

Landesrechtliche Anforderungen an medizinische Register: Was zu beachten ist

Eine Praxishilfe für medizinische Register und datenliefernde Krankenhäuser

Erarbeitet von

Arbeitsgruppe „Datenschutz und IT-Sicherheit im
Gesundheitswesen“ (DIG) der
Deutsche Gesellschaft für Medizinische Informatik, Biometrie
und Epidemiologie e. V. (GMDS)



Deutsche Gesellschaft für Unfallchirurgie (DGU)



Gesellschaft für Datenschutz und Datensicherheit e. V.
Arbeitskreis „Datenschutz und Datensicherheit im Gesundheits- und
Sozialwesen“



Berufsverband der Datenschutzbeauftragten Deutschlands e. V.
Ausschuss Recht & Politik



Version 1.0

Stand der Bearbeitung: 15. November 2021

Autoren (alphabetisch)

Andrea Backer-Heuveloop	ds2 Unternehmensberatung GmbH & Co. KG
David Koepe	Vivantes - Netzwerk für Gesundheit GmbH
Lukas Mempel	Sana Kliniken AG
Mark Rüdlin	Kanzlei Rüdlin
Dr. Bernd Schütze	Deutsche Telekom Healthcare and Security GmbH
Gerald Spyra	Sozietät Ratajczak & Partner mbB
Dr. Thilo Weichert	Netzwerk Datenschutzexpertise

Geschlechtergerechte Sprache

Hinweis bzgl. geschlechtsneutraler Formulierung im gesamten Text:

- Eine gleichstellungsgerechte Gesellschaft erfordert eine geschlechterneutrale Sprache. Geschlechterneutrale Sprache muss im deutschen Umfeld drei Geschlechtern gerecht werden: Divers, Frauen und Männern.
- Im folgenden Text werden, soweit möglich und sinnvoll, entsprechende Formulierungen genutzt (z. B. Paarformeln, Ableitungen). Personenbezeichnungen, bei denen es sich um juristische Fachbegriffe handelt, die sowohl natürliche als auch juristische Personen bezeichnen können, werden im folgenden Text nicht durch Paarformeln ersetzt. Dies gilt auch für technische Fachbegriffe, Definitionen und Zitate aus Normen (z. B. DIN EN ISO) und gesetzlichen Vorschriften. Entsprechende Begriffe sind im Sinne der Gleichbehandlung geschlechtsneutral zu interpretieren.
- Wo aus Gründen der leichteren Lesbarkeit bei personenbezogenen Substantiven und Pronomen nur ein Geschlecht dargestellt wurde, impliziert dies jedoch keine Benachteiligung der anderen beiden Geschlechter, sondern soll im Sinne der sprachlichen Vereinfachung als geschlechtsneutral verstanden werden.

Haftungsausschluss

Das vorliegende Werk ist nach bestem Wissen erstellt, der Inhalt wurde von den Autoren mit größter Sorgfalt zusammengestellt. Dennoch ist diese Ausarbeitung nur als Standpunkt der Autoren aufzufassen, eine Haftung für die Angaben übernehmen die Autoren nicht. Die in diesem Werk gegebenen Hinweise dürfen daher nicht direkt übernommen werden, sondern müssen vom Leser für die jeweilige Situation anhand der geltenden Vorschriften geprüft und angepasst werden.

Die Autoren sind bestrebt, in allen Publikationen die Urheberrechte der verwendeten Texte zu beachten, von ihnen selbst erstellte Texte zu nutzen oder auf lizenzfreie Texte zurückzugreifen.

Alle innerhalb dieses Dokumentes genannten und ggf. durch Dritte geschützten Marken- und Warenzeichen unterliegen uneingeschränkt den Bestimmungen des jeweils gültigen Kennzeichenrechts und den Besitzrechten der jeweiligen eingetragenen Eigentümer. Allein aufgrund der bloßen Nennung ist nicht der Schluss zu ziehen, dass Markenzeichen nicht durch Rechte Dritter geschützt sind!

Copyright

Für in diesem Dokument veröffentlichte, von den Autoren selbst erstellte Objekte gilt hinsichtlich des Copyrights die folgende Regelung:

Dieses Werk ist unter einer Creative Commons-Lizenz (4.0 Deutschland Lizenzvertrag) lizenziert. D. h. Sie dürfen:



- Teilen: Das Material in jedwedem Format oder Medium vervielfältigen und weiterverbreiten
- Bearbeiten: Das Material remixen, verändern und darauf aufbauen

und zwar für beliebige Zwecke, sogar kommerziell. Der Lizenzgeber kann diese Freiheiten nicht widerrufen, solange Sie sich an die Lizenzbedingungen halten.

Die Nutzung ist unter den folgenden Bedingungen möglich:

- Namensnennung: Sie müssen angemessene Urheber- und Rechteangaben machen, einen Link zur Lizenz beifügen und angeben, ob Änderungen vorgenommen wurden. Diese Angaben dürfen in jeder angemessenen Art und Weise gemacht werden, allerdings nicht so, dass der Eindruck entsteht, der Lizenzgeber unterstütze gerade Sie oder Ihre Nutzung besonders.
- Weitergabe unter gleichen Bedingungen: Wenn Sie das Material remixen, verändern oder anderweitig direkt darauf aufbauen, dürfen Sie Ihre Beiträge nur unter derselben Lizenz wie das Original verbreiten.
- Keine weiteren Einschränkungen: Sie dürfen keine zusätzlichen Klauseln oder technische Verfahren einsetzen, die anderen rechtlich irgendetwas untersagen, was die Lizenz erlaubt.

Im Weiteren gilt:

- Jede der vorgenannten Bedingungen kann aufgehoben werden, sofern Sie die Einwilligung des Rechteinhabers dazu erhalten.
- Diese Lizenz lässt die Urheberpersönlichkeitsrechte unberührt.

Um sich die Lizenz anzusehen, gehen Sie bitte ins Internet auf die Webseite:

<https://creativecommons.org/licenses/by-sa/4.0/deed.de>

bzw. für den vollständigen Lizenztext

<https://creativecommons.org/licenses/by-sa/4.0/legalcode.de>

Inhaltsverzeichnis

Vorwort	1
1 Einleitung	4
2 Abgrenzung	5
3 Identifizierung einer Person: Unterschied bei Datenschutz, Schweigepflicht und im Berufsrecht	6
3.1 Datenschutzrecht	6
3.2 Gesetzliche Schweigepflicht / Strafrecht (§ 203 StGB)	6
3.2.1 Person nicht identifizierbar: Keine unbefugte Offenbarung	7
3.3 Ärztliche Schweigepflicht / Berufsrecht (§ 9 MBO-Ä)	8
4 Begriffsbestimmungen	11
5 Qualitätssicherung und Forschung: Zwei verschiedene Zwecke	12
6 Anforderungen aus der DS-GVO	13
6.1 Wo findet man weitergehende Informationen?	18
7 Anforderungen an eine Vorratsdatenspeicherung	20
7.1 Daraus resultierende Anforderungen	20
8 Gesetzliche Anforderungen für Qualitätssicherung und Forschung	22
8.1 Erlaubnistatbestand zur Verarbeitung von Daten durch ein Register	22
8.1.1 Erlaubnistatbestand zur Verarbeitung von Patientendaten zu Zwecken der Qualitätssicherung	22
8.1.2 Erlaubnistatbestand zur Verarbeitung von Patientendaten zu Forschungszwecken	24
8.2 Anforderungen für bundesweit tätige Register (Qualitätssicherung)	27
8.3 Anforderungen für bundesweit tätige Register (Forschung)	28
8.4 Beispielhafte Skizzierung, wie ein Register den Anforderungen entsprechen kann	29
9 Was Krankenhäuser prüfen sollten	33
9.1 Anforderungen, die ein Krankenhaus vor Datenübermittlung an ein Register zu Zwecken der Qualitätssicherung prüfen sollte	33
9.2 Anforderungen, die ein Krankenhaus vor Datenübermittlung an ein Register zu Forschungszwecken prüfen sollte	34
10 Sonderfall	37
10.1 Datenschutz bei Verstorbenen	37
11 Checkliste	38
11.1 Grundlegende Punkte, die von Krankenhaus und Register geprüft werden sollten	38
11.2 Anforderungen an Krankenhäuser für die Übermittlung von Patientendaten zu Zwecken der Qualitätssicherung ohne Einwilligung	39

11.3 Anforderungen an Krankenhäuser für die Übermittlung von Patientendaten zu Zwecken der Forschung ohne Einwilligung _____	41
12 Abkürzungen _____	44
12.1 Bundesländer _____	44
12.2 Landesgesetze _____	44
12.3 Im Text verwendete Abkürzungen _____	45
Anhang 1: Ausgewählte Beispiele für die Heterogenität von Landesgesetzen bzgl. Datenschutz im Krankenhaus _____	46
Anhang 1.1: Geltungsbereich der Landeskrankenhausesetze _____	47
Anhang 1.2: Begriffsbestimmungen – „Patientendaten“ _____	49
Anhang 1.3: Verarbeitung im Auftrag (Auftragsverarbeitung) _____	50
Anhang 1.4: Erlaubnistatbestände für die Verarbeitung von Patientendaten durch das jeweilige Krankenhaus _____	54
Anhang 2: Internetadressen verschiedener Gesetze _____	56
Anhang 2.1: Bundesrecht _____	56
Anhang 2.2: Landesrecht _____	56
Anhang 2.3: Krankenhäuser der Bundeswehr _____	61

Vorwort

Die Rechtslage in Deutschland ist für bundesweit agierende medizinische Register aufgrund ihrer Heterogenität derart unübersichtlich, dass die Existenz dieser Register schon an ein Wunder grenzt. Die gespaltene Gesetzgebung, die Bund und Ländern u- a. Kompetenzen zur Gesetzgebung für den Krankenhausbereich verleiht, führt zu einer Diversität, sodass die i. d. R. von wissenschaftlich-medizinischen Fachgesellschaften initiierten medizinischen Register kaum eine Chance haben, die Rechtslage in ihrer Arbeit länderübergreifend abzubilden.

Dies zeigt sich bereits an den unterschiedlichen Ausgestaltungen der sachlichen und persönlichen Anwendungsbereiche der einschlägigen datenschutzrechtlichen Bestimmungen und der unterschiedlichen Definition der Adressaten der Landeskrankenhausgesetze. Beispielhaft sei auf die unterschiedliche Vorgabe zum Geltungsbereich der Landeskrankenhausgesetze hingewiesen (siehe auch Anhang 1:):

- Einige Landesgesetzgeber verweisen bzgl. des Geltungsbereiches ihrer Landeskrankenhausgesetzgebung auf § 107 Abs. 1, 2 SGB V, sodass der Geltungsbereich auf nahezu alle Krankenhäuser, Vorsorge- oder Rehabilitationseinrichtungen ausgedehnt wird.
- Andere Landesgesetzgeber legen den Geltungsbereich auf die Krankenhäuser fest, die nach dem KHG förderfähig sind. Dieses schließt wiederum Krankenhäuser im Straf- oder Maßregelvollzug, Polizeikrankenhäuser sowie Krankenhäuser der Träger der allgemeinen Rentenversicherung aus, da für diese entsprechend § 3 KHG das KHG nicht gilt. In § 5 KHG erfolgen zudem weitere Ausschlüsse bzgl. der Förderfähigkeit, sodass der Geltungsbereich dieser Landeskrankenhausgesetze deutlich eingeschränkter ist, als der Gesetze, die sich auf § 107 Abs. 1, 2 SGB V beziehen.
- Dann gibt es Landesgesetzgeber, die schlicht und ergreifend ihre Landesgesetzgebung auf „alle“ Krankenhäuser im Land beziehen, ohne den Begriff eines Krankenhauses zu definieren. Das Problem hierbei ist, dass verschiedene Definitionen von „Krankenhaus“ existieren wie bspw. die Begriffsbestimmungen in § 2 Ziff. 1 KHG und § 107 Abs. 1 SGB V zeigen. D. h. was unter „Krankenhaus“ zu verstehen ist, muss in diesen Fällen zunächst auch einmal geklärt werden.
- Ein Landesgesetzgeber verzichtet sogar völlig auf die Angabe eines Geltungsbereichs und nimmt die damit einhergehende Rechtsunsicherheit für Krankenhäuser zumindest billigend in Kauf.

Noch unübersichtlicher sind die jeweils einschlägigen Regelungen der Berechtigung zur Verarbeitung zu registerrelevanten Tätigkeiten. So dürfen bspw. in einem Bundesland alle im Krankenhaus beschäftigten Ärztinnen und Ärzte die im Krankenhaus angefallenen Patientendaten für ihre medizinische Forschung nutzen. In anderen Bundesländern beschränkt sich die Befugnis nur auf die Patientendaten, die in der Abteilung, in der sie arbeiten, angefallen sind. Wieder andere Länder beschränken die Forschungsmöglichkeiten auf die Patientendaten, an deren Behandlung sie beteiligt waren.

Auch die Anforderungen für die Nutzung von Patientendaten für medizinische Forschung sind höchst unterschiedlich. Beispielsweise verlangen einige Landesgesetzgeber von den Krankenhäusern, dass schutzwürdige Interessen der betroffenen Patienten der Verarbeitung ihrer Daten nicht entgegenstehen dürfen. Andere für Krankenhäuser geltende Landesgesetze verlangen wiederum, dass überwiegende schutzwürdige Interessen der betroffenen Patienten der Verarbeitung ihrer Daten nicht entgegenstehen. Die Auswirkungen, die durch das Wort „überwiegend“ entsteht, sind immens. Denn was in einem Bundesland erlaubt ist, weil keine *überwiegenden* Interessen des Betroffenen

entgegenstehen, ist im anderen Bundesland verboten, denn es gibt aus Sicht des Datenschutzes fast immer entgegenstehende Interessen, welche die Datenverarbeitung verhindern würden.

Dabei kann die Wichtigkeit der medizinischen Register sowohl für die Qualitätssicherung der medizinischen Versorgung als auch für die medizinische Forschung kaum genug hervorgehoben werden. Zwar gibt es für 15¹ ausgewählte (Krankenhaus-) Leistungen bundes- bzw. landesrechtlich definierte, qualitätssichernde Maßnahmen, aber einerseits werden dabei sehr, sehr viele Leistungen, die aus medizinischer Sicht einer Qualitätssicherung bedürfen, nicht erfasst, und andererseits werden bei der gesetzlichen Qualitätssicherung häufig wichtige Aspekte nicht oder nur unzureichend erfasst, weswegen beispielsweise neben der gesetzlichen Qualitätssicherung für Mammachirurgie oder Koronarchirurgie ergänzend die deutlich umfangreicheren Erhebungen und Auswertungen der entsprechenden medizinischen Fachgesellschaften existieren. Dieses ist auch notwendig, denn das ärztliche Berufsethos verlangt ein qualitativ hochwertiges Monitoring für die eigene Leistung. Wertet man die Qualitätsberichte von freiwilligen Qualitätssicherungseinrichtungen wie dem Deutschen Onkologie Centrum oder von OnkoZert einmal über einen längeren Zeitraum von 10-15 Jahren aus, so zeigt sich, dass in S3-Leitlinien enthaltene Behandlungsempfehlungen nur durch diese freiwillige Qualitätssicherung entsprechend bekannt und dadurch in den jeweiligen Krankenhäusern eingesetzt wurden.

Daneben ist der Nachweis einer entsprechenden qualitativen Versorgung der Patienten durch Krankenhäuser auch aus Abrechnungsgründen essenziell. Entsprechend der Rechtsprechung des Bundessozialgerichtes² ist „eine nach zwingenden normativen Vorgaben ungeeignete Versorgung Versicherter nicht im Rechtssinne "erforderlich" mit der Folge, dass das Krankenhaus hierfür keine Vergütung beanspruchen kann. [...] Krankenhäuser sind dementsprechend – außer in Notfällen – auch innerhalb ihres Versorgungsauftrags weder befugt, ungeeignet zu behandeln noch berechtigt, eine Vergütung hierfür zu fordern.“

Die Wichtigkeit der medizinischen Forschung ist nicht erst seit Corona gegeben, aber gerade durch Corona wurde diese Wichtigkeit, insbesondere auch die institutions- und länderübergreifende medizinische Forschung, auch der Öffentlichkeit bewusst. Man hätte mit gutem Grund annehmen können, dass eine Pandemie ausreicht, damit sich Bundes- und Landesgesetzgeber bzgl. einheitlicher Rahmenbedingungen für medizinische Forschung einigen können. Leider geschah dies jedoch nicht. Auch unter Pandemiebedingungen mussten Forscher ihre Arbeit unter einer Rechtsunsicherheit leisten und sich eigentlich fragen „muss ich dafür, dass ich für die Gemeinschaft an der Bekämpfung einer Erkrankung arbeite, vielleicht ins Gefängnis?“

Die rechtliche Situation der bundesweit agierenden medizinischen Register, die nicht aufgrund einer gesetzlichen Regelung arbeiten, ist kaum überblickbar. Die vorliegende Praxishilfe soll einen ersten Überblick über die wichtigsten der geltenden rechtlichen Rahmenbedingungen bzgl. der Erlaubnistatbestände zur Nutzung von Patientendaten seitens medizinischer Register geben. Ferner greift sie die Fragen auf: Was muss ein Register an Anforderungen erfüllen, damit Krankenhäuser Patientendaten dorthin übermitteln dürfen?³ Und was sollte ein Krankenhaus vor Beginn der Übermittlung von Patientendaten an ein Register prüfen?

¹ Gemeinsame Bundesausschuss (G-BA): Richtlinie zur datengestützten einrichtungsübergreifenden Qualitätssicherung. [Online, zitiert am 2021-09-23]: verfügbar unter <https://www.g-ba.de/richtlinien/105/>

² BSG, Urt. v. 2016-04-19 Az: B 1 KR 28/15 R. [Online, zitiert am 2021-10-20]: verfügbar unter <https://dejure.org/2016,7295>

³ Hinweise zu weiteren datenschutzrechtlichen Themen wie Benennung eines Datenschutzbeauftragten usw. speziell für klinische Register finden sich z. B. in der Ausarbeitung von GMDS, GDD und ZTG: Klinische Register

Dabei wird an verschiedenen Stellen auf tiefergehende Ausführungen zur jeweiligen Thematik verwiesen, denn die Erfüllung datenschutzrechtlicher Anforderungen ist so komplex wie der Bau einer Mauer oder die Durchführung einer Appendektomie: Für die, die es lernten, erscheint es fast schon trivial – für alle anderen ist es eine fast unüberwindbare Herausforderung, die Aufgabe zu meistern.

In diesem Sinne stellt diese Praxishilfe nur einen Einstieg dar. Krankenhäuser sollen eine Hilfe erhalten, um zu prüfen, ob sie Daten an ein medizinisches Register übermitteln dürfen. Und medizinische Register sollen eine Unterstützung erhalten, damit sie den Anforderungen genügen, um Daten von Krankenhäusern bekommen zu dürfen.

1 Einleitung

Klinische Register sammeln patientenbezogene medizinische Daten in einem vordefinierten medizinischen Bereich wie beispielsweise „Brustkrebs“. Einige wenige dieser klinischen Register arbeiten auf einer gesetzlichen Grundlage, wie beispielsweise Krebsregister. Diese agieren aufgrund der jeweiligen Landeskrebsregistergesetze. Die meisten klinischen Register in Deutschland, die nicht gesetzlich geregelt werden, werden häufig von medizinischen Fachgremien oder von diesen gegründeten privatwirtschaftlichen Institutionen betrieben.

Register verfolgen dabei häufig mehrere Zwecke, wie z. B.:

- Erfassung der vom Register benötigten und definierten Versorgungsdaten in einem standardisierten Prozess, wobei die Versorgungsdaten strukturiert erfasst werden sollten.
- Qualitätssicherung. Dabei geht es sowohl um die Ergebnis- und Indikationsqualität bzgl. der erfolgten Behandlungen. Grundsätzlich können die Daten dabei auch dazu dienen, die gesundheitsökonomische Entwicklung für die vom Register adressierte Erkrankung darzustellen.
- Schaffung einer Datenbasis, welche die Erforschung von Fragen ermöglicht, die mit der Datenmenge einer einzelnen Versorgungseinrichtung zumeist nicht möglich ist.
- Idealerweise bietet das Register selbst auch Unterstützung bei Forschungsfragen, z. B. durch entsprechende Auswertungen der Registerdaten oder durch methodische Beratungen.

Klinische Register erfüllen – nicht nur in Deutschland – eine wichtige Aufgabe: Im Rahmen der Qualitätssicherung wird dafür Sorge getragen, dass neue Methoden der Behandlung nicht nur in versorgenden Einrichtungen wie beispielsweise Krankenhäusern bekannt werden, sondern dass diese Methoden auch in der Praxis angewendet werden. Und natürlich bilden die in klinischen Registern enthaltenen medizinischen Daten eine wichtige Grundlage für klinische Forschung.

Klinische Register „leben“ von Patientendaten. Die Patientendaten werden in den versorgenden Einrichtungen jedoch grundsätzlich nur zu Zwecken der Patientenversorgung erhoben, nicht um die Daten in einem Register zu speichern. Sollen die zu Versorgungszwecken erhobenen Daten für ein Register genutzt werden, ist dieses im Rahmen einer „Sekundärnutzung“ der Daten möglich, wenn ein entsprechender Rechtsgrund dieses legitimiert. Somit müssen klinische Register datenschutzrechtliche Vorgaben einhalten und insbesondere die Verarbeitung der Patientendaten auf eine gesetzliche Erlaubnis in Form einer Rechtsnorm oder einer ausdrücklichen Einwilligung der betroffenen Patienten stützen können. Bedingt durch den Föderalismus in Deutschland sind die gesetzlichen Anforderungen leider sehr heterogen. Damit ein klinisches Register bundesweit Daten von Krankenhäusern aus unterschiedlichen Ländern erhalten darf, muss ein Register letztlich allen Anforderungen aus den jeweiligen Landesgesetzen genügen, auch wenn diese eigentlich nur für die Krankenhäuser selbst gelten.

Aufgrund des Vorrangs von EU-Recht muss ein Register immer auch allen Vorgaben der DS-GVO wie auch dem Bundesrecht genügen. Im Folgenden werden einige wichtige Anforderungen dargestellt, ohne hierbei jedoch vollständig das Spektrum der datenschutzrechtlichen Anforderungen abzudecken. So wird beispielsweise nicht beschrieben, wie eine Interessensabwägung konkret durchzuführen ist, wie ein öffentliches Interesse an der Verarbeitung der personenbezogenen Daten nachgewiesen werden kann oder welchen Anforderungen eine Einwilligung unterliegt. Hierzu existieren diverse Praxishilfen bspw. der GMDS und vieler anderer Gruppen (vgl. Kapitel 4 bzw. Kapitel 6.1).

Es geht in dieser Ausarbeitung vielmehr darum, sowohl Registern als auch Krankenhäusern einen kurzen, einführenden Beitrag zur Thematik an die Hand zu geben. Damit sollen sie in die Lage versetzt

werden, zu beurteilen, was man als Register leisten muss bzw. was ein Krankenhaus bei einem Register prüfen muss, um zu entscheiden, ob man dem Register Daten überlassen kann.

2 Abgrenzung

Krankenhäuser sind die wichtigste Quelle für medizinische Register. Daher beschäftigt sich diese Ausarbeitung mit den für die Krankenhäuser relevanten Landeskrankenhausgesetzen.

Neben diesen Landeskrankenhausgesetzen gibt es diverse weitere landesspezifischen Vorschriften wie z. B.:

- Landesberufsordnung für Ärzte bzw. Apotheker
- Landesspezifische Regelungen für Universitätskliniken
- Landesgesetze über die Krebsregistrierung
- Landesgesetze über den öffentlichen Gesundheitsdienst
- Heilberufesetze der Länder
- Rettungsdienstgesetze der Länder
- Landesspezifische Gesetze über Hilfen und Schutzmaßnahmen bei psychischen Krankheiten, sogenannte „Psychisch-Kranken-Gesetze“ (PsychKG).

Je nach Ausrichtung medizinischer Register bzw. welche Art von Patientendaten das Register für seine Arbeit benötigt, können sich aus diesen landesspezifischen Regelungen weitere Anforderungen ergeben, welche durch die jeweilige Versorgungseinrichtung bei der Bewertung der Zulässigkeit einer Übermittlung an das Register geprüft und beachtet werden sollte. So enthalten beispielsweise Landesgesetze für psychisch Kranke oft gesonderte Regelungen, die beim Umgang mit Daten dieser Betroffenen durch die zuständigen Stellen (v. a. Behörden und Krankenhäuser) zusätzlich beachtet werden müssen.

Die neben dem Landeskrankenhausrecht bestehenden Regelungen der verschiedenen Bundesländer wie z. B. die landesspezifischen Psychisch-Kranken-Gesetze werden in dieser Ausarbeitung nicht betrachtet, da die Arbeit der großen Mehrheit der medizinischen Register von diesen Spezialgesetzen nicht oder nur unwesentlich berührt wird.

3 Identifizierung einer Person: Unterschied bei Datenschutz, Schweigepflicht und im Berufsrecht

Damit ein Register Patientendaten erhalten kann, müssen verschiedene Rechtsbereiche unabhängig voneinander betrachtet werden:

- 1) Datenschutzrecht: Die Weitergabe von Patientendaten seitens des Krankenhauses an das Register muss datenschutzrechtlich erlaubt sein.
- 2) Strafrecht: Die Weitergabe der Daten darf keinen Verstoß gegen das in § 203 StGB enthaltene Offenbarungsverbot darstellen.
- 3) Ärztliches Berufsrecht: Weiterhin darf die Übermittlung der Patientendaten an das Register keinen Verstoß gegen die in § 9 MBO-Ä in der Fassung der jeweiligen Berufsordnung der Landesärztekammer enthaltene Schweigepflicht darstellen.

Im Folgenden werden die Unterschiede im jeweiligen Recht insbesondere hinsichtlich der Identifizierbarkeit einer Person betrachtet.

3.1 Datenschutzrecht

Entsprechend Art. 4 Ziff. 1 DS-GVO sind personenbezogene Daten „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen“. Damit fallen darunter nicht nur Informationen, die direkt eine Person identifizieren, sondern auch alle Informationen, welche über Zwischenschritte eine Person identifizieren. D. h. soweit und solange die Informationen aus sich heraus Rückschluss auf eine einzelne Person zulassen, handelt es sich um Daten einer bestimmten Person⁴.

Der Begriff „identifizierbar“ muss daher im Sinne von „als Einzelperson wahrnehmbar“ bzw. einer „Einzelperson zuordenbar“ verstanden werden. Somit muss nicht zwingend der Name einer Person bekannt sein, damit eine Person im datenschutzrechtlichen Sinn identifizierbar ist. Ausreichend ist vielmehr, wenn durch das Datum bzw. die Daten eine betroffene Person individualisiert werden kann und Aussagen über deren sachliche und persönliche Verhältnisse möglich sein können; ein Name muss nicht vorhanden sein⁵.

Viele Landeskrankenhausgesetze stellen jedoch nicht allein auf die Verarbeitung von Gesundheitsdaten der Patienten ab, sondern erweitern die Legaldefinition der „Patientendaten“ auch auf Informationen über in Zusammenhang mit der Behandlung der Patienten bekannt gewordene Daten von Angehörigen, Begleitpersonen und sonstigen Dritten.

3.2 Gesetzliche Schweigepflicht / Strafrecht (§ 203 StGB)

Der „Personenbezug“ eines Patienten spielt auch bei dem in § 203 StGB enthaltenem Verbot der unbefugten Offenbarung von Privatgeheimnissen eine bedeutende Rolle. § 203 StGB schützt Privatheimnisse natürlicher Personen, deren Kenntnis Berufsgeheimnisträger, wie beispielsweise Ärzte oder Krankenpflegerinnen/Krankenpfleger, in beruflicher Eigenschaft erlangten. Zu den durch diese Regelung geschützten Geheimnissen gehört schon die Information, dass ein bestimmter Patient von einem bestimmten Arzt behandelt wird oder auch die Tatsache, dass eine vertragliche Beziehung zu einem in § 203 Abs. 1 Ziff. 1 StGB genannten Angehörigen eines Heilberufes besteht. Der durch § 203 StGB gegebene Schutzbereich ist also als sehr weitgehend aufzufassen. Die Schweigepflicht dauert entsprechend § 203 Abs. 5 StGB über den Tod des Patienten hinaus.

⁴ Karg M. (2015) Anonymität, Pseudonyme und Personenbezug revisited. DuD: 520-526

⁵ Artikel-29-Datenschutzgruppe. WP 136 „Stellungnahme 4/2007 zum Begriff 'personenbezogene Daten'“, S. 16: [...] ein Name zur Identifizierung einer Person jedoch keineswegs immer notwendig ist“. [Online, zitiert am 2021-09-23]: verfügbar unter http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf

Von § 203 StGB geschützte Geheimnisse dürfen grundsätzlich keinem, der nicht an der Behandlung beteiligt ist, offenbart werden. Ein Offenbaren im Sinne des § 203 StGB ist jede Mitteilung über die geheim zu haltende Tatsache an einen Dritten⁶. Somit liegt eine Offenbarung immer dann vor, wenn das Geheimnis in irgendeiner Weise einem anderen offenbart wird⁷. Weiterhin verlangt § 203 StGB von Berufsheimnisträgern nicht lediglich nur Verschwiegenheit, sondern Berufsheimnisträger müssen für die Wahrung des Geheimnisses Sorge tragen. Daher ist ein Offenbaren auch durch Unterlassen möglich, z. B. wenn eine Ärztin/ein Arzt die Einsichtnahme in Krankenblätter oder gar deren Mitnahme nicht verhindert.⁸

Grundsätzliche Voraussetzung für eine Offenbarung ist, dass sowohl das Geheimnis selbst als auch die Person, um deren Geheimnis es geht, offenbart wird; Mitteilungen, aus denen die Person des Betroffenen nicht ersichtlich ist, erfüllen, mangels Personenbeziehbarkeit, daher nicht den Tatbestand der Offenbarung⁹. Daraus folgt, dass die Weitergabe von Informationen, welche keine Möglichkeit der Identifizierung beinhalten, auch keine unbefugte Offenbarung darstellen kann.

3.2.1 Person nicht identifizierbar: Keine unbefugte Offenbarung

Dementsprechend stellt die Weitergabe von anonymen Daten grundsätzlich keine Offenbarung i. S. d. § 203 StGB dar¹⁰. Insbesondere dürfen Patientendaten wie beispielsweise Behandlungsverläufe zu wissenschaftlichen Zwecken anonymisiert verarbeitet werden, wenn Dritte den Patienten sicher nicht identifizieren können¹¹. Ebenfalls ist eine wissenschaftliche Erörterung praktischer Fälle in Veröffentlichungen und Vorträgen in anonymisierter oder pseudonymisierter Form möglich, da in diesen Fällen eine Individualisierung des betroffenen Patienten nicht möglich ist¹².

Fraglich ist jedoch, ob sog. pseudonymisierte Daten im Rahmen der gesetzlichen Schweigepflicht wie anonyme Daten behandelt werden sollen. Art. 4 Ziff. 5 DS-GVO definiert pseudonyme Daten als Daten, welche „ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können“. D. h. auch bei der Weitergabe von pseudonymen Daten i. S. d. DS-GVO können Dritte einen Patienten grundsätzlich nicht sicher identifizieren, somit erfolgt auch hierbei keine Offenbarung im Sinne des § 203 StGB¹³.

⁶ Ehrmann C.: Outsourcing von medizinischen Daten – strafrechtlich betrachtet, 2008, S. 60. [Online, zitiert am 2021-09-23]; verfügbar unter <https://d-nb.info/990729230/34>

⁷ Kargl W.: § 203 Rn. 19. In Kindhäuser/Neumann/Paefgen (Hrsg.) Strafgesetzbuch. 5. Auflage 2017. ISBN 978-3-8487-3106-0

⁸ So z. B.

- Eisele J.: § 203 Rn. 23. In Schönke/Schröder (Hrsg.) Strafgesetzbuch: StGB. 30. Auflage 2019. ISBN 978-3-406-70383-6
- Weidemann M.: § 203 Rn. 33. In Heintschel-Heinegg (Hrsg.) BeckOK StGB 50. Ed. vom 1. Mai 2021

⁹ Eisele J.: § 203 Rn. 20. In Schönke/Schröder (Hrsg.) Strafgesetzbuch: StGB. 29. Auflage 2014. ISBN 978-3-406-65226-4

¹⁰ Siehe z. B.

- Weidemann M.: § 203 Rn. 33. In Heintschel-Heinegg (Hrsg.) BeckOK StGB 50. Ed. vom 1. Mai 2021
- Kargl W.: § 203 Rn. 8. In Kindhäuser / Neumann / Paefgen (Hrsg.) Strafgesetzbuch. 5. Auflage 2017. ISBN 978-3-8487-3106-0
- Fischer T.: § 203 Rn. 33. In Fischer. Strafgesetzbuch: StGB. 65. Auflage 2018. ISBN 978-3-406-70874-9

¹¹ Gaede K.: Teil 8 Die Verletzung der ärztlichen Schweigepflicht (§§ 203-205 StGB) und das Sanktionsregime der DSGVO, Rn. 1053. In: Ulsenheime/Gaede: Arztstrafrecht in der Praxis. C. F. Müller Verlag, 6. Auflage 2021. ISBN 978-3-8114-0637-7

¹² Cierniak/Niehaus § 203 Rn. 54. In Münchener Kommentar zum Strafgesetzbuch Band 4: §§ 185-262, 4. Aufl. 2021, ISBN 978-3-406-74601-7

¹³ So z. B. zu finden in:

- Cierniak/Niehaus § 203 Rn. 118. In Münchener Kommentar zum Strafgesetzbuch Band 4: §§ 185-262, 4. Aufl. 2021, ISBN 978-3-406-74601-7

Zu beachten: Register, die Qualitätssicherung betreiben, nutzen hierzu häufig auch Audits vor Ort, insbesondere, wenn auch Zertifizierungen Bestandteil der Qualitätssicherung sind. Hierbei ist regelmäßig die Einsichtnahme in Originalunterlagen der Patienten erforderlich. Hierzu ist zwingend eine Schweigepflichtentbindung des Patienten erforderlich, wenn eine Anonymität des Patienten (z. B. durch Prüfung von Kopien, in denen alle Informationen, die einen Patienten identifizieren könnten, geschwärzt wurden) nicht gewährleistet werden kann.

3.3 Ärztliche Schweigepflicht / Berufsrecht (§ 9 MBO-Ä)

Der in § 9 MBO-Ä enthaltene ärztliche Schweigepflicht unterliegt alles, was einer Ärztin oder Arzt in seiner/ihrer beruflichen Eigenschaft anvertraut wurde oder sonst bekannt geworden ist.¹⁴ Dies umfasst nicht nur fremde Geheimnisse wie § 203 StGB, sondern alle nicht allgemein bekannten Tatsachen.¹⁵ Nur Tatsachen, die beliebigen Dritten bekannt sind (z. B. weil ein Patient die Daten im Internet frei zugänglich veröffentlichte), unterliegen nicht der Schweigepflicht.¹⁶ Weiterhin gilt die ärztliche Schweigepflicht unbeschränkt, d. h. gegenüber jedem, der nicht in das Arzt-Patienten-Verhältnis einbezogen ist.¹⁷ Die Schweigepflicht dauert entsprechend § 9 Abs. 1 S. 1 MBO-Ä grundsätzlich über den Tod des Patienten hinaus.

Weiterhin geht § 9 MBO-Ä in gewisser Weise über den Schutz in § 203 StGB enthaltene Schutz hinaus, da von § 9 MBO-Ä auch fahrlässige Verstöße erfasst werden.¹⁸

Grundsätzlich muss ein Patient, dessen Behandlungsdaten für biomedizinische Forschung herangezogen werden sollen, hierin gesondert einwilligen und den Arzt von seiner beruflichen Schweigepflicht entbinden.¹⁹ **Bleibt die Identität des Patienten hingegen anonym, kann die Einwilligung – analog zu den Vorgaben bei § 203 StGB – jedoch entfallen¹⁹.**

Hinweis: Verletzt ein Arzt/eine Ärztin die Schweigepflicht, können hieraus berufs- und standesrechtliche Konsequenzen durch die kammerbezogene Berufsgerichtsbarkeit resultieren. Die Heilberufsgesetze bzw. die Kammergesetze für Heilberufe der Länder enthalten Vorgaben, wonach ein Pflichtverstoß beispielsweise durch nachfolgend aufgeführte Sanktionen geahndet werden kann.²⁰

- Eisele J.: § 203 Rn. 20. In Schönke/Schröder (Hrsg.) Strafgesetzbuch: StGB. 30. Auflage 2019. ISBN 978-3-406-70383-6

¹⁴ Wollersheim U.: § 6 Ärztliches Berufsrecht, Rn. 152. In: Clausen/Schroeder-Printzen (Hrsg.) Münchener Anwaltshandbuch Medizinrecht. C. h. Beck Verlag, 3. Auflage 2020. ISBN 978-3-406-72937-9

¹⁵ Scholz K.: § 9 MBO-Ä Rn. 2. In: Spickhoff (Hrsg.) Medizinrecht. C. H. Beck Verlag, 3. Auflage 2018. ISBN 978-3-406-72099-4

¹⁶ Lippert H-D: § 9 Rn. 4. in Ratzel R, Lippert H-D, Prütting J. (Hrsg.) Kommentar zur (Muster-)Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte – MBO-Ä 1997. Springer Verlag, 7. Auflage 2018. ISBN 978-3-662-55165-3

¹⁷ Lippert H-D: § 9 Rn. 7. In Ratzel R, Lippert H-D, Prütting J. (Hrsg.) Kommentar zur (Muster-)Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte – MBO-Ä 1997. Springer Verlag, 7. Auflage 2018. ISBN 978-3-662-55165-3

¹⁸ So z. B.

- Wollersheim U.: § 6 Ärztliches Berufsrecht, Rn. 153. In: Clausen/Schroeder-Printzen (Hrsg.) Münchener Anwaltshandbuch Medizinrecht. C. h. Beck Verlag, 3. Auflage 2020. ISBN 978-3-406-72937-9
- Sobotta D.: § 9 MBO-Ä Rn. 2. In Bergmann/Pauge/Steinmeyer (Hrsg.) Gesamtes Medizinrecht. Nomos, 3. Auflage 2018. ISBN 978-3-8487-2318-8
- Scholz K.: § 9 MBO-Ä Rn. 2. In: Spickhoff (Hrsg.) Medizinrecht. C. H. Beck Verlag, 3. Auflage 2018. ISBN 978-3-406-72099-4

¹⁹ Lippert H-D: § 9 Rn. 40. In Ratzel R, Lippert H-D, Prütting J. (Hrsg.) Kommentar zur (Muster-)Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte – MBO-Ä 1997. Springer Verlag, 7. Auflage 2018. ISBN 978-3-662-55165-3

²⁰ Katzenmeier C.: IX. Berufsgeheimnis und Dokumentation, Rn. 5. In: Laufs/Katzenmeier/Lipp - Arztrecht. C. h. Beck Verlag, 8. Auflage 2021. ISBN 978-3-406-73675-9

- Verwarnung
- Verweis
- Entziehung des aktiven Berufswahlrechts
- Entziehung des passiven Berufswahlrechts
- Geldbuße
- Teilnahme an einer bestimmten Fortbildung zur Qualitätssicherung auf eigene Kosten
- Feststellung der Unwürdigkeit zur Ausübung des Berufs

Genauerer regeln die Landesgesetze für kammergerichtliche Verfahren:

Bundesland	Mögliche Sanktionen
BW (§ 58 HBKG BW)	<ul style="list-style-type: none"> • Verwarnung • Verweis • Geldbuße bis zu 50.000 Euro
BY (§ 67 HKaG BY)	<ul style="list-style-type: none"> • Verwarnung • Geldbuße bis zu 100.000 Euro
BE (§ 76 BlnHKG)	<ul style="list-style-type: none"> • Verwarnung • Geldbuße bis zu 100.000 Euro • Teilnahme an einer bestimmten Fortbildung zur Qualitätssicherung auf eigene Kosten • Feststellung der Unwürdigkeit zur Ausübung des Berufs
BB (§ 59 HeilBerG BB)	<ul style="list-style-type: none"> • Verwarnung • Verweis • Entziehung des passiven Berufswahlrechts • Geldbuße bis zu 50.000 Euro • Feststellung der Unwürdigkeit zur Ausübung des Berufs
HB (§ 65 HeilBerG HB)	<ul style="list-style-type: none"> • Verwarnung • Entziehung des aktiven Berufswahlrechts • Entziehung des passiven Berufswahlrechts • Geldbuße bis zu 25.000 Euro • Feststellung der Unwürdigkeit zur Ausübung des Berufs
HH (§ 3 HeilBerGerG HA)	<ul style="list-style-type: none"> • Verwarnung • Entziehung des aktiven Berufswahlrechts • Entziehung des passiven Berufswahlrechts • Geldbuße bis zu 50.000 Euro • Feststellung der Unwürdigkeit zur Ausübung des Berufs
HE (§ 50 Heilberufsgesetz HE)	<ul style="list-style-type: none"> • Verwarnung • Verweis • Geldbuße bis zu 100.000 Euro • Feststellung der Unwürdigkeit zur Ausübung des Berufs
MV (§ 64 HeilBerG MV)	<ul style="list-style-type: none"> • Verwarnung • Verweis • Entziehung des passiven Berufswahlrechts • Geldbuße bis zu 50.000 Euro • Feststellung der Unwürdigkeit zur Ausübung des Berufs
NI (§ 63 HKG NI)	<ul style="list-style-type: none"> • Verweis • Geldbuße bis zu 100.000 Euro • Feststellung der Unwürdigkeit zur Ausübung des Berufs
NW (§ 60 HeilBerG NW)	<ul style="list-style-type: none"> • Verweis • Entziehung des passiven Berufswahlrechts • Geldbuße bis zu 100.000 Euro

Bundesland	Mögliche Sanktionen
	<ul style="list-style-type: none"> • Teilnahme an einer bestimmten Fortbildung zur Qualitätssicherung auf eigene Kosten • Feststellung der Unwürdigkeit zur Ausübung des Berufs
RP (§ 52 HeilBG RP)	<ul style="list-style-type: none"> • Verwarnung • Verweis • Geldbuße bis zu 200.000 Euro
SL (§ 33 SHKG)	<ul style="list-style-type: none"> • Verweis • Entziehung des aktiven Berufswahlrechts • Entziehung des passiven Berufswahlrechts • Geldbuße bis zu 50.000 Euro
SN (§ 55 SächsHKaG)	<ul style="list-style-type: none"> • Verweis • Geldbuße bis zu 50.000 Euro
ST (§ 48 KGHB-LSA)	<ul style="list-style-type: none"> • Verweis • Entziehung des aktiven Berufswahlrechts • Entziehung des passiven Berufswahlrechts • Geldbuße bis zu 25.000 Euro • Feststellung der Unwürdigkeit zur Ausübung des Berufs
SH (§ 58 HBKG SH)	<ul style="list-style-type: none"> • Verweis • Entziehung des passiven Berufswahlrechts • Geldbuße bis zu 50.000 Euro
TH (§ 48 ThürHeilBG)	<ul style="list-style-type: none"> • Verwarnung • Verweis • Entziehung des aktiven Berufswahlrechts • Entziehung des passiven Berufswahlrechts • Geldbuße bis zu 50.000 Euro • Feststellung der Unwürdigkeit zur Ausübung des Berufs

Weiterhin ist zu beachten, dass gemäß § 5 Abs. 2 i. V. m. § 3 Abs. 1 S. 1 Nr. 2 Bundesärzteordnung eine Approbation widerrufen werden kann, wenn sich eine Ärztin oder ein Arzt eines Verhaltens schuldig gemacht hat, aus dem sich seine Unwürdigkeit oder Unzuverlässigkeit zur Ausübung des ärztlichen Berufs ergibt. Insbesondere kann neben einer kammerbezogenen Berufsgerichtsbarkeit somit auch ein Verstoß gegen § 203 StGB und ein daraus resultierendes Urteil ebenfalls zum Widerruf einer Approbation führen; jedoch erfolgte bis heute bei keiner Ärztin und keinem Arzt in Deutschland (siehe Stand der Ausarbeitung) aufgrund eines Verstoßes gegen § 203 StGB ein Widerruf der Approbation.

Hinweis: Auch in Bezug auf die ärztliche Schweigepflicht gilt der Hinweis bzgl. Audits vor Ort, der bei den Ausführungen zu § 203 StGB enthalten ist, d. h. es kann das Erfordernis entsprechender Schweigepflichtentbindung der Patienten für die Durchführung der jeweiligen Audits gegeben sein.

4 Begriffsbestimmungen

Diese Praxishilfe soll eine Übersicht in die komplexe Materie der datenschutzrechtlichen Vorgaben bei der Nutzung von Patientendaten in Deutschland zu Zwecken der Forschung und der Qualitätssicherung bieten. Aufgrund dessen wird an dieser Stelle auf entsprechende Begriffsbestimmungen verzichtet und lediglich Verweise auf andere Stellen gegeben, wo entsprechende Begriffsbestimmungen zu finden sind:

- Angemessenes Schutzniveau / Stand der Technik
Gemeinsame Ausarbeitung GMDS Arbeitsgruppe DIG / bvitg Arbeitsgruppe Datenschutz & IT-Sicherheit „Sicherheit personenbezogener Daten: Umgang mit Art. 32 DS-GVO“, Kapitel 3 bzw. Kapitel 3.1. [Online, zitiert am 2021-10-05]: verfügbar unter https://gesundheitsdatenschutz.org/html/sicherheit_verarbeitung.php
- Anonymisierung / Pseudonymisierung
GMDS Arbeitsgruppe DIG: „Arbeitshilfe zur Pseudonymisierung/Anonymisierung“, Kapitel 4 [Online, zitiert am 2021-10-05]: verfügbar unter https://gesundheitsdatenschutz.org/html/pseudonymisierung_anonymisierung.php
- Erforderlichkeit / Notwendigkeit
Gemeinsame Ausarbeitung GMDS Arbeitsgruppe DIG / GDD Arbeitskreis Medizin „Datenschutzrechtliche Anforderungen an die medizinische Forschung unter Berücksichtigung der EU Datenschutz-Grundverordnung (DS-GVO)“, Kapitel 4.7. [Online, zitiert am 2021-10-05]: verfügbar unter <https://gesundheitsdatenschutz.org/html/forschung.php>
- Forschung / wissenschaftliche Forschung / historische Forschung
Gemeinsame Ausarbeitung GMDS Arbeitsgruppe DIG / GDD Arbeitskreis Medizin „Datenschutzrechtliche Anforderungen an die medizinische Forschung unter Berücksichtigung der EU Datenschutz-Grundverordnung (DS-GVO)“, Kapitel 4.1, 4.2, 4.3. [Online, zitiert am 2021-10-05]: verfügbar unter <https://gesundheitsdatenschutz.org/html/forschung.php>
- Interessensabwägung
Gemeinsame Ausarbeitung GMDS Arbeitsgruppe DIG / GDD Arbeitskreis Medizin „Datenschutzrechtliche Anforderungen an die medizinische Forschung unter Berücksichtigung der EU Datenschutz-Grundverordnung (DS-GVO)“, Kapitel 4.8. [Online, zitiert am 2021-10-05]: verfügbar unter <https://gesundheitsdatenschutz.org/html/forschung.php>
- Löschen
Gemeinsame Ausarbeitung GMDS Arbeitsgruppe DIG / GDD Arbeitskreis Medizin / bvitg Arbeitsgruppe Datenschutz & IT-Sicherheit: „Leitfaden für die Erstellung von Löschkonzepten im Gesundheitswesen“, Kapitel 2.1, ergänzend Kapitel 2.7. [Online, zitiert am 2021-10-05]: verfügbar unter <https://gesundheitsdatenschutz.org/html/loeschkonzept.php>
- Öffentliches Interesse
Gemeinsame Ausarbeitung GMDS Arbeitsgruppe DIG / GDD Arbeitskreis Medizin „Datenschutzrechtliche Anforderungen an die medizinische Forschung unter Berücksichtigung der EU Datenschutz-Grundverordnung (DS-GVO)“, Kapitel 4.5 und 4.6. [Online, zitiert am 2021-10-05]: verfügbar unter <https://gesundheitsdatenschutz.org/html/forschung.php>

5 Qualitätssicherung und Forschung: Zwei verschiedene Zwecke

Forschung und Qualitätssicherung stellen zwei verschiedene, streng voneinander zu trennende Verwendungszwecke von Patientendaten dar, wie auch schon Art. 9 DS-GVO verdeutlicht: Art. 9 Abs. 2 lit. i DS-GVO adressiert die Qualitätssicherung, Art. 9 Abs. 2 lit. j DS-GVO die Forschung. Beide Erlaubnistatbestände sind nur auf Grundlage nationalen oder Unionsrechts, welches angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person vorsieht, anwendbar. Die unterschiedlichen Anforderungen an diese Verwendungszwecke müssen insbesondere auch im Hinblick auf die Erlaubnistatbestände von den Verantwortlichen getrennt voneinander analysiert und die daraus resultierenden Anforderungen entsprechend umgesetzt werden.

Weiterhin stellt die Nutzung von zur medizinischen Versorgung von Patienten verarbeiteten personenbezogenen Daten zu Zwecken der Forschung und/oder Qualitätssicherung grundsätzlich eine Zweckänderung dar. Entsprechend Art. 13 Abs. 3 DS-GVO bzw. bei Dritterhebung Art. 14 Abs. 4 DS-GVO muss der Verantwortliche betroffenen Personen bei einer Zweckänderung vor dieser Weiterverarbeitung immer Informationen über diesen anderen Zweck und alle anderen maßgeblichen Informationen zur Verfügung stellen. Nicht immer können Patienten nach einer Entlassung gut erreicht werden, aber diese Informationspflicht kennt keine Ausnahme: Kann die Patientin bzw. der Patient nicht informiert werden und die Daten werden trotzdem zu einem anderen Zweck verarbeitet, so stellt dies einen Verstoß dar, der nach Art. 83 Abs. 5 lit. b DS-GVO mit Geldbußen von bis zu 20 Millionen Euro oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs geahndet werden kann. Daher sollten entsprechende Informationen betroffenen Patienten idealerweise direkt bei der Aufnahme zur Verfügung gestellt werden. Dies kann auch zusammen mit den Datenschutzhinweisen bzgl. der Patientenversorgung erfolgen.

Die in Art. 9 Abs. 2 lit. i DS-GVO angesprochene Qualitätssicherung geht über die reine Patientenversorgung durch ein Krankenhaus, wie sie in den meisten deutschen Landesgesetzen für Krankenhäuser enthalten sind (siehe auch Abschnitt 9.1), hinaus. Neben der Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung wird auch die Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei Arzneimitteln und Medizinprodukten adressiert. Insbesondere können Patientendaten – entsprechende nationale Gesetze vorausgesetzt – auch zu Zwecken der Qualitätssicherung bei Arzneimittelwechselwirkungen oder auch der Optimierung der Usability von Software-Medizinprodukten genutzt werden.

Hinweise:

- Bei Einholung einer Einwilligung im Falle unterschiedlicher Zwecke muss ErwGr. 43 DS-GVO beachtet werden²¹: Entsprechend ErwGr. 43 gilt eine Einwilligung auch dann nicht als freiwillig, wenn „zu verschiedenen Verarbeitungsvorgängen von personenbezogenen Daten nicht gesondert eine Einwilligung erteilt werden kann, obwohl dies im Einzelfall angebracht ist“.
- Eine Einwilligung in Form eines sogenannten „broad consent“²² gemäß ErwGr. 33 DS-GVO kann nur „für bestimmte Bereiche wissenschaftlicher Forschung“ rechtswirksam sein, aber nie (siehe auch die durch Art. 9 Abs. 2 lit. i, j DS-GVO gegebene Abgrenzung) für Zwecke der Qualitätssicherung. Register, die sowohl Zwecken der Qualitätssicherung als auch der

²¹ Ausführlicher zum Thema: Gemeinsame Ausarbeitung GMDS Arbeitsgruppe DIG / GDD Arbeitskreis Medizin „Die datenschutzrechtliche Einwilligung: Freund (nicht nur) des Forschers“, Kapitel 4.2.1. [Online, zitiert am 2021-10-05]: verfügbar unter <https://gesundheitsdatenschutz.org/html/einwilligung.php>

²² Zu „broad consent“ siehe auch gemeinsame Ausarbeitung GMDS Arbeitsgruppe DIG / GDD Arbeitskreis Medizin „Die datenschutzrechtliche Einwilligung: Freund (nicht nur) des Forschers“, Kapitel 7. [Online, zitiert am 2021-10-05]: verfügbar unter <https://gesundheitsdatenschutz.org/html/einwilligung.php>

Forschung dienen und die einen broad consent verwenden, müssen daher darauf achten, dass für die Zwecke der Qualitätssicherung ein anderer Erlaubnistatbestand als der broad consent vorhanden ist.

6 Anforderungen aus der DS-GVO

Europäische Verordnungen wie beispielsweise die Datenschutz-Grundverordnung (DS-GVO) sind verbindliche Rechtsakte, gelten unmittelbar und sind in allen ihren Teilen verbindlich für alle Mitgliedsstaaten. Zudem genießt entsprechend Art. 288 Abs. 2 AEUV²³ unmittelbar anwendbares Unionsrecht, also auch die DS-GVO, Vorrang gegenüber nationalem Recht²⁴. D. h. die DS-GVO ist gegenüber einfachgesetzlichem deutschen Recht vorrangig anzuwenden. Deutsches Recht kann somit die Anforderungen der DS-GVO nicht ändern, wenn das Europarecht keine entsprechenden Öffnungen für nationale Vorgaben vorsieht. Daher gelten die Anforderungen der DS-GVO natürlich auch für in Europa/Deutschland tätige Register.

Bei der Auslegung der DS-GVO ist zudem zu beachten, dass Erwägungsgründe keinen Gesetzescharakter haben. D. h. Erwägungsgründe können die Vorschriften in Richtlinien und Verordnungen nicht ändern²⁵. Erwägungsgründe begründen Rechtsvorschriften und sind daher ausschließlich Hilfsmittel zur Interpretation. Daher kann beispielsweise ErwGr. 33 (sog. „Broad Consent“) die normativen Anforderungen der Artikel nicht ändern. Im Falle des Broad Consent muss deshalb jede Einwilligung auch den Anforderungen der Definitionen in Art. 4 Ziff. 11 genügen, die Einhaltung der in Art. 7 DS-GVO genannten Anforderungen gewährleisten und im Falle von Patientendaten den Vorgaben von Art. 9 Abs. 2 lit. a DS-GVO genügen.

Die in Art. 5 DS-GVO genannten „Grundsätze für die Verarbeitung personenbezogener Daten“ sind zwingend bei jeder Verarbeitung einzuhalten und deren **Einhaltung muss nachgewiesen werden**. Diese Grundsätze sind:

- 1) Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
 - Rechtmäßigkeit: Jede Verarbeitung erfordert zwingend immer eine Rechtsgrundlage. Art. 9 Abs. 1 DS-GVO enthält ein grundsätzliches Verbot der Verarbeitung von besonderen Kategorien personenbezogener Daten wie genetischen, biometrischen oder Gesundheitsdaten: Das bedeutet somit, dass nur wenn eine Verarbeitung ausdrücklich erlaubt ist – sei es durch eine Einwilligung der betroffenen Person oder durch eine gesetzliche Regelung – dürfen diese äußerst sensiblen Daten verarbeitet werden. Daher ist ein Erlaubnistatbestand sowohl für die Übermittlung von Patientendaten durch ein Krankenhaus an ein Register (Erlaubnistatbestand, den das Krankenhaus benötigt) als auch die Verarbeitung der Daten im Register (Erlaubnistatbestand, den das Register benötigt) zwingend erforderlich. Dabei ist zu beachten, dass der in Art. 5 Abs. 1 lit. b DS-GVO enthaltene Hinweis, dass wissenschaftliche oder historische Forschungszwecke nicht als unvereinbar mit den ursprünglichen Zwecken gelten, selbst keinen Erlaubnistatbestand darstellt, sondern

²³ Konsolidierte Fassung des Vertrags über die Arbeitsweise der Europäischen Union. [Online, zitiert am 2021-09-25]: verfügbar unter <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A12012E%2FTXT>

²⁴ EuGH, Urt. v. 05.12.2017 Az. C-42/17. [Online, zitiert am 2021-09-23]: verfügbar unter <https://dejure.org/2017,46354>

²⁵ Siehe hierzu auch: Gemeinsamer Leitfaden des Europäischen Parlaments, des Rates und der Kommission für Personen, die an der Abfassung von Rechtstexten der Europäischen Union mitwirken, Leitlinien 10.1, 10.5, 10.5.2. [Online, zitiert am 2021-09-23]: verfügbar unter <https://publications.europa.eu/de/publication-detail/-/publication/3879747d-7a3c-411b-a3a0-55c14e2ba732/language-de>

lediglich den in Art. 6 Abs. 4 DS-GVO²⁶ gefordertem Nachweis der Vereinbarkeit der Zwecke bei einer Zweckänderung darstellt: Werden Daten zur Versorgung von Patienten verarbeitet und sollen anschließend zu Zwecken der Forschung oder Qualitätssicherung genutzt werden, so stellt dies grundsätzlich eine Zweckänderung dar.

- Verarbeitung nach Treu und Glauben: Zum Verständnis hilft es, sich den englischen Begriff anzusehen: Jede Verarbeitung personenbezogener Daten muss „fair“ erfolgen. D. h., Patienten müssen wissen, wozu und von wem die Daten unter welchen Umständen wann und wo verarbeitet werden. Im Falle von Registern kann dies beispielsweise beinhalten:
 - Von wem werden die Daten verarbeitet:
Wer ist das Register? Und welchen Forschern werden Daten zu Forschungszwecken zur Verfügung gestellt? (Z. B. alle Ärzte dürfen Daten anfordern, nur Universitätskliniken, alle Krankenhäuser, Krankenkassen, Pharmafirmen oder auch „jeder“)
 - Wozu werden die Daten verarbeitet:
Die Aufgaben und Zwecke des Registers müssen klar und gut verständlich (siehe auch Transparenz-Anforderung) beschrieben sein. Aber auch die Forschungszwecke, zu denen Registerdaten ggf. von Forschern angefordert werden können, müssen beschrieben werden. Dies können z. B. bei einem onkologischen Register Forschungen im Bereich des kolorektalen Karzinoms oder bei einem Notfallregister Forschungen bei der Versorgung von Unfallpatienten sein.
 - Unter welchen Umständen werden Daten verarbeitet:
Hierzu gehört beispielsweise, ob die Daten anonymisiert oder pseudonymisiert verarbeitet werden. Gleichmaßen gehören aber auch Angaben hinzu, wann es evtl. zu einer Re-Identifikation kommen kann (z. B. wenn ein Krankenhaus im Rahmen einer Auditierung aufgesucht und die Originaldaten begutachtet werden müssen). Ebenfalls gehören hierzu Angaben, unter welchen Umständen Forschende Daten aus dem Register anfordern dürfen. Denkbar ist hier etwa, dass zunächst das Votum einer deutschen Ethikkonferenz vorliegen muss, ein Datenschutz- und IT-Sicherheitskonzept der forschenden Stelle vom Register geprüft werden muss und nur bei Gewährleistung eines ausreichenden Schutzniveaus Daten bereitgestellt, usw.
 - Wann werden die Daten verarbeitet:
Es muss immer auch die Zeitdauer der Verarbeitung angegeben werden (siehe auch Speicherbegrenzung). Dies gilt auch für die Daten, die ggf. Forschern bereitgestellt werden. Ferner sollte aufgezeigt werden, welche Vorgaben das Register den Forschern bzgl. der Speicherdauer stellt, wann die bereitgestellten Daten von den Empfängern gelöscht werden müssen, usw.
 - Wo werden die Daten verarbeitet:
Es muss verständlich dargestellt werden, wo die Daten ggf. verarbeitet werden: Werden die Daten ausschließlich in Deutschland verarbeitet? Oder in

²⁶ Hinweis: Das Bundesarbeitsgericht fragte den EuGH in einer Vorabentscheidung u. a. zum Verhältnis von Art. 9 Abs. 2 DS-GVO zu Art. 6 Abs. 1 DS-GVO. Beschluss vom 26.08.2021, Az. 8 AZR 253/20 (A). [Online, zitiert am 2021-10-12]: verfügbar unter <https://www.bundesarbeitsgericht.de/sitzungsergebnis/8-azr-253-20-a/> bzw. Übersicht bei dejure.org <https://dejure.org/2021,34647>

Europa? Oder können weltweit Forscher Daten beim Register anfragen? Cave: Bei der Verarbeitung in Drittländern (= Länder außerhalb der EU/EWR) oder bei Verarbeitungen durch internationale Organisationen müssen zwingend die Vorgaben in Kapitel V DS-GVO eingehalten werden!

- **Transparenz:** Die Verarbeitung muss – sowohl im Register selbst als auch bei der Verarbeitung durch Forschende – für betroffene Personen transparent erfolgen. Dies beinhaltet in erster Linie die Gewährleistung der im 3. Kapitel genannten Rechte von betroffenen Personen unter Beachtung der Vorgaben von Art. 12 DS-GVO, d. h. alle Informationen müssen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache gegeben werden. Zu beachten ist ferner, dass zu den Rechten betroffener Personen insbesondere auch gehört, dass sie entsprechend Art. 21 Abs. 6 DS-GVO der Verarbeitung ihrer Daten zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken widersprechen können. Ein Widerspruch kann jedoch nur dann erfolgen, wenn die betroffene Person zuvor über die Forschung informiert wurde. Die Anforderung nach „Transparenz“ beinhaltet also auch die Vorgabe, dass der betroffenen Person ausreichende Informationen bereitgestellt werden, sodass diese sich darüber informieren kann, zu welchen Forschungsvorhaben ihre Daten verwendet werden sollen. Da Register i. d. R. nur pseudonymisierte Daten verarbeiten, ist in diesen Fällen eine direkte Information der betroffenen Person durch das Register nicht möglich, aber es können beispielsweise auf zwei Seiten des Registers geplante und durchgeführte Forschungsvorhaben in Verbindung mit der Angabe, aus welchen Krankenhäusern die Daten stammen, aufgelistet und die betroffene Person darauf hingewiesen werden, dass sie sich bzgl. eines Widerspruchs an das jeweilige Krankenhaus, welches die Patientendaten an das Register übermittelte und wo der Patient behandelt wurde, wenden soll, da im Register, wo nur pseudonymisierte Daten vorgehalten werden, eine Zuordnung des Widerspruchs nicht möglich ist.

2) Zweckbindung

Die Verarbeitung personenbezogener Daten darf nur im Rahmen von festgelegten, eindeutigen und legitimen Zwecken erfolgen. Somit scheidet insbesondere eine Verarbeitung für noch unbekanntes Zwecke aus. Eine „Vorratsdatenspeicherung“ ist daher nicht mit den Vorgaben der DS-GVO vereinbar. Auch aus diesem Grund muss die Information der betroffenen Person bzgl. Weitergabe von Daten zu Forschungszwecken durch das Register gut überlegt erfolgen, da nachträgliche Ausweitungen von Forschungsvorhaben nicht möglich sind.

Auch eine Anonymisierung personenbezogener Daten benötigt einen Erlaubnistatbestand, da es sich dabei ebenfalls um eine Verarbeitung dieser Daten handelt. Eine Anonymisierung ohne Vorliegen eines Erlaubnistatbestandes, um Daten des Registers zu anderen Forschungszwecken weiterzugeben, ist rechtswidrig. Jedoch kann in der Aufklärung des Patienten entsprechend den in Kapitel III (genauer Artt. 13, 14 DS-GVO) enthaltenen Informationspflichten (siehe Transparenz) die Information erteilt werden, dass die Daten zu vom Register genannten Forschungszwecken in pseudonymer Form, zu anderen medizinischen Forschungszwecken jedoch ausschließlich in anonymer Form verwendet werden. Jedoch muss hierbei neben dem Nachweis des Erlaubnistatbestands auch die ordnungsgemäße Anonymisierung nachgewiesen werden, d. h. es darf keine Möglichkeit der Identifizierung einer Einzelperson vorhanden sein (siehe Abschnitt 3.1).

3) Datenminimierung

Die Verarbeitung personenbezogener Daten muss für den verfolgten Zweck **erforderlich** und **angemessen** sein. Auch aus diesem Grund ist eine eindeutige Angabe der

Verarbeitungszwecke erforderlich. Denn nur mittels einer klaren, eindeutigen Zweckdarstellung ist es möglich nachzuweisen, dass die Verarbeitung der Daten wirklich erforderlich und angemessen ist.

Erforderlich ist die Verarbeitung personenbezogener Daten nur dann, wenn ohne diese Datenverarbeitung der verfolgte Zweck nicht erreicht werden kann. D. h. die Daten sind für die Erreichung der verfolgten Zwecke unverzichtbar.

Angemessenheit liegt vor, wenn es zu der Verarbeitung kein „milderes“ Mittel gibt, welches weniger in die Rechte und Freiheiten natürlicher Personen eingreift.

Datenminimierung beinhaltet keine Beschränkung der absoluten Datenmenge! Es kann durchaus die Verarbeitung einer sehr großen Menge an personenbezogenen Daten erforderlich und angemessen sein. Big Data und Datenschutz schließen sich nicht aus. Aber die Erforderlichkeit und Angemessenheit der Daten muss nachgewiesen werden.

Ein Register muss also für alle Daten den Nachweis der Erforderlichkeit und Angemessenheit führen. Register, die sowohl der Qualitätssicherung als auch der Forschung dienen, verfolgen zwei unterschiedliche Zwecke. Dabei kann es vorkommen, dass Daten zu dem einen Zweck verwendet werden dürfen, aber nicht zu dem anderen Zweck, da hierfür die Erforderlichkeit und Angemessenheit nicht nachgewiesen werden kann.

4) Richtigkeit

Die Daten müssen für die Dauer der Verarbeitung, die von der Erhebung der Daten bis zu deren Löschung andauert („Lebenszyklus“ der Daten), sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein.

Es müssen alle „angemessenen“ Maßnahmen getroffen werden, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden. Ein Register sollte daher mit einem Krankenhaus ggf. vereinbaren, dass Korrekturen bei Patientendaten nachgemeldet werden müssen.

Cave: Während eine Berichtigung falscher Daten auch bei einem Register immer erfolgen muss, ist eine Aktualisierung der Daten bei einem Register nicht immer erforderlich. Auch für eine Aktualisierung muss der Nachweis von Erforderlichkeit und Angemessenheit geführt werden.

5) Speicherbegrenzung

Personenbezogene Daten dürfen nur so lange in einer die Identifizierung der betroffenen Personen erlaubenden Form gespeichert werden, wie es für die verfolgten Zwecke erforderlich ist.

D. h. grundsätzlich müssen alle Daten gelöscht werden. Betroffenen Personen muss die Information, wann eine Löschung erfolgt, bereits im Rahmen der Information nach Artt. 13, 14 DS-GVO gegeben werden. Dabei ist es nicht erforderlich, eine konkrete Zeitdauer zu nennen (z. B. „nach 5 Jahren werden alle Daten gelöscht“), sondern es können auch Kriterien für die Festlegung dieser Dauer angegeben werden, beispielsweise „alle ihre Daten werden gelöscht, wenn diese innerhalb von 2 Jahren nicht zu Forschungszwecken genutzt wurden“. Die Kriterien müssen für betroffene Personen nachvollziehbar sein, d. h. betroffene Personen müssen eine Möglichkeit haben, zu prüfen, ob ihre Daten für Forschungszwecke genutzt wurden oder nicht (siehe beispielhafte Darstellung einer entsprechenden Internetseite bei den Ausführungen zu „Transparenz“).

Hinweis: Auch eine Anonymisierung kann eine Form der Löschung darstellen.²⁷

6) Integrität und Vertraulichkeit

²⁷ Siehe hierzu auch die Entscheidung der Datenschutzbehörde Österreich vom 5. Dezember 2018, Geschäftszahl DSB-D123.270/0009-DSB/2018. [Online, zitiert am 2021-09-23]; verfügbar unter https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT_20181205_DSB_D123_270_0009_DSB_2018_00/DSBT_2018_1205_DSB_D123_270_0009_DSB_2018_00.html

Bei jeder Verarbeitung muss die Integrität der Daten sowie der Schutz vor unbefugter Kenntnisnahme und Verarbeitung gewährleistet werden (ausreichende Datensicherheit). Dies wird insbesondere durch die Umsetzung der Anforderungen von Artt. 25, 32 und 35 DS-GVO gewährleistet.

- Art. 25 DS-GVO „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“ („Privacy by Design/Default“): Die Inhalte der aus Art. 25 DS-GVO resultierenden Pflichten bestehen insbesondere in der Festlegung und Umsetzung geeigneter technisch-organisatorischer Maßnahmen (Art. 25 Abs. 2 DS-GVO)
 - zur Umsetzung der Grundsätze für die Verarbeitung personenbezogener Daten (Art. 5 DS-GVO)
 - zur Durchsetzung der Betroffenenrechte (Kap. 3, Artt. 12-22 DS-GVO) unter Berücksichtigung (Art. 25 Abs. 1 DS-GVO)
 - des Stands der Technik
 - der Implementierungskosten
 - der Art, Umfang, Umstände und Zwecke
 - der Eintrittswahrscheinlichkeiten und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen.

Diese Maßnahmen müssen bereits bei der Planung der Verarbeitung, also bei der (konzeptionellen) Planung eines Registers erfolgen.

- Art. 32 DS-GVO „Sicherheit personenbezogener Daten“: Art. 32 DS-GVO schreibt vor, dass sowohl der für die Verarbeitung Verantwortliche als auch – sofern vorhanden – der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen treffen müssen, um ein dem *Risiko angemessenes Schutzniveau* zu gewährleisten. Dies beinhaltet, dass Risiken dargestellt und zu diesen Risiken passende Schutzmaßnahmen ergriffen wurden.

Art. 32 DS-GVO enthält dabei insbesondere die Forderung, dass die Vertraulichkeit, die Integrität, die Verfügbarkeit und die Belastbarkeit für Systeme und Dienste im Zusammenhang mit der Verarbeitung der personenbezogenen Daten auf Dauer sicherzustellen sind. Dies beinhaltet u. a. die Forderung, dass die Verfügbarkeit der personenbezogenen Daten nach einem physischen oder technischen Zwischenfall „rasch“ wiederherstellbar sein muss, desgleichen der Zugang zu den Daten, wobei „rasch“ abhängig von der Art der Verarbeitung ist: Daten zur Patientenversorgung müssen ggf. innerhalb eines Tages wieder hergestellt werden, bei einem Forschungsvorhaben kann „rasch“ ggf. auch eine längere Zeitspanne, beispielsweise 14 Tage, bedeuten.

Diese (Sicherheits-)Maßnahmen sind nicht nur einmalig zu planen und umsetzen, sondern die Wirksamkeit dieser Maßnahmen muss regelmäßig überprüft werden und sie sind ggf. anzupassen.

- Art. 35 „Datenschutz-Folgenabschätzung und vorherige Konsultation“: Eine Datenschutz-Folgenabschätzung (DSFA) ist insbesondere bei einer „umfangreichen Verarbeitung besonderer Kategorien von personenbezogenen Daten“ gemäß Art. 9 Abs. 1 DS-GVO (Art. 35 Abs. 3 lit. b DS-GVO) erforderlich. Die europäischen Aufsichtsbehörden schreiben bzgl. der Bewertung, ob eine umfangreiche Verarbeitung erfolgt, dass folgende Faktoren berücksichtigt werden sollten:²⁸

²⁸ Artikel-29-Datenschutzgruppe: Leitlinien in Bezug auf Datenschutzbeauftragte („DSB“), Abschnitt 2.1.3 auf Seite 9. Online, zitiert am 2021-09-26: verfügbar unter http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048

- die Zahl der betroffenen Personen – entweder als bestimmte Zahl oder als Anteil an der maßgeblichen Bevölkerung
- das Datenvolumen und/oder das Spektrum an in Bearbeitung befindlicher Daten
- die Dauer oder Permanenz der Datenverarbeitungstätigkeit
- die geografische Ausdehnung der Verarbeitungstätigkeit.

Bundesweit tätige medizinische Register erfüllen regelmäßig diese Voraussetzungen, denn:

- Es wird versucht, möglichst 100% der jeweils erkrankten Patienten im Register zu erfassen.
- Das Spektrum der Daten umfasst besonders schützenswerte Gesundheits- oder genetische Daten.
- Medizinische Register speichern Daten über einen längeren Zeitraum.
- Die geographische Ausdehnung umfasst das gesamte Bundesgebiet, einige Register erheben sogar Daten benachbarter europäischer Länder.

Eine DSFA wird daher für Register eher regelhaft zwingend erforderlich sein.

Hinweis: Entsprechend § 38 Abs. 1 S. 2 BDSG müssen Verantwortliche, die Verarbeitungen, welche einer DSFA unterliegen, vornehmen, einen Datenschutzbeauftragten benennen.

Diese Grundsätze werden in den anderen Regelungen noch einmal konkretisiert. So stellen die Regelungen in Kapitel III (Rechte der betroffenen Person) u. a. eine Konkretisierung der Transparenzforderung oder die beispielsweise in Artt. 25, 32 und 35 enthaltenen Regelungen eine Ausprägung der Anforderungen von Integrität und Vertraulichkeit dar.

Um den Anforderungen bzgl. eines Nachweises der Erfüllung der Anforderungen nachzukommen, ist zur Umsetzung der datenschutzrechtlichen Rechenschaftspflichten, die insbesondere in Art. 5 Abs. 2 DS-GVO vorgegeben werden, eine entsprechende Dokumentation erforderlich. Dies beinhaltet regelhaft u. a.:

- Das Vorliegen entsprechender Konzepte wie beispielsweise Datenschutzkonzept, IT-Sicherheitskonzept, Pseudonymisierungskonzept oder auch Löschkonzept. Diese Konzepte beschreiben die Rahmenbedingungen der Verarbeitung im Sinne von Pflichtenheften. In den gemäß Art. 32 Abs. 1 lit. d DS-GVO zwingend durchzuführenden Audits wird anhand der Konzepte geprüft, ob die in den Konzepten genannten Maßnahmen auch umgesetzt wurden.
- Eine Datenschutz-Folgenabschätzung muss vor Beginn der Verarbeitung durchgeführt worden sein und danach regelmäßig wiederholt werden.

6.1 Wo findet man weitergehende Informationen?

Insbesondere zu den rechtlichen Fragen, die sich aus der DS-GVO ergeben, sind Gesetzeskommentare zu empfehlen, insbesondere die Großkommentare

- Eßer/Kramer/Lewinski (Hrsg.) Auernhammer, DSGVO / BDSG – Kommentar. Carl Heymanns Verlag, 7. Auflage. 2020. ISBN 978-3-452-29526-2
- Kühling/Buchner (Hrsg.), DS-GVO – BDSG. Datenschutz-Grundverordnung. Bundesdatenschutzgesetz. C.H.Beck Verlag, 3. Auflage 2020. ISBN 978-3-406-74994-0
- Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.) Datenschutzrecht - DSGVO mit BDSG. Nomos Verlagsgesellschaft, 1. Auflage 2019. ISBN 978-3-8487-3590-7

In Kooperation erstellten verschiedene Verbände, darunter GMDS und GDD, verschiedene Papiere, die kostenfrei und unter einer freien Lizenz (Creative Commons, CC BY-SA 4.0) zum Download im Internet

zur Verfügung stehen. Dazu gehören u. a. Ausarbeitungen, welche die in diesem Kapitel angesprochenen Themen behandeln, z. B.:

- Datenschutzrechtliche Anforderungen an eine Einwilligung, Stand 30. April 2021
URL: <https://gesundheitsdatenschutz.org/html/einwilligung.php>
- Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, Stand 28. April 2018
URL: https://gesundheitsdatenschutz.org/html/privacy_design_default.php
- Sicherheit personenbezogener Daten: Umgang mit Art. 32 DS-GVO, Stand 16. Februar 2018
URL: https://gesundheitsdatenschutz.org/html/sicherheit_verarbeitung.php
- Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO, Stand 17. September 2019
URL: <https://gesundheitsdatenschutz.org/html/dsfa.php>
- Arbeitshilfe zur Pseudonymisierung/Anonymisierung, Stand 29. Juni 2018
URL: https://gesundheitsdatenschutz.org/html/pseudonymisierung_anonymisierung.php
- Leitfaden zur Erstellung eines Datenschutzkonzeptes, Stand 12. Dezember 2016
URL: <https://gesundheitsdatenschutz.org/html/datenschutzkonzept.php>
- Leitfaden zur Erstellung eines IT-Sicherheitskonzeptes, Stand 29. September 2017
URL: <https://gesundheitsdatenschutz.org/html/itsicherheitskonzept.php>
- Leitfaden für die Erstellung von Löschkonzepten im Gesundheitswesen, Stand 20. Juni 2020
URL: <https://gesundheitsdatenschutz.org/html/loeschkonzept.php>
- Praxishilfe zur Protokollierung und zur Erstellung von Protokollierungskonzepten im Gesundheitswesen, Stand 23. September 2020
URL: <https://gesundheitsdatenschutz.org/html/protokollierungskonzept.php>
- Klinische Register und Datenschutz, Stand 13. Dezember 2019
URL: https://gesundheitsdatenschutz.org/html/klin_register.php

7 Anforderungen an eine Vorratsdatenspeicherung

Letztlich stellt die Schaffung einer Datenbasis, welche der Erforschung von medizinischen Fragestellungen dient, die zum Zeitpunkt der Erhebung der Daten noch nicht bekannt sind, eine Form der Vorratsdatenspeicherung dar, insbesondere, wenn zudem i. d. R. keine Speicherbegrenzung i. S. v. Art. 5 Abs. 1 lit. e DS-GVO seitens des Registers erfolgt. Auch wenn diese Vorratsdatenspeicherung eines medizinischen Registers nicht der Überwachung von Menschen dient – wenngleich pseudonyme Daten theoretisch auch hierfür genutzt werden können, z. B. bei der Beantwortung, wie verantwortungsbewusst einzelne Menschen Präventivuntersuchungen annehmen, um daraus die Höhe von Versicherungsprämien zu berechnen –, sind hierfür die Vorgaben der Gerichte an eine Vorratsdatenspeicherung anzulegen. Auch gesetzliche Vorgaben, welche entsprechende Datensammlungen durch medizinische Register erlauben, müssen den Vorgaben genügen.

Denn wenngleich bei beiden der nachfolgend genannten Urteile bzgl. der Vorratsspeicherung personenbezogener Daten die Grundlage für die Urteile des EuGH bzw. des EGMR die Nutzung der Daten für Zwecke der Strafverfolgung betraf, beruht die Begründung der Urteile durch die Gerichte neben dem europäischen Datenschutzrecht insbesondere auch auf der Charta der Grundrechte der Europäischen Union²⁹, hier insbesondere auf Artikel 7 (Achtung des Privat- und Familienlebens) und Artikel 8 (Schutz personenbezogener Daten) der Charta. Die Argumente der Urteile des EuGH sowie des EGMR sind daher auf jede Form der Vorratsdatenspeicherung analog anwendbar, dementsprechend muss den in den Urteilen enthaltenen Anforderungen genügt werden.

2016 urteilte der EuGH³⁰, dass eine Vorratsdatenspeicherung immer einer verhältnismäßigen Ausgestaltung bedarf, also nur erforderliche Daten zu festgelegten Zwecken gesammelt werden dürfen sowie die Daten auch entsprechend ihrer Sensibilität geschützt werden müssen. Auch soll der Zugang zu den Daten einer unabhängigen Kontrolle unterliegen. Zudem muss es ein „objektives Kriterium“ geben, welches den Zugang zu den Daten auf konkrete Zwecke beschränkt. Weiterhin müssen die betreffenden Daten im Gebiet der Europäischen Union gespeichert werden.

Der EGMR verlangt in seinem Urteil³¹ aus dem Jahr 2021, dass in jeder Phase des Prozesses eine Bewertung der Notwendigkeit und der Verhältnismäßigkeit der getroffenen Maßnahmen vorzunehmen ist. Ferner sieht der EGMR es als zwingend notwendig an, dass die Datennutzung einer unabhängigen Genehmigung unterliegen sollte, durch die Gegenstand und Umfang des Einsatzes festgelegt werden. Weiterhin muss die Nutzung der Daten durch eine Ex-post-facto-Kontrolle überprüfbar sein.

7.1 Daraus resultierende Anforderungen

Aus den von den beiden Gerichten aufgestellten Forderungen resultieren Anforderungen, die auch für die Datenverarbeitung von Registern beachtet werden müssen und die im Nachfolgenden kurz dargestellt sind:

- Register müssen die Patientendaten im Gebiet der Europäischen Union oder des Europäischen Wirtschaftsraums speichern.
- Register müssen vor Beginn der Datensammlung festlegen, zu welchen Forschungszielen welche Daten genutzt werden dürfen. Bei Änderung dieser Vorgaben muss darauf geachtet

²⁹ Charta der Grundrechte der Europäischen Union. [Online, zitiert am 2021-10-17]: verfügbar unter <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:12012P/TXT>

³⁰ EuGH, 21.12.2016 - C-203/15, C-698/15. [Online, zitiert am 2021-10-06]: verfügbar unter <https://dejure.org/2016,47053>

³¹ Europäischer Gerichtshof für Menschenrechte (EGMR): Urteil der Großen Kammer des EGMR vom 25. Mai 2021 in der Rechtssache. Big Brother Watch u. a. vs. Vereinigtes Königreich (App.No. 58170/13, 62322/14, 24960/15). [Online, zitiert am 2021-10-06]: verfügbar unter <https://dejure.org/2018,28003>

werden, dass nur Daten zu den geänderten Zielen genutzt werden können, die ab dem Änderungszeitpunkt erhoben wurden.

- Register müssen darlegen, dass die erhobenen Patientendaten für die Erreichung der vom Register unterstützten Forschungsziele notwendig sind. Dies wird in der Regel dergestalt erfolgen, dass das Register den medizinischen Zusammenhang zwischen den Daten und den Forschungszielen darlegt, z. B. kann der Zusammenhang zwischen dem Wert „Hb“ und dem Blutverlust eines Patienten die Notwendigkeit der Nutzung des Hb-Wertes bei operierten Patienten belegen.
- Register dürfen Daten nur Forschungsprojekten zur Verfügung stellen, die die Notwendigkeit der Daten zur Erlangung des Forschungszieles nachgewiesen haben.
- Register dürfen Daten nur Forschungsprojekten zur Verfügung stellen, welche die Verhältnismäßigkeit des Forschungsnutzens in Bezug auf die Grundrechtseingriffe betroffener Personen nachgewiesen haben.
- Register dürfen Daten nur Forschungsprojekten zur Verfügung stellen, in denen eine unabhängige Stelle das Forschungsvorhaben begutachtete und die Datennutzung für legitim bewertete; dies wird in Deutschland i. d. R. durch ein entsprechendes Votum einer Ethikkommission umgesetzt.
- Betroffene Personen müssen nachvollziehen / kontrollieren können, welche ihrer Daten zu welchen Forschungsprojekten genutzt wurden. Dies kann z. B. dadurch erreicht werden, dass ein Register auf einer Webseite darlegt, zu welchen Forschungsprojekten Daten aus welchem Krankenhaus genutzt wurden, abgestuft nach Zeiträumen der Datenlieferung. So kann ein Patient, der zu einem bestimmten Zeitraum in einer bestimmten Abteilung eines Krankenhauses versorgt wurde, prüfen, zu welchen Projekten seine Daten genutzt wurden. Idealerweise wird eine entsprechende Such- bzw. Filterfunktion angeboten.

Fast alle der Anforderungen lassen sich auch aus den Vorgaben der DS-GVO ableiten, so z. B. die Festlegung der Forschungsziele aus Art. 5 Abs. 1 lit. b DS-GVO oder die Erforderlichkeit sowohl der Daten als auch der Verarbeitung zur Erreichung der Forschungsziele aus Art. 5 Abs. 1 lit. c DS-GVO. Entsprechend ErwGr. 4 DS-GVO achtet die DS-GVO alle Freiheiten und Grundsätze, die mit der Charta anerkannt wurden und in den Europäischen Verträgen verankert sind. Wenn in der DS-GVO daher von „Rechte und Freiheiten natürlicher Personen“ die Rede ist, so betrifft dies nicht nur Art. 8 der Charta, sondern auch die anderen Grundrechte. Daher ist selbst die Forderung nach der Verhältnismäßigkeit der Verarbeitung von Patientendaten in Hinsicht auf die Einschränkung der Grundrechte der Patienten bereits in den Anforderungen der DS-GVO enthalten.

Letztlich ist lediglich die Anforderung, dass Register Patientendaten in der EU bzw. dem EWR verarbeiten, eine rein aus den Urteilen ableitbare Anforderung.

8 Gesetzliche Anforderungen für Qualitätssicherung und Forschung

Hinweis: Träger medizinischer Register sind häufig juristische Personen wie beispielsweise eine GmbH. In diesen Fällen gelten – neben dem Europarecht – eigentlich nur die datenschutzrechtlichen Vorgaben des Bundes für das jeweilige Register. Damit Krankenhäuser aber Patientendaten an ein Register übermitteln dürfen, müssen diese Register auch die Vorgaben der jeweiligen für das Krankenhaus geltenden Vorgaben zur Übermittlung von Patientendaten erfüllen. Krankenhäuser sollten sich die Einhaltung auch vertraglich bestätigen lassen.

8.1 Erlaubnistatbestand zur Verarbeitung von Daten durch ein Register

Für die Arbeit eines Registers sind zwei Aspekte relevant:

- 1) Ein medizinisches Register benötigt Patientendaten aus Kliniken. Damit die Kliniken Daten an ein Register zu Zwecken der Qualitätssicherung übermitteln dürfen, muss das betreffende Register den hierfür in den Landeskrankenhausgesetzen enthaltenen Anforderungen genügen.
- 2) Nachdem ein Register die Daten erhalten hat, müssen die Patientendaten gespeichert, ausgewertet, d. h. verarbeitet werden. Aufgrund des in Art. 9 Abs. 1 DS-GVO enthaltenen Verbots der Verarbeitung von Gesundheitsdaten sowie genetischen Daten, benötigt ein Register hierfür einen Erlaubnistatbestand. Dieser findet sich in § 22 Abs. 1 lit. c BDSG.

8.1.1 Erlaubnistatbestand zur Verarbeitung von Patientendaten zu Zwecken der Qualitätssicherung

§ 22 Abs. 1 lit. c BDSG nutzt die in Art. 9 Abs. 2 lit. i DS-GVO enthaltene Öffnungsklausel und stellt einen Erlaubnistatbestand³² u. a. für die Verarbeitung von Gesundheitsdaten sowie genetischen Daten zu Zwecken der „Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung“, jedoch ausschließlich „aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit“. D. h. kann dieser Erlaubnistatbestand von einem medizinischen Register genutzt werden, ist keine Einwilligung zur Legitimierung der Verarbeitung des Registers erforderlich, gleichwohl muss natürlich eine Information entsprechend Art. 13 bzw. 14 DS-GVO erfolgen.

Entsprechend der Begründung im BDSG-Gesetzesentwurf der Bundesregierung³³ legt § 22 Abs. 1 BDSG fest, „unter welchen Voraussetzungen die Verarbeitung besonderer Kategorien personenbezogener Daten ausnahmsweise zulässig ist.“, stellt also einen Erlaubnistatbestand i. S. d. DS-GVO dar. Art. 9 Abs. 2 lit. i DS-GVO verlangt, dass bei derartigen nationalen Regelungen „angemessene und spezifische

³² So z. B.

- Bundesärztekammer, Kassenärztliche Bundesvereinigung: Hinweise und Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis. Abschnitt „zur Erfüllung spezieller Pflichten im öffentlichen Gesundheitsinteresse“, Seite A7. [Online, zitiert am 2021-10-26]: verfügbar unter https://www.bundesaerztekammer.de/fileadmin/user_upload/downloads/pdf-Ordner/Recht/Hinweise_und_Empfehlungen_aerztliche_Schweigepflicht_Datenschutz_Datenverarbeitung_09.03.2018.pdf
- Buckstegge S.: § 15 Datenschutz im Gesundheitswesen, Rn. 137. In: Saalfrank, Handbuch des Medizin- und Gesundheitsrechts. Wissenschaftliche Verlagsgesellschaft, 2020. ISBN 978-3-8047-4126-3
- Dochow C.: 4.1.2 Überblick zu den Erlaubnisgründen für die Verarbeitung von Gesundheitsdaten, Tabelle 4.1. In: Dochow/Dörfer/Halbe/Hübner/Ippach/Schröder/Schütz/Strüve, Datenschutz in der ärztlichen Praxis. Deutscher Ärzte-Verlag, 1. Auflage 2019. ISBN 978-3-7691-3689-0
- Heckmann D, Scheurer M.: § 22 Rn. 30. In: Gola/Heckmann (Hrsg.) Bundesdatenschutzgesetz. C. H. Beck Verlag, 13. Auflage 2019. ISBN 978-3-406-72878-5
- Petri T.: Art. 9 DS-GVO Rn. 25. in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.) Datenschutzrecht - DSGVO mit BDSG. Nomos Verlag, 1. Auflage 2019. ISBN 978-3-8487-3590-7

³³ Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU). Seite 94, „Zu § 22“, zweiter Absatz. [Online, zitiert am 2021-10-26]: verfügbar unter <https://dserver.bundestag.de/btd/18/113/1811325.pdf>

Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person, insbesondere des Berufsgeheimnisses“ getroffen werden. § 22 Abs. 1 lit. c BDSG enthält die Verpflichtung, dass die berufsrechtlichen und strafrechtlichen Vorgaben zur Wahrung des Berufsgeheimnisses einzuhalten sind. Desgleichen müssen die Vorgaben von § 22 Abs. 2 BDSG eingehalten werden; die Regelungen von § 22 Abs. 2 S. 1, 2 BDSG setzen laut der Gesetzesbegründung³⁴ das Erfordernis aus Art. 9 Abs. 2 lit. b, g und i DS-GVO um, ‚geeignete Garantien für die Grundrechte und die Interessen der betroffenen Person‘ bzw. ‚angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person“ vorzusehen‘.³⁵

Bei Nutzung der in § 22 Abs. 1 enthaltenen Erlaubnistatbestände ist jedoch zu beachten, dass relevante Sachverhalte in Spezialgesetzen geregelt sind.³⁶ Diese in Spezialgesetzen (beispielsweise dem SGB V oder dem Arzneimittelgesetz, aber auch den Berufsordnungen der Ärzte oder Apotheker) enthaltenen Regelungen sind ggf. als „lex specialis“ vorrangig gegenüber § 22 Abs. 2 BDSG anzuwenden.

Weiterhin muss beachtet werden, dass gemäß ErwGr. 54 S. 4 DS-GVO Patientendaten, die zu Zwecken der Qualitätssicherung verarbeitet werden, nicht Dritten weitergegeben und auch nicht zu anderen Zwecken verarbeitet werden dürfen.³⁷ Es gilt eine strenge Zweckbindung.

Damit ein medizinisches Register die eigene Verarbeitung der von Krankenhäusern übermittelten Patientendaten mittels § 22 Abs. 1 lit. c BDSG legitimieren kann, müssen folgende Voraussetzungen erfüllt sein:

- 1) Die Verarbeitung muss „aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit“ erfolgen.

Hinweis: Gemäß ErwGr. 54 DS-GVO muss der Begriff „öffentliche Gesundheit“ im Sinne der Verordnung (EG) Nr. 1338/2008³⁸ des Europäischen Parlaments und des Rates ausgelegt werden. Art. 3 lit. c VO 1338/2008 lautet:

„Öffentliche Gesundheit“ alle Elemente im Zusammenhang mit der Gesundheit, nämlich den Gesundheitszustand einschließlich Morbidität und Behinderung, die sich auf diesen Gesundheitszustand auswirkenden Determinanten, den Bedarf an Gesundheitsversorgung, die der Gesundheitsversorgung zugewiesenen Mittel, die Bereitstellung von und den allgemeinen Zugang zu Gesundheitsversorgungsleistungen sowie die entsprechenden Ausgaben und die Finanzierung und schließlich die Ursachen der Mortalität.

- 2) Berufsrechtliche und strafrechtliche Vorgaben zur Wahrung des Berufsgeheimnisses müssen eingehalten werden.
- 3) Die Vorgaben von § 22 Abs. 2 BDSG müssen umgesetzt werden. Dies beinhaltet insbesondere:
 1. Einsatz von technisch organisatorischen Maßnahmen, welche sicherstellen, dass die Verarbeitung gemäß DS-GVO erfolgt.

³⁴ DSAnpUG-EU, Entwurf der Bundesregierung: Seite 95, siebenter Absatz

³⁵ Petri T.: Art. 9 DS-GVO Rn. 25. In: Simitis/Hornung/Spiecker gen. Döhmman (Hrsg.) Datenschutzrecht - DSGVO mit BDSG. Nomos Verlag, 1. Auflage 2019. ISBN 978-3-8487-3590-7

³⁶ . Heckmann D, Scheurer M.: § 22 Rn. 32. In: Gola/Heckmann (Hrsg.) Bundesdatenschutzgesetz. C. h. Beck Verlag, 13. Auflage 2019. ISBN 978-3-406-72878-5

³⁷ Petri T: Art. 9 DS-GVO Rn. 96. In: Simitis/Hornung/Spiecker gen. Döhmman (Hrsg.) Datenschutzrecht - DSGVO mit BDSG. Nomos Verlag, 1. Auflage 2019. ISBN 978-3-8487-3590-7

³⁸ Verordnung (EG) Nr. 1338/2008 des Europäischen Parlaments und des Rates vom 16. Dezember 2008 zu Gemeinschaftsstatistiken über öffentliche Gesundheit und über Gesundheitsschutz und Sicherheit am Arbeitsplatz. [Online, zitiert am 2021-10-26]: verfügbar unter URL <https://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1488734966720&uri=CELEX:32008R1338>

2. Ergreifung von Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt worden sind.
3. Sensibilisierung der an Verarbeitungsvorgängen Beteiligten.
4. Benennung einer oder eines Datenschutzbeauftragten.
5. Beschränkung des Zugangs zu den personenbezogenen Daten innerhalb der verantwortlichen Stelle und von Auftragsverarbeitern.
6. Pseudonymisierung personenbezogener Daten, wann immer möglich.
7. Verschlüsselung personenbezogener Daten, wann immer möglich. Insbesondere, wenn Daten übermittelt werden, kann hierauf regelhaft nicht verzichtet werden.
8. Sicherstellung der Fähigkeit, Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten, einschließlich der Fähigkeit, die Verfügbarkeit und den Zugang bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen.
9. Zur Gewährleistung der Sicherheit der Verarbeitung muss
 - a. die Einrichtung eines Verfahrens zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen erfolgen oder
 - b. spezifische Verfahrensregelungen, die im Fall einer Übermittlung oder Verarbeitung für andere Zwecke die Einhaltung der Vorgaben dieses Gesetzes sowie der DS-GVO sicherstellen, vorhanden sein und die Umsetzung und Einhaltung der Regelungen sichergestellt sein.

Hinweis: Die Anforderungen 6, 7, 8 und 9 entsprechen nahezu wortwörtlich den Anforderungen von Art. 32 Abs. 1 lit. a, b, c und d DS-GVO und die Erfüllung der Anforderungen aus Art. 32 DS-GVO muss grundsätzlich bei jeder Verarbeitung sichergestellt sein. Anforderung 5 resultiert unmittelbar aus Art. 5 Abs. 1 lit. f DS-GVO und Anforderung 2 muss gemäß dem Urteil des Europäischen Gerichtshofs für Menschenrechte nach Art. 8 der Europäischen Menschenrechtskonvention³⁹ ebenfalls unabhängig von einer Forderung des BDSG erfüllt werden. Anforderung 1 enthält letztlich nur die Anforderung, dass die DS-GVO bei der Verarbeitung personenbezogener Daten eingehalten wird. Damit enthält § 22 Abs. 2 BDSG eigentlich nur zwei „neue“ Anforderungen: Sensibilisierung der mit der Verarbeitung beauftragten Personen sowie Benennung eines Datenschutzbeauftragten.

8.1.2 Erlaubnistatbestand zur Verarbeitung von Patientendaten zu Forschungszwecken

Art. 9 Abs. 2 lit. j DS-GVO enthält eine Öffnungsklausel, nach der nationale Gesetzgeber Erlaubnistatbestände zur Nutzung von in Art. 9 Abs. 1 DS-GVO genannten Kategorien von Daten zu Forschungszwecken erlassen können. Diese Möglichkeit nutzte der deutsche Gesetzgeber und schuf mit § 27 BDSG auf Basis von Art. 9 Abs. 2 lit. j DS-GVO eine Regelung im nationalen Recht, welcher die Verarbeitung besonderer Kategorien personenbezogener Daten, zu denen insbesondere Gesundheitsdaten sowie genetischen Daten gehören, zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken gestattet⁴⁰, d. h. einen Erlaubnistatbestand zur Verarbeitung entsprechender Daten zu Forschungszwecken ohne Einholung einer Einwilligung⁴¹. Bei

³⁹ Right to Privacy Requires Strict Controls, Safeguards and Protection of Health Information. I v Finland [2008] ECHR 20511/03 (17 July 2008). [Online, zitiert am 2021-10-26]: verfügbar unter URL <http://www.cl.cam.ac.uk/~rja14/Papers/echr-finland.pdf>

⁴⁰ Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU). Seite 99, „Zu § 27“, erster Absatz. [Online, zitiert am 2021-10-26]: verfügbar unter <https://dserver.bundestag.de/btd/18/113/1811325.pdf>

⁴¹ So z. B.

Nutzung dieses Erlaubnistatbestandes benötigt ein Register keine Einwilligung zur Legitimierung der Verarbeitung der Patientendaten, gleichwohl muss natürlich eine Information entsprechend Art. 13 bzw. 14 DS-GVO erfolgen.

Die Verarbeitung zu entsprechenden Forschungszwecken ist entsprechend § 27 Abs. 1 BDSG nur erlaubt, wenn

- 1) die Verarbeitung zu diesen Zwecken erforderlich ist und
- 2) die Interessen des Verantwortlichen an der Verarbeitung die Interessen der betroffenen Person an einem Ausschluss der Verarbeitung erheblich überwiegen.

Durch diese Anforderung räumt der Gesetzgeber dem Interesse der betroffenen Person an der Nichtverarbeitung der sie betreffenden Daten einen Vorrang gegenüber dem Forschungsinteresse ein, welches nur durch ein erheblich überwiegendes Forschungsinteresse überwunden werden kann.⁴²

Weiterhin muss der Verantwortliche (= das Register bzw. die Forschenden) angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person gemäß § 22 Abs. 2 S. 2 BDSG vorsehen (siehe Abschnitt 8.1.2). Der Verweis auf § 22 Abs. 2 BDSG entbindet Verantwortliche jedoch nicht von der Pflicht, gegebenenfalls weitere oder auch andere Maßnahmen zu treffen, wenn dies aufgrund des konkreten Schutzbedarfes erforderlich ist.⁴³

Die personenbezogenen Daten sind gemäß § 27 Abs. 3 BDSG zu anonymisieren, sobald dies nach dem Forschungszweck möglich ist, es sei denn, berechnete Interessen der betroffenen Person stehen einer Anonymisierung entgegen. Solange eine Anonymisierung nicht möglich ist, dürfen nur pseudonyme Daten verarbeitet zu wissenschaftlichen oder historischen Forschungszwecken werden.

Entsprechend der Gesetzesbegründung sind spezialgesetzliche Regelungen zur Datenverarbeitung gegenüber dem bereichsspezifischen Recht vorrangig anzuwenden⁴⁴.

Weiterhin ist zu beachten, dass eine betroffene Person entsprechend Art. 21 Abs. 6 DS-GVO jederzeit das Recht hat, „aus Gründen, die sich aus ihrer besonderen Situation ergeben, gegen die sie betreffende Verarbeitung sie betreffender personenbezogener Daten“ zu wissenschaftlichen oder historischen Forschungszwecken zu widersprechen. Gemäß Art. 21 Abs. 4 DS-GVO muss die betroffene Person „in einer verständlichen und von anderen Informationen getrennten Form“ ausdrücklich auf ihr Widerspruchsrecht hingewiesen werden. Diese Pflicht gilt jedoch nur für Art. 21 Abs. 1, 2 DS-GVO, d. h. für Verarbeitungen, die entweder auf Grundlage von Art. 6 Abs. 1 lit. e (= Verarbeitung erfolgt in einer im öffentlichen Interesse liegenden Aufgabe oder in Ausübung öffentlicher Gewalt) oder f (= Verarbeitung erfolgt aufgrund einer Interessensabwägung) DS-GVO oder zu Zwecken der Direktwerbung erfolgen; medizinische Forschung beruht regelhaft auf einem Erlaubnistatbestand in Art. 9 DS-GVO. Jedoch ist zweifelhaft, ob der europäische Gesetzgeber für die weitaus sensibleren in Art. 9 Abs. 1 DS-GVO genannten Daten eine Ausnahme machen wollte, wenn für die „allgemeinen“

-
- Buchner B.: § 27 BDSG Rn. 8. In: Kühling/Buchner (Hrsg.), DS-GVO – BDSG. Datenschutz-Grundverordnung. Bundesdatenschutzgesetz. C. H. Beck Verlag, 3. Auflage 2020. ISBN 978-3-406-74994-0
 - Greve H.: § 27 BDSG Rn. 12. In: Eßer/Kramer/Lewinski (Hrsg.) Auernhammer, DSGVO / BDSG. Carl Heymanns, 7. Auflage. 2020. ISBN 978-3-452-29526-2
 - Krohm N.: § 27 Rn. 11. In: Gola/Heckmann (Hrsg.) Bundesdatenschutzgesetz. C. h. Beck Verlag, 13. Auflage 2019. ISBN 978-3-406-72878-5

⁴² Greve H.: § 27 BDSG Rn. 14. In: Eßer/Kramer/Lewinski (Hrsg.) Auernhammer, DSGVO / BDSG. Carl Heymanns, 7. Auflage. 2020. ISBN 978-3-452-29526-2

⁴³ Krohm N.: § 27 Rn. 31. In: Gola/Heckmann (Hrsg.) Bundesdatenschutzgesetz. C. h. Beck Verlag, 13. Auflage 2019. ISBN 978-3-406-72878-5

⁴⁴ DSAnpUG-EU, Entwurf der Bundesregierung: Seite 100, dritter Absatz

Daten die Pflicht des Hinweises besteht. Daher wird dazu geraten, auch bei Vorliegen entsprechender Tatbestände, die auf Art. 9 DS-GVO beruhen, der Informationspflicht zu genügen.

Ein Widerspruch ist nicht möglich, wenn die Verarbeitung zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe erforderlich ist. Die Darlegungslast, dass die Forschung einer im öffentlichen Interesse liegenden Aufgabe dient und die Verarbeitung erforderlich ist, liegt beim Verantwortlichen. Die in Art. 21 Abs. 6 DS-GVO genutzte Wendung „es sei denn“ enthält eine normative Wertung für eine Non-liquet-Konfliktentscheidung, d. h. sind beide Interessen gleichwertig, setzt sich das Privatsphärenschutzinteresse des Betroffenen durch; erst durch überwiegendes Interesse des Verantwortlichen ist ein Widerspruch nicht mehr möglich⁴⁵. Zu den Tatbestandsvoraussetzungen gehört weiterhin, dass es nicht genügt, dass ein öffentliches Interesse vorliegt, sondern der Verantwortliche muss eine im öffentlichen Interesse liegende Aufgabe wahrnehmen. Und natürlich muss ein Erfordernis für die Verarbeitung der Daten zur Erreichung des konkreten Forschungszweckes gegeben sein.

Entsprechend § 27 Abs. 2 i. V. m. Art. 89 Abs. 2 DS-GVO ist das Widerspruchsrecht betroffener Personen weiterhin eingeschränkt, wenn die Wahrnehmung dieses Rechtes durch die jeweilige betroffene Person „voraussichtlich die Verwirklichung der spezifischen Zwecke unmöglich machen oder ernsthaft beeinträchtigen und solche Ausnahmen (vom Widerspruchsrecht) für die Erfüllung dieser Zwecke notwendig sind“. „Unmöglich“ bedingt eine Prognose und die Bedingung kann nur als erfüllt angesehen werden, wenn es keine umsetzbare Möglichkeit gibt, die Forschungszwecke ohne Beschränkung der Rechte des Betroffenen zu erreichen⁴⁶. Eine „ernsthafte Einschränkung“ kann angenommen werden, wenn durch die Wahrnehmung der Betroffenenrechte der angestrebte Forschungszweck nur in erheblich geringerem Umfang erreicht werden kann.⁴⁶ Weiterhin muss die Beschränkung der Betroffenenrechte für die Erfüllung des Forschungszweckes notwendig sein, d. h. die Forschungszwecke können ausschließlich durch die Beschränkung des Betroffenenrechtes erreicht werden.⁴⁷

Herausforderung für Register bei Nutzung dieses Erlaubnistatbestandes

§ 27 BDSG setzt einen konkreten Forschungszweck voraus, medizinische Register verfolgen hingegen keinen eigenen Forschungszweck, sondern halten medizinische Daten für die Forschungen Dritter bereit. Somit kann ein Register regelhaft nicht, wie in § 27 Abs. 1 BDSG gefordert, nachweisen, dass die Patientendaten sowie die Verarbeitung dieser Patientendaten erforderlich sind. Dies ginge nur mit einer abschließenden Aufzählung der konkreten Forschungszwecke.

Alternativ müsste die Verarbeitung der Patientendaten auf eine Einwilligung gestützt werden, soweit dies die Landeskrankenhausgesetze erlauben. Ohne Angabe eines konkreten Zweckes könnte nur ein sogenannter „broad consent“ genutzt werden, wobei der Europäische Datenschutzausschuss zwingend zu beachtende Vorgaben erstellte, damit ein broad consent genutzt und als legitim angesehen werden kann.⁴⁸

⁴⁵ Martini M.: Art. 21, Rn. 60. In: Paal/Pauly (Hrsg.) DS-GVO BDSG. C. H. Beck Verlag, 3. Auflage 2021. ISBN 978-3-406-75374-9

⁴⁶ Pauly D.: § 27 Rn. 11. In: Paal/Pauly (Hrsg.) DS-GVO BDSG. C. H. Beck Verlag, 3. Auflage 2021. ISBN 978-3-406-75374-9

⁴⁷ Pauly D.: § 27 Rn. 11. In: Paal/Pauly (Hrsg.) DS-GVO BDSG. C. H. Beck Verlag, 3. Auflage 2021. ISBN 978-3-406-75374-9

⁴⁸ Näheres zu den Rahmenbedingungen bei „broad consent“ kann in in Kapitel 7 der Praxishilfe „Datenschutzrechtliche Anforderungen an eine Einwilligung“ (Stand 30. April 2021) nachgelesen werden. [Online, zitiert am 2021-10-16]: verfügbar unter URL: <https://gesundheitsdatenschutz.org/html/einwilligung.php>

8.2 Anforderungen für bundesweit tätige Register (Qualitätssicherung)

Hinweis: Erläuterungen finden sich bei den Ausführungen für Krankenhäuser im Abschnitt 9.2.

Vorliegen von

- Rechtsgrundlage für die Verarbeitung
 - Für die Übermittlung von Patientendaten durch das Krankenhaus an das Register: I. d. R. Einwilligung⁴⁹ der Patienten
 - Für die Qualitätssicherung des Registers: § 22 Abs. 1 lit. c BDSG i. V. m. Art. 9 Abs. 2 lit. i DS-GVO
- Voraussetzungen:
 1. Verarbeitung erfolgt aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit,
 2. Berufsrechtliche und strafrechtliche Vorgaben zur Wahrung des Berufsgeheimnisses werden eingehalten
 3. Verarbeitung zu diesen Zwecken muss erforderlich sein
 4. Angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person gemäß § 22 Abs. 2 S. 2 BDSG existieren
- Nachweis von:
 - Erforderlichkeit der Daten
 - Überwiegende schutzwürdige Interessen des Betroffenen stehen Verarbeitung nicht entgegen
 - Berechtigte Interesse der Allgemeinheit überwiegt das Geheimhaltungsinteresse der Patientin oder des Patienten erheblich
 - Empfänger ist Arzt oder eine ärztlich geleitete Stelle
 - Empfänger muss Fachpersonal i. S. v. Art. 9 Abs. 3 DS-GVO sein, Geheimhaltungspflicht unterliegen
 - Pseudonymisiert, wenn anonymisiert nicht möglich, dies beinhaltet den Nachweis, dass Zwecke nicht mit anonymisierten Daten erreicht werden können
 - Aussagekräftiger Dokumentation des Empfängers, über die Art der zu übermittelnden Daten und der betroffenen Patienten
 - Datenschutzbeauftragte sind einzuschalten
 - Berufsrechtliche und strafrechtliche Vorgaben zur Wahrung des Berufsgeheimnisses sind einzuhalten
 - Datenschutz-Folgenabschätzung, welche ergibt, dass für betroffene Personen/Patienten kein hohes Risiko existiert

Da Krankenhäuser Daten nur bei Erfüllung der für eine Übermittlung erforderlichen Anforderungen an ein Register weitergeben müssen, müssen Krankenhäuser diese Erfüllung vorab prüfen. Ein Register sollte sich hier vorbereiten und Unterlagen wie die Datenschutz-Folgenabschätzung und Konzepte wie beispielsweise Datenschutz- und IT-Sicherheitskonzept für den Nachweis der Erfüllung bereithalten.

⁴⁹ Zu den genauen Anforderungen an eine rechtskonforme Einwilligung wie beispielsweise Freiwilligkeit und Bestimmtheit sowie im Falle von besonderen Kategorien wie Gesundheitsdaten oder genetischen Daten bzw. Einwilligungen für die Übermittlung/Verarbeitung in Drittstaaten die Ausdrücklichkeit siehe z. B. die Praxishilfe „Datenschutzrechtliche Anforderungen an eine Einwilligung“ (Stand 30. April 2021). [Online, zitiert am 2021-10-16]; verfügbar unter URL: <https://gesundheitsdatenschutz.org/html/einwilligung.php>

8.3 Anforderungen für bundesweit tätige Register (Forschung)

Hinweis: Erläuterungen finden sich bei den Ausführungen für Krankenhäuser im Abschnitt 9.1.

Vorliegen von

- Rechtsgrundlage für die Verarbeitung
 - Für Übermittlung Krankenhaus an Register: I. d. R. Einwilligung der Patienten
 - Für Forschungsvorhaben des Registers: § 27 BDSG i. V. m. Art. 9 Abs. 2 lit. j DS-GVO
- Voraussetzungen:
 1. Nachweis über wissenschaftliche oder historische Forschung liegt vor,
 2. Verarbeitung der Daten zu diesen Zwecken ist erforderlich,
 3. die Interessen des Registers an der Verarbeitung überwiegen die Interessen der betroffenen Person an einem Ausschluss der Verarbeitung **erheblich**,
 4. angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person gemäß § 22 Abs. 2 S. 2 BDSG existieren und
 5. Daten wurden anonymisiert oder, falls nicht möglich, pseudonymisiert
- Nachweis von:
 - Methode der Pseudonymisierung sowie dem Nachweis, dass das Ergebnis der Pseudonymisierung einen hinreichenden Schutz vor einer Re-Identifizierung bietet
 - Zwecke können nicht mit anonymisierten Daten erreicht werden
 - Interessen des Verantwortlichen an der Durchführung des Forschungsvorhabens überwiegt Interessen der Patientin oder des Patienten erheblich
 - Überwiegende schutzwürdige Interessen des Betroffenen stehen Verarbeitung nicht entgegen
 - Berechtigtes Interesse der Allgemeinheit an der Durchführung des Forschungsvorhabens überwiegt das Geheimhaltungsinteresse der Patientin oder des Patienten erheblich
 - Dokumentation von Empfänger, die Art der zu übermittelnden Daten, die betroffenen Patienten und das Forschungsvorhaben sind zu dokumentieren
 - Datenschutz-Folgenabschätzung, welche ergibt, dass für betroffene Personen/Patienten kein hohes Risiko existiert

Da Krankenhäuser Daten nur bei Erfüllung der für eine Übermittlung erforderlichen Anforderungen an ein Register weitergeben dürfen, müssen Krankenhäuser diese Erfüllung vorab prüfen. Ein Register sollte sich hier vorbereiten und Unterlagen wie die Datenschutz-Folgenabschätzung und Konzepte wie beispielsweise Datenschutz- und IT-Sicherheitskonzept für den Nachweis der Erfüllung bereithalten.

8.4 Beispielhafte Skizzierung, wie ein Register den Anforderungen entsprechen kann

Anforderung	Beispielhafte Skizzierung einer Umsetzungsmöglichkeit
Nachweis der Rechtmäßigkeit der Verarbeitung	Darstellung der Erlaubnistatbestände (= Dokumentation der Erlaubnistatbestände im Datenschutzkonzept)
Verarbeitung nach Treu und Glauben	Dokumentation im Datenschutzkonzept <ul style="list-style-type: none"> - Von wem werden die Daten verarbeitet? - Wozu werden die Daten verarbeitet? - Unter welchen Umständen werden Daten verarbeitet? - Wann werden die Daten verarbeitet? - Wo werden die Daten verarbeitet?
Transparenz der Verarbeitung	Entsprechende Informationen nach Artt. 13, 14 DS-GVO wurden unter Beachtung der Vorgaben von Art. 12 DS-GVO bereitgestellt
Nachweis der Zweckbindung	Dokumentation im Datenschutzkonzept, wie eine Zweckänderung verhindert wird
Nachweis der Datenminimierung, zugleich Nachweis der Erforderlichkeit	Nachweis, dass ohne die verarbeiteten Daten die Zwecke nicht erreicht werden können
Nachweis der Richtigkeit der Daten	Entsprechende Vertragsgestaltung mit dem die Daten liefernden Krankenhaus
Nachweis der Speicherbegrenzung	Festlegung im Löschkonzept ⁵⁰ , wann und wie gelöscht wird; falls Anonymisierung als Löschmethode angegeben wird, muss dargestellt werden, wie gewährleistet wird, dass niemand eine Re-Identifikation durchführen kann
Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“ („Privacy by Design/Default“)	Darstellung, wie bei der Konzeption und im Betrieb der bestmögliche Datenschutz gewährleistet wird
Umsetzung der Vorgaben von Art. 32 DS-GVO	Datenschutz- und IT-Sicherheitskonzept ⁵¹

⁵⁰ Praxishilfe zur Umsetzung z. B.

- Leitfaden für die Erstellung von Löschkonzepten im Gesundheitswesen. [Online, zitiert am 2021-10-06]: verfügbar unter <https://gesundheitsdatenschutz.org/html/loeschkonzept.php>

⁵¹ Praxishilfen bei der Umsetzung z. B.

- Leitfaden zur Erstellung eines Datenschutzkonzeptes. [Online, zitiert am 2021-10-06]: verfügbar unter <https://gesundheitsdatenschutz.org/html/datenschutzkonzept.php>
- Leitfaden zur Erstellung eines IT-Sicherheitskonzeptes. [Online, zitiert am 2021-10-06]: verfügbar unter <https://gesundheitsdatenschutz.org/html/itsicherheitskonzept.php>

Anforderung	Beispielhafte Skizzierung einer Umsetzungsmöglichkeit
Zugleich: Einsatz von technisch organisatorischen Maßnahmen, welche sicherstellen, dass die Verarbeitung gemäß DS-GVO erfolgt	
Datenschutz-Folgenabschätzung	Nutzung von öffentlich verfügbaren Tools ⁵²
Nachweis des öffentlichen Interesses	Darstellung, wie Ergebnisse der Arbeit des Registers, insbesondere <ul style="list-style-type: none"> - Die Versorgung von Patienten verbesserten (Z. B. höhere Lebensqualität oder spürbare Erhöhung der Überlebenszeit) - Verbesserung des Kosten-Nutzen-Verhältnisses, d. h. <ul style="list-style-type: none"> o Bei weniger Geld aus der GKV mindestens gleich gute Versorgung o Spürbar bessere Versorgung der Patienten bei gleichem Ressourceneinsatz durch die GKV Für jeden Zweck muss dies separat dargestellt werden, d. h. eine Darstellung im Bereich Qualitätssicherung begründet kein öffentliches Interesse für die Forschung und umgekehrt.
Verarbeitung erfolgt im Bereich der öffentlichen Gesundheit“	Darstellung der Arbeit des medizinischen Registers und Zuordnung zu der Definition in Verordnung (EU) 1338/2008
Überprüfbarkeit, wer wann welche Daten eingegeben, verändert oder entfernt hat	Protokollierungskonzept ⁵³
Sensibilisierung der an Verarbeitungsvorgängen Beteiligten	Regelmäßige (z. B. jährliche) Schulungen der Personen mit Verpflichtung auf das Datengeheimnis
Benennung einer oder eines Datenschutzbeauftragten	Benennung einer entsprechend qualifizierten Person
Beschränkung des Zugangs zu den personenbezogenen Daten innerhalb der	Berechtigungskonzept

⁵² Z. B.

- Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO, Stand 17. September 2019. [Online, zitiert am 2021-10-06]: verfügbar unter <https://gesundheitsdatenschutz.org/html/dsfa.php>
- CNIL: Privacy Impact Assessment (PIA):. [Online, zitiert am 2021-10-06]: verfügbar unter <https://www.cnil.fr/en/privacy-impact-assessment-pia>

⁵³ Praxishilfe zur Umsetzung z. B.

- Praxishilfe zur Protokollierung und zur Erstellung von Protokollierungskonzepten im Gesundheitswesen. [Online, zitiert am 2021-10-06]: verfügbar unter <https://gesundheitsdatenschutz.org/html/protokollierungskonzept.php>

Anforderung	Beispielhafte Skizzierung einer Umsetzungsmöglichkeit
verantwortlichen Stelle und von Auftragsverarbeitern	
Anonymisierung nicht möglich	Darstellung, warum aus medizinischen Gründen die Zwecke mit anonymisierten Daten nicht erreicht werden können, z. B. weil Follow-Up-Daten zugeordnet werden müssen
Pseudonymisierung personenbezogener Daten	Pseudonymisierungskonzept, in welchem auch dargestellt wird, warum eine Re-Identifizierung für das Register nicht möglich ist, z. B. durch <ul style="list-style-type: none"> - Angabe der Werte von k, l und t von k-Anonymität, l-Diversität und t-Closeness - Krankenhäuser auditierende Personen sind keine Beschäftigten des Registers und vertraglich wird vereinbart, dass auditierende Personen nur einen Abschlussbericht abgeben, jedoch nie patientenidentifizierende Details an das Register weitergeben
Verschlüsselung personenbezogener Daten	Beispielsweise durch Darstellung <ul style="list-style-type: none"> - Transportverschlüsselung bei Übermittlung der Daten - Verschlüsselung der Datenbank im Datenschutz- und/oder IT-Sicherheitskonzept
Einrichtung eines Verfahrens zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen	Regelmäßige - ggf. externe - Auditierung
Sicherstellung der Fähigkeit, Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste	Datenschutz- und IT-Sicherheitskonzept
Berufsrechtliche und strafrechtliche Vorgaben zur Wahrung des Berufsgeheimnisses werden eingehalten	Darstellung, dass durch die Unmöglichkeit der namentlichen Identifizierung von Patienten keine Offenbarung i. S. v. Straf- oder Berufsrecht vorliegt
<ul style="list-style-type: none"> - Überwiegende schutzwürdige Interessen des Betroffenen stehen Verarbeitung nicht entgegen - Berechtigte Interesse der Allgemeinheit überwiegt das Geheimhaltungsinteresse der Patientin oder des Patienten erheblich 	<ul style="list-style-type: none"> - Interessensabwägung unter Nutzung der Vorteile, welche das Register der Allgemeinheit oder sogar der jeweiligen betroffenen Person selbst bringt, wie sie beim Nachweis des öffentlichen Interesses dargestellt wurde - Zeigen, dass diese Vorteile für alle Menschen bzw. alle von der entsprechenden Erkrankung betroffenen Personen die Nachteile für die jeweilige einzelne Person überwiegen, bei gleichzeitiger Darstellung, wie gering das Risiko für die Rechte und Freiheiten der betroffenen Person ist
Empfänger ist Arzt/Ärztin oder eine ärztlich geleitete Stelle	Einsetzen einer entsprechenden Person

Anforderung	Beispielhafte Skizzierung einer Umsetzungsmöglichkeit
	Hinweis: Dies muss nicht zwingend in der Geschäftsführung oder hauptberuflich erfolgen, jedoch muss diese Person die medizinischen Vorgaben/Inhalte unabhängig festlegen und deren Einhaltung auch prüfen können
Aussagekräftige Dokumentation des Empfängers, über die Art der zu übermittelnden Daten und der betroffenen Patienten	Protokollierung, Nachweis durch Protokollierungskonzept
Empfänger muss Fachpersonal i. S. v. Art. 9 Abs. 3 DS-GVO sein und entsprechender Geheimhaltungspflicht unterliegen	Register sind eigenständige Verantwortliche, daher sind die Vorgaben aus § 203 StGB auf diese vom Krankenhaus aus nicht übertragbar Mit einem hauptberuflichen ärztlichen Geschäftsführer könnte man argumentieren, dass Qualitätssicherung (§ 5 i.V.m. Präambel MBO-Ä) und Forschung (§ 15 MBO-Ä) ärztliche Aufgaben sind und somit § 9 Abs. 1 MBO-Ä (bzw. die entsprechende landesrechtliche Berufsordnung) anzuwenden ist. Dann wäre mit § 9 Abs. 3 MBO-Ä auch die Geheimhaltungspflicht für alle Beschäftigten (nach Verpflichtung) gegeben
Verarbeitung erfolgt ausschließlich in der EU/EWR	- Darstellung, wo die Verarbeitung erfolgt

9 Was Krankenhäuser prüfen sollten

Hinweis: Träger medizinische Register sind häufig juristische Personen wie beispielsweise eine GmbH. In diesen Fällen gelten – neben dem Europarecht – eigentlich nur die datenschutzrechtlichen Vorgaben des Bundes für das jeweilige Register. Damit Krankenhäuser aber Patientendaten an ein Register übermitteln dürfen, müssen diese Register auch die Vorgaben der jeweiligen für das Krankenhaus geltenden Vorgaben zur Übermittlung von Patientendaten erfüllen; Krankenhäuser sollten sich die Einhaltung auch vertraglich bestätigen lassen.

9.1 Anforderungen, die ein Krankenhaus vor Datenübermittlung an ein Register zu Zwecken der Qualitätssicherung prüfen sollte

Wie im Vorwort erwähnt gibt es vom G-BA für einige wenige medizinische Leistungen Qualitätssicherungsmaßnahmen, jedoch sind die Länder nicht daran gebunden. Gemäß § 6 Abs. 1a S. 2 KHG kann die Geltung der Qualitätsindikatoren des G-NA durch Landesrecht ganz oder teilweise ausgeschlossen oder eingeschränkt werden. Weiterhin können durch Landesrecht weitere Qualitätsanforderungen zum Gegenstand der Krankenhausplanung gemacht werden. Die Qualitätssicherung für Krankenhäuser wird also weitestgehend durch Landesrecht bestimmt.

In den meisten Landeskrankenhausgesetzen sind dementsprechend Voraussetzungen angegeben, wann Daten zu Zwecken der Qualitätssicherung genutzt werden dürfen. In diesen Fällen können die Daten auch ohne Einwilligung zu **Zwecken der Qualitätssicherung des Krankenhauses** genutzt werden. Wenn ein Register beispielsweise einen Benchmarking-Bericht herausgibt, anhand dessen ein Krankenhaus feststellen kann, wo es im bundesweiten Vergleich bei der Behandlung dem Standard entspricht und wo ggf. noch Optimierungspotenzial besteht, so dient die Qualitätssicherung des Registers auch den Zwecken des Krankenhauses.

Entsprechende Regelungen, welche eine Erlaubnis zur Nutzung von Patientendaten **zur Qualitätssicherung in der stationären Versorgung** vorsehen, finden sich in folgenden Landesgesetzen:

- Baden-Württemberg: § 45 Abs. 3 Ziff. 1 LKHG BW
- Berlin: § 24 Abs. 4 Ziff. 4 LKG BE
- Brandenburg: § 29 Ziff. 2 BbgKHEG
- Bremen: § 38 Abs. 1 Ziff. 5 BremKrhG
- Hamburg: § 10 Abs. 1 Ziff. 7 HmbKHG
- Hessen: § 12 Abs. 2 Ziff. 7 HKHG 2011 i. m. § 20 Abs. 1 Ziff. 3 HDSIG
- Mecklenburg-Vorpommern: § 34 Abs. 1 Ziff. 2 LKHG M-V
- Nordrhein-Westfalen: § 11 Abs. 2 GDSG NW
- Rheinland-Pfalz: § 36 Abs. 2 Ziff. 2 LKG RP
- Saarland: § 13 Abs. 4 Ziff. 10 SKHG
- Sachsen: § 33 Abs. 3 Ziff. 4 SächsKHG
- Sachsen-Anhalt: § 16 Abs. 3 Ziff. 6 KHG LSA
- Schleswig-Holstein: § 36 Abs. 1 Ziff. 10 LKHG SH
- Thüringen: § 27 Abs. 6 Ziff. 4 ThürKHG

Zu beachten ist hierbei, dass die Anforderungen grundsätzlich bei der Verarbeitung von Patientendaten zur Qualitätssicherung erfüllt werden müssen, i. d. R. selbst dann, wenn eine Einwilligung der betreffenden Patienten vorliegen sollte.

Demgemäß muss ein Krankenhaus als Verantwortlicher vor einer Übermittlung an ein Register prüfen, ob die entsprechenden Voraussetzungen zur Übermittlung beim empfangenden Register erfüllt sind. Dies beinhaltet insbesondere das Vorliegen von:

- Positives Votum des Datenschutzbeauftragten liegt vor
(DE)
- Datenschutzkonzept, IT-Sicherheitskonzept, Pseudonymisierungskonzept, Löschkonzept des Registers liegt vor und wurde durch das Krankenhaus als ausreichend beurteilt
(DE)
- Datenschutz-Folgenabschätzung des Registers wurde durch das Krankenhaus als ausreichend beurteilt und enthält keine Risiken, die Patienten nicht zumutbar sind
(DE)
- Verarbeitung erfolgt ausschließlich in der EU/EWR, idealerweise in Deutschland
(DE)
- Nachweis, dass die Daten für Qualitätssicherung erforderlich sind, liegt vor
(DE)
- Überwiegende schutzwürdige Interessen des Betroffenen stehen Verarbeitung nicht entgegen
(BW, BE, BB, SL, SH, HE, RP)
- Berechtigte Interesse der Allgemeinheit an der Durchführung überwiegt das Geheimhaltungsinteresse der Patientin oder des Patienten erheblich
(NI, SN)
- Empfänger ist Arzt oder eine ärztlich geleitete Stelle
(BW, BE, BB, HE, SL, ST)
- Daten wurden ausreichend pseudonymisiert, wenn eine Anonymisierung nicht möglich ist
(HB, HE, MV, NW, RP, SL, ST, SH)
- Empfänger, die Art der zu übermittelnden Daten und die betroffenen Patienten sind zu dokumentieren
(DE, aber ausdrücklich auch MV, SI)
- Datenschutzbeauftragte ist einzuschalten
(DE)
- Empfänger muss Fachpersonal i.S.v. Art. 9 Abs. 3 DS-GVO sein und dieses der Geheimhaltungspflicht unterliegen
(ST)
- Berufsrechtliche und strafrechtliche Vorgaben zur Wahrung des Berufsgeheimnisses sind einzuhalten
(DE, aber ausdrücklich auch NI)

Hinweis: Deutschlandweit geltende Vorgaben (DE) für Krankenhäuser als Verantwortliche in obiger Darstellung ergeben sich i. d. R. direkt aus der DS-GVO.

9.2 Anforderungen, die ein Krankenhaus vor Datenübermittlung an ein Register zu Forschungszwecken prüfen sollte

Die meisten Landeskrankenhausesetze enthalten Forschungsprivilegien, d. h. Patientendaten können auch ohne Einwilligung von Patienten genutzt werden. Dies betrifft jedoch regelhaft entweder Forschungsvorhaben des Krankenhauses oder sogar nur Forschungsvorhaben der behandelnden Ärzte, sodass selbst Ärzte des Krankenhauses, die nicht an der Behandlung beteiligt waren, einer Einwilligung der betreffenden Patienten bedürfen.

Entsprechende Regelungen finden sich in folgenden Landesgesetzen:

- Baden-Württemberg: § 46 Abs. 2a LKHG BW
- Bayern: Art. 27 Abs. 4 BayKrG
- Berlin: § 25 LKG BE
- Brandenburg: § 31 BbgKHEG i. V. m. § 25 BbgDSG)

- Bremen: § 39 BremKrhG
- Hamburg: § 12 HmbKHG
- Hessen: § 12 Abs. 3 HKHG 2011 i. V. m. § 24 HDSIG
- Mecklenburg-Vorpommern: § 37 LKHG M-V
- Nordrhein-Westfalen: § 6 GDSG NW
- Rheinland-Pfalz: § 37 LKG RP
- Saarland: § 14 SKHG
- Sachsen: § 34 SächsKHG
- Schleswig-Holstein: § 38 LKHG SH
- Thüringen: § 27a ThürKHG

Diese Regelungen können Vorgaben enthalten, welche grundsätzlich bei der Verarbeitung von Patientendaten zu Forschungszwecken eingehalten werden müssen. In diesen Fällen sind diese Vorgaben selbst dann einzuhalten, wenn eine Einwilligung der betreffenden Patienten vorliegen sollte.

Zehn Landeskrankenhausgesetze enthalten Regelungen, nach denen Patientendaten unter bestimmten Bedingungen anonymisiert oder – wenn eine Anonymisierung nicht möglich ist – pseudonymisiert an Dritte, d. h. an Stellen außerhalb des Krankenhauses übermittelt werden dürfen. Hierzu gehören:

- Berlin: § 25 Abs. 3 LKG BE
(Hinweis: § 25 Abs. 3 LKG BE enthält eine Erlaubnisnorm zur Übermittlung von pseudonymisierten Patientendaten an Forschungsregister)
- Brandenburg: § 31 BbgKHEG
- Bremen: § 39 Abs. 2 BremKrhG
- Hamburg: § 12 Abs. 3 S. 4 HmbKHG
- Mecklenburg-Vorpommern: § 37 Abs. 2 LKHG M-V
- Nordrhein-Westfalen: § 6 Abs. 2 GDSG NW
- Rheinland-Pfalz: § 37 Abs. 3 LKG RP
- Saarland: § 14 Abs. 2 SKHG
(Hinweis: § 14 Abs. 3 SKHG enthält eine Erlaubnisnorm zur Übermittlung von Patientendaten an Krankheitsregister, Krankenhausaufsichts- und Datenschutzbehörde zustimmen)
- Sachsen: § 34 Abs. 3 KHG LSA
- Thüringen: § 27a Abs. 2, 3 ThürKHG

Ein Krankenhaus sollte vor einer Übermittlung von Patientendaten an ein Register prüfen, ob die für eine Übermittlung ggf. geltenden Voraussetzungen beim empfangenden Register erfüllt sind. Dies beinhaltet insbesondere:

- Positives Votum des Datenschutzbeauftragten liegt vor (DE)
- Datenschutzkonzept, IT-Sicherheitskonzept, Pseudonymisierungskonzept, Löschkonzept des Registers liegt vor und wurde durch das Krankenhaus als ausreichend beurteilt (DE)
- Datenschutz-Folgenabschätzung des Registers wurde durch das Krankenhaus als ausreichend beurteilt und enthält keine Risiken, die Patienten nicht zumutbar sind (DE)
- Verarbeitung erfolgt ausschließlich in der EU/EWR, idealerweise in Deutschland (DE)
- Erforderlichkeitsnachweis der Daten für Forschungsvorhaben liegt vor (DE)

- Daten dürfen ausschließlich für genanntes Forschungsprojekt verwenden
(NI, NW, RP, SL, SN)
- Vorliegen einer Einwilligung zur Übermittlung an ein Register
(zwingend erforderlich für SH)
- Wenn keine Einwilligung vorliegt, fordern einige Bundesländer Nachweis des Vorliegens der Nicht-Zumutbarkeit der Einholung einer Einwilligung
(BE, HB, NW, RP, SL, SN, ST)
- Nachweis
 - Zwecke des Registers können nicht mit anonymisierten Daten erreicht werden
(BW, HE, RP)
 - Methode und Ergebnis der Pseudonymisierung entspricht Vorgaben der DS-GVO
 - Interessensabwägung positiv bzgl. Übermittlung an Register
(NI, Bund)
 - Berechtigte Interesse der Allgemeinheit an der Durchführung des Forschungsvorhabens überwiegt das Geheimhaltungsinteresse der Patientin oder des Patienten erheblich
(BE, BB, HB, HH, NI, NW, RP, SL, SN, ST)
 - Schutzwürdige Interessen des Betroffenen stehen Verarbeitung nicht entgegen
(BE, MV, SN; BW, BB, HW verlangen überwiegende schutzwürdige Interessen)
- Vorherige Zustimmung Rechtsaufsicht, zuständige Behörde, usw. eingeholt
(BB, HB, MV, NI, ST)
- Empfänger, die Art der zu übermittelnden Daten, die betroffenen Patienten, die betroffenen Patienten und das Forschungsvorhaben sind zu dokumentieren

Hinweis: Deutschlandweit geltende Vorgaben (DE) ergeben sich i. d. R. direkt aus der DS-GVO.

10 Sonderfall

10.1 Datenschutz bei Verstorbenen

Datenschutzrechtliche Bestimmungen sind eine Ausprägung der informationellen Selbstbestimmung, jedoch existiert bei verstorbenen Menschen keine Möglichkeit zur Selbstbestimmung. Daher enden aufgrund der fehlenden Verfügungsgewalt datenschutzrechtliche Regelungen regelhaft mit dem Tod der betroffenen Personen.

Dabei sind aber zwei Besonderheiten zu beachten:

- 1) In ErwGr. 27 DS-GVO heißt es: „Diese Verordnung gilt nicht für die personenbezogenen Daten Verstorbener. Die Mitgliedstaaten können Vorschriften für die Verarbeitung der personenbezogenen Daten Verstorbener vorsehen.“ Dieser Möglichkeit, eine Regelung über den Tod hinaus zu treffen, nutzte Hamburg. § 7 Abs. 1 S. 3 HmbKHG lautet: „Der Datenschutz endet nicht mit dem Tode der Patientin oder des Patienten“. D. h. in Hamburg gilt – als einzigem Bundesland in Deutschland – der Datenschutz über den Tod hinaus. In Bremen umfasst die Definition von Patientendaten auch die Daten verstorbener Personen. § 37 Abs. 1 S. 1,2 BremKrhG lautet: „Patientendaten sind alle personenbezogenen Daten der Patientinnen und Patienten des Krankenhauses. Als Patientendaten gelten auch personenbezogene Daten von verstorbenen Patientinnen und Patienten, [...]“. Hierbei handelt es sich um eine Klarstellung in der Form, dass auch die Daten verstorbener Patienten rechtlich als Patientendaten gelten. Dies gilt analog zu den Daten verstorbener Personen, bei denen es sich immer noch um personenbezogene Daten handelt, speziell eben nur um die Daten des Betroffenenkreises verstorbener Personen. Im Gegensatz zu Hamburg existiert jedoch keine Regelung, dass der Datenschutz über den Tod hinaus gilt. Nach § 36 Abs. 1 BremKrhG ist vorrangig die DS-GVO anzuwenden, wonach der Datenschutz eben nicht für verstorbene Personen gilt. Daher muss aufgrund der fehlenden ausdrücklichen Regelung davon ausgegangen werden, dass Bremen im Gegensatz zu Hamburg keine Erweiterung des datenschutzrechtlichen Schutzes über den Tod hinaus beinhaltet.
- 2) Medizinische Daten, die noch lebende Personen betreffen, unterliegen weiterhin datenschutzrechtlichen Bestimmungen, denn lebende Personen sind geschützt. Dies betrifft z. B. genetische Daten, welche regelhaft Informationen über Verwandte wie Eltern, Geschwister usw. enthalten. Aber auch familiäre Erkrankungen unterliegen i. d. R. weiterhin datenschutzrechtlichen Bestimmungen. Kurz: Immer, wenn die Daten neben Informationen zur verstorbenen Person auch Informationen über noch lebende Personen beinhalten, müssen ggf. weiterhin datenschutzrechtliche Bestimmungen beachtet werden.

Zu beachten ist jedoch, dass sowohl die berufrechtliche Schweigepflicht (siehe hierzu auch Abschnitt 3.3) als auch das strafrechtliche Offenbarungsverbot (siehe hierzu auch Abschnitt 3.2) über den Tod der Patientin bzw. des Patienten hinaus gelten.

11 Checkliste

11.1 Grundlegende Punkte, die von Krankenhaus und Register geprüft werden sollten

Anforderung	Qualitätssicherung	Forschung
Nachweis Erfüllung Vorgaben EuGH sowie EGMR durch das Register vorhanden		X
Rechtsgrundlage für die Verarbeitung durch Register gegeben	X	X
Rechtsgrundlage für die Übermittlung Krankenhaus an Register gegeben ⁵⁴	X	X
Nachweis Erforderlichkeit Daten erbringen	X	
Interessen des Verantwortlichen an der Durchführung des Forschungsvorhabens überwiegt Interessen der Patientin oder des Patienten erheblich		X
Nachweis, dass überwiegende schutzwürdige Interessen des Betroffenen der Verarbeitung nicht entgegenstehen	X	X
Nachweis, dass das berechnete Interesse der Allgemeinheit an der Durchführung das Geheimhaltungsinteresse der Patientin oder des Patienten erheblich überwiegt	X	X
Empfänger ist Arzt oder eine ärztlich geleitete Stelle	X	
Nachweis einer ausreichenden Pseudonymisierung (beinhaltet Nachweis, dass Anonymisierung nicht möglich ist)	X	X
Nachweis, dass Empfänger, die Art der zu übermittelnden Daten und die betroffenen Patienten dokumentiert werden (Bei Forschung auch das Forschungsvorhaben)	X	X
Datenschutzbeauftragte (sowohl Krankenhaus wie auch Register) wurde in Prozess integriert	X	
Empfänger muss Geheimhaltungspflicht unterliegen	X	
Berufsrechtliche und strafrechtliche Vorgaben zur Wahrung des Berufsgeheimnisses sind einzuhalten	X	

Ergänzend muss seitens des Krankenhauses in einigen Bundesländern ggf. zuvor die vorherige Zustimmung der Rechtsaufsicht, der zuständige Behörde, usw. eingeholt werden (BB, HB, MV, NI, ST).

⁵⁴ Unrechtmäßig erlangte Daten können prinzipiell nicht rechtskonform verarbeitet werden

11.2 Anforderungen an Krankenhäuser für die Übermittlung von Patientendaten zu Zwecken der Qualitätssicherung ohne Einwilligung

Die Anforderungen sind zur Übersicht verkürzt dargestellt, daher müssen die genauen Formulierungen im jeweiligen Landesrecht nachgelesen werden.

Anforderung⁵⁵ ↓	Bundesland →	Baden-Württemberg (§ 45, 46 Abs. 3 Ziff. 1 LKHG BW)	Berlin (§ 24 Abs. 4 Ziff. 4 LKG BE)	Brandenburg (§ 29 Ziff. 2 BbgKHG)	Bremen (§ 38 Abs. 1 Ziff. 5 BremKrhG)	Hessen (§ 12 Abs. 2 Ziff. 7 HKHG 2011 i. V. m. § 20 Abs. 1 Ziff. 3 HDSIG)	Mecklenburg-Vorpommern (§ 34 Abs. 1 Ziff. 2 LKHG M-V)	Nordrhein-Westfalen (§ 11 Abs. 2 GDSG NW)	Rheinland-Pfalz (§ 36 Abs. 2 Ziff. 2 LKG RP)	Saarland (§ 33 Abs. 4 Ziff. 10 SKHG)	Sachsen (§ 16 Abs. 3 Ziff. 6 SächsKHG)	Sachsen-Anhalt (§ 16 Abs. 3 Ziff. 6 KHG LSA)	Schleswig-Holstein (§ 36 Abs. 1 Ziff. 10 LKHG SH)	Thüringen (§ 27 Abs. 6 Ziff. 4 ThürKHG)
Daten und deren Verarbeitung durch Dritte ist erforderlich					X	X	X							
Anonymisierung nicht möglich, daher Pseudonymisierung	X	X	X	X	X	X		X	X	X		X	X	
Pseudonymisierung nicht möglich			X		X				X	X		X	X	
Überwiegende schutzwürdige Interessen des Betroffenen stehen Verarbeitung nicht entgegen	X	X	X			X	X		X	X			X	
Interesse der Allgemeinheit an der Durchführung der beabsichtigten Maßnahme überwiegt die schutzwürdigen Belange des Patienten erheblich											X			X

⁵⁵ In dieser Liste sind nur Anforderungen aus dem jeweiligen Landesrecht dargestellt, um eine Übersicht zu den verschiedenen Regelungen anzubieten. Viele Anforderungen lassen sich auch direkt aus der DS-GVO ableiten (z. B. Nachweis der Erforderlichkeit der Daten ist aus Art. 5 Abs. 1 c DS-GVO ableiten, die Anforderungen bzgl. Pseudonymisierung sind in Art. 32 Abs. 1 lit. a DS-GVO enthalten), sodass entsprechende Anforderungen entsprechend dem vorrangig anzuwendenden europäischen Recht für alle Krankenhäuser in Deutschland gelten.

Anforderung ⁵⁵ ↓	Bundesland →												
	Baden-Württemberg (§ 45, 46 Abs. 3 Ziff. 1 LKHG BW)	Berlin (§ 24 Abs. 4 Ziff. 4 LKG BE)	Brandenburg (§ 29 Ziff. 2 BbgKHEG)	Bremen (§ 38 Abs. 1 Ziff. 5 BremKrhG)	Hessen (§ 12 Abs. 2 Ziff. 7 HKHG 2011 i. V. m. § 20 Abs. 1 Ziff. 3 HDSIG)	Mecklenburg-Vorpommern (§ 34 Abs. 1 Ziff. 2 LKHG M-V)	Nordrhein-Westfalen (§ 11 Abs. 2 GDSG NW)	Rheinland-Pfalz (§ 36 Abs. 2 Ziff. 2 LKG RP)	Saarland (§ 33 Abs. 4 Ziff. 10 SKHG)	Sachsen (§ 16 Abs. 3 Ziff. 6 SächsKHG)	Sachsen-Anhalt (§ 16 Abs. 3 Ziff. 6 KHG LSA)	Schleswig-Holstein (§ 36 Abs. 1 Ziff. 10 LKHG SH)	Thüringen (§ 27 Abs. 6 Ziff. 4 ThürKHG)
Empfänger ist Arzt oder eine ärztlich geleitete Stelle	X	X	X		X				X		X		
Berufsrechtliche und strafrechtliche Vorgaben zur Wahrung des Berufsgeheimnisses sind einzuhalten	X				X								X
Empfänger ist Fachpersonal im Sinne von Art. 9 Abs. 3 DS-GVO oder unterliegt in anderer Weise der Geheimhaltungspflicht gemäß Art. 9 Abs. 3 DS-GVO											X		
Pseudonymisierte Daten sind zu anonymisieren oder zu löschen, sobald der Zweck es zulässt, spätestens jedoch nach Ablauf eines Jahres nach der Zweckänderung.						X							
Empfänger verpflichtet sich zur Einhaltung Landesrecht						X							
Empfänger, die Art der zu übermittelnden Daten und Betroffene sind zu dokumentieren						X							
Datenschutzbeauftragte des Krankenhauses ist einzuschalten						X							

11.3 Anforderungen an Krankenhäuser für die Übermittlung von Patientendaten zu Zwecken der Forschung ohne Einwilligung

Die Anforderungen sind zur Übersicht verkürzt dargestellt, daher müssen die genauen Formulierungen im jeweiligen Landesrecht nachgelesen werden.

Bundesland →	Baden-Württemberg (§ 46 Abs. 2a LKHG BW)	Berlin (§ 25 Abs. 3 LKG BE)	Brandenburg (§ 31 BbgKHEG i. V. m. § 25 BbgDSG)	Bremen (§ 39 BremKrhG)	Hamburg ⁵⁷ (§ 12 HmbKHG)	Hessen (§ 12 Abs. 3 HKHG 2011 i. V. m. § 24 HDSIG)	Mecklenburg-Vorpommern (§ 37 LKHG M-V)	Nordrhein-Westfalen (§ 6 GDSG NW)	Rheinland-Pfalz (§ 37 LKG RP)	Saarland (§ 14 SKHG)	Sachsen (§ 34 SächsKHG)	Sachsen-Anhalt (§ 16 Abs. 3 Ziff. 6 KHG LSA)	Thüringen (§ 27a ThürKHG)
Anforderung ⁵⁶ ↓													
Forschungsvorhaben des Krankenhauses	X												
Daten und deren Verarbeitung durch Dritte ist erforderlich					X	X							
Anonymisierung nicht möglich, dann Pseudonymisierung	X	X	X		X		X		X			X	
Pseudonymisierung nicht möglich												X	
Einholung Einwilligung nicht zumutbar und Forschungszweck anders nicht erreichbar		X		X			X	X	X	X	X		X
Schutzwürdige Belange des Patienten werden nicht beeinträchtigt										X	X		X

⁵⁶ In dieser Liste sind nur Anforderungen aus dem jeweiligen Landesrecht dargestellt, um eine Übersicht zu den verschiedenen Regelungen anzubieten. Viele Anforderungen lassen sich auch direkt aus der DS-GVO ableiten (z. B. Nachweis der Erforderlichkeit der Daten ist aus Art. 5 Abs. 1 c DS-GVO ableiten, die Anforderungen bzgl. Pseudonymisierung sind in Art. 32 Abs. 1 lit. a DS-GVO enthalten), sodass entsprechende Anforderungen entsprechend dem vorrangig anzuwendenden europäischen Recht für alle Krankenhäuser in Deutschland gelten.

⁵⁷ § 12 Abs. 1 HmbKHG enthält die Regelung, dass ein Krankenhaus Patientendaten, welche es für wissenschaftliche Forschungszwecke an Dritte weitergegeben hat, bei Dritten erneut erheben und verarbeiten darf. § 12 Abs. 3 S. 5 HmbKHG enthält Anforderungen bzgl. Anonymisierung/Pseudonymisierung vor einer Weitergabe von Daten für wissenschaftliche Forschung. Aufgrund der Tatsache, dass § 11 Abs. 1 HmbKHG eine abschließende Aufzählung, welche Verarbeitungen auf Grundlage einer Einwilligung möglich sind, enthält, Forschung selbst jedoch hier nicht enthalten ist, muss § 12 HmbKHG implizit einen Erlaubnistatbestand zur Weitergabe von Patientendaten zur wissenschaftlichen Forschung darstellen, wenn die Anforderungen erfüllt sind.

Bundesland →	Baden-Württemberg (§ 46 Abs. 2a LKHG BW)	Berlin (§ 25 Abs. 3 LKG BE)	Brandenburg (§ 31 BbgKHEG i. V. m. § 25 BbgDSG)	Bremen (§ 39 BremKrhG)	Hamburg ⁵⁷ (§ 12 HmbKHG)	Hessen (§ 12 Abs. 3 HKHG 2011 i. V. m. § 24 HDSIG)	Mecklenburg-Vorpommern (§ 37 LKHG M-V)	Nordrhein-Westfalen (§ 6 GDSG NW)	Rheinland-Pfalz (§ 37 LKG RP)	Saarland (§ 14 SKHG)	Sachsen (§ 34 SächsKHG)	Sachsen-Anhalt (§ 16 Abs. 3 Ziff. 6 KHG LSA)	Thüringen (§ 27a ThürKHG)
Anforderung ⁵⁶ ↓													
Überwiegende schutzwürdige Interessen des Betroffenen stehen Verarbeitung nicht entgegen	X											X	
Schutzwürdige Interessen des Betroffenen stehen Verarbeitung nicht entgegen			X										
Interessen des Verantwortlichen an der Verarbeitung überwiegen die Interessen der betroffenen Person an einem Ausschluss der Verarbeitung						X							
Berechtigte Interesse der Allgemeinheit an der Durchführung der beabsichtigten Maßnahme überwiegt die schutzwürdigen Belange des Patienten erheblich		X	X	X				X	X	X	X		
Öffentliche Interesse an der Durchführung des Forschungsvorhabens überwiegt die schutzwürdigen Belange der Patientinnen und Patienten erheblich					X		X						X
Berufsrechtliche und strafrechtliche Vorgaben zur Wahrung des Berufsgeheimnisses sind einzuhalten	X												
Empfänger, die Art der zu übermittelnden Daten und Betroffene sind zu dokumentieren								X		X	X		
Daten dürfen nur für angegebenes Forschungsvorhaben genutzt werden								X		X	X		

Anforderung⁵⁶ ↓	Bundesland →	Baden-Württemberg (§ 46 Abs. 2a LKHG BW)	Berlin (§ 25 Abs. 3 LKG BE)	Brandenburg (§ 31 BbgKHEG i. V. m. § 25 BbgDSG)	Bremen (§ 39 BremKrhG)	Hamburg⁵⁷ (§ 12 HmbKHG)	Hessen (§ 12 Abs. 3 HKHG 2011 i. V. m. § 24 HDSIG)	Mecklenburg-Vorpommern (§ 37 LKHG M-V)	Nordrhein-Westfalen (§ 6 GDSG NW)	Rheinland-Pfalz (§ 37 LKG RP)	Saarland (§ 14 SKHG)	Sachsen (§ 34 SächsKHG)	Sachsen-Anhalt (§ 16 Abs. 3 Ziff. 6 KHG LSA)	Thüringen (§ 27a ThürKHG)
Anzeige bzw. Bestätigung der zuständigen Behörde				X	X			X						X
Empfänger ist Fachpersonal im Sinne von Art. 9 Abs. 3 DS-GVO oder unterliegt in anderer Weise der Geheimhaltungspflicht gemäß Art. 9 Abs. 3 DS-GVO													X	
Empfänger verpflichtet sich zur Einhaltung Landesrecht				X										
Angemessene technische und organisatorische Maßnahmen							X		X	X		X		
Empfangende Stelle muss Datenschutzaufsicht der übermittelnden Stelle auf Verlangen Einsicht gewähren									X	X		X		

12 Abkürzungen

12.1 Bundesländer

BW	=	Baden-Württemberg
BY	=	Bayern
BE	=	Berlin
BB	=	Brandenburg
DE	=	Deutschland
HB	=	Bremen
HH	=	Hamburg
HE	=	Hessen
MV	=	Mecklenburg-Vorpommern
NI	=	Niedersachsen
NW	=	Nordrhein-Westfalen
RP	=	Rheinland-Pfalz
SL	=	Saarland
SN	=	Sachsen
ST	=	Sachsen-Anhalt
SH	=	Schleswig-Holstein
TH	=	Thüringen

12.2 Landesgesetze

BayKrG	Bayerisches Krankenhausgesetz
BbgKHEG	Gesetz zur Entwicklung der Krankenhäuser im Land Brandenburg (Brandenburgisches Krankenhausentwicklungsgesetz)
BlnHKG	Berliner Heilberufekammergesetz
BremKrhG	Bremisches Krankenhausgesetz
GDSG NW	Gesetz zum Schutz personenbezogener Daten im Gesundheitswesen (Gesundheitsdatenschutzgesetz)
HDSIG	Hessisches Datenschutz- und Informationsfreiheitsgesetz
HeilBerGerG HA	Gesetz über die Berufsgerichtsbarkeit der Heilberufe
HKHG 2011	Zweites Gesetz zur Weiterentwicklung des Krankenhauswesens in Hessen (Hessisches Krankenhausgesetz 2011)
HmbKHG	Hamburgisches Krankenhausgesetz
KGHB-LSA	Gesetz über die Kammern für Heilberufe Sachsen-Anhalt
KHG LSA	Krankenhausgesetz Sachsen-Anhalt
KHG SL	Saarländisches Krankenhausgesetz
LKG BE	Landeskrankenhausgesetz Berlin
LKG RP	Landeskrankenhausgesetz Rheinland-Pfalz
LKHG BW	Landeskrankenhausgesetz (LKHG) Baden-Württemberg
LKHG M-V	Krankenhausgesetz für das Land Mecklenburg-Vorpommern (Landeskrankenhausgesetz)
LKHG SH	Krankenhausgesetz für das Land Schleswig-Holstein-Landeskrankenhausgesetz
NDSG	Niedersächsisches Datenschutzgesetz
NKHG	Niedersächsisches Krankenhausgesetz
SächsHKaG	Sächsisches Heilberufekammergesetz
SächsKHG	Gesetz zur Neuordnung des Krankenhauswesens (Sächsisches Krankenhausgesetz)
SHKG	Saarländisches Heilberufekammergesetz
ThürHeilBG	Thüringer Heilberufegesetz
ThürKHG	Thüringer Krankenhausgesetz

12.3 Im Text verwendete Abkürzungen

Abs.	Absatz
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
Art.	Artikel
Artt.	Artikel (Mehrzahl)
BDSG	Bundesdatenschutzgesetz
DSFA	Datenschutz-Folgenabschätzung
DS-GVO	Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)
EGMR	Europäischer Gerichtshof für Menschenrechte
ErwGr.	Erwägungsgrund
EU	Europäische Union
EuGH	Europäische Gerichtshof
EWR	Europäischer Wirtschaftsraum
G-BA	Gemeinsame Bundesausschuss
GG	Grundgesetz
HBKG	Heilberufe-Kammergesetz
HeilBerG	Heilberufsgesetz
HeilBG	Heilberufsgesetz
HKaG	Heilberufe-Kammergesetz
HKG	Kammergesetz für die Heilberufe
Kap.	Kapitel
KHG	Gesetz zur wirtschaftlichen Sicherung der Krankenhäuser und zur Regelung der Krankenhauspflegesätze (Krankenhausfinanzierungsgesetz)
Lit.	littera (lat. „Buchstabe“)
MBO-Ä	(Muster-)Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte
Rn.	Randnummer
SGB	Sozialgesetzbuch
StGB	Strafgesetzbuch
TOM	Technisch-organisatorische Maßnahme(n)
WP	Working Paper
Ziff.	Ziffer

Anhang 1: Ausgewählte Beispiele für die Heterogenität von Landesgesetzen bzgl. Datenschutz im Krankenhaus

Die Heterogenität der landesgesetzlichen Ausgestaltung der für ein Krankenhaus geltenden Regelungen wurden für die Forschung ausführlich dargestellt. Nachfolgend werden in aller Kürze noch einige wenige für die Forschung relevante Beispiele aufgeführt, die zeigen, wie uneinheitlich und unübersichtlich die landesspezifischen Regelungen für den Datenschutz in Krankenhäusern aussehen. Die im Folgenden dargestellten Beispiele sind:

1) Der Geltungsbereich der jeweiligen Gesetze

Nicht in jedem Bundesland gelten die Regelungen der jeweiligen Landesgesetze auch für alle an der Versorgung beteiligten Krankenhäuser. Ob die jeweiligen Regelungen überhaupt anwendbar sind, wird nur durch eine Prüfung, ob das eigene Krankenhaus vom Geltungsbereich der im Bundesland geltenden Landesrechts umfasst wird, erkennbar.

2) Patientendaten

Häufig wird in datenschutzrechtlichen Regelungen der Landesgesetze für Krankenhäuser auf den Begriff „Patientendaten“ Bezug genommen. Die von diesem Begriff adressierte Bedeutung ist daher wesentlich für die Frage, welche Regelungen auf welche Daten angewendet werden müssen.

3) Auftragsverarbeitung

Auch in der Forschung ist oftmals eine Verarbeitung im Auftrag erforderlich; sei es die Datenbank, die gewartet und gepflegt werden muss, oder die Unterstützung durch Experten bei der statistischen Auswertung. Daher können die in den jeweiligen Landesgesetzen enthaltenen Vorgaben, die bei einer Auftragsverarbeitung zu beachten sind, auch für Forschungsvorhaben relevant sein.

4) Erlaubnistatbestände für die Verarbeitung von Patientendaten durch das jeweilige Krankenhaus

In Landeskrankenhausgesetzen enthaltene Erlaubnistatbestände bestimmen maßgeblich ob und wie Patientendaten für Forschung oder Qualitätssicherung genutzt werden dürfen. Daneben existieren je nach Bundesland mehr oder weniger viele Erlaubnistatbestände wie z. B. die Verwendung von Patientendaten zur Aus-, Fort- und Weiterbildung des im Krankenhaus eingesetzten medizinischen Personals.

Dabei ist die Anzahl der Erlaubnistatbestände von Bundesland zu Bundesland sehr unterschiedlich, z. B. existieren vereinzelt auch Erlaubnistatbestände zur Überprüfung der Tätigkeit der Beschäftigten.

Anhang 1.1: Geltungsbereich der Landeskrankenhausgesetze

In nachfolgender Tabelle erfolgt ist übersichtsartig dargestellt, wie der Geltungsbereich der Landeskrankenhausgesetze im jeweiligen Bundesland definiert wurde:

	§ 107 Abs. 1 SGB V	§ 107 Abs. 2 SGB V	Förderfähig nach KHG	Alle Krankenhäuser
Baden-Württemberg	X	X		
Bayern			X	
Berlin				X
Brandenburg				X
Bremen				X
Hamburg				X
Hessen				X
Mecklenburg-Vorpommern				X
Niedersachsen				X
Nordrhein-Westfalen	X	X		
Rheinland-Pfalz			X	
Saarland				X
Sachsen			X	
Sachsen-Anhalt				
Schleswig-Holstein			X	
Thüringen			X	

Dabei unterscheiden sich die in den Paragraphen enthaltenen Bestimmungen, für welche Krankenhäuser die Regelungen der Landeskrankenhausgesetze gelten:

- § 107 Abs. 1 SGB V:
 - § 107 Abs. 1 SGB V definiert, was im Sinne dieser Regelung als „Krankenhaus“ verstanden wird. Demnach gilt als Krankenhaus eine Einrichtung, welche
 1. der Krankenhausbehandlung oder Geburtshilfe dient,
 2. fachlich-medizinisch unter ständiger ärztlicher Leitung steht, zudem über ausreichende, ihrem Versorgungsauftrag entsprechende diagnostische und therapeutische Möglichkeiten verfügen und nach wissenschaftlich anerkannten Methoden arbeitet,
 3. mit Hilfe von jederzeit verfügbarem ärztlichem, Pflege-, Funktions- und medizinisch-technischem Personal darauf eingerichtet ist, vorwiegend durch ärztliche und pflegerische Hilfeleistung Krankheiten der Patienten zu erkennen, zu heilen, ihre Verschlimmerung zu verhüten, Krankheitsbeschwerden zu lindern oder Geburtshilfe zu leisten, und in denen
 4. Patienten untergebracht und gepflegt werden können.
- § 107 Abs. 2 SGB V:
 - § 107 Abs. 2 SGB V enthält die Begriffsbestimmung für „Vorsorge- oder Rehabilitationseinrichtungen“.
- Förderfähig gemäß KHG:
 - Entsprechend § 2 Ziff. 1 sind Krankenhäuser „Einrichtungen, in denen durch ärztliche und pflegerische Hilfeleistung Krankheiten, Leiden oder Körperschäden festgestellt, geheilt oder gelindert werden sollen oder Geburtshilfe geleistet wird und in denen die zu versorgenden Personen untergebracht und gepflegt werden können“.
 - Gemäß § 3 KHG ist das KHG jedoch nicht anwendbar auf

1. Krankenhäuser im Straf- oder Maßregelvollzug,
 2. Polizeikrankenhäuser,
 3. Krankenhäuser der Träger der allgemeinen Rentenversicherung
 4. und, soweit die gesetzliche Unfallversicherung die Kosten trägt, Krankenhäuser der Träger der gesetzlichen Unfallversicherung und ihrer Vereinigungen; das gilt nicht für Fachkliniken zur Behandlung von Erkrankungen der Atmungsorgane, soweit sie der allgemeinen Versorgung der Bevölkerung mit Krankenhäusern dienen.
- Da die Regelungen in den Landeskrankenhausgesetzen aber auf die Förderfähigkeit gemäß KHG abzielen, muss § 5 KHG zur Abgrenzung, welche Krankenhäuser unter das Landeskrankenhausgesetz fallen oder nicht, betrachtet werden. Gemäß § 5 KHG sind nachfolgend genannte Einrichtungen nicht förderungsfähige:
 1. Krankenhäuser, die nach den landesrechtlichen Vorschriften für den Hochschulbau gefördert werden; dies gilt für Krankenhäuser, die Aufgaben der Ausbildung von Ärzten nach der Approbationsordnung für Ärzte vom 27. Juni 2002 (BGBl. I S. 2405), zuletzt geändert durch Artikel 71 des Gesetzes vom 21. Juni 2005 (BGBl. I S. 1818), erfüllen, nur hinsichtlich der nach den landesrechtlichen Vorschriften für Hochschulen förderfähigen Maßnahmen,
 2. Krankenhäuser, die nicht die in § 67 der Abgabenordnung bezeichneten Voraussetzungen erfüllen,
 3. Einrichtungen in Krankenhäusern,
 - a) soweit die Voraussetzungen nach § 2 Nr. 1 nicht vorliegen, insbesondere Einrichtungen für Personen, die als Pflegefälle gelten,
 - b) für Personen, die im Maßregelvollzug aufgrund strafrechtlicher Bestimmungen untergebracht sind,
 4. Tuberkulosekrankenhäuser mit Ausnahme der Fachkliniken zur Behandlung von Erkrankungen der Atmungsorgane, soweit sie nach der Krankenhausplanung des Landes der allgemeinen Versorgung der Bevölkerung mit Krankenhäusern dienen,
 5. Krankenhäuser, deren Träger ein nicht bereits in § 3 S. 1 Nr. 4 genannter Sozialleistungsträger ist, soweit sie nicht nach der Krankenhausplanung des Landes der allgemeinen Versorgung der Bevölkerung mit Krankenhäusern dienen,
 6. Versorgungskrankenhäuser,
 7. Vorsorge- oder Rehabilitationseinrichtungen nach § 107 Abs. 2 SGB V, soweit die Anwendung dieses Gesetzes nicht bereits nach § 3 S. 1 Nr. 4 ausgeschlossen ist,
 8. die mit den Krankenhäusern verbundenen Einrichtungen, die nicht unmittelbar der stationären Krankenversorgung dienen, insbesondere die nicht für den Betrieb des Krankenhauses unerlässlichen Unterkunfts- und Aufenthaltsräume,
 9. Einrichtungen, die aufgrund bundesrechtlicher Rechtsvorschriften vorgehalten oder unterhalten werden; dies gilt nicht für Einrichtungen, soweit sie auf Grund des § 30 des Infektionsschutzgesetzes vom 20. Juli 2000 (BGBl. I S. 1045) vorgehalten werden,
 10. Einrichtungen, soweit sie durch die besonderen Bedürfnisse des Zivilschutzes bedingt sind,
 11. Krankenhäuser der Träger der gesetzlichen Unfallversicherung und ihrer Vereinigungen.

Anhang 1.2: Begriffsbestimmungen – „Patientendaten“

Einige Landesgesetzgeber verzichten auf die Definition von „Patientendaten“, wobei der Begriff zum Teil dennoch benutzt wird. In zehn Landesgesetzen wird der Begriff „Patientendaten“ definiert, wobei häufig die Daten von Angehörigen und „sonstigen Dritten“ zu den Patientendaten gezählt werden. Einige Landesgesetzgeber definieren ergänzend zu dem Begriff „Patientendaten“ noch den Begriff „Betroffene“.

Eine Begriffsbestimmung „Patientendaten“ findet sich in den folgenden Landesgesetzen:

1) § 43 Abs. 4 LKHG BW

Personenbezogene Daten im Sinne dieses Gesetzes sind **Einzelangaben über** persönliche oder sachliche Verhältnisse **bestimmter oder bestimmbarer Patienten des Krankenhauses sowie ihrer Angehörigen, Begleitpersonen und sonstigen Bezugspersonen (Betroffene)**, die im Krankenhaus im Zusammenhang mit der stationären Versorgung des Patienten bekannt werden (**Patientendaten**). Patientendaten in diesem Sinne sind auch Daten, die im Zusammenhang mit einer ambulanten Behandlung stehen, die das Krankenhaus im Rahmen einer Institutsambulanz oder einer institutionellen Ermächtigung erbringt. Im Übrigen sind die Begriffsbestimmungen des Landesdatenschutzgesetzes maßgebend.

2) § 37 Abs. 1 BremKrhG

Patientendaten sind alle personenbezogenen **Daten der Patientinnen und Patienten des Krankenhauses**. Als Patientendaten gelten auch personenbezogene **Daten von verstorbenen Patientinnen und Patienten, Angehörigen oder anderen Bezugspersonen der Patientin oder des Patienten sowie sonstiger Dritter, die dem Krankenhaus im Zusammenhang mit der Behandlung des Patienten oder der Patientin bekannt werden**. Patientendaten in diesem Sinne sind auch Daten, die im Zusammenhang mit einer ambulanten Behandlung stehen, die das Krankenhaus im Rahmen einer Ambulanz oder einer institutionellen Ermächtigung erbringt.

3) § 7 Abs. 1 S. 2 HmbKHG

Zu den Patientendaten gehören auch **die personenbezogenen Daten von Angehörigen einer Patientin oder eines Patienten oder von sonstigen Dritten, wenn die Daten dem Krankenhaus im Zusammenhang mit der Behandlung der Patientin oder des Patienten bekannt werden**.

4) § 2 Abs. 1 GDSG NW

Dieses Gesetz gilt für die Verarbeitung der personenbezogenen Daten

1. von **Personen**, die, auch aufgrund eines gesonderten ärztlichen Behandlungsvertrages, **in einem zugelassenen Krankenhaus** im Sinne von § 107 Abs. 1, § 108 und in einer Vorsorge- und Rehabilitationseinrichtung gemäß § 107 Abs. 2, § 111 des Sozialgesetzbuches, Fünftes Buch - Gesetzliche Krankenversicherung - (SGB V) vom 20. Dezember 1988 (BGBl. I S. 2477) in der jeweils geltenden Fassung, deren Träger nicht der Bund oder eine bundesunmittelbare Körperschaft gemäß Artikel 87 Abs. 2 des Grundgesetzes ist, (Einrichtung) ambulant oder stationär untersucht oder **behandelt werden**,
2. von **Personen**, für die Maßnahmen **aufgrund des Gesetzes über Hilfen und Schutzmaßnahmen bei psychischen Krankheiten (PsychKG)** vom 17. Dezember 1999 (GV. NW. S. 662) in der jeweils geltenden Fassung getroffen werden,
3. von **Personen, die vom Gesundheitsamt untersucht oder von dessen Maßnahmen betroffen werden**.

(Patientendaten). Den Patientendaten sind **gleichgestellt personenbezogene Daten Dritter, die bei Tätigkeiten nach Satz 1 den dort genannten Stellen bekannt werden**.

5) § 36 Abs. 1 S. 3, 4 LKG RP

Sofern im Rahmen der Aufgabenerfüllung **genetische oder biometrische Daten oder Gesundheitsdaten** verarbeitet werden, sind die Anforderungen des Artikels 9 der Verordnung (EU) 2016/679 und des § 19 LDSG zu beachten. **Patientendaten im Sinne der folgenden Bestimmungen sind auch personenbezogene Daten von Angehörigen oder anderen Bezugspersonen der Patientin oder des Patienten sowie sonstiger Dritter, die dem Krankenhaus im Zusammenhang mit der Behandlung bekanntwerden.**

6) § 13 Abs. 1 SKHG

Alle Daten von Patientinnen und Patienten (**Patientendaten**) im Krankenhaus unterliegen unabhängig von der Art ihrer Verarbeitung dem Datenschutz. Patientendaten sind auch personenbezogene **Daten von Angehörigen oder anderen Bezugspersonen der Patientin oder des Patienten sowie sonstiger Dritter, die dem Krankenhaus im Zusammenhang mit der Behandlung bekannt werden.**

7) § 33 Abs. 1 S. 2, 3 SächsKHG

Patientendaten sind alle Einzelangaben über persönliche oder sachliche Verhältnisse **bestimmter oder bestimmbarer Patienten** aus dem Bereich der Krankenhäuser. Patientendaten sind auch die personenbezogenen **Daten von Angehörigen, anderen Bezugspersonen des Patienten sowie sonstiger Dritter, die dem Krankenhaus im Zusammenhang mit der Behandlung bekannt werden.**

8) § 16 Abs. 1 KHG LSA

Patientendaten sind alle Einzelangaben über persönliche oder sachliche Verhältnisse

1. bestimmter oder bestimmbarer **Patienten aus dem Bereich des Krankenhauses** sowie
2. der **Angehörigen des Patienten, anderer Bezugspersonen und sonstiger Dritter (Betroffene),**

die im Krankenhaus im Zusammenhang mit einer Behandlung bekannt werden.

9) § 35 Abs. 2 LKHG SH

Patientendaten im Sinne dieses Gesetzes sind Einzelangaben über persönliche oder sachliche Verhältnisse **bestimmter und bestimmbarer Patientinnen und Patienten eines Krankenhauses**. Als Patientendaten gelten **auch** personenbezogene **Daten von Angehörigen oder anderen Bezugspersonen der Patientinnen und Patienten sowie sonstiger Dritter, die dem Krankenhaus im Zusammenhang mit einer Behandlung bekannt werden.**

10) § 27 Abs. 2 S. 2, 3

Patientendaten sind alle Einzelangaben über persönliche oder sachliche Verhältnisse **bestimmter oder bestimmbarer Patienten** aus dem Bereich der Krankenhäuser. Patientendaten sind **auch** personenbezogene **Daten von Angehörigen oder anderen Bezugspersonen der Patienten sowie sonstiger Dritter, die dem Krankenhaus im Zusammenhang mit der Behandlung bekannt werden.**

Anhang 1.3: Verarbeitung im Auftrag (Auftragsverarbeitung)

Die Voraussetzungen, unter denen Krankenhäusern eine Auftragsverarbeitung (AV) erlaubt werden und was sie für eine Auftragsverarbeitung ggf. zu beachten haben, sind sehr unterschiedlich:

1) § 48 LKHG BW erlaubt Auftragsverarbeitung, wenn

- eine Benachrichtigung Datenschutzaufsichtsbehörde erfolgt,
- die aus § 203 StGB resultierende Schweigepflicht gewahrt bleibt,
- technisch-organisatorischen Maßnahmen schriftlich vereinbart wurden,
- die Daten im Gewahrsam des Krankenhauses bleiben.

2) Art. 27 Abs. 4 BayKrG

- Auftragsverarbeitung von Daten der medizinischen Behandlung nur durch andere Krankenhäuser

- Patientendaten, die zur verwaltungsmäßigen Abwicklung der Behandlung der Patienten erforderlich sind, dürfen auch durch Nicht-Krankenhäuser im Auftrag verarbeitet werden
- 3) § 24 Abs. 7 LKG Berlin
- Genetische Daten und Gesundheitsdaten sind grundsätzlich im Krankenhaus oder im Auftrag durch ein anderes Krankenhaus oder durch mehrere Krankenhäuser als gemeinsam Verantwortliche i. S. d. Art. 26 DS-GVO zu verarbeiten.
 - Auftragsverarbeitung ist nur zulässig
 - der Auftragsverarbeiter der gleichen Unternehmensgruppe i. S. d. Art. 4 Nr. 19 DS-GVO oder der Unternehmensgruppe eines anderen Krankenhauses, das in den Anwendungsbereich dieses Gesetzes fällt, angehört und
 - gewährleistet ist, dass die Verarbeitung ausschließlich durch Personen erfolgt, die nach dem Unionsrecht oder dem Recht eines Mitgliedstaates der Europäischen Union einer Geheimhaltungspflicht unterliegen.
- Andere Stellen dürfen nur mit einer Auftragsverarbeitung beauftragt werden, wenn durch technische Schutzmaßnahmen sichergestellt ist, dass der Auftragnehmer keine Möglichkeit hat, bei einem Zugriff auf Patientendaten den Personenbezug herzustellen.
- Hinweis: Entsprechend Artikel 57 Absatz 2 des Gesetzes vom 12. Oktober 2020 (GVBl. S: 807) tritt § 24 Absatz 7 mit Wirkung vom 25.10.2022 in Kraft
- 4) § 10 BremKrhG erlaubt Auftragsverarbeitung, wenn
- die Wahrung der Vorgaben des BremKHDSG beim Auftragnehmer gewährleistet ist,
 - der Auftragnehmer sich der Kontrolle des Landesbeauftragten für den Datenschutz unterwirft,
 - die technisch-organisatorischen Maßnahmen die Vorgaben nach § 7 Abs. 4 BremDSG berücksichtigen,
 - bei Prüfung/Wartung von Datenverarbeitungs-Anlagen das Krankenhaus die Patientendaten im Einzelfall freigibt, denn ein genereller Zugriff ist nicht statthaft.
- 5) § 38 LKHG M-V erlaubt Auftragsverarbeitung, wenn
- Störungen im Betriebsablauf sonst nicht vermieden werden können,
 - die Datenverarbeitung dadurch erheblich kostengünstiger gestaltet werden kann oder
 - das Krankenhaus seinen Betrieb einstellt.
- Weiterhin ist zu beachten
- Dem Auftragnehmer dürfen Patientendaten nur insoweit offenbart werden, als dies für die Auftragserfüllung erforderlich ist.
 - Eine über drei Monate hinausgehende Speicherung von Patientendaten durch einen Auftragnehmer ist außerhalb des Krankenhauses nur zulässig, wenn die Patientendaten auf getrennten Datenträgern gespeichert sind, die der Auftragnehmer für den Krankenhausträger verwahrt.
 - Eine Auftragsverarbeitung außerhalb des Geltungsbereichs des Grundgesetzes ist nur zulässig, wenn die Patientin oder der Patient in die Auftragsverarbeitung im Ausland ausdrücklich eingewilligt hat oder der Auftragsverarbeiter nach dem Recht seines Sitzlandes selbst einer gesetzlichen Geheimhaltungspflicht unterliegt.
- 6) § 17 NDSG erlaubt Auftragsverarbeitung, wenn
- eine Sicherstellung der Feststellbarkeit, ob und von wem Daten verarbeitet wurden, gegeben ist,
 - eine Beschränkung der Befugnisse auf das erforderliche Maß erfolgt ist,
 - eine Sensibilisierung der mit der Verarbeitung betrauten Personen gegeben ist.
- 7) § 7 GDSG NW erlaubt Auftragsverarbeitung, wenn

- sonst Störungen im Betriebsablauf nicht vermieden werden können oder
- Teilvorgänge der automatischen Datenverarbeitung hierdurch erheblich kostengünstiger vorgenommen werden können.

Weiterhin ist zu beachten

- Beim Auftragnehmer muss die Wahrung der Datenschutzbestimmungen des GDSG NW und die Wahrung der ärztlichen Schweigepflicht sichergestellt sein,
- Patientendaten aus dem ärztlichen Bereich sind vom Auftragnehmer auf physisch getrennten Dateien zu verarbeiten

8) § 37 LKHG SH erlaubt Auftragsverarbeitung, wenn

- dem Auftragsverarbeiter Patientendaten nur offenbart werden, soweit dies für die Auftragserfüllung erforderlich ist.
- Der Krankenhausträger hat, soweit dies für den Auftragszweck ausreichend ist, dem Auftragsverarbeiter anonymisierte Daten zur Verfügung zu stellen; ist eine Anonymisierung nicht möglich, müssen die Daten pseudonymisiert werden

9) § 13a KHG SL erlaubt Auftragsverarbeitung, wenn

- Störungen im Betriebsablauf sonst nicht vermieden werden können,
- die Datenverarbeitung dadurch erheblich kostengünstiger gestaltet werden kann oder
- das Krankenhaus seinen Betrieb einstellt

Weiterhin ist zu beachten

- Vor der Erteilung eines Auftrags zur Verarbeitung von Patientendaten außerhalb des Krankenhauses ist zu prüfen, ob dies im wohlverstandenen Interesse der Patientin oder des Patienten liegt oder der Zweck auch mit verschlüsselten oder pseudonymisierten Patientendaten erreicht werden kann.
- Eine über drei Monate hinausgehende Speicherung von Patientendaten durch einen Auftragnehmer ist außerhalb des Krankenhauses nur zulässig, wenn die Patientendaten auf getrennten Datenträgern gespeichert sind, die der Auftragnehmer für den Krankenhausträger verwahrt.
- Eine Abschrift des Vertrages zur Auftragsverarbeitung sowie der vereinbarten technisch-organisatorischen Maßnahmen hat der Krankenhausträger dem Unabhängigen Datenschutzzentrum Saarland und der Krankenhausaufsichtsbehörde unverzüglich zu übersenden.

10) § 33 Abs. 8 SächsKHG erlaubt Auftragsverarbeitung, wenn

- die zuständige Behörde der Auftragsverarbeitung zustimmte,
- die aus § 203 StGB resultierende Schweigepflicht gewahrt bleibt,
- der Auftragsverarbeiter einen Datenschutzbeauftragten benannt hat.

11) § 16 Abs. 4 KHG LSA erlaubt Auftragsverarbeitung, wenn

- keine Anhaltspunkte bestehen, dass durch die Auftragsdatenverarbeitung schutzwürdige Belange des Patienten oder des Betroffenen beeinträchtigt werden
- jede an der Auftragsdatenverarbeitung beteiligte Person zur Geheimhaltung verpflichtet wird.

Der Patient ist vorab über die Auftragsdatenverarbeitung zu informieren; der Patient kann der Verarbeitung der ihn betreffenden Daten widersprechen.

12) § 27b ThürKHG erlaubt Auftragsverarbeitung, wenn

- sonst Störungen im Betriebsablauf nicht vermieden werden können oder Teilvorgänge der automatischen Datenverarbeitung hierdurch erheblich kostengünstiger vorgenommen werden können,

- die Einhaltung der Datenschutzbestimmungen des ThürKHG sowie eine den Voraussetzungen des § 203 des Strafgesetzbuchs entsprechende Schweigepflicht beim Auftragsverarbeiter sichergestellt ist und
- der Verantwortliche der Aufsichtsbehörde nach § 32 Abs. 2 ThürKHG rechtzeitig vor Auftragserteilung Art, Umfang und die technischen und organisatorischen Maßnahmen der beabsichtigten Datenverarbeitung im Auftrag schriftlich angezeigt hat.

Anhang 1.4: Erlaubnistatbestände für die Verarbeitung von Patientendaten durch das jeweilige Krankenhaus

Die nachfolgende tabellarische Darstellung dient nur der Übersicht, welche Regelungen in welchen Landesgesetzen für Krankenhäuser enthalten sind. Die Rahmenbedingungen, unter welchen Bedingungen ein Erlaubnistatbestand gilt, ist im jeweiligen Gesetz nachzulesen.

	Versorgung des Patienten	Verwaltungsmäßige Abwicklung des Behandlungsverhältnisses	Krankenhausseelsorge	Sozialen Betreuung und Beratung	Qualitätssicherung der Versorgung/Behandlung	Ausbildung, Fortbildung und Weiterbildung	Erkennung, Verhütung und Bekämpfung von Krankenhausinfektionen	Rechnungsprüfung	Prüfung und Wartung von automatisierten Verfahren der Datenverarbeitung	Wahrnehmung von Aufsichts- und Kontrollbefugnissen	Medizinische Forschungsvorhaben des Krankenhauses	Verteidigung von Beschäftigten in Rechtsgeschäften	Überprüfung der Tätigkeit der Mitarbeiterinnen und Mitarbeiter	Unterrichtung von Angehörigen oder anderen Bezugspersonen
Baden-Württemberg §§ 45,46 LKG BW	X	X	X		X	X	X	X	X	X	X			
Bayern Art. 27 BayKrG	X	X				X					X			
Berlin §§ 24, 25 LKG				X	X				X		X			
Brandenburg §§ 28, 31 BbgKHEG	X	X	X	X	X	X	X				X	X		
Bremen §§ 38, 39 BremKrhG	X	X			X	X	X				X			
Hamburg § 8, 10, 12 HmbKHG	X	X		X	X	X					X		X	
Hessen § 12 HKHG 2011 i. V. m. §§ 20, 24 HDSIG	X	X							X		X			

	Versorgung des Patienten	Verwaltungsmäßige Abwicklung des Behandlungsverhältnisses	Krankenhausseelsorge	Sozialen Betreuung und Beratung	Qualitätssicherung der Versorgung/Behandlung	Ausbildung, Fortbildung und Weiterbildung	Erkennung, Verhütung und Bekämpfung von Krankenhausinfektionen	Rechnungsprüfung	Prüfung und Wartung von automatisierten Verfahren der Datenverarbeitung	Wahrnehmung von Aufsichts- und Kontrollbefugnissen	Medizinische Forschungsvorhaben des Krankenhauses	Verteidigung von Beschäftigten in Rechtsgeschäften	Überprüfung der Tätigkeit der Mitarbeiterinnen und Mitarbeiter	Unterrichtung von Angehörigen oder anderen Bezugspersonen
Mecklenburg-Vorpommern §§ 33, 34 LKHG	X	X	X		X	X		X			X			
Niedersachsen														
Nordrhein-Westfalen §§ 6, 10, 11 GDSG NW	X	X			X						X			
Rheinland-Pfalz § 36, 37 LKG	X				X	X					X			
Saarland § 9, 13, 14 SKHG	X	X	X			X					X			
Sachsen § 33 SächsKHG	X					X					X			
Sachsen-Anhalt §§ 16, 17 KHG LSA	X	X		X	X	X	X	X			X		X	
Schleswig-Holstein §§ 36, 38 LKHG	X			X	X	X		X			X		X	X
Thüringen §§ 23, 27, 27a ThürKHG	X				X	X								

Anhang 2: Internetadressen verschiedener Gesetze

Anhang 2.1: Bundesrecht

- Grundgesetz (GG)
URL: <https://www.gesetze-im-internet.de/gg/index.html>
 - Art 87 GG
URL: https://www.gesetze-im-internet.de/gg/art_87.html
- Gesetz zur wirtschaftlichen Sicherung der Krankenhäuser und zur Regelung der Krankenhauspflegesätze (Krankenhausfinanzierungsgesetz - KHG)
URL: <https://www.gesetze-im-internet.de/khg/index.html>
 - § 2 Begriffsbestimmungen
URL: https://www.gesetze-im-internet.de/khg/_2.html
 - § 3 Anwendungsbereich
URL: https://www.gesetze-im-internet.de/khg/_3.html
 - § 5 Nicht förderungsfähige Einrichtungen
URL: https://www.gesetze-im-internet.de/khg/_5.html
- Sozialgesetzbuch Fünftes Buch (SGB V) - Gesetzliche Krankenversicherung
URL: https://www.gesetze-im-internet.de/sgb_5/
 - § 107 Krankenhäuser, Vorsorge- oder Rehabilitationseinrichtungen
URL: http://www.gesetze-im-internet.de/sgb_5/_107.html
- Siebtes Buch Sozialgesetzbuch (SGB VII) - Gesetzliche Unfallversicherung
URL: https://www.gesetze-im-internet.de/sgb_7/
 - § 33 Behandlung in Krankenhäusern und Rehabilitationseinrichtungen
URL: https://www.gesetze-im-internet.de/sgb_7/_33.html
 - § 34 Durchführung der Heilbehandlung
URL: https://www.gesetze-im-internet.de/sgb_7/_34.html
- Bundesdatenschutzgesetz (BDSG)
URL: https://www.gesetze-im-internet.de/bdsg_2018/
 - § 1 Anwendungsbereich des Gesetzes
URL: https://www.gesetze-im-internet.de/bdsg_2018/_1.html
 - § 22 Verarbeitung besonderer Kategorien personenbezogener Daten
URL: https://www.gesetze-im-internet.de/bdsg_2018/_22.html
 - § 27 Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken
URL: https://www.gesetze-im-internet.de/bdsg_2018/_27.html

Anhang 2.2: Landesrecht

- Landeskrankenhausgesetz (LKHG) Baden-Württemberg
URL: <https://www.landesrecht-bw.de/jportal/?quelle=jlink&query=KHG+BW&psml=bsbawueprod.psml&max=true>
 - § 2 Geltungsbereich
URL: <https://www.landesrecht-bw.de/jportal/?quelle=jlink&docid=jlr-KHGBW2008pP2&psml=bsbawueprod.psml&max=true>
 - § 43 Anwendungsbereich, Begriffsbestimmungen
URL: <https://www.landesrecht-bw.de/jportal/?quelle=jlink&docid=jlr-KHGBW2008pP43&psml=bsbawueprod.psml&max=true>
 - § 45 Zulässigkeit der Erhebung, Speicherung, Veränderung und Nutzung
URL: <https://www.landesrecht-bw.de/jportal/?quelle=jlink&docid=jlr-KHGBW2008pP45&psml=bsbawueprod.psml&max=true>

- § 46 Zulässigkeit der Übermittlung
URL: <https://www.landesrecht-bw.de/jportal/?quelle=jlink&docid=jlr-KHGBW2008pP46&psml=bsbawueprod.psml&max=true>
- § 49 Befugtes Offenbaren
URL: <https://www.landesrecht-bw.de/jportal/?quelle=jlink&docid=jlr-KHGBW2008pP49&psml=bsbawueprod.psml&max=true>
- § 50 Einwilligung
URL: <https://www.landesrecht-bw.de/jportal/?quelle=jlink&docid=jlr-KHGBW2008pP50&psml=bsbawueprod.psml&max=true>
- Bayerisches Krankenhausgesetz (BayKrG)
URL: <https://www.gesetze-bayern.de/Content/Document/BayKrG>
 - Art. 2 Geltungsbereich
URL: <https://www.gesetze-bayern.de/Content/Document/BayKrG-2>
 - Art. 27 Datenschutz
URL: <https://www.gesetze-bayern.de/Content/Document/BayKrG-27>
- Landeskrankenhausgesetz (LKG) Berlin
URL: https://www.gesetze.berlin.de/perma?j=KHG_BE
 - § 2 Geltungsbereich
URL: <https://www.gesetze.berlin.de/perma?d=jlr-KHGBE2011pP2>
 - § 24 Verarbeitung von genetischen Daten und Gesundheitsdaten
URL: <https://www.gesetze.berlin.de/perma?d=jlr-KHGBE2011V4P24>
 - § 25 Verarbeitung von genetischen Daten und Gesundheitsdaten zu wissenschaftlichen Forschungszwecken
URL: <https://gesetze.berlin.de/bsbe/document/jlr-KHGBE2011V4P25>
- Gesetz zur Entwicklung der Krankenhäuser im Land Brandenburg (Brandenburgisches Krankenhausentwicklungsgesetz - BbgKHEG)
URL: <https://bravors.brandenburg.de/gesetze/bbgkheg>
 - § 28 Verarbeitung von Patientendaten mit Ausnahme der Offenlegung
URL: <https://bravors.brandenburg.de/gesetze/bbgkheg#28>
 - § 29 Offenlegung von Patientendaten
URL: <https://bravors.brandenburg.de/gesetze/bbgkheg#29>
 - § 31 Datenschutz bei Forschungsvorhaben
URL: <https://bravors.brandenburg.de/gesetze/bbgkheg#31>
 - § 33 Klinisches Krankheitsregister
URL: <https://bravors.brandenburg.de/gesetze/bbgkheg#33>
- Bremisches Krankenhausgesetz - (BremKrhG)
URL: https://www.transparenz.bremen.de/vorschrift_detail/bremen2014_tp.c.159875.de
 - § 1 Geltungsbereich
URL: https://www.transparenz.bremen.de/metainformationen/bremisches-krankenhausgesetz-bremkrhg-vom-24-november-2020-159875?asl=bremen203_tpgesetz.c.55340.de&template=20_gp_ifg_meta_detail_d#jlr-KHGBR2020pP1
 - § 36 Anwendungsbereich
URL: https://www.transparenz.bremen.de/metainformationen/bremisches-krankenhausgesetz-bremkrhg-vom-24-november-2020-159875?asl=bremen203_tpgesetz.c.55340.de&template=20_gp_ifg_meta_detail_d#jlr-KHGBR2020pP36

- § 38 Verarbeitung
URL: https://www.transparenz.bremen.de/metainformationen/bremisches-krankenhausgesetz-bremkrhg-vom-24-november-2020-159875?asl=bremen203_tpgesetz.c.55340.de&template=20_gp_ifg_meta_detail_d#lr-KHGBR2020pP38
- § 39 Verarbeitung von Patientendaten zu Forschungszwecken
URL: https://www.transparenz.bremen.de/metainformationen/bremisches-krankenhausgesetz-bremkrhg-vom-24-november-2020-159875?asl=bremen203_tpgesetz.c.55340.de&template=20_gp_ifg_meta_detail_d#lr-KHGBR2020pP39
- § 40 Übermitteln von Patientendaten an Stellen außerhalb des Krankenhauses
URL: https://www.transparenz.bremen.de/metainformationen/bremisches-krankenhausgesetz-bremkrhg-vom-24-november-2020-159875?asl=bremen203_tpgesetz.c.55340.de&template=20_gp_ifg_meta_detail_d#lr-KHGBR2020pP40
- Hamburgisches Krankenhausgesetz (HmbKHG)
URL: <http://www.landesrecht-hamburg.de/jportal/portal/page/bshaprod.psml?showdoccase=1&st=lr&doc.id=jlr-KHGHArahmen>
 - § 2 Geltungsbereich
URL: <http://www.landesrecht-hamburg.de/jportal/portal/page/bshaprod.psml?nid=5&showdoccase=1&doc.id=jlr-KHGHA4P2&st=lr>
 - § 7 Grundsatz
URL: <http://www.landesrecht-hamburg.de/jportal/portal/page/bshaprod.psml?nid=g&showdoccase=1&doc.id=jlr-KHGHA7P7&st=lr>
 - § 10 Verwendung von Patientendaten innerhalb des Krankenhauses
URL: <https://www.landesrecht-hamburg.de/bsha/document/jlr-KHGHA6P10>
 - § 11 Offenlegung von Patientendaten
URL: <https://www.landesrecht-hamburg.de/bsha/document/jlr-KHGHA7P11>
 - § 12 Forschungsvorhaben und Sammlungen von Proben
URL: <https://www.landesrecht-hamburg.de/bsha/document/jlr-KHGHA7P12>
- Zweites Gesetz zur Weiterentwicklung des Krankenhauswesens in Hessen (Hessisches Krankenhausgesetz 2011 - HKHG 2011)
URL: <https://www.rv.hessenrecht.hessen.de/bshe/document/jlr-KHGHE2011rahmen>
 - § 2 Geltungsbereich
URL: <https://www.rv.hessenrecht.hessen.de/bshe/document/jlr-KHGHE2011V8P2>
 - § 12 Datenschutz im Krankenhaus
URL: <https://www.rv.hessenrecht.hessen.de/bshe/document/jlr-KHGHE2011V8P12>
- Hessisches Datenschutz- und Informationsfreiheitsgesetz (HDSIG)
URL: <https://www.rv.hessenrecht.hessen.de/bshe/document/jlr-DSIFGHErahmen>
 - § 20 Verarbeitung besonderer Kategorien personenbezogener Daten
URL: <https://www.rv.hessenrecht.hessen.de/bshe/document/jlr-DSIFGHEp20>
 - § 24 Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken
URL: <https://www.rv.hessenrecht.hessen.de/bshe/document/jlr-DSIFGHEp24>

- Krankenhausgesetz für das Land Mecklenburg-Vorpommern (Landeskrankenhausgesetz LKHG M-V -)
 - URL: <https://www.landesrecht-mv.de/bsmv/document/jlr-LKHGMV2011rahmen>
 - § 3 Geltungsbereich
 - URL: <https://www.landesrecht-mv.de/bsmv/document/jlr-LKHGMV2011pP3>
 - § 32 Anwendungsbereich und Begriffsbestimmungen
 - URL: <https://www.landesrecht-mv.de/bsmv/document/jlr-LKHGMV2011V1P32>
 - § 34 Weitere Verarbeitung von Daten
 - URL: <https://www.landesrecht-mv.de/bsmv/document/jlr-LKHGMV2011V1P34>
 - § 37 Datenverarbeitung für Forschungszwecke
 - URL: <https://www.landesrecht-mv.de/bsmv/document/jlr-LKHGMV2011V1P37>
- Niedersächsisches Krankenhausgesetz (NKHG)
 - URL: <http://www.nds-voris.de/jportal/?quelle=jlink&query=KHG+ND&psml=bsvorisprod.psml&max=true>
 - Enthält keinerlei datenschutzrechtliche Regelungen, daher ist entweder NDSG oder BDSG anwendbar.
- Niedersächsisches Datenschutzgesetz (NDSG)
 - URL: <http://www.nds-voris.de/jportal/?quelle=jlink&query=DSG+ND&psml=bsvorisprod.psml&max=true>
 - § 1 Regelungsgegenstand und Anwendungsbereich
 - URL: <http://www.nds-voris.de/jportal/?quelle=jlink&query=DSG+ND+%C2%A7+1&psml=bsvorisprod.psml&max=true>
 - § 13 Verarbeitung personenbezogener Daten zu wissenschaftlichen oder historischen Forschungszwecken
 - URL: <http://www.nds-voris.de/jportal/?quelle=jlink&query=DSG+ND+%C2%A7+13&psml=bsvorisprod.psml&max=true>
 - § 17 Verarbeitung besonderer Kategorien personenbezogener Daten
 - URL: <http://www.nds-voris.de/jportal/?quelle=jlink&query=DSG+ND+%C2%A7+17&psml=bsvorisprod.psml&max=true>
- Gesetz zum Schutz personenbezogener Daten im Gesundheitswesen (Gesundheitsdatenschutzgesetz - GDSG NW)
 - URL: https://recht.nrw.de/lmi/owa/br_text_anzeigen?v_id=10000000000000000495
 - § 2 Geltungsbereich
 - URL: https://recht.nrw.de/lmi/owa/br_bes_detail?sg=0&menu=0&bes_id=4283&anw_nr=2&aufgehoben=N&det_id=357746
 - § 5 Übermittlung, Zweckbindung
 - URL: https://recht.nrw.de/lmi/owa/br_bes_detail?sg=0&menu=0&bes_id=4283&anw_nr=2&aufgehoben=N&det_id=357749
 - § 6 Datenverarbeitung für wissenschaftliche Zwecke
 - URL: https://recht.nrw.de/lmi/owa/br_bes_detail?sg=0&menu=0&bes_id=4283&anw_nr=2&aufgehoben=N&det_id=357750

- § 11 Übermittlung und Nutzung von Daten
URL: https://recht.nrw.de/lmi/owa/br_bes_detail?sg=0&menu=0&bes_id=4283&anw_nr=2&aufgehoben=N&det_id=357755
- Landeskrankenhausgesetz (LKG) Rheinland-Pfalz
URL: <http://landesrecht.rlp.de/jportal/portal/t/15bc/page/bsrlpprod.psml?doc.hl=1&doc.id=jlr-KHGRPrahen&documentnumber=3&numberofresults=52&doctyp=Norm&showdoccase=1&doc.part=R¶mfromHL=true#focuspoint>
 - § 3 Geltungsbereich
URL: http://landesrecht.rlp.de/jportal/portal/t/c7l/page/bsrlpprod.psml/action/portlets.jw.MainAction?p1=5&eventSubmit_doNavigate=searchInSubtreeTOC&showdoccase=1&doc.hl=0&doc.id=jlr-KHGRPV7P3&doc.part=S&toc.poskey=#focuspoint
 - § 36 Datenschutz
URL: http://landesrecht.rlp.de/jportal/portal/t/c9l/page/bsrlpprod.psml/action/portlets.jw.MainAction?p1=17&eventSubmit_doNavigate=searchInSubtreeTOC&showdoccase=1&doc.hl=0&doc.id=jlr-KHGRPV12P36&doc.part=S&toc.poskey=#focuspoint
 - § 37 Datenschutz bei Forschungsvorhaben
URL: http://landesrecht.rlp.de/jportal/portal/t/c9u/page/bsrlpprod.psml/action/portlets.jw.MainAction?p1=18&eventSubmit_doNavigate=searchInSubtreeTOC&showdoccase=1&doc.hl=0&doc.id=jlr-KHGRPV12P37&doc.part=S&toc.poskey=#focuspoint
- Saarländisches Krankenhausgesetz (KHG SL)
URL: <https://recht.saarland.de/bssl/document/jlr-KHGSL2015rahmen>
 - § 2 Geltungsbereich
URL: <https://recht.saarland.de/bssl/document/jlr-KHGSL2015V2P2>
 - § 13 Patientendatenschutz
URL: <https://recht.saarland.de/bssl/document/jlr-KHGSL2015V3P13>
 - § 14 Forschung und Patientendaten
URL: <https://recht.saarland.de/bssl/document/jlr-KHGSL2015pP14>
- Sächsisches Krankenhausgesetz (SächsKHG)
URL: <https://www.revosax.sachsen.de/vorschrift/1051-Saechsisches-Krankenhausgesetz>
 - § 2 Anwendungsbereich
 - § 33 Datenschutz
 - § 34 Datenschutz bei Forschungsvorhaben
- Krankenhausgesetz Sachsen-Anhalt (KHG LSA)
URL: https://www.landesrecht.sachsen-anhalt.de/perma?j=KHG_ST
Keine Festlegung des Geltungsbereiches. Evtl. kann aus den Zielen in § 1 gefolgert werden, dass es für alle Krankenhäuser gilt.
 - § 1 Ziel des Gesetzes
URL: https://www.landesrecht.sachsen-anhalt.de/perma?j=KHG_ST_!_1
 - § 16 Verarbeitung von Patientendaten
URL: https://www.landesrecht.sachsen-anhalt.de/perma?j=KHG_ST_!_16
 - § 17 Verarbeitung von Patientendaten zu Forschungszwecken
URL: https://www.landesrecht.sachsen-anhalt.de/perma?j=KHG_ST_!_17
- Krankenhausgesetz für das Land Schleswig-Holstein-Landeskrankenhausgesetz- (LKHG)

URL: https://www.schleswig-holstein.de/DE/Landesregierung/IV/Service/GVOBl/GVOBl/2020/gvobl_22_2020.pdf?blob=publicationFile&v=3

- § 2 Geltungsbereich
 - § 36 Datenverarbeitung im Krankenhaus
 - § 38 Verarbeiten von Patientendaten im Rahmen von Forschungsvorhaben
- Thüringer Krankenhausgesetz (ThürKHG)

URL: https://landesrecht.thueringen.de/perma?j=KHG_TH

- § 3 Geltungsbereich
URL: <https://landesrecht.thueringen.de/perma?d=jlr-KHGTH2003pP3>
- § 27 Schutz der Persönlichkeit und Datenschutz
URL: <https://landesrecht.thueringen.de/perma?d=jlr-KHGTH2003V3P27>

Anhang 2.3: Krankenhäuser der Bundeswehr

- Gesetz über die Rechtsstellung der Soldaten (Soldatengesetz - SG)

URL: <https://www.gesetze-im-internet.de/sg/>

- § 1 Begriffsbestimmungen
URL: https://www.gesetze-im-internet.de/sg/_1.html
- § 29a Verarbeitung von besonderen Kategorien personenbezogener Daten
URL: https://www.gesetze-im-internet.de/sg/_29a.html
- § 29e Befugtes Offenbaren von Privatgeheimnissen
URL: https://www.gesetze-im-internet.de/sg/_29e.html

Hinweis: Bei der Verarbeitung von Daten ist die zentrale Dienstvorschrift „Informationssicherheit“ (A-960/1, https://media.frag-den-staat.de/files/foi/174322/A_960_1.pdf) einzuhalten, bei Forschung insbesondere die Kapitel

- 4.2 „Wehrtechnische Forschung & Technologie sowie sonstige Forschungsvorhaben, Erprobungen, Truppenversuche und Wehrtechnische Aufträge (F)“
- 6.3.4 „Informationssicherheitskonzept Forschung und Wissenschaft (F, W)“
- 11.5.1 „Anwendungsbereich Wehrtechnische Forschung & Technologie sowie sonstige Forschungsvorhaben, Erprobungen, Truppenversuche und Wehrtechnische Aufträge (F)“
- 11.7.2 „Vorhaben Forschung und Wissenschaft (F, W)“