweitergabe muss im Rahmen der Transparenzpflicht informiert werden. So ist der Betroffene darüber zu informieren, unter welchen Bedingungen eine Weitergabe der Daten an Dritte (andere Forschungseinrichtungen, Register etc.) möglich ist.

6. Widerrufbarkeit

Der **Widerruf** richtet sich nach den Grundsätzen unter **B. II. 5**. Er ist jederzeit und ohne Angabe von Gründen möglich; bereits erfolgte Verarbeitungen bleiben hiervon unberührt.

7. Hinweise und Rechtsgrundlagen

Auch bei der weiten Einwilligung ist die DSGVO (hier insbes. die [Art. 4 Nr. 11](#), [Art. 7](#), [Art. 13, 14](#), [Art. 89](#)) zu beachten. Daneben sind die einschlägigen Normen des GDNG für die rechtliche Zulässigkeit und dem Genügen der ethischen Standards von hervorgehobener Bedeutung. Das Erfordernis nachweislicher Schutzmaßnahmen ist beim broad consent wesentlich ausgeprägter und rechtlich relevanter als beim klassischen informed consent. Hintergrund dessen ist der unterschiedliche Regelungs- und Risikohorizont: Während sich die klassische informierte Einwilligung auf konkret benannte Zwecke, Empfänger und Verarbeitungen bezieht, die Risiken für die betroffenen Personen also relativ gut einschätzbar sind, müssen bei der weiten Einwilligung die Unsicherheiten, die aus der Unbestimmtheit resultieren, durch nachweisbare Schutzmaßnahmen (technisch und organisatorisch) kompensiert werden.

Gemäß § 6 Abs. 3 S. 1 GDNG ist die **Weitergabe der personenbezogenen Daten an Dritte** im Rahmen der Weiterverarbeitung nach Abs. 1 (dort: Weiterverarbeitung möglich soweit zur Qualitätssicherung und zur Förderung der Patientensicherheit; zur medizinischen, zur rehabilitativen und zur pflegerischen Forschung; oder zu statistischen Zwecken, einschließlich der Gesundheitsberichtserstattung erforderlich) **untersagt**. S. 4 sieht hierfür eine **Ausnahme** vor (vgl. dazu B. VI. 2.).

Beispiel für eine abgestufte Einwilligung im „Broad-Consent-Format“:

Ich wurde darüber aufgeklärt und stimme freiwillig zu, dass meine personenbezogenen Daten, insbesondere Gesundheitsdaten, im Rahmen der Studie „Gesundes Essen“ zu den in der angehängten Informationsschrift beschriebenen Zwecken erhoben und in pseudonymisierter Form aufgezeichnet, analysiert und ausgewertet werden dürfen.

☐ Ja

Ich willige ein, dass – abgesehen von meinem Namen – meine personenbezogenen Daten im Rahmen von wissenschaftlichen Publikationen und Analysen zur genannten Studie veröffentlicht werden dürfen.

☐ Ja

Ich willige in die Speicherung meiner personenbezogenen Daten inklusive meiner Kontaktdaten für die Dauer von 10 Jahren ab dem Zeitpunkt der Einwilligung ein, damit meine Daten über die genannte Studie hinaus für eventuelle Folgeprojekte zur Erforschung von gesundem Essen genutzt werden können.

☐ Ja

Abb. 9.3: Beispiel einer informierten Einwilligung im „Broad-Consent-Format“, Quelle: Baumann/Krahn 2020

Weiterführende Informationen

Einige Fachdisziplinen bieten Hilfestellungen und Formulierungsbeispiele für schriftlich verfasste informierte Einwilligungen (vgl. z. B. [VerbundFDB](#), RatSWD).

- [Mustererklärung für mündliche oder schriftliche Interviews](#) des Arbeitskreis Deutscher Markt- und Sozialinstitute
- [Empfehlungen und Muster-Einwilligungserklärungen](#) des RatSWD
- [Formulierungsbeispiele für "informierte Einwilligungen"](#) des VerbundFDB
- Vorlage für die [informierte Einwilligung zur Verarbeitung personenbezogener Daten](#)
- [Handreichung zur Informierten Einwilligung \(Erläuterungen zur Verwendung der QS-Vorlagen\)](#)

Während der *informed consent* auf individuelle Autonomie zielt, basiert der *broad consent* auf Vertrauen in institutionelle Verantwortung und gesellschaftliche Nutzenabwägung – ein Spannungsfeld, das im folgenden Abschnitt näher betrachtet wird.

VI. Spannungsfeld der Einwilligungsarten

1. Regelungshorizont

Wie dargestellt, richtet sich die **informierte Einwilligung (informed consent)** in erster Linie auf die **Aufklärung und Freiwilligkeit** der Datenfreigabe. Schutzmaßnahmen werden zwar ebenfalls verlangt (vgl. Art. 5, 24 und 25 DSGVO), gehören jedoch **nicht zum Kernkonzept der Einwilligung selbst**, sondern zu den **allgemeinen Pflichten des Verantwortlichen** bei der Datenverarbeitung.

Die **weite Einwilligung (broad consent)** geht darüber hinaus: Sie setzt eine **institutionalisierte Verantwortung** voraus und verlangt **verstärkte Schutz-, Dokumentations- und Nachweispflichten**, die zugleich **Voraussetzung der Wirksamkeit** werden. Dazu zählen insbesondere:

- die **Einbindung von Datenschutzaufsichtsbehörden und Ethikkommissionen**,
- die Beachtung **spezialgesetzlicher Vorgaben**, insbesondere nach dem **Gesundheitsdatennutzungsgesetz (GDNG)**,
- sowie die Implementierung von **technischen und organisatorischen Schutzmaßnahmen** nach Art. 32 DSGVO und die Einhaltung von **Art. 89 Abs. 1 DSGVO** („geeignete Garantien“).

Während beim *informed consent* die **individuelle Autonomie** im Mittelpunkt steht, zielt der *broad consent* auf eine **institutionell abgesicherte Verantwortungsgemeinschaft**. Damit verschiebt sich der Regelungshorizont von der persönlichen Entscheidung hin zur **governance-basierten Kontrolle** der Datennutzung.

Beispielhaft konkretisiert § 6 Abs. 3 S. 4 GDNG diese Anforderungen: Eine Weitergabe von Gesundheitsdaten zu Forschungszwecken darf nur erfolgen, wenn geeignete Garantien – etwa Pseudonymisierung, sichere Verarbeitungsumgebungen und datenschutzrechtliche Prüfverfahren – nachweislich bestehen.

Das Spannungsfeld zwischen individueller Einwilligung und institutioneller Verantwortung wirft damit grundlegende Fragen der **Verhältnismäßigkeit, Datenminimierung und Widerrufbarkeit** auf, die im folgenden Abschnitt näher beleuchtet werden.

2. Rechtliche Fundamente für Schutzmaßnahmen beim broad consent

Weite Zwecke müssen durch zusätzliche Garantien abgesichert werden, Art. 5 Abs. 1 lit. a und b (Zweckbindung, Transparenz). Die sog. Forschungsausnahme des Art. 89 Abs. 1 DSGVO fordert ebenfalls angemessene Garantien, insbesondere Datensparsamkeit und Pseudonymisierung. Diese ergeben sich aus mehreren Ebenen des Datenschutzrechts:

a) Datenschutzrechtliche Grundprinzipien

Nach **Art. 5 Abs. 1 lit. a und b DSGVO** müssen auch bei weiter gefassten Einwilligungen die Grundsätze der **Rechtmäßigkeit, Transparenz und Zweckbindung** beachtet werden. Die sog. **Forschungsausnahme** des **Art. 89 Abs. 1 DSGVO** verlangt hierbei *angemessene Garantien*, insbesondere **Datenminimierung** und **Pseudonymisierung**. Diese „Safeguards“ dienen dazu, die weite Zweckbestimmung mit dem Grundrecht auf Datenschutz (Art. 8 GRCh) in Einklang zu bringen.

b) Rechenschaftspflicht und „Privacy by Design“

Die **Rechenschaftspflicht** (Art. 5 Abs. 2 DSGVO) und die Grundsätze des **Datenschutzes durch Technikgestaltung** (*privacy by design*) sowie des **datenschutzfreundlichen Voreinstellungen** (*privacy by default*) ergeben sich aus **Art. 24 und 25 DSGVO**. Sie verpflichten den Verantwortlichen, **technische und organisatorische Maßnahmen (TOMs)** bereits bei der Planung eines Verarbeitungssystems

vorzusehen und deren Wirksamkeit **nachweisen** zu können. Ziel ist es, Datenschutz **strukturell** und **präventiv** in die Datenverarbeitung zu integrieren („Datenschutz durch Technikgestaltung“). → Vgl. hierzu die Definition unter dsgvo-gesetz.de/themen/privacy-by-design.

Hinter dem Begriff „Privacy by design“ verbirgt sich nichts Weiteres als „Datenschutz durch Technikgestaltung“. Dahinter steckt der Gedanke, dass der Datenschutz bei Datenverarbeitungsvorgängen am besten eingehalten wird, wenn er bei deren Erarbeitung bereits technisch integriert ist“ (<https://dsgvo-gesetz.de/themen/privacy-by-design/>).

c) Ausnahmen und Kompensationsrechte nach Art. 89 DSGVO

Art. 89 DSGVO erlaubt, unter bestimmten Voraussetzungen **Abweichungen von einzelnen Datenschutzgrundsätzen**, sofern diese zur Durchführung wissenschaftlicher Forschung erforderlich sind und gleichzeitig **Kompensationsrechte** der betroffenen Personen bestehen. Dazu zählen insbesondere:

- das **Auskunftsrecht** (Art. 15 DSGVO),
- das **Recht auf Berichtigung** (Art. 16 DSGVO),
- das **Recht auf Einschränkung der Verarbeitung** (Art. 18 DSGVO) und
- das **Widerspruchsrecht** (Art. 21 DSGVO).

Diese Rechte dürfen nur insoweit eingeschränkt werden, als sie die Forschungs- oder Statistikzwecke **unmöglich machen oder ernsthaft beeinträchtigen** und die Beschränkung **notwendig** ist. Eine systematische Auslegung ergibt sich aus den **Erwägungsgründen 156–163 DSGVO**, die den Ausgleich zwischen Forschungsfreiheit und Datenschutz näher konkretisieren (u. a. Verweis auf **VO (EU) Nr. 536/2014** über klinische Prüfungen).

d) Nationale Konkretisierung durch § 27 BDSG

Korrespondierend erlaubt § 27 Abs. 1 BDSG Abweichungen für wissenschaftliche Zwecke nur bei geeigneten und spezifischen Maßnahmen nach Art. 89 DSGVO. **§ 27 Abs. 2 BDSG beschränkt** dann iSd. des Art. 89 Abs. 2 DSGVO die Rechte aus **Art. 15, 16, 18, 21 DSGVO** (o.g. Rechte der betroffenen Person) **insoweit**, wie sie die Forschungs-/Statistikzwecke unmöglich machen oder ernsthaft beeinträchtigen und die Beschränkung **notwendig** ist. Zusätzlich besteht die Sonderregel zu Art. 15 DSGVO, die den unverhältnismäßigen Aufwand berücksichtigt: „*Das Recht auf Auskunft gemäß Artikel 15 der Verordnung (EU) 2016/679 besteht darüber hinaus nicht, wenn die Daten für Zwecke der wissenschaftlichen Forschung erforderlich sind und die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde.*“

e) Spezielle Regelungen des Gesundheitsdatennutzungsgesetzes (GDNG)

Nach **§ 6 Abs. 3 S. 1 GDNG** ist die **Weitergabe personenbezogener Gesundheitsdaten an Dritte** grundsätzlich **verboten**.

- **Satz 2** erlaubt Ausnahmen nur bei einer **Einwilligung** oder auf Grundlage einer **besonderen Rechtsvorschrift**.
- **Satz 3** gestattet die **Übermittlung anonymisierter Daten**.
- **Satz 4** enthält eine wichtige **Sonderregel für die Verbundforschung**: Eine gemeinsame („standortübergreifende“) Nutzung und Verarbeitung personenbezogener Daten ist zulässig, wenn
 1. die Nutzung für Zwecke des Abs. 1 erforderlich ist,
 2. geeignete **Safeguards** (insbesondere Pseudonymisierung, Anonymisierung, Transparenz) eingehalten werden,
 3. die Interessen der Verantwortlichen die Interessen der betroffenen Person **erheblich überwiegen**, und
 4. die zuständige **Datenschutzaufsichtsbehörde** zustimmt.

Damit **durchbricht § 6 Abs. 3 S. 4 GDNG** das grundsätzliche Weitergabeverbot des Satzes 1, sofern die genannten Voraussetzungen kumulativ erfüllt sind. Nach der **Gesetzesbegründung (BT-Drs. 20/9046, S. 67 ff.)** handelt es sich dabei **nicht** um eine Einschränkung von Betroffenenrechten im Sinne des **Art. 89 Abs. 2 DSGVO**, sondern um eine **Forschungserlaubnis mit eingebauten Sicherungsmechanismen**.

f) Forschungsethische Leitlinien

Ergänzend fordern **wissenschaftliche und forschungsethische Kodizes** (z. B. **DFG-Kodex „Leitlinien zur Sicherung guter wissenschaftlicher Praxis“**, **OECD Guidelines on Human Biobanks and Genetic Research Databases**) die **nachweisliche Einrichtung und regelmäßige Überprüfung** solcher Schutzmaßnahmen. Diese dienen dazu, die geringere Spezifität des *broad consent* **inhaltlich zu kompensieren** und das Vertrauen der betroffenen Personen zu sichern.

Das GDNG enthält insoweit **keine weitergehende Ermächtigung**, sondern setzt die unionsrechtlichen Vorgaben in nationales Recht um.

Zum grundsätzlichen Verständnis sei noch einmal erwähnt, dass die Weitergabe von personenbezogenen Daten an Dritte generell verboten ist (§ 6 Abs. 3 S. 1 GDNG). Auch das GDNG sieht vor, dass dies nur mit einer Einwilligung oder im Wege einer speziellen Rechtsvorschrift (§ 6 Abs. 3 S. 2 GDNG) zulässig ist. Anonymisierte Daten dürfen übermittelt werden (§ 6 Abs. 3 S. 3 GDNG) (BT Drs 20/9046). Der die Verbundforschung betreffende § 6 Abs. 3 S. 4 GDNG erlaubt abweichend vom Verbot die gemeinsame Nutzung und Verarbeitung zwischen Einrichtungen („standortübergreifend“), wenn kumulativ:

- die Nutzung für Zwecke des Abs. 1 erforderlich ist,
- die Safeguards (u.a. Pseudonymisierung/Anonymisierung, Transparenz) eingehalten werden,
- die Interessen des Verantwortlichen die Interessen der betroffenen Person an einem Ausschluss der Verarbeitung erheblich überwiegen, und
- die zuständige Datenschutzaufsichtsbehörde zustimmt (hier gilt es die Fristen zu beachten).

Damit durchbricht § 6 Abs. 3 S. 4 GDNG das Weitergabeverbot des § 6 Abs. 3 S. 1 GDNG unter den genannten Bedingungen. Es handelt sich nicht um eine Einschränkung von Betroffenenrechten i.S.v. Art. 89 Abs. 2 DSGVO (BT Drs 20/9046).

3. Praktische Ausgestaltung der Nachweis- und Schutzpflicht

Beim broad consent müssen Schutz- und Nachweispflichten bereits im Vorfeld festgelegt, dokumentiert und überprüfbar sein.

Technische Maßnahmen umfassen insbesondere:

- Pseudonymisierung oder – soweit möglich – Anonymisierung,
- Zugriffsbeschränkungen (Role-Based Access Control),
- Verschlüsselung bei Speicherung und Übertragung,
- sowie Logging- und Monitoring-Prozesse für Datenzugriffe.

Organisatorische Maßnahmen betreffen:

- eine Governance-Struktur (z. B. Ethikkommission, Data Access Committee),
- klare Kriterien für zukünftige Datennutzungsentscheidungen,
- die Verpflichtung der Empfänger auf Vertraulichkeit,
- sowie regelmäßige Schulungen und Sensibilisierungen der Beteiligten.

Hinzu treten eine dokumentierte Nachweisführung, die Eintragung der Verarbeitungstätigkeiten in das Verzeichnis nach Art. 30 DSGVO, ggf. ein Ethikvotum oder eine Datenschutz-Folgenabschätzung (DSFA) nach Art. 35 DSGVO, sowie regelmäßige Audit- und Review-Verfahren.

Diese Instrumente gewährleisten, dass die weite Einwilligung durch überprüfbare technische und organisatorische Sicherungen flankiert wird.

4. Spannungsfeld / Zusammenfassung

Die informierte Einwilligung verlangt einen konkret zu bestimmenden Zweck, während die breite Einwilligung eine (in Grenzen erlaubte) Zustimmung zu „Bereichen“ der Forschung ermöglicht, wenn der konkrete Zweck bei Erhebung noch nicht feststeht. Das kollidiert mit Spezifitäts-, Transparenz- und Widerrufserfordernissen und wird nur durch strenge Safeguards abgedeckt (Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_de.pdf).

Im Wesentlichen bestehen die Spannungen also zwischen der Spezifität und Flexibilität: So muss die informierte Einwilligung „freiwillig, spezifisch, informiert, unmissverständlich“ (Art. 4 Nr. 11 DSGVO)

sein, während sich die weite Einwilligung mit Erwägungsgrund 33 auf höherwertige Ziele (etwa bestimmte Bereiche der wissenschaftlichen Forschung) stützt, wenngleich auch betont wird, dass eine ausreichende Bestimmtheit weiterhin nötig ist (<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A32016R0679>).

Hinsichtlich der Rechtsgrundlage und Zweckbindung ist bei Gesundheitsdaten (Art. 9 DSGVO) eine ausdrückliche Einwilligung möglich, allerdings wird oft für die Sekundärnutzungen (= spätere Nutzung der Daten, die im Wege der Primärnutzung durch etwa Behandlung und Abrechnung zur Patientenversorgung erhoben wurden) Art. 9 Abs. 2 lit. j i.V.m. Art. 89 DSGVO (Forschung + Safeguards) gewählt. Hier stellen sich Abwägungsfragen, welche die Autonomie durch Einwilligung, der Praktikabilität durch das Forschungsprivileg gegenüberstellen.

Ebenfalls im Spannungsverhältnis stehen der Widerruf und die Datenminimierung. Grundsätzlich muss ein Widerruf jederzeit möglich bleiben (Art. 7 Abs. 3 DSGVO), zugleich verfolgt Art. 89 DSGVO Safeguards hinsichtlich der Pseudonymisierung und Anonymisierung, was die Rückverfolgbarkeit und damit letztlich den Widerruf erschwert. Zugleich ist das Gebot der Transparenz nicht gewahrt.

Beispiel: Ein Forschungsprojekt speichert Gesundheitsdaten nur pseudonymisiert und der Schlüssel zur Identität der Proband:innen liegt bei einer separaten Stelle („Trusted Third Party“). Wenn die betroffene Person ihre Einwilligung widerruft, muss der Forscher diesen Widerruf über den Schlüssel zurückverfolgen können. Wird der Schlüssel aber gelöscht (also faktisch anonymisiert), kann der Widerruf nicht mehr wirksam umgesetzt werden, da kein Bezug zur Person mehr besteht. Darüber hinaus ist das Transparenzgebot (Art. 5 Abs. 1 lit. a DSGVO) nicht mehr gewahrt, weil die Proband:innen nicht mehr vollumfänglich darüber informiert werden können, inwieweit die Daten nach entsprechend gestalteten Pseudonymisierungs- oder Anonymisierungsverfahren verarbeitet werden.

Die Transparenz kollidiert prinzipiell auch mit der Erwartungssteuerung. So verlangt die weite Einwilligung eine klare Rahmenbeschreibung der Forschungsbereiche und fortlaufende Information als Schutz vor „Überrumpelungseffekte“ trotz formaler Einwilligung (vgl. EDPB-Leitlinie, Erwägungsgrund 33).

Insgesamt kann die weite Einwilligung wissenschaftliche Flexibilität schaffen, setzt allerdings durch die Spezifität im Forschungsrahmen, den Safeguards, dem Widerruf und ggf. Rechtebeschränkungen nach Art. 89 DSGVO bzw. § 27 BDSG, enge Leitplanken.

Mögliche Erlaubnistatbestände, die eine Einwilligung zum redundanten Beiwerk machen könnten, sind genaustens an ihren Merkmalen zu überprüfen. Rechtssachverständige prüfen Tatbestände wie § 27 BDSG und auch die vielen Landesdatenschutzgesetze (z. B. § 17 DSG-NRW, § 13 LDSG-BW, § 13 NDSG) auf Ausnahmen für wissenschaftliche Forschungszwecke. Danach ist die Verarbeitung von personenbezogenen Daten erlaubt, wenn die mit dem Forschungsvorhaben verfolgten Interessen diejenigen der betroffenen Personen überwiegen (vgl. [forschungsdaten.info](https://www.forschungsdaten.info)). Da dies jedoch nur selten zutrifft, solltest du im Zweifelsfall immer eine Einwilligung einholen.

Damit wird deutlich: Der *broad consent* ist kein Ersatz, sondern eine **erweiterte Form der Einwilligung**, die wissenschaftliche Offenheit mit rechtlich-ethischen Sicherungen verbindet. Seine Wirksamkeit

hängt maßgeblich von der **technischen Nachweisführung**, der **organisatorischen Kontrolle** und der **institutionellen Transparenz** ab.

B. Datenschutzerfordernisse

I. Datenschutzrechtliche Grundlagen bei der Verarbeitung von Forschungsdaten

Zur Wiederholung: Bei der Erhebung, Speicherung, Verarbeitung und Weitergabe von Forschungsdaten mit Personenbezug sind Datenschutzrechte zu beachten. Wenn du als Wissenschaftler:in an einer Hochschule mit entsprechenden Daten arbeitest, empfiehlt es sich die Grundzüge insbesondere der folgenden Gesetzestexte zu kennen:

- Datenschutz-Grundverordnung der Europäischen Union (DSGVO)
- Bundesdatenschutzgesetz (BDSG)
- Die jeweiligen Datenschutz- und Informationsfreiheitsgesetze der Länder

Daten ohne Personenbezug bzw. anonymisierte Informationen fallen dagegen nicht unter das Datenschutzrecht und können grundsätzlich unter Berücksichtigung sonstiger Rechte (z. B. Urheberrechte) frei verarbeitet werden.

Darüber hinaus gibt es in der Rechtsprechung Datenkategorien, die als **besonders sensibel** angesehen werden. Hierzu zählen bspw. Daten über den Gesundheitszustand einer Person, deren sexuelle Orientierung sowie politische oder religiöse Ansichten. Eine Auflistung dieser **besonderen Kategorien personenbezogener Daten** findet sich in [Art. 9 DSGVO](#).

Diese Daten unterliegen grundsätzlich (zu den Ausnahmen vgl. die Ausführungen zum GDNG) einem besonderen Schutz und besonderen Sorgfaltspflichten bei der Verarbeitung. Dies bedeutet bspw., dass Teilnehmer:innen wissenschaftlicher Studien der Verarbeitung dieser besonderen Kategorien personenbezogener Daten vor der Datenerhebung ggf. ausdrücklich zustimmen müssen.

Bei der Verarbeitung personenbezogener Daten sind die sog. allgemeinen Datenverarbeitungsgrundsätze ([Art. 5 DSGVO](#)) zu beachten:

- Personenbezogene Forschungsdaten dürfen nur erhoben werden, wenn sie zum Erreichen des Forschungszweckes **erforderlich** sind.
- Die Erhebung und Verarbeitung muss gegenüber den betroffenen Personen **transparent** und mit der gebotenen Redlichkeit geschehen.
- Die Betroffenen müssen jederzeit die Möglichkeit haben, die Verarbeitung ihrer persönlichen Daten **nachvollziehen** zu können, und dürfen nicht durch falsche und unterbliebene Informationen in die Irre geführt werden.
- Der **Schutz der Privatsphäre** durch Schutz der personenbezogenen Daten sollte bei allen Überlegungen zur Erhebung und Verarbeitung im Mittelpunkt stehen.
- Die Daten müssen zudem die Lebensumstände der betreffenden Person **korrekt** wiedergeben, dürfen sie also nicht verfälschen.

- Sie sind im Rahmen des Zumutbaren vor Missbrauch (z. B. Entnahme, Veränderung, Beschädigung) **technisch und organisatorisch** zu schützen.

II. Mittel zur Entfernung identifizierender Merkmale

Allgemein gilt, dass personenbezogene Forschungsdaten nach der Erhebung, sobald es der Forschungszweck zulässt (spätestens mit Abschluss des Forschungsvorhabens), **anonymisiert werden müssen (A. II. 4 d)**.

Der erste Schritt ist dabei die **Entfernung direkter Identifikationsmerkmale** (Name, Adresse, Telefonnummer usw.). Oftmals reicht dies jedoch nicht aus, um einen Personenbezug auszuschließen. In diesem Fall kann die **Reduzierung der Informationsgenauigkeit** (Aggregation) ein wirksames Mittel sein, das zudem erlaubt gewisse Informationsteile trotzdem zu behalten.

Aggregation

Zusammenfassung mehrerer gleichartiger Einzelwerte zur Verringerung der Granularität von Informationen. Aus der zusammengefassten Information ist ein Rückschluss auf die Einzelinformationen nicht mehr möglich.

Hierbei werden also detaillierte Einzelinformationen (z. B. Gehalt im letzten Monat) in Klassen gruppiert (z. B. Unter-, Mittel-, Oberschicht). Der Grad der Aggregation, der nötig ist um einen Personenbezug auszuschließen kann dabei variieren. Er hängt im Wesentlichen davon ab, welche weiteren potenziellen Identifikationsmerkmale in den Daten vorhanden sind oder aus externen Quellen zugespielt werden können.

Beispiel für eine graduelle Aggregation:

Adresse → Ort → Bundesland → Ost/West → Land → Kontinent

Es ist in jedem Fall sorgfältig zu prüfen, welche der zur Verfügung stehenden Mittel am geeignetsten und verhältnismäßigsten erscheinen, die identifizierenden Merkmale so zu entfernen, dass auch mit etwaigem Zusatzwissen sowie umfangreichen Kapazitäten zur Datenrecherche und -aggregation keine oder nur eine sehr eingeschränkte De-Anonymisierung möglich ist.

Ein **Aufschub der Anonymisierung** ist nur dann möglich, wenn jene Merkmale, mit deren Hilfe ein Personenbezug hergestellt werden kann, **zum Erreichen des Forschungszweckes oder einzelner Forschungsschritte benötigt** werden. Dies ist beispielsweise während eines noch laufenden Forschungsprojektes, welches auf biometrische Daten zurückgreift, der Fall.

In diesem Fall müssen die personenbezogenen Merkmale jedoch unmittelbar nach der Erhebung **getrennt und sicher gespeichert** werden. Dies kann bspw. durch eine Pseudonymisierung der personenbezogenen Forschungsdaten erfolgen.

Ein Beispiel ist die Verwendung einer **Schlüsseltabelle**, die den Klarnamen von Personen entsprechende **ID-Codes** zuweist. So kann der Personenbezug nur hergestellt werden, wenn man im Besitz der Schlüsseltabelle ist. Diese kann ggf. auch von einem unabhängigen Treuhänder verwahrt werden.

Die auf diese Weise verarbeiteten Daten weisen aber bis zur Löschung der separat zu speichernden personenbezogenen Merkmale weiterhin einen Personenbezug auf und unterliegen damit den datenschutzrechtlichen Vorgaben.

I. Geheimhaltungspflicht

„Geheimhaltung“ im Kontext der Gesundheitsdatennutzung bezeichnet den Schutz vor unbefugter Kenntnisnahme, Offenbarung oder Weitergabe von Daten, die Rückschlüsse auf den Gesundheitszustand, Behandlungen oder personenbezogene Krankheitsdaten zulassen. Sie ist ein Kernelement der ärztlichen Schweigepflicht, des Datenschutzrechts und – seit 2024 – ausdrücklich auch der Forschungsnutzung von Gesundheitsdaten.

1. Begriff und Funktion

Die Geheimhaltungspflicht bedeutet, dass Gesundheitsdaten grundsätzlich nur von den zur Behandlung oder Forschung befugten Personen eingesehen und verarbeitet werden dürfen. Damit wird vor allem der Schutz der Vertraulichkeit und die Wahrung des Patientenvertrauens verfolgt. Ebenso wie die Einwilligung, leitet sich die Geheimhaltung aus den Grundrechten ab. Sie ist eine Ausprägung der informationellen Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG und des Datenschutzes (Art. 7, 8 GRCh; Art. 8 EMRK).

Neben dem Patient:innenvertrauen, der informationellen Selbstbestimmung und der Datensicherheit, dient die Geheimhaltungspflicht der Integrität von Forschung und Versorgung. So sind seit 2024 auch die sog. speziellen Forschungsgeheimnisse geregelt (s.u.).

In praxi ist die Geheimhaltung auch die Grundlage für die Schweigepflicht und strafbewehrte Missbrauchsverbote.

2. Rechtsgrundlagen

a) Berufsrechtliche Schweigepflichten

Von hervorgehobener Bedeutung – und bezogen auf sämtliche Gesundheitsdaten – ist die Strafbarkeit der Verletzung von Privatgeheimnissen nach § 203 StGB. Die von der Strafnorm erfassten Geheimnisträger sind u.a. Ärzte, Psychotherapeuten, Angehörige anderer Heilberufe, Behördenmitarbeiter im Gesundheitswesen sowie Personen, die an deren beruflicher Tätigkeit mitwirken.

Auch Forschungsprojekte, die auf Gesundheitsdaten zugreifen, können in die Reichweite des § 203 StGB fallen, wenn Daten von Geheimnisträgern stammen oder von ihnen offenbart werden. Sofern also im jeweiligen Forschungsvorhaben Gesundheitsdaten erhoben bzw. verarbeitet werden, die aus ärztlicher Behandlung, Therapie oder Verwaltung stammen, fallen die Forschenden unter die Schweigepflicht des Abs. 1. Neben weiteren Geheimnisträgern, die von Abs. 2 erfasst werden, sind „mitwirkende Personen“ i.S.d. Abs. 3 zur Verschwiegenheit verpflichtet. Demnach dürfen sich Geheimnisträger berufsmäßig tätiger Gehilfen und sonstiger mitwirkender Personen bedienen, müssen diese aber ausdrücklich zur Verschwiegenheit verpflichten. Zu dieser Personengruppe zählen sämtliche Projektpartner, IT-Dienstleister, Forschende, studentische Hilfskräfte oder externe Entwickler, die Zugang zu Gesundheitsdaten haben. Ohne diese Verpflichtungen riskieren die Akteure strafbare Offenbarungen.

Andersherum dürfen die Geheimnisträger die Geheimnisse nur an Mitwirkende weitergeben, wenn diese zur Verschwiegenheit verpflichtet wurden. Sobald Ärzte, Krankenkassen oder Behörden Gesundheitsdaten ins Projekt einspeisen, dürfen sie diese nur dann weitergeben, wenn auf der Empfängerseite die Verschwiegenheitspflicht organisatorisch und rechtlich abgesichert ist. Diese organisatorische und rechtlich Absicherung der Verschwiegenheitspflicht ergibt sich aus Abs. 4.

Gem. Abs. 5 sind auch die Mitwirkenden i.S.d. Abs. 3 selbst strafbar, wenn sie Geheimnisse unbefugt offenbaren. Auch der Versuch ist strafbar (Abs. 6).

Weitere, mit dem Berufsrecht in Verbindung zu bringende Regelungen ergeben sich aus den jeweiligen Berufsordnungen der Ärzte, Rechtsanwälte, Notare, Steuerberater usw. Diese enthalten eigenständige Schweigepflichten. So bestimmt etwa § 9 der (nicht unmittelbar geltenden) *Musterberufsordnung für Ärzte (MBO-Ä)* die ärztliche Schweigepflicht. Die MBO-Ä dient jedoch lediglich als Vorlage und wird durch die 17 Landesärztekammern in ihren eigenen Berufsordnungen umgesetzt, die jeweils verbindlich gelten.

b) Weitere Rechtsgrundlagen für die Geheimhaltungspflicht

Grundsätzlich lässt sich festhalten, dass sämtliche Gesetze und Normen, die das Datenschutzrecht betreffen, eine gewisse Geheimhaltung implizieren. Gemäß der erwähnten Art. 5, 6, 9 DSGVO und der §§ 22 ff. BDSG, ist etwa die Verarbeitung von Gesundheitsdaten nur bei Vorliegen strenger Voraussetzungen zu gestatten.

Im Sozialrecht sind die §§ 67 ff. SGB X zu nennen. Diese regeln den Schutz von Sozialdaten (vgl. oben) und werden durch spezielle Vorschriften im SGB V und SGB VII (etwa zur Weitergabe an den Medizinischen Dienst) ergänzt.

Daneben gibt es gesundheitsrechtliche Spezialnormen wie § 6 GDNG; der die Geheimhaltungspflichten im Kontext von Gesundheitsdatennutzung für Forschung regelt. Vgl. auch § 11 Transplantationsgesetz und die §§ 6 – 15a Infektionsschutzgesetz.

3. Rechtmäßigkeit / Rechtfertigung

Nimmt medizinisches Personal Patientendaten (d.h. Geheimnisse, s.o.) auf, indem diese anvertraut oder bekannt werden, wird die datenaufnehmende Person i.d.R. dazu befugt sein. Problematisch i.S.v. strafbar wird es dann, wenn dieses Geheimnis wiederum unbefugt offenbart wird. Hier könnte der Straftatbestand des § 203 StGB erfüllt sein.

Besonders problematisch sind dabei **Konstellationen mit Mehrpersonenverhältnissen**. Die Verletzung der Geheimhaltungspflicht kann aber auch dann „gerechtfertigt“ sein. Juristisch müsste hier zwischen dem tatbestandsausschließenden Einverständnis und der Einwilligung als Rechtfertigungsgrund für die tatbestandlich gegebene Verletzung des Privatgeheimnisses unterschieden werden. Nur so viel: Ein Offenbaren von Geheimnissen ist schon (tatbestandlich) nicht gegeben, wenn an die berufsmäßig tätigen Gehilfen oder die in den Betrieb eingebundene Personen als „**zum Wissen Berufene**“ gelten. Der

Berufsgeheimnisträger handelt daher rechtmäßig, wenn er diesen Personen Zugang zu geheimhaltungsbedürftigen Informationen ermöglicht. Vertraut jedoch ein Gehilfe selbst unbefugt Geheimnisse Dritten an, macht er sich nach § 203 Abs. 4 strafbar. Strafrechtlich bleibt die Offenbarung von Geheimnissen gegenüber extern Mitwirkenden zwar grundsätzlich tatbestandsmäßig, sie ist jedoch erlaubt, soweit sie für die Inanspruchnahme ihrer Tätigkeit erforderlich ist. Dies gilt auch für mehrstufige Unterauftragsverhältnisse. Allerdings dürfen Offenbarungen nicht über das Notwendige hinausgehen.

Die Geheimnissphäre soll grundsätzlich beim Berufsgeheimnisträger verbleiben; notwendige Offenbarungen sind auf das erforderliche Maß zu beschränken. **Beispiele** sind Telefondienste, externe Schreibdienste oder IT-Wartungen, die zwangsläufig Kenntnismöglichkeiten eröffnen. Schon die bloße Möglichkeit der Einsicht in Geheimnisse gilt als Offenbarung. Alles, was darüber hinausgeht, etwa die Mitteilung zusätzlicher Inhalte an einen IT-Mitarbeiter, bleibt strafbar (BeckOK StGB/Weidemann, 66. Ed. 1.8.2025, StGB § 203 Rn. 38-39.1, beck-online).

Demgegenüber kann die tatbestandsmäßig erfüllte Offenbarung dennoch gerechtfertigt sein. Nach herrschender Meinung führt jedoch bereits die Befugnis des Täters zur Offenbarung zum Ausschluss der Rechtswidrigkeit. Ein den Tatbestand rechtfertigender Grund lässt sich immer über die Einwilligung erreichen. Daher sollte sie von dir nach Möglichkeit eingeholt werden.

Die Konstellation der **mutmaßlichen Einwilligung** rechtfertigt eine Handlung, wenn sie im Interesse des Betroffenen liegt und anzunehmen ist, dass er zustimmen würde, aber eine ausdrückliche Einwilligung nicht rechtzeitig eingeholt werden kann. Für § 203 StGB bedeutet das, dass die Offenbarung nur zulässig ist, wenn das Interesse des Betroffenen daran offensichtlich ist, etwa bei Bewusstlosigkeit oder bestimmten postmortalen Konstellationen. Ein bloßes Schweigen oder fehlendes Einverständnis reicht nicht aus, um automatisch eine mutmaßliche Einwilligung anzunehmen (BeckOK StGB/Weidemann, 66. Ed. 1.8.2025, StGB § 203 Rn. 52- 53, beck-online). Im Kontext der Forschung ist dies wohl eher unwahrscheinlich.

Für die Nutzung von Gesundheitsdaten und deren Einbindung in Forschung bestehen allerdings auch bestimmte **gesetzliche Offenbarungspflichten und -befugnisse**. Besonders relevant sind dabei die Vorschriften des Infektionsschutzgesetzes, die Meldungen bestimmter Krankheiten verlangen, sowie das Transplantationsgesetz, das Offenbarungen im Bereich der Organtransplantation regelt. Auch das Sozialrecht enthält einschlägige Vorgaben: Krankenkassen haben kein originäres Einsichtsrecht in Behandlungsunterlagen, sondern können nur über den Medizinischen Dienst Daten erhalten, der hierzu ausdrücklich befugt ist. Daneben bestehen Offenbarungsrechte im Bereich der Unfallversicherung. Zudem ist der Datenschutzbeauftragte mit Kontroll- und Überwachungsbefugnissen ausgestattet. Für Forschungsvorhaben spielen auch Sachverständige eine wichtige Rolle: Während Befundtatsachen im Rahmen eines gerichtlichen Gutachtens weitergegeben werden dürfen, sind zusätzliche Informationen, die nicht Teil des Untersuchungsauftrags sind, nur mit Zustimmung des Betroffenen verwertbar. Eine Wiederverwendung von Daten aus früheren Gutachten in anderen Verfahren ist ohne erneute Zustimmung ebenfalls ausgeschlossen (BeckOK StGB/Weidemann, 66. Ed. 1.8.2025, StGB § 203 Rn. 54- 56, beck-online).

Wir merken uns:

- Nur Daten, die durch Einwilligung, gesetzliche Grundlage (hierzu besser eine Abklärung mit der Rechtsabteilung) oder nach Anonymisierung (vgl. oben) zugänglich gemacht wurden, dürfen genutzt werden.
- Alle externen Mitwirkenden (IT, Forschung usw.) sind ausdrücklich zur Verschwiegenheit zu verpflichten.

C. Entscheidungsbefugnis

Neben dem Datenschutz ist eine weitere wichtige Frage, wer über den Umgang mit den Forschungsdaten, insbesondere über ihre Veröffentlichung, entscheiden kann. In der Regel kann diejenige Person, der die Forschungsdaten "zugeordnet" sind, auch über deren Umgang wie z. B. deren Veröffentlichung entscheiden. Eine solche "Zuordnung" kann sich etwa aus dem Urheberrecht, dem Dienstvertragsrecht oder dem Patentrecht ergeben.

I. Urheberrechte und Leistungsschutzrechte

In der Regel kann **die urheberrechtliche Schutzfähigkeit einzelner Forschungsdaten nur im Einzelfall** und selbst dann nicht mit hinreichender Rechtssicherheit beurteilt werden. Gleichwohl lassen sich verschiedenen Fallgruppen von Forschungsdaten nach der konkreten Art der verkörperten Informationen und vor allem deren Gewinnung unterscheiden:

- **Qualitative Forschungsdaten** sind z. B. Sprachwerke wie qualitative Interviews oder längere Texte. Sie **können grundsätzlich urheberrechtlich geschützte Formulierungen, Strukturen und Gedankenführungen enthalten**. Ein urheberrechtlicher Schutz ist ausgeschlossen, wenn Formulierungen, Struktur und Gedankenführung im Wesentlichen durch fachliche Gepflogenheiten vorgegeben sind.
- **Wissenschaftliche Darstellungen**, wie Zeichnungen, Pläne, Karten, Skizzen und Tabellen, **können einem urheberrechtlichen Schutz unterliegen**, wenn die Darstellung nicht durch Sachzwänge oder fachwissenschaftliche Gepflogenheiten vorgegeben ist, sondern ein Gestaltungsspielraum der Wissenschaftler:innen besteht.
- Unter den gleichen Voraussetzungen sind auch **Fotografien und andere Lichtbilder urheberrechtlich geschützt**. Hierunter fallen neben Fotografien auch Aufnahmen aus bildgebenden Verfahren, wie z. B. Röntgen-, Kernspin und Computertomografiebilder sowie Fotografien und Einzelbilder aus Filmen.

- **Quantitative Daten** sind z. B. Messergebnisse oder statistische Daten. Im Rahmen standardisierter Erhebungen wird **in den meisten Fällen kein urheberrechtlicher Schutz** bestehen.
- Bei (quantitativen) Forschungsdaten, deren Anordnung und Zusammenstellung individualitätsbegründend wirkt, handelt es sich um ein sog. **Datenbankwerk** (§ 4 UrhG). Nur dessen Struktur und nicht die Informationen als solche **unterliegen einem urheberrechtlichen Schutz**.
- **Metadaten** sind meist relativ kurze, rein beschreibende Darstellungen. Sie sind **meist nicht urheberrechtlich geschützt**. Eine Schutzfähigkeit kommt grundsätzlich nur in den seltenen Fällen in Betracht, in denen Sie z. B. längere Textabschnitte oder Lichtbilder enthalten.

Fotografien und andere Lichtbilder können zudem durch ein Leistungsschutzrecht nach § 72 UrhG geschützt sein. Die folgende Abbildung von *Brettschneider* (2020) unternimmt den Versuch einer Pauschalisierung der Schutzfähigkeit von Forschungsdaten als urheberrechtliche Werke:

Versuch einer Pauschalisierung

Schutz von Forschungsdaten als urheberrechtliche Werke?	
Tendenziell ja	Tendenziell nein
Qualitative Forschungsdaten	Quantitative Forschungsdaten
Geisteswissenschaften	Naturwissenschaften



Aber: Fotografien, Videos, Infrarot- und Röntgenaufnahmen, etc.

Hier besteht zumindest immer ein Leistungsschutzrecht nach § 72 UrhG. Ausnahme: bloße Reproduktionen!

Abb. 9.4: Werkqualität von Forschungsdaten, Quelle: <https://zenodo.org/record/3763031>, Folie 5.

Zusammenstellungen von Forschungsdaten im Rahmen einer Datenbank können - außer, dass sie als Datenbankwerk urheberrechtlich geschützt sein können - zudem durch das **Datenbankherstellerrecht (§87a UrhG)** geschützt werden. Dieses Leistungsschutzrecht erfordert einen wesentlichen Investitionsaufwand hinsichtlich der Sammlung, Ordnung und Zugänglichmachung der Forschungsdaten.

Inhaber:in der Datenbankherstellerrechte ist regelmäßig die Person, die die wesentlichen Investitionen erbringt, z. B. die Vergütung der Forschenden zahlt und das wirtschaftliche Risiko trägt. Gemeinhin ist dies ebenfalls die anstellende Hochschule oder Forschungseinrichtung. Im Einzelfall kommt auch eine Inhaberschaft der Drittmittel- oder Auftraggebenden in Frage.

Bei nicht geschützten Forschungsdaten (z. B. [Messergebnissen](#)) ist rechtlich weitgehend ungeklärt, wem im konkreten Einzelfall die Entscheidungsbefugnis über die Daten obliegt. Ob ein mögliches Persönlichkeitsrecht der Wissenschaftler*innen auch in diesen Fällen eine Zuordnung der Forschungsdaten zu einer Person erlaubt, ist umstritten.

II. Nutzungsrechtseinräumungen im Rahmen von Dienst- und Arbeitsverträgen

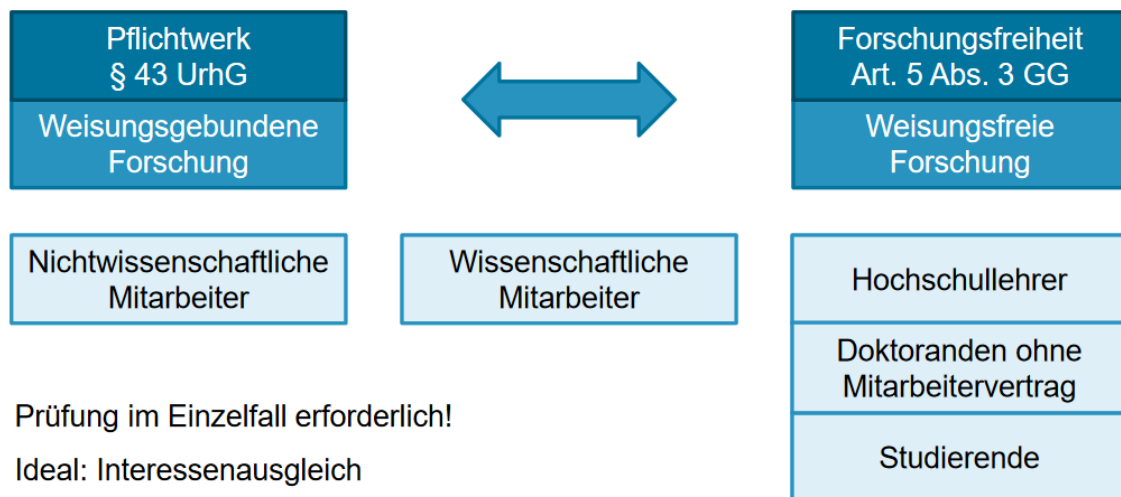
Gehört die Schaffung urheberrechtlich geschützter Werke zu den arbeitsvertraglichen Pflichten oder zentralen Aufgaben, werden der/dem Arbeitgeber:in aufgrund des Arbeitsvertrages oder Dienstverhältnisses an diesen sog. „Pflichtwerken“ Nutzungsrechte eingeräumt (§ 43 UrhG). Die folgenden „Zuordnungen“ von Forschungsdaten ergeben sich aus dem Interessenausgleich mit der Freiheit der Forschung (Art. 5 Abs. 3 GG):

- **Hochschullehrer:innen** stehen im Regelfall alle Verwertungs-, Nutzungs- und Veröffentlichungsrechte an denen von ihnen geschaffenen Werken zu, sofern keine ausdrücklichen vertraglichen Abreden bestehen (z. B. Drittmittelförderung, Geheimhaltungsabreden). § 43 UrhG (sog. "Pflichtwerke") findet hier keine Anwendung.
- **Wissenschaftliche Assistent:innen und Mitarbeiter:innen** sind gemäß Art. 5 Abs. 3 GG privilegiert, wenn und soweit die wissenschaftliche Arbeit weisungsfrei erfolgt. Erfolgt die Forschung weisungsabhängig, ist eine stillschweigende Nutzungsrechtseinräumung an den erzeugten Forschungsdaten anzunehmen.
- Bei **Studierenden und externen Promovierenden** findet grundsätzlich keine Nutzungsrechteinräumung an die Hochschule statt, da diese keine Arbeitnehmer:innen sind. Jedoch können abweichende vertragliche Vereinbarungen getroffen werden, z. B. bei Drittmittelprojekten, durch die z. B. der Hochschule Nutzungsrechte eingeräumt werden

Die folgende Abbildung veranschaulicht die Fragen nach dem Übergang von Verwertungsrechten auf den Arbeitgeber ("Pflichtwerk" nach § 43 UrhG) und den Interessenausgleich mit der Freiheit der Forschung (Art. 5 Abs. 3 GG) nach Rollen, wie sie im wissenschaftlichen Bereich im Einzelfall abzuwägen sind:

5. Übergang von Rechten auf den Arbeitgeber?

- Grundlage: **Arbeitsvertrag**
- Übertragbar sind nur **Verwertungsrechte**
- **Urheberpersönlichkeitsrecht** (insb. Recht auf Namensnennung) verbleibt beim Arbeitnehmer



- Prüfung im Einzelfall erforderlich!
- Ideal: Interessenausgleich

Abb. 9.5: Rechtsinhaberschaft bei Forschungsdaten, Quelle: <https://zenodo.org/record/3763031>, Folie 7

Zu beachten ist, dass Nutzungsrechtseinräumungen im Rahmen von Dienst- und Arbeitsverträgen ggf. auch stillschweigend erfolgen können, soweit die Nutzungsrechtseinräumung nicht ausdrücklich im Vertrag geregelt ist. Im Rahmen der (stillschweigenden) Einräumung überlässt die/der Wissenschaftler:in der/dem Arbeitgeber:in auch das Recht zu bestimmen, ob und wie das Werk veröffentlicht wird. Dagegen behält jede/r Wissenschaftler:in ihr/sein Recht auf Namensnennung.

Rechtspositionen bei Forschungsdaten



D. Veröffentlichung und Lizenzierung von Forschungsdaten

Bevor Daten öffentlich zugänglich gemacht werden können, gilt es, eine Vielzahl rechtlicher Aspekte zu beachten – denn nicht alle Daten können oder sollten veröffentlicht werden. Die wichtigsten rechtlichen Aspekte berücksichtigt die folgende Entscheidungshilfe in Form eines Flussdiagramms. Die Beantwortung der gestellten Fragen führt dich durch den Entscheidungsprozess bis zu einer Empfehlung:

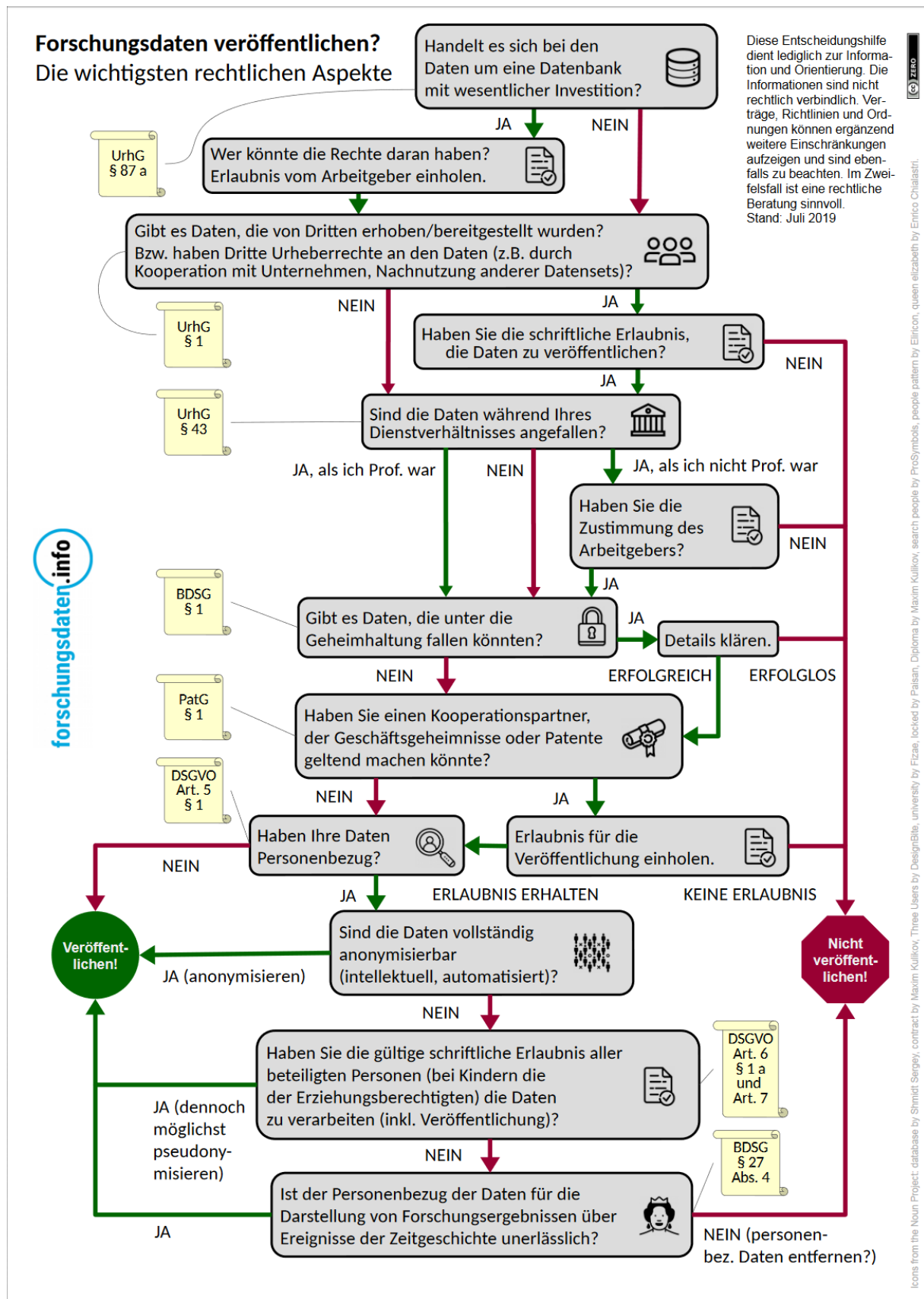


Abb. 9.6: Entscheidungsprozess Datenveröffentlichung, Quelle: forschungsdaten.info, <https://zenodo.org/record/3368293>

Im Wesentlichen, jedoch nicht ausschließlich, sind vor der Veröffentlichung Fragen des Datenschutzes und des Urheberrechts zu klären. Die entscheidenden Weichenstellungen für die Möglichkeit zur Veröffentlichung von Forschungsdaten in einem Repository erfolgen deshalb häufig bereits bei der Erhebung der Daten und der Einholung entsprechender Einwilligungserklärungen.

I. Was sind geeignete Lizenzierungsmodelle?

Damit Andere deine urheberrechtlich geschützten Daten auch wirklich nutzen dürfen, müssen die Bedingungen der Nutzung geregelt sein. Dies geschieht durch die Vergabe einer Lizenz. Existiert keine Lizenz, dürfen urheberrechtlich geschützten Daten nur mit ausdrücklicher Zustimmung der Urheber:innen verwendet werden.

Hingegen sollten nicht urheberrechtlich geschützte Forschungsdaten, deren Nutzung bereits ohne vertragliche Erlaubnis (z. B. Lizenz) zulässig ist, weder eingeschränkt noch mit Bedingungen belegt werden. Aus diesem Grund besteht z. B. unter der CC-BY 4.0-Lizenz auch keine durchsetzbare Verpflichtung zur Attribution (s. [Klausel 8a](#) des Lizenzvertrags).

Häufig werden für das Bereitstellen von Forschungsdaten die [Creative Commons](#) Lizenzen verwendet. Neben der Europäischen Kommission im Rahmen von [Horizon 2020](#) empfiehlt auch die [DFG](#) die Verwendung dieser Lizenztypen. Bei der Entscheidung für eine konkrete Lizenz gilt die Maßgabe “So offen wie möglich, so restriktiv wie nötig”:

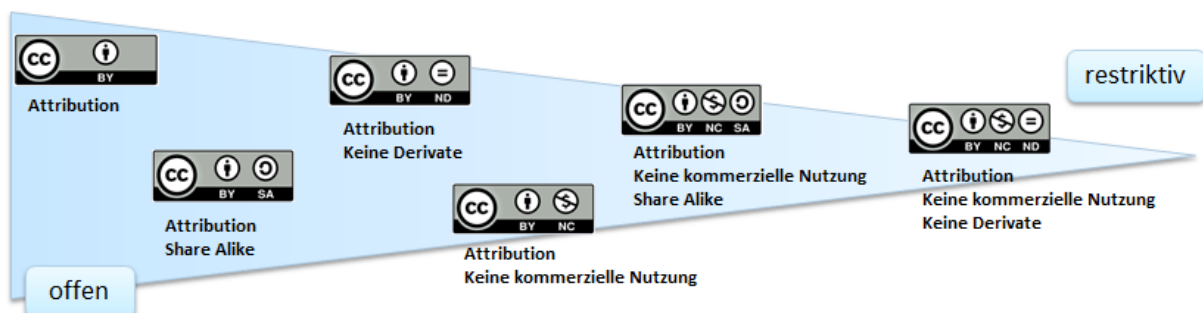


Abb. 9.7: Nutzungsmöglichkeiten von Daten unter verschiedenen Creative Commons-Lizenzen, Quelle: Apel et al. 2017

Die “Kurzfassung des Gutachtens zu den rechtlichen Rahmenbedingungen des Forschungsdatenmanagements” des BMBF geförderte DataJus Projekts an der Technischen Universität Dresden, das die rechtlichen Rahmenbedingungen des Forschungsdatenmanagements untersucht hat, spricht sich für die beiden folgenden Lizenzen aus:

Lizenz	Beschreibung
CC0 (Plus)	Die CC0-Lizenz ermöglicht die maximale Freigabe der Daten und erleichtert die Nachnutzung. Ein Recht auf Namensnennung besteht <u>nicht</u> . Insbesondere für Metadaten ist diese Lizenzierung zu empfehlen.
CC-BY 4.0	Die CC-BY 4.0-Lizenz ist sinnvoll, wenn eine Namensnennung gewünscht ist. Zugleich wird dem Gebot der Quellenangabe genügt (Sicherung guter wissenschaftlicher Praxis). Die CC-BY 4.0-Lizenz wird daher für die Veröffentlichung von Forschungsdaten empfohlen.

Die Verwendung weiterer Lizenzbausteine sei nicht zu empfehlen. So schließen z. B. die [Creative Commons \(CC\) Lizenzen](#) mit dem Attribut „ND“ (z. B. CC-BY-ND) die Weitergabe „abgewandelten“ Materials aus. Somit bliebe die [öffentliche Zugänglichmachung](#) einer neuen Datenbank, die aus Teilen anderer Datenbanken geschaffen wurde, ausgeschlossen.

Software benötigt, im Gegensatz zu vielen anderen Forschungsdaten, eine gesonderte Lizenz. Die Verwendung von Creative Commons Lizenzen ist hierfür nicht zu empfehlen. Es stehen aber ebenfalls unterschiedliche Lizenzen zur Verfügung: [MIT-Lizenz](#), [GNU General Public License \(GPL\)](#), [GNU Lesser General Public License \(LGPL\)](#), [Apache-Lizenz](#).

II. Was kann einer Veröffentlichung entgegenstehen?

Nicht alle Forschungsdaten dürfen oder sollten auch tatsächlich veröffentlicht werden. Bevor Sie ggf. gänzlich auf eine Veröffentlichung verzichten, solltest du in jedem Fall prüfen, ob du Maßnahmen ergreifen kannst, um eine rechtlich und ethisch unbedenkliche Veröffentlichung doch noch zu ermöglichen. Einen Überblick über mögliche rechtliche Hürden und entsprechende Lösungen gibt folgende Abbildung:



Abb. 9.8: Entscheidungsbaum zur Datenveröffentlichung, Quelle: Böker/Brettschneider (2020)

Darüber hinaus solltest du auch **forschungsethische Aspekte** in deine Entscheidung über eine Veröffentlichung deiner Forschungsdaten einfließen lassen. Die folgenden Punkte sollten dir einige Anhaltspunkte ohne Anspruch auf Vollständigkeit an die Hand geben:

- Können die Daten in einer Weise genutzt werden, die der Gesellschaft schadet?
- Bestehen durch die Veröffentlichung z. B. Risiken für die beforschten Personen (auch wenn diese der Verwendung ihrer Daten zugestimmt haben)?
- Haben beteiligte Arbeitsgruppenmitglieder berechnigte Interessen die Datenveröffentlichung zu unterbinden oder hinauszuzögern (z. B. für die Fertigstellung von Qualifikationsarbeiten)?

III. Schutz vertraulicher Informationen in Forschungsdatenzentren

Durch die Nutzung von Datenzentren oder auch Archiven ist es möglich, den Zugriff auf vertrauliche und sensible Daten zu beschränken und zugleich eine Datenfreigabe für Forschungs- und Bildungszwecke zu ermöglichen. Die in Datenzentren und Archiven gehaltenen Daten sind im Allgemeinen nicht öffentlich zugänglich. Ihre Verwendung nach der Benutzerregistrierung ist auf bestimmte Zwecke beschränkt. Nutzer unterzeichnen eine Endbenutzer-Lizenz, in der sie sich mit bestimmten Bedingungen einverstanden erklären, z. B. Daten nicht zu kommerziellen Zwecken zu nutzen oder potenziell identifizierbare Personen nicht zu identifizieren. Welche Art von [Datenzugriff](#) erlaubt ist, wird vorher mit dem Urheber festgelegt. Darüber hinaus können Datenzentren zusätzliche Zugangsregelungen für vertrauliche Daten verhängen (forschungsdaten.info).

F. Bedeutung für die Forschungspraxis

I. Publikationsfreiheit vs. Rechte Dritter

Es existieren einige rechtliche Problemstellungen, die einer Veröffentlichung entgegenstehen können. Ganz wesentlich sind dabei die organisatorischen Abläufe, die bereits im Vorfeld einer Forschung und mit Blick auf den gesamten Forschungsdatenzyklus klar definiert und vorbereitet sein sollten. Dazu zählt auch eine möglichst differenzierte und ergebnisorientierte Einwilligungserklärung.

Zur Veröffentlichung der Ergebnisse gilt, dass Forschende im Rahmen ihrer Publikationsfreiheit (Art. 5 GG) entscheiden, ob und wann sie sie veröffentlichen. Generell sind aber auch hierbei die Rechte Dritter zu achten. Hier ist zu verstehen, dass die Publikationsfreiheit den Forschenden jedoch keine Eigentumsrechte (Art. 14 GG) verleiht. Forschende erhalten grundsätzlich Urheberrechte an ihren wissenschaftlichen Werken. Bei Daten ist es jedoch etwas komplizierter. Nicht alle Forschungsdaten haben die notwendige Schöpfungshöhe, um urheberrechtlich geschützt zu sein. Das hängt stets vom Einzelfall ab. Bei geisteswissenschaftlichen Texten ist das eher der Fall als beispielsweise bei zahlenbasierten Naturwissenschaften. Qualitative Forschungsdaten sind tendenziell eher geschützt als quantitative Forschungsdaten.

Nicht alle Forschungsdaten genießen einen urheberrechtlichen Schutz. Die Einzelfallprüfung berücksichtigt die konkrete Art der Forschungsdaten. Bei den naturwissenschaftlichen Daten fallen typischerweise Bilddaten und Fotografien (wie etwa Röntgenbilder) eher unter das Urheberrecht. Andererseits können auch Dritte an ihren Texten und Daten Urheberrechtspositionen geltend machen. Das gilt insbesondere, wenn ihre Texte nachgenutzt werden. Das bezieht sich auch auf fremde Forschungsdaten.

Daneben kann auch der Datenschutz, Dritten, Rechte an deinen Forschungsdaten geben. Das ist dann der Fall, wenn ihre Text- und/oder Datenpublikation Informationen über andere Menschen enthalten, die es erlauben sie zu identifizieren. -dadurch keine eigentumsrechtliche Stellung, aber ggf. ein Verbot der Datenverarbeitung.

Sonstige Hindernisse. Z. B. geplante Patentierung. Patentiert werden kann nur eine Erfindung, wenn sie neu ist. Wenn die Erfindung bereits in einer Publikation beschrieben ist, ist sie nicht mehr neu – und damit nicht mehr patentwürdig. Wenn du eine Patentierung planst, solltest du also darauf verzichten, die Ergebnisse vorab zu veröffentlichen.

Außerdem gibt es Geheimhaltungsabreden (z. B. Arbeitsverträge, Kooperationsabreden mit Projektpartnern), die einer Publikation entgegenstehen.

Eine weitere Dimension liegt in den Daten selbst. So benötigen die Datenbanken, auf denen die Daten gespeichert werden Software, die ebenfalls auf Datenträgern gespeichert ist. Hier bestehen ebenfalls Rechtspositionen, die es zu beachten gilt. An den einzelnen Daten oder an den Datensätzen kann ein Werkschutz und/ oder Leistungsschutzrechte (z. B. bei Fotografien) bestehen. Bei Datenbanken können nebeneinander zwei unterschiedliche urheberrechtliche Rechtspositionen bestehen. Das sind die

Rechte am Datenbankwerk und dem Datenbankherstellerrecht. Ersteres besteht, wenn in die Konzeption ein ausreichendes Maß an Qualität und Originalität geflossen ist. Zweiteres setzt nicht etwa die Kreativleistung, sondern die Investition (finanziell und durch Arbeitsleistung) in eine Datenbank. Auch Software genießt einen Werkschutz und auch an den Datenträgern besteht ein Eigentumsrecht, welches erlaubt, unbefugten Dritten den Zugriff auf die auf diesen Datenträgern gespeicherten Daten, Datenbanken und Software zu verweigern. Problematisch ist das vor allem dann, wenn ein Forschender die Institution wechselt. Darf er dann etwa weiterhin auf „seine“ Daten, die auf einem nun fremden Server liegen, zugreifen?

Jedoch sind nicht alle Forschungsdaten geschützt. So können etwa urheberrechtlich Schutzlücken existieren, wobei juristisch umstritten ist, ob und wie sich diese Schutzlücken schließen lassen. Ein Ansatz dazu ist das sog. Wissenschaftler-Persönlichkeitsrecht, das dem Wissenschaftler zumindest die Entscheidungshoheit darüber einräumen, ob und wann seine Daten an die Öffentlichkeit gelangen. Daneben ist auch der Datenschutz beachtlich und zwar immer dann, wenn die Forschungsdaten Informationen enthalten, die es erlauben, lebende Menschen zu identifizieren.

Aus der Vielzahl der Rechtspositionen folgt, dass auch eine Vielzahl von Personen Rechte an Forschungsdaten haben können. Diese Rechte konfliktieren, laufen parallel oder konkurrieren mitunter. Dabei steht der Forschende selbst an erster Stelle, weil er selbst an den von ihm geschaffenen Daten, den Datenbanken oder gar an der Software Urheberrechte haben kann. Voraussetzung dessen ist stets eine ausreichende Schöpfungshöhe oder das Vorliegen eines Leistungsschutzrechtes. Daneben können Patente an den eigenen Erfindungen bestehen und der Forschende hat das Eigentum an privaten Rechnern und Servern. Dem stehen insbesondere bei der Nachnutzung die gleichen Rechte von Dritten gegenüber. Außerdem können Kooperations- oder Projektpartner Miturheber der gemeinsam erarbeiteten Forschungsdaten sein. Auch Universitäten und andere Forschungseinrichtungen können Rechtspositionen an den Forschungsdaten erwerben (z. B. Datenbankherstellerrecht). Daneben kann es bei sog. weisungsgebundener Forschung zu Urheberrechten auf den Arbeitgeber kommen. Soweit Forschung aber unter die Wissenschaftsfreiheit fällt, ist dies nicht der Fall. Hochschulprofessor:innen trifft dies nie, wissenschaftliche Mitarbeiter jedoch schon, wenn sie Forschungsdaten auf Anweisung eines Vorgesetzten erzeugt haben. Auch Forschungsförderer können Rechte an ihren Forschungsdaten haben. Auch hier kommt das Datenbankherstellerrecht in Betracht.

Drei Empfehlungen:

1. Frühzeitig Beratung in Anspruch nehmen. Hier gilt es die Rechtsabteilungen, Datenschutzbeauftragte und Ethikräte zu kontaktieren.
2. Vertragliche Regelungen treffen. Viele Konflikte lassen sich von vornherein vermeiden, wenn bereits zu Projektbeginn vertragliche Regelungen mit allen Beteiligten getroffen werden.
3. Einwilligungen einholen. Es sollten die Einwilligungen aller Parteien eingeholt werden, deren Rechte von der Veröffentlichung betroffen sind oder sein könnten.

II. Erlaubnisfreie Nachnutzung fremder Werke

Zu prüfen ist, ob das Werk gemeinfrei ist. Das Urheberrecht erlischt 70 Jahre nach dem Tod des Urhebers / der Urheberin (§ 46 UrhG). Ab diesem Zeitpunkt ist jede Art der Nutzung ohne Zustimmung der Erben / Erben des Urhebers / der Urheberin zulässig. Ist ein Werk nicht gemeinfrei, kann die Nutzung dennoch durch eine sog. Urheberrechtsschranke gedeckt sein. Insbesondere bei Texten ist die Nutzung gegebenenfalls durch das Zitatrecht (Ausfluss der Urheberrechtsschranke) gedeckt. So sind Zitate ohne Zustimmung des Urhebers / der Urheberin nach § 51 UrhG erlaubt, wenn es sich 1. um ein veröffentlichtes Werk (also eben nicht private Tagebücher / Dokumente handelt – problematisch z. B. bei Archivalien) handelt, 2. das Zitat als Beleg für die eigenen Aussagen bzw. zur Erörterungsgrundlage dient und nicht nur zur Illustration bzw. zur Ausschmückung genutzt wird (insbesondere bei Abbildungen problematisch) und 3., entsprechend der Grundsätze der guten wissenschaftlichen Praxis, die eindeutigen Quellenangabe vorgenommen wird.

Bezüglich der Daten kommt insbesondere § 60 d UrhG in Betracht, was beim sog. Text- und Data-Mining auch die Archivierung der Forschungsdaten bei Bildungseinrichtung erlaubt.