REGELUNGEN ZUM DATENSCHUTZ IN DER MEDIZINISCHEN FOR-SCHUNG UND OPTIONEN ZUR VERBESSERUNG

Unterstützt durch:

Koordiniert von Dierks+Company.

EHDS-Koalition

Koordiniert durch Dierks+Company
Rechtsanwaltsgesellschaft mbH

HELIX HUB
Invalidenstraße 113
D-10115 Berlin

T +49 30 586 930-000
F +49 30 586 930-099
info@ehds-koalition.de
www.ehds-koalition.de

Registernummer:
R006064

Vertretungsberechtigte Personen:
Prof. Dr. Dr. Christian Dierks
Juliana Dierks
Dr. Dominik Roters

Inhaltsverzeichnis

1. Das politische Versprechen: Bessere Rahmenbedingungen für klinische Forschung

Mit der Ankündigung des Medizinforschungsgesetzes am 1. Dezember 2023 wurde das Versprechen verbunden, die medizinische Forschung in Deutschland zu stärken.

In dem Gesetzesentwurf sollten nach Ankündigung des BMG unter anderem folgende Maßnahmen umgesetzt werden:[1]

- „Es wird eine interdisziplinär zusammengesetzte Bundes-Ethik-Kommission beim Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) errichtet.
- Strahlenschutzrechtliche Anzeige- und Genehmigungsverfahren werden in das Genehmigungsverfahren der klinischen Prüfung integriert.
- Das BfArM wird künftig die Koordinierung und das Verfahrensmanagement für Zulassungsverfahren und Anträge zu klinischen Prüfungen für alle Arzneimittel, ausgenommen Impfstoffe und Blutprodukte übernehmen.
- Mustervertragsklauseln für die Durchführung klinischer Studien werden bekannt gegeben.
- Die Bearbeitungszeiten bei mononationalen klinischen Prüfungen werden verkürzt.
- Die Durchführung dezentraler klinischer Prüfungen wird ermöglicht."

Das Strategiepapier der Bundesregierung „Verbesserung der Rahmenbedingungen für den Pharmabereich in Deutschland Handlungskonzepte für den Forschungs- und Produktionsstandort" vom 13. Dezember 2023 beschreibt Problem und Ziele zutreffend:

> „Der Forschungs- und Entwicklungsstandort Deutschland hat insbesondere im Vergleich zu anderen europäischen Standorten relativ an Wettbewerbsfähigkeit verloren."
>
> Und weiter: „Um die Attraktivität des Pharmastandorts Deutschland wieder zu erhöhen und auszubauen sowie eine zuverlässige Versorgung sicherzustellen, setzt sich die Bundesregierung dafür ein, dass die Rahmenbedingungen für eine starke, nachhaltige und international wettbewerbsfähige Pharmaindustrie insbesondere in Deutschland und auch in der Europäischen Union (EU) verbessert werden. […] Unerlässlich hierfür sind eine gute Forschungsinfrastruktur mit hochqualifizierten Fachkräften sowie eine enge Kooperation mit entsprechenden Forschungseinrichtungen."

[1] Vgl. https://www.bundesgesundheitsministerium.de/ministerium/meldungen/lauterbach-forschung-und-medizinproduktion-in-deutschland-staerken-01-12-23 (abgerufen am 20.12.2023)

Das Medizinforschungsgesetz liegt nunmehr (Stand 10. Juni 2024) in der Fassung des Regierungsentwurfes vor[2] und hält die meisten Versprechungen aus dem letzten Dezember. Es adressiert viele wichtige Punkte, um die Rahmenbedingungen für die medizinische Forschung zu verbessern. **Allerdings bleibt ein entscheidender Aspekt ungelöst – der Datenschutz.**

Die sich aus dem gegenwärtigen Datenschutzrecht ergebenden, bedeutenden Hindernisse für die Forschung mit Gesundheitsdaten bleiben bestehen, da die Forschenden in Deutschland weiterhin mit einem „datenschutzrechtlichen Dschungel" konfrontiert sind. Das Regelungsgewirr mit unterschiedlichen, oft unklaren Voraussetzungen und mehrfachen Zuständigkeiten führt zu erheblichen negativen Auswirkungen auf die Dauer und den Aufwand zur Erlangung erforderlicher Zustimmungen, Voten und Genehmigungen. Dies hat zur Folge, dass immer wieder wichtige Forschungsprojekte entweder gar nicht gestartet oder in andere Länder verlagert werden.

Dieses Gutachten will dazu beitragen, den Forschungs- und Entwicklungsstandort Deutschland durch Verbesserung der Forschungsinfrastruktur zu stärken. Dazu untersucht es spezifisch die Forschungsbarrieren, welche aus den unterschiedlichen **Anforderungen und Zuständigkeiten für die Verarbeitung von Daten** bei klinischen Forschungsprojekten durch Datenschutzbestimmungen der Länder und der Kirchen bestehen und macht Vorschläge, wie diese überwunden werden können.

[2] Gesetzentwurf der Bundesregierung mit Stand 25.03.2024; https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/3_Downloads/Gesetze_und_Verordnungen/GuV/M/Kabinettsbeschluss_Entwurf_eines_Medizinforschungsgesetzes.pdf (zuletzt abgerufen 10.06.2024)

2. Die für die klinische Forschung erforderliche Datenverarbeitung

Die Verbesserung von Forschungsbedingungen durch Abbau von Verarbeitungsbarrieren für Daten hat sich an den tatsächlichen Erfordernissen und damit an den typischen Datenflüssen für Forschungsvorhaben zu orientieren. Zur Bestimmung dieser Erfordernisse werden zunächst die verschiedenen Felder medizinischer Forschung beschrieben (2.1) und sodann die typischen (und atypischen) Datenflüsse aufgezeigt, welche datenschutzrechtlich zu sichern sind (2.2).

2.1 Unterschiede und Voraussetzungen der verschiedenen Felder klinischer Forschung

Der Begriff „klinische Forschung“ ist sehr weitgehend und umfasst methodisch unterschiedliche Ansätze der grundlagenorientierten, der krankheitsorientierten und der patientenorientierten Forschung.[3] Ihr wichtigstes Instrument sind klinische Studien, welche Wirksamkeit und Unbedenklichkeit neuer Verfahren wissenschaftlich belegen.[4]

2.1.1 Klinische Prüfungen nach CTR und AMG

Die seit dem 31. Januar 2022 anzuwendende Verordnung (EU) Nr. 536/2014 (Verordnung über klinische Prüfungen mit Humanarzneimitteln; **CTR**) definiert in Art. 2 Abs. 2 Nr. 1 die klinische Studie mit Arzneimitteln und legt unter anderem fest, dass nur „am Menschen durchgeführte Untersuchungen“ die Definition erfüllen können. Unter Nr. 2 findet sich an gleicher Stelle folgende Definition für klinische Prüfungen:

> „2. ´**klinische Prüfung**´ eine klinische Studie, die mindestens eine der folgenden Bedingungen erfüllt:
>
> a) Der Prüfungsteilnehmer wird vorab einer bestimmten Behandlungsstrategie zugewiesen, die nicht der normalen klinischen Praxis des betroffenen Mitgliedstaats entspricht;
>
> b) die Entscheidung, die Prüfpräparate zu verschreiben, wird zusammen mit der Entscheidung getroffen, den Prüfungsteilnehmer in die klinische Studie aufzunehmen, oder
>
> c) an den Prüfungsteilnehmern werden diagnostische oder Überwachungsverfahren angewendet, die über die normale klinische Praxis hinausgehen;“

Das deutsche Recht übernimmt in § 4 Abs. 23 AMG diese Definition.

---

[3] Vgl. Denkschrift „Klinische Forschung“ der Deutschen Forschungsgemeinschaft vom 11.02.2000 Seite 3. (abgerufen unter www.dfg.de/resource/blob/169194/8443993e4fd0c2676b95f4121bdf3d36/denkschrift-klin-forschung-data.pdf am 20.12.2023)

[4] Vgl. Eintrag klinische Forschung im Dossier des Bundesministeriums für Bildung und Forschung (abgerufen unter https://www.gesundheitsforschung-bmbf.de/de/klinische-forschung-6456.php am 20.12.2023)

Klinische Prüfungen dienen somit dem **Nachweis der Wirksamkeit und Unbedenklichkeit** von Arzneimitteln, die unter ärztlicher Aufsicht an Testpersonen erprobt werden. Sie folgen einem **vorab festgelegten Prüfplan**, was sie von nicht-interventionellen Prüfungen unterscheidet. Bei Letzteren erfolgt die Behandlung und Beobachtung nicht nach einem Prüfplan, sondern ausschließlich nach den medizinischen Erfordernissen des Patienten, also entsprechend der gewöhnlichen ärztlichen Praxis.[5]

Mit der klinischen Prüfung von Arzneimitteln darf nach § 40 Abs. 1 AMG in Deutschland nur begonnen werden, wenn die zuständige Bundesoberbehörde die klinische Prüfung nach Artikel 8 CTR genehmigt hat. Für eine **Genehmigung** sind nach Art. 7 CTR unter anderem folgende, für unsere Fragestellung relevanten Aspekte zu prüfen:

- Einhaltung der Voraussetzungen für die Einwilligung zur Teilnahme nach Aufklärung gemäß Kap. V (Art. 7 Abs. 1 lit. a)
- Übereinstimmung mit der Datenschutzrichtlinie 95/46/EG [jetzt DSGVO] (Art. 7 Abs. 1 lit. d)
- Übereinstimmung mit den Bestimmungen über die Gewinnung, Lagerung und zukünftige Nutzung der vom Prüfungsteilnehmer genommenen biologischen Proben (Art. 7 Abs. 1 lit. h)

Für die klinische Prüfung liegen in CTR und AMG unterschiedliche Definitionen vor. Im Ergebnis erfordert eine klinische Prüfung nach Art. 7 CTR u.a. die Einwilligung der Studienteilnehmer zur Teilnahme nach Aufklärung und die Einhaltung weiterer Bedingungen, vor allem aber auch des Datenschutzes. Durch diese arzneimittelrechtliche Vorgabe wird das bundesdeutsche Regelungsdickicht des Datenschutzrechts zum Hemmschuh für die klinische Forschung.

2.1.2 Klinische Bewertungen und Prüfungen nach MDR und IVDR

Auch klinische Prüfungen mit Medizinprodukten und In-vitro-Diagnostika erhalten in Deutschland das datenschutzrechtliche Regelwerk ohne Rechtsgrundlage im EU-Recht „übergestülpt". Diese Prüfungen sind zunächst etwas anders als in der CTR definiert: So bezeichnet die Verordnung (EU) 2017/745 vom 5. April 2017 über Medizinprodukte (MDR) unter Art. 2 Nr. 45 MDR die „**klinische Prüfung**" als

> „eine systematische Untersuchung, bei der ein oder mehrere menschliche Prüfungsteilnehmer einbezogen sind und die zwecks Bewertung der Sicherheit oder Leistung eines Produkts durchgeführt wird."

Klinische Prüfungen sind allerdings nach Art. 61 Abs. 4 MDR nur für die Zertifizierung von implantierbaren Produkten und Produkten der Klasse III erforderlich.

Alle anderen Medizinprodukte erfordern in der Regel[6] lediglich eine klinische Bewertung, welche in Art. 2 Nr. 44 MDR wie folgt definiert ist: „`**klinische Bewertung**` bezeichnet einen systematischen und

[5] Vgl. a. Definition nach Art. 2 Abs. 2 Nr. 4 CTR.
[6] Zu den genauen Anforderungen siehe Art. 61 Abs. 1-3 MDR.

geplanten Prozess zur kontinuierlichen Generierung, Sammlung, Analyse und Bewertung der klinischen Daten zu einem Produkt, mit dem Sicherheit und Leistung, einschließlich des klinischen Nutzens, des Produkts bei vom Hersteller vorgesehener Verwendung überprüft wird;“

Diese Unterscheidung ist für die vorliegende Untersuchung insofern wichtig, als eine **Einwilligungserfordernis** zur Teilnahme nach Art. 62 Abs. 4 lit. f MDR (und § 29 MPDG) zwar für klinische Prüfungen, aber nicht für klinische Bewertungen besteht.[7]

Ähnliche Regelungen finden sich in Verordnung (EU) 2017/746 vom 5. April 2017 über In-vitro-Diagnostika (IVDR), welche in Art 2 Nr. 42 IVDR definiert: „´**Leistungsstudie**´ bezeichnet eine Studie zur Feststellung oder Bestätigung der Analyseleistung oder der klinischen Leistung eines Produkts“.

Auch die Leistungsstudie erfordert nach Art. 58 Abs. 5 lit. f IVDR (und § 29 MPDG) eine **Einwilligung** der Prüfungsteilnehmer zur Teilnahme. Demgegenüber ist die Verpflichtung zur datenschutzkonformen Verarbeitung der personenbezogenen Daten in Art. 73 Abs. 3 MDR, für IVD in Art. 86 Abs. 3 IVDR geregelt. Nach EU-Recht bedarf es dafür keiner gesonderten Einwilligung.

Der Widerruf der Einwilligung zur Teilnahme lässt die Datenverarbeitung unberührt, vgl. Art. 28 Abs. 3 Satz 2 CTR, Art. 62 Abs. 5 Satz 2 MDR, Art. 58 Abs. 6 Satz 2 IVDR. Weder MDR oder IVDR erfordern eine Einwilligung in die Datenverarbeitung im Rahmen einer klinischen Prüfung oder Studie. Die Rechtsgrundlage für die Verarbeitung personenbezogener Daten in klinischen Prüfungen oder Studien erfolgt entweder

- auf Basis der durch das Gesetz verbindlich vorgegebenen Verarbeitungen (z.B. Sicherheitsberichterstattung nach Artikel 41 bis 43 CTR und Verpflichtungen zur Archivierung der Dokumentation über die klinische Prüfung nach Artikel 58 CTR) oder
- zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse gem. Art. 6 Abs. 1 lit. e DSGVO oder
- im berechtigten Interesse des Verantwortlichen gem. Art. 6 Abs. 1 lit. f i.V.m. Art. 9 Abs. 2 lit. i oder j liegt.[8]

Allerdings ist nach deutschem Recht eine Einwilligung in die Datenverarbeitung gesondert zur Einwilligung in die Teilnahme erforderlich, vgl. § 40b Abs. 6 AMG, § 29 MPDG, auch wenn der Widerruf die Datenverarbeitung nicht umfänglich verhindern kann, vgl. Art. 40b Abs. 6 Satz 2 Nr. 2 AMG, § 29 Satz 2 Nr. 2 MPDG. Im Folgenden wird daher für Deutschland von einem Einwilligungserfordernis für die Datenverarbeitung ausgegangen.

Zwischenergebnis: Das deutsche Recht fordert abweichend vom europäischen Recht eine gesonderte Einwilligung in die Verarbeitung personenbezogener Daten bei klinischen Prüfungen. Damit besteht trotz bereits erfolgter Einwilligung in die Teilnahme einer Prüfung die Notwendigkeit, vom

[7] Im Einzelnen s. u. 8.3

[8] Vgl. Nr. 14 der Stellungnahme 3/2019 des EDSA zu den Fragen und Antworten zum Zusammenspiel der Verordnung über klinische Prüfungen und der Datenschutz-Grundverordnung (DSGVO) (Artikel 70 Absatz 1 Buchstabe b), angenommen am 23. Januar 2019, abrufbar hier.

Patienten ein Opt-in bezüglich der Datenverarbeitung zu erhalten. Es wird zu einem späteren Zeitpunkt zu untersuchen sein, ob diese Abweichungen zulässig sind. Nach gegenwärtiger Rechtslage wird damit jedoch die Einhaltung der komplexen datenschutzrechtlichen Vorgaben Deutschlands Bestandteil der Genehmigungsvoraussetzungen für eine Prüfung.

2.1.3 Das Einwilligungserfordernis als Weichenstellung

Damit zeigt sich bereits an dieser Stelle eine Weichenstellung, welche in der weiteren Darstellung der erforderlichen Rechtsgrundlagen für die Datenverarbeitung in der klinischen Forschung wieder aufgegriffen werden wird (2.3.2):

- Für **Klinische Prüfungen** nach CTR/AMG und MDR sowie **Leistungsstudien** nach IVDR, ist zu untersuchen, welche Anforderungen an die **Einwilligung** der Studienteilnehmer (Opt-in) zu stellen sind, damit alle erforderlichen Datenverarbeitungsvorgänge von dieser umfasst sind, und welche gesetzlichen Regelungen für die Datenverarbeitung trotz Einwilligung einschränkend eingreifen oder noch ergänzend erforderlich sind.

- Für **nicht-interventionelle Studien und klinische Forschung außerhalb von klinischen Prüfungen** (insbesondere klinische Bewertungen nach MDR) ist hingegen zu untersuchen, auf welche Rechtsgrundlage Datenverarbeitungsvorgänge **ohne Einwilligung von Patientinnen und Patienten** (No-opt) gestützt werden kann, weil deren Einholung entweder nicht (mehr) möglich ist (z.B. bei retrospektiver Forschung mit Daten von unter Umständen bereits verstorbenen Patienten) oder einen zu großen Aufwand erzeugen würde.

Allgemein festgehalten werden kann an dieser Stelle außerdem, dass die Verarbeitung **anonymisierter Daten** ohne Rechtsgrundlage (ohne gesetzliche Grundlage oder Einwilligung) in der Regel möglich ist. Die Herausforderung liegt in der Forschung mit personenbezogenen, also pseudonymisierten oder identifizierenden Daten, z.B. bei Studien zur Wirksamkeit und Unbedenklichkeit von Arzneimitteln und Medizinprodukten, deren **Langzeitbeobachtung** der Patienten einer periodenübergreifenden Verknüpfung über den Studienzeitraum (z.B. über ein Pseudonym) bedarf.[9]

2.2 Datenflüsse innerhalb und außerhalb von klinischen Prüfungen

Die von klinischen Prüfungen verfolgten Wirksamkeitsnachweise werden durch **prospektive kontrollierte Studien** geführt. Diese haben ein typisches Setting, in dem Datenflüsse schematisch abgebildet werden können (vergleiche 4.4.1). Dies ermöglicht zugleich eine gute Bestimmung der erforderlichen Rechtsgrundlagen für die notwendigen Datenverarbeitungen. Sehr heterogen stellt sich hingegen das Forschungsgeschehen außerhalb der klinischen Prüfungen und Leistungsstudien dar (2.2.2). Dementsprechend schwieriger gestaltet sich eine Bestimmung der für das jeweilige Forschungsprojekt erforderlichen Verarbeitungsprozesse und datenschutzrechtlichen Rechtsgrundlagen.

[9] Ebenso: Pommerening/Drepper/Helbing/Ganslandt: Leitfaden zum Datenschutz in medizinischen Forschungsprojekten, 2014, S. 77.

2.2.1 Datenflussdiagramm

Die typischen Datenflüsse einer klinischen Prüfung könnten an den **Hauptakteuren** Studienteilnehmer, Sponsor und Prüfer/Studienverantwortlicher angeknüpft werden. Es sind aber **weitere Akteure** in das Diagramm mit einzubeziehen, die zumindest in einer Reihe von Studien eine gewichtige Rolle spielen. Bestimmte Aufgaben (mit Verarbeitung personenbezogener Daten) werden nämlich typischerweise nicht von dem Studienverantwortlichen übernommen (hierzu zählen insbesondere die Lagerung von Biomaterialien und das Datenmanagement). Darüber hinaus werden die Studienergebnisse zur Validierung häufig mit Behandlungsdaten von anderen medizinischen Einrichtungen, anderen Forschungseinrichtungen und Krankenkassen abgeglichen. In besonderen Fällen können auch Daten anderer Dritter (wie z.B. Register) erforderlich sein.

Für die Datenflüsse, welche regelhaft bei Durchführung klinischer Prüfungen bedient werden, sind somit die folgenden Module zu unterscheiden (Datenflussdiagramm):[10]

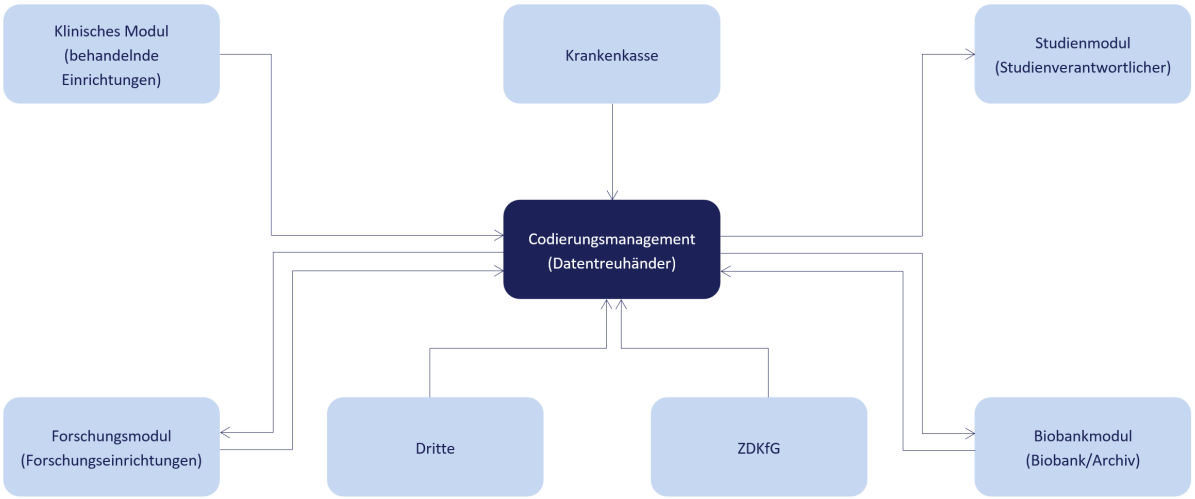

Abbildung 1: Datenflussdiagramm klinische Prüfung

(1) Das **klinische Modul** stellt Forschungsdaten aus dem normalen Behandlungsgeschehen zur Verfügung, ohne zusätzliche erhebliche Intervention zu Forschungszwecken (beispielsweise im Rahmen von Beobachtungsstudien oder der Dokumentation von Heilversuchen).

(2) Das **Forschungsmodul** stellt medizinische Daten hoher Qualität, insbesondere epidemiologische oder gesundheitspolitische Daten zur Verfügung. Das **Biobankmodul** enthält Probenbanken zusammen mit organisatorischen oder administrativen Daten zu den Proben oder Biomaterialien.

(3) Des **Studienmodul** sichert Durchführung und Administration von klinischen Forschungsprojekten.

[10] Pommerening/Drepper/Helbing/Ganslandt: Leitfaden zum Datenschutz in medizinischen Forschungsprojekten, 2014, S. 61 ff.

(4) Darüber hinaus können für das Forschungsprojekt Daten von weiteren Stellen, insbesondere von **Krankenkassen** sowie die durch das GDNG geschaffene Zentrale Datenzugangs- und Koordinierungsstelle für Gesundheitsdaten (**ZDKfG**) oder weitere **Dritte** (z.B. Register) erforderlich sein.

Das **Codierungsmanagement** oder Identitätsmanagement dient in dem Forschungsverbund dazu personenbezogene Daten korrekt zuzuordnen und dabei die Identität durch Pseudonymisierung zu verbergen.

Da in den jeweiligen Modulen mit zumindest pseudonymisierten Daten zu arbeiten ist, um eine Zuordnung zu dem jeweiligen Studienteilnehmer zu erreichen, braucht es datenschutzrechtlicher Ermächtigungsgrundlagen für die Verarbeitung dieser personenbezogenen Daten. Diese können sich aus den Verpflichtungen zur Datenverarbeitung in CTR, MDR und IVDR oder der DSGVO ergeben (s.o. 2.1.2 a. Ende).

Das Codierungsmanagement wird dabei nicht selten aus Gründen der Qualitätssicherung oder der Wirtschaftlichkeit outgesourct (**Auftragsdatenverarbeitung**) und insbesondere bei multizentrischen Studien zentral übernommen.

2.2.2 Keine typischen Abläufe bei klinischer Forschung außerhalb von klinischen Prüfungen

Aufgrund der Heterogenität klinischer Forschung außerhalb der klinischen Prüfungen (siehe oben 2.1) lassen sich außerhalb der klinischen Prüfungen und Leistungsstudien – zumindest auf den ersten Blick - keine typischen Abläufe skizzieren, welche zu einem Datenflussdiagramm zusammengeführt werden könnten. Eine datenschutzrechtliche Grundlage braucht aber auch bei dieser Forschung nur die Verarbeitung von personenbezogenen, also **pseudonymisierten Daten**. Diese liegen aber nur bei bestimmbaren Stellen, und zwar insbesondere bei Krankenkassen, medizinischen Einrichtungen und Registern (z.B. die klinischen Krebsregister). Damit zeigt sich, dass das Datenflussdiagramm auch bei der Forderung außerhalb der klinischen Prüfungen (ohne das Studienmodul) die zumindest datenschutzrechtlich relevanten Datenflüsse abbilden kann.

Es spricht vieles dafür, dass schon in naher Zukunft der Bedarf an Forschung mit personenbezogenen Daten außerhalb von klinischen Prüfungen **erheblich steigen** wird. Wesentliche Faktoren dafür sind:

- Die Möglichkeiten, insbesondere durch **automatisierte Auswertungen** mittels KI auf Bestandsdaten (sogenannte Real-World-Daten) zurückzugreifen, macht diese zur einer wesentlichen Erkenntnisquelle für eine Vielzahl von medizinischen Forschungsfragen.

- Auch deutet sich an, dass gerade bei **seltenen Erkrankungen** klinische Prüfungen eine höhere Validität ihrer Aussagen dadurch erlangen können, dass sie mit diesen Bestandsdaten zusammengeführt werden.

- Die **elektronische Patientenakte** und gesetzliche Regelungen, mit denen eine größere Transparenz über bestehende Register geschaffen wird, werden die Bedeutung der Forschung mit Bestandsdaten erheblich steigern.

Es darf somit davon ausgegangen werden, dass klinische Forschung mit personenbezogenen Daten außerhalb von klinischen Prüfungen eine erhebliche Bedeutung erlangen wird.

2.2.3 Zwischenergebnis

Die für die medizinische Forschung typischerweise erforderlichen Patientendatenflüsse sind heterogen und beruhen auf unterschiedlichen Rechtsgrundlagen. Es wird im Folgenden (ab 4. Kapitel) zu untersuchen sein, welche datenschutzrechtlichen Rechtsgrundlagen für die Verarbeitung von Patientendaten im Gesetz zu finden sind. Dann kann im Anschluss festgestellt werden, ob diese für die abgebildeten Datenflüsse hinreichende Rechtsgrundlagen bieten oder ob Hindernisse bestehen, welche durch Veränderung oder Erweiterung der datenschutzrechtlichen Befugnisse beseitigt werden können.

2.3 Wesentliche datenschutzrechtliche Einschränkungen

Einschränkungen der klinischen Forschung mit patientenbezogenen Daten können durch datenschutzrechtlich hervorgerufene überwindbare und unüberwindbare Hindernisse entstehen.

2.3.1 Überwindbare Hindernisse für Datentransfer im Zusammenhang mit Forschung

Überwindbare Einschränkungen ergeben sich immer dann, wenn Anforderungen und Zuständigkeiten **unklar** sind, weil dann entweder ein **mühsamer Aufklärungsprozess** stattfinden muss oder aufgrund der Unklarheiten zu hohe oder zu niedrige Anforderungen an die Datenverarbeitungsprozesse und deren Rechtsgrundlagen gestellt werden. Dies führt schlimmstenfalls zur Rechtswidrigkeit der Datenverarbeitung und Bußgeldern nach Art. 83 DSGVO (mit Geldbußen bis zu 20 000 000 EUR).

Darüber hinaus können lange Verfahrensdauern die Forschung erheblich **verzögern**. Insbesondere die **Zuständigkeit mehrerer Datenschutzbeauftragter** (z.B. in multizentrischen Studien) kann zu divergierenden Auffassungen über gleiche Vorgänge führen und verhindert einen Beginn des Forschungsprojekts bis zum Eingang der letzten Genehmigung.

2.3.2 Unüberwindbare Einschränkungen für Auftragsverarbeiter und Probleme der Drittlandsübermittlung

Zum Teil stehen sinnvolle und in anderen europäischen Ländern auch zulässige Datenverarbeitungen in Deutschland wegen nationaler Bestimmungen nicht zur Verfügung. Unüberwindbar sind diese Hindernisse, wenn die Anforderungen (z.B. ein zwingendes Einwilligungserfordernis) nicht erfüllt werden können. Multinationale Projekte können in diesen Fällen nur ohne deutsche Studienzentren durchgeführt werden.

Dies ist insbesondere dann nicht mehr nachvollziehbar, wenn ein großes Forschungsprojekt am Widerspruch eines einzelnen Landesdatenschutzbeauftragten oder kirchlichen Datenschutzbeauftragten scheitert. Da die jeweiligen Regelungen abhängig sind von dem Träger der medizinischen Einrichtung, greift das kirchlische Datenschutzrecht in diesen konfessionellen Häusern auch dann, wenn der Patient, welche durch diese Regelung geschützt werden soll, konfessionslos ist. Dies wirft die Frage auf, inwieweit die Regelungsbefugnisse von Ländern und Kirchen für das Datenschutzrecht in den Krankenhäusern tatsächlich Ausdruck der Subsidiarität sind.

2.4 Zwischenergebnis

Klinische Prüfungen nach CTR, MDR und Leistungsstudien nach IVDR erfordern eine prospektive kontrollierte Studie und setzen die Einwilligung der Studienteilnehmer in die Teilnahme voraus. Diese muss in Deutschland mit einer datenschutzrechtlichen Einwilligung verknüpft werden. Medizinische Forschung außerhalb der prospektiven Studien kann die Einwilligung der Patienten hingegen nur mit erheblichem Aufwand oder z.T. auch gar nicht erlangen.

Für die Prüfung, ob die aktuellen Rechtsgrundlagen den tatsächlichen Erfordernissen entsprechen, sind die Datenflüsse auf (un-)überwindbare Hindernisse für die medizinische Forschung auch untersuchbar.

3. Rechtsgrundlagen, Terminologie und Grundsätze

3.1 Maßgebliche Rechtsgrundlagen

Übergreifend gilt, dass **personenbezogene Daten**, auch in klinischen Prüfungen, nur mit einer entsprechenden Rechtsgrundlage verarbeitet werden dürfen, Art. 5 Abs. 1 lit. a) DSGVO.

Für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen, gilt – außer für kirchliche Einrichtungen – die Datenschutz-Grundverordnung (**DSGVO**). Ihre für klinische Prüfungen relevanten Rechtsgrundlagen werden **unter 4** dargelegt, wo auch das für privatwirtschaftliche Unternehmen in Deutschland und öffentliche Stellen des Bundes (neben der DSGVO) geltende Bundesdatenschutzgesetz (**BDSG**) auf seine einschlägigen Bestimmungen untersucht wird.

Für medizinische Einrichtungen in kirchlicher Trägerschaft gilt das **Datenschutzrecht der jeweiligen Kirche** (**DSG-EKD** für die Evangelische Kirche und **KDG** für die Katholische Kirche), wozu **unter 5.** ausgeführt wird.

Sofern es sich bei der medizinischen Einrichtung um eine Einrichtung in Trägerschaft eines Bundeslandes handelt, gilt für sie vorrangig das **Landesdatenschutzgesetz** des jeweiligen Bundeslandes. Für Krankenhäuser gelten unabhängig von der Trägerschaft zudem die **Landeskrankenhausgesetze** des jeweiligen Bundeslandes (s. 6.). Schließlich müssen medizinische Einrichtungen auch die straf- und **berufsrechtlichen Vorschriften** zur Schweigepflicht einhalten, wozu unter 6.3. ausgeführt wird. Abschließend werden die datenschutzrechtlichen Regelungen einzelner **für die medizinische Forschung relevanter Gesetze** untersucht (s. 8.). Neben den einzelnen Berufsordnungen für Ärzte ergeben sich keine regionalen Besonderheiten aus den Regelungen der einzelnen Kassenärztlichen Vereinigungen.

3.2 Terminologie: Datentypen

In den unterschiedlichen Rechtsquellen tauchen unterschiedliche Begriffe auf, die der Rechtsanwender ein- und zuordnen können sollte.

3.2.1 Personenbezogene (Identifizierende und pseudonymisierte) und anonyme/anonymisierte Daten

Personenbezogene Daten sind gemäß Art. 4 Nr. 1 DSGVO *„alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.“*

Die datenschutzrechtlichen Vorschriften – einschließlich des Rechtmäßigkeits- und des Zweckbindungsgrundsatzes – greifen dann nicht, wenn es sich bei den Daten nicht (mehr) um personenbezogene Daten handelt. Das ist das der Fall, wenn es sich um **anonyme oder anonymisierte Daten** handelt.

Anonym und damit nicht (mehr) personenbezogen sind Daten nur dann, wenn die Informationen sich (i) von vornherein nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder (ii) die personenbezogenen Daten in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann, vgl. ErwG 26 S. 5 DSGVO. „*Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die […] nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren, wie beispielsweise das Aussondern*“, vgl. ErwG 26 S. 4 DSGVO. „*Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind*“, vgl. ErwG 26 S. 5 DSGVO.

Anonymisierte Daten müssen von **pseudonymisierten** Daten unterschieden werden. Pseudonymisiert Daten dann, wenn sie so verarbeitet wurden, dass sie „*ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden*“, Art. 4 Nr. 5 DSGVO.

Auch wenn sie keine direkt identifizierenden Merkmale mehr enthalten, sind pseudonymisierte Daten **weiterhin personenbezogene** Daten, für die die datenschutzrechtlichen Bestimmungen gelten. Wann die Veränderung der Daten die Schwelle von Pseudonymisierung zur Anonymisierung überschreitet, hängt u.a. vom Inhalt, Umfang und der Komplexität des Datensatzes ab. So sind z.B. bestimmte Bilddaten (wie Aufnahmen von Gesichtern) oder genetische Information nur durch erhebliche Beschneidung im Sinne einer Teillöschung der Informationen – sofern überhaupt – anonymisierbar.

Identifizierende und pseudonymisierte Daten sind personenbezogene Daten und unterfallen den datenschutzrechtlichen Bestimmungen. Anonymisierte Daten sind nicht personenbezogen, sodass das Datenschutzrecht nicht auf sie anzuwenden ist. Wann Daten anonymisiert sind, ist anhand des Inhalts und des Umfangs des Datensatzes zu beurteilen. Konkrete gesetzliche Vorgaben, wann eine Pseudonymisierung oder Anonymisierung als „sicher“ gelten kann, fehlen.

3.2.2 Gesundheitsdaten, Patientendaten, genetische Daten, Geheimnisse

Gesundheitsdaten sind eine besondere Kategorie personenbezogener Daten nach Art. 9 Abs. 1 DSGVO. Gemäß Art. 4 Nr. 15 DSGVO sind Gesundheitsdaten „*personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von*

Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen". Der Begriff ist weit auszulegen und umfasst nicht nur „medizinische Daten".[11]

Zu unterscheiden ist der Begriff von dem in einigen Landesgesetzen verwendeten Begriff „**Patientendaten**". Dies ist kein Begriff der DSGVO und nicht mit dem Terminus „Gesundheitsdaten" gleichzusetzen. Patientendaten werden z.B. definiert, als „*alle Einzelangaben über persönliche oder sachliche Verhältnisse bestimmter oder bestimmbarer Patienten aus dem Bereich der Krankenhäuser*" (vgl. Art. 27 Abs. 1 S. 1 BayKrG; noch umfassender: § 43 Abs 4 LKHG BW). Sie gehen also über den Begriff der Gesundheitsdaten hinaus und umfassen z.T. sogar die Daten der Angehörigen von Patienten. Für Patientendaten gelten die Vorschriften des jeweiligen Landesgesetzes (vgl. unten Ziffer 6).

Von Gesundheitsdaten (und auch Patientendaten) zu unterscheiden sind jedoch andere in Krankenhäusern verarbeitete Daten, die keinen Gesundheits- (oder Patienten)bezug aufweisen. Hierzu gehören etwa Daten, die bereits keinen Personenbezug aufweisen (z. B. Einkaufsdaten) oder Daten, die sich zwar auf Personen nicht jedoch auf Patienten beziehen (z. B. Daten des medizinischen Personals). Für solche Daten gelten die Anforderungen des Gesundheits- (oder Patienten)datenschutzes nicht.

Genetische Daten i.S.d. Art. 4 Nr. 13 DSGVO sind „*personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern und insbesondere aus der Analyse einer biologischen Probe der betreffenden natürlichen Person gewonnen wurden*."

„**Geheimnis**" ist ein Begriff aus dem Straf- und Berufsrecht. Hierunter versteht man Einzelangaben zum persönlichen Lebensbereich eines anderen, die dem Berufsgeheimnisträger, z.B. einem Arzt, im Rahmen seiner Tätigkeit anvertraut oder bekanntgeworden sind, § 203 StGB.

Gesundheitsdaten und genetische Daten sind Begriffe der DSGVO. Patientendaten ist ein Begriff aus landeskrankenhausrechtlichen Vorschriften, der weiter ist als der Begriff der Gesundheitsdaten. Geheimnisse ist ein Begriff aus dem Straf- und Berufsrecht. Alle Begriffe beziehen sich auf personenbezogene Daten. Diese Heterogenität der Definitionen erschwert dem Forschenden eine Zuordnung und führt zu erheblicher Rechtsunsicherheit.

3.2.3 Verarbeitungszwecke, Verantwortlicher und Auftragsverarbeitung

Verarbeitung meint gemäß Art. 4 Nr. 2 DSGVO

> *„jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der*

[11] Weichert, in Kühling/Buchner, DSGVO, 2. Aufl. 2020, Art. 4 Nr. 15 Rn. 1.

Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung".

Die medizinischen Einrichtungen werden die Daten in der Regel und im Wesentlichen für die folgenden **Zwecke** verarbeiten (lassen): Versorgung und Behandlung der Patienten, Qualitätssicherung, Reporting, Meldungen an Register und Krankenkassen, Behandlungsverbesserungen und Forschungsvorhaben.

„**Verantwortlicher**" ist nach Art. 4 Nr. 7 DSGVO die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

An gleicher Stelle unter Nr. 8 wird der „**Auftragsverarbeiter**" definiert als „eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet".

3.3 Grundsätze der Datenverarbeitung nach der DSGVO

Bei jeder Verarbeitung von personenbezogenen Daten sind die **Grundsätze der Datenverarbeitung** gemäß Art. 5 DGSVO im Blick zu behalten:

- **Rechtmäßigkeit**: Personenbezogene Daten müssen auf rechtmäßige Weise verarbeitet werden, Art. 5 Abs. 1 lit. a) DSGVO. Welche rechtliche Grundlage für die Verarbeitung heranzuziehen ist, entscheidet sich nach dem Zweck, für den die Daten verarbeitet werden. Über den Zweck der Verarbeitung entscheidet derjenige, der für die Verarbeitung verantwortlich ist (vgl. Art. 4 Nr. 7 DSGVO)
- **Treu und Glauben (Fairness):** Personenbezogene Daten müssen „*nach Treu und Glauben*" verarbeitet werden, Art. 5 Abs. 1 lit. a) DSGVO. Der Grundsatz von Treu und Glauben lässt sich als Rücksichtnahmepflicht auf die Interessen der betroffenen Person verstehen und ist damit Ausprägung des Grundsatzes der Verhältnismäßigkeit. Der Verantwortliche soll die Interessen und Erwartungen der betroffenen Person berücksichtigen und nicht grundlos übergehen; Daten dürfen nicht erschlichen werden und betroffene Personen müssen in der Lage sein, ihre Rechte auszuüben.[12]
- **Transparenz**: Das Transparenzgebot aus Art. 5 Abs. 1 lit. a) DSGVO ist eine Ausprägung der Verarbeitung nach Treu und Glauben und erfordert, dass die betroffene Person Kenntnis von der Datenverarbeitung ihrer Daten hat und diese nachvollziehen kann.
- **Zweckbindung**: Das Prinzip der Zweckbindung nach Art. 5 Abs. 1 lit. b) DSGVO besteht aus zwei Hauptkomponenten, die verlangen, dass personenbezogene Daten (i) für festgelegte, eindeutige und rechtmäßige Zwecke erhoben und (ii) nicht in einer mit diesen Zwecken unvereinbaren Weise weiterverarbeitet werden. Die Verarbeitung personenbezogener Daten darf lediglich die Zwecke verfolgen, die vor der Erhebung der Daten festgelegt wurden. Nachträgliche Änderungen der Zwecke sind nur eingeschränkt möglich und bedürfen einer Rechtfertigung.

[12] Schantz, in: BeckOK DatenschutzR, 37. Ed. Stand: 01.05.2021, DS-GVO Art. 5 Rn. 8.

- **Richtigkeit**: Art. 5 Abs. 1 lit. d) DSGVO verlangt, personenbezogene Daten richtig, vollständig und – soweit erforderlich – auf dem aktuellen Stand zu speichern.
- **Datenminimierung und Angemessenheit**: Personenbezogene Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein, Art. 5 Abs. 1 lit. c) DSGVO.
- **Speicherbegrenzung**: Personenbezogene Daten müssen gelöscht oder anonymisiert werden, sobald sie für die Zwecke, für die sie erhoben wurden, nicht mehr benötigt werden, Art. 5 Abs. 1 lit. e) DSGVO. Dieses Prinzip der Speicherbegrenzung kann als der zeitliche Aspekt des Datenminimierungsprinzips angesehen werden.
- **Integrität und Vertraulichkeit:** Für personenbezogene Daten gilt das Datengeheimnis. Sie müssen im persönlichen Umgang vertraulich behandelt werden und durch angemessene organisatorische und technische Maßnahmen gegen unberechtigten Zugriff, unrechtmäßige Verarbeitung oder Weitergabe, sowie unbeabsichtigte oder unzulässige Zerstörung, Löschung, Verfälschung, Offenbarung oder nicht legitimierte Verarbeitungsformen gesichert werden, Art. 5 Abs. 1 lit. f) DSGVO.
- **Rechenschaftspflicht**: Verantwortliche haben eine Rechenschaftspflicht gemäß Art. 5 Abs. 2 DSGVO und müssen die Einhaltung der vorgenannten Grundsätze der Verarbeitung nachweisen.

Die Grundsätze der Datenverarbeitung werden durch **einzelne Pflichten** konkretisiert, insbesondere:

- Vorliegen einer Rechtsgrundlage gemäß Art. 6, 7 oder 9 DSGVO
- Gewährleistung der Betroffenenrechte (Art. 12ff. DSGVO), insbesondere
  - Information über die Datenverarbeitung (Art. 13, 14 DSGVO)
  - Auskunft über verarbeitete Daten (Art. 15 DSGVO)
  - Berichtigung verarbeiteter Daten (Art. 16 DSGVO)
  - Löschung verarbeiteter Daten (Art. 17 DSGVO)
  - Einschränkung der Verarbeitung (Art. 18 DSGVO)
  - Datenportabilität (Art. 20 DSGVO)
  - Widerspruchsrecht (Art. 21 DSGVO)
- Ggf. Abschluss erforderlicher Verträge mit
  - Gemeinsam Verantwortlichen (Art. 26 DSGVO)
  - Auftragsverarbeitern (Art. 28 DSGVO)
- Führen eines Verzeichnisses von Verarbeitungstätigkeiten (Art. 30 DSGVO)
- Gewährleistung der Sicherheit der Verarbeitung (Art. 32 DSGVO)
- Maßnahmen zur Wahrung der Betroffeneninteressen (§ 22 Abs. 2 BDSG)
- Pflicht zur Meldung von Datenschutzverletzungen (Art. 33f. DSGVO)
- Erforderlichkeitsprüfung und ggf. Durchführung einer Datenschutz-Folgenabschätzung (Art. 35 DSGVO)
- Bestellung eines Datenschutzbeauftragten (Art. 37 DSGVO)
- Erfüllung zusätzlicher Voraussetzung im Falle der Datenübermittlung in sog. Drittländer außerhalb der EU/des EWR (Art. 45ff. DSGVO).

Alle Datenverarbeitungen müssen durch eine Rechtsgrundlage legitimiert sein, mit einem angemessenen Sicherheitsniveau durchgeführt werden. Die datenschutzrechtlichen Informations-, Dokumentations- und Meldepflichten müssen eingehalten und durch entsprechende Prozesse sichergestellt sein. Es besteht Unklarheit darüber, ob die Rechtsgrundlagen in einem bestimmten Rangverhältnis zueinander stehen. In jüngerer Zeit verdichtet sich die Annahme, dass gesetzliche Rechtsgrundlagen der Einwilligung vorzuziehen sind.

4. Rechtsgrundlagen für die Verarbeitung personenbezogener Daten nach der DSGVO

Entscheidend dafür, ob personenbezogene Daten im Rahmen klinischer Forschung verarbeitet werden dürfen, ist das Vorliegen einer gesetzlichen Grundlage oder einer qualifizierten Einwilligung des Studienteilnehmers , Art. 5 Abs. 1 DSGVO.

Seit der Anwendbarkeit der DSGVO am 25. Mai 2018 regelt diese unmittelbar das deutsche Datenschutzrecht. Das Bundesdatenschutzgesetz (BDSG) enthält lediglich konkretisierende Regelungen im Rahmen der von der DSGVO eingeräumten nationalen Befugnisse. Wir werden uns zunächst deren gesetzlichen Verarbeitungsbefugnissen widmen (4.1) und dann der Einwilligung zuwenden (4.4).

4.1 Gesetzliches Verarbeitungsrecht für Gesundheitsdaten nach Art. 9 Abs. 2 DSGVO

Für Gesundheitsdaten sind die Verarbeitungsbefugnisse der DSGVO in Art. 9 geregelt. Ein gesetzliches Verarbeitungsrecht kann sich nach DSGVO daraus ergeben,

- dass die Verarbeitung zur Vertragserfüllung erforderlich ist (vgl. Art. 6 Abs. 1 lit. b oder Art. 9 Abs. 2 lit. h DSGVO) oder
- die Verarbeitung für Forschungszwecke gestattet wird (vgl. Art. 9 Abs. 2 lit. j DSGVO).
- Eine Verarbeitungspflicht (vgl. Art. 6 Abs. 1 lit. c oder Art. 9 Abs. 2 lit. b, lit. i DSGVO) kann sich auch aus gesetzlichen Melde- oder Qualitätssicherungspflichten ergeben.

Welche Rechtsgrundlagen herangezogen werden können, richtet sich auch nach der Kategorie der Daten, die verarbeitet werden. So bestehen hinsichtlich der Verarbeitung besonderer Kategorien von Daten i.S.d. Art. 9 Abs. 1 DSGVO, wozu auch die Gesundheitsdaten zählen, eingeschränktere Verarbeitungsbefugnisse als bei Daten, die nicht zu den besonderen Kategorien gehören.

Soweit die medizinische Einrichtung Verantwortlicher ist (vgl. oben 3.2.3), richtet sich die Rechtsgrundlage nach den für sie einschlägigen datenschutzrechtlichen Vorschriften. Aufgrund der verschiedenen Zwecke, zu denen bei den medizinischen Einrichtungen bei klinischen Prüfungen verarbeitet werden, kommen je nach Anwendungsfall verschiedene Rechtsgrundlagen in Betracht:

- Soweit die Datenverarbeitung erfolgt, damit die medizinische Einrichtung ihren Behandlungsvertrag gegenüber ihrem Patienten erfüllen kann, oder um einer gesetzlichen Meldepflicht, wie z.B.

Anzeigepflicht des Sponsors nach § 67 Abs. 1 S. 6 AMG, nachzukommen, kann sie die Verarbeitung auf Art. 9 Abs. 2 lit. h) DSGVO stützen.

- Soweit die Datenverarbeitung zu Qualitätssicherung erfolgt, kann die Rechtsgrundlage hierfür Art. 9 Abs. 2 lit. i) DSGVO i.V.m. der Qualitätssicherungspflicht der jeweiligen Berufsordnung für Ärzte[13] sein.
- Soweit die medizinischen Einrichtungen die Daten zu Forschungszwecken nutzen, können sie u.U. – soweit für sie keine landeskrankhausrechtlichen Spezialvorschriften gelten – Art. 9 Abs. 2 lit. j) DSGVO i.V.m. § 27 BDSG als Rechtsgrundlage heranziehen.

Während somit - abhängig von dem jeweiligen Zweck der Datenverarbeitung - verschiedene Rechtsgrundlagen nach Art. 9 Abs. 2 DSGVO in Betracht kommen, ist für die Datenverarbeitung zu Forschungszwecken insbesondere Art. 9 Abs. 2 lit. j) DSGVO relevant.

Im Folgenden werden die sich aus der DSGVO ergebenden gesetzlichen Anforderungen beim Einsatz von Auftragsverarbeitern und bei Drittlandsübermittlung (dazu 4.2) sowie bei der Verwendung von Daten für Forschungszwecke (dazu 4.3) erläutert und die Möglichkeiten und Limitationen einer Einwilligung dargestellt (4.4).

4.2 Auftragsverarbeitung und Drittlandsübermittlung

Die Anforderungen an Auftragsbearbeitung und Drittlandsübermittlung ergeben sich sowohl aus DSGVO als auch BDSG.

4.2.1 Anforderungen an die Auftragsverarbeitung nach Art. 28 Abs. 1 DSGVO

Auftragsverarbeiter i.S.d. DSGVO[14] müssen die Anforderungen des Art. 28 Abs. 1 DSGVO erfüllen, indem sie „*hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.*“ Weiterhin ist die Verarbeitung durch einen Auftragsverarbeitungsvertrag mit den gemäß Art. 28 Abs. 3 DSGVO erforderlichen Regelungsgegenständen zu vereinbaren.

Zu betonen ist außerdem, dass auch der Auftragsverarbeiter die Sicherheit der Verarbeitung gemäß Art. 32 DSGVO zu gewährleisten und auch nachzuweisen hat. Mit Blick auf eingesetzte **Unterauftragsverarbeiter** ist nach Absatz 4 des Artikels sicherzustellen, dass diese die in Art. 28 DSGVO festgesetzten Standards ebenfalls erfüllen. In jedem Fall sind nach § 27 Abs. 1 S. 2 BDSG die Anforderungen nach § 22 Abs. 2 S: 2 BDSG ergänzend zu erfüllen.

[13] Vgl. beispielhaft § 5 MBO-Ä.
[14] Zur Begriffsbestimmung s.o. 3.2.3.

4.2.2 Anforderungen an die Drittlandsübermittlung nach Art. 44 DSGVO

Dies erfordert mit Blick auf eine ggf. erfolgende Übermittlung von personenbezogenen Daten in sog. **Drittländer** außerhalb der EU zusätzliche Maßnahmen i.S.d. Art. 44 DSGVO.

Eine Drittlandsübermittlung lässt sich ggf. durch Wahl des Speicherorts und entsprechende Konfiguration der Dienste ausschließen. Ist ein Ausschluss nicht möglich, kann eine Übermittlung an Unternehmen in die USA aufgrund des **Angemessenheitsbeschlusses** der EU-Kommission vom 10.07.2023 legitimiert sein, wenn das Unternehmen unter dem neuen Datenschutzrahmen EU-USA **zertifiziert** ist.[15] Eine Übermittlung an Unternehmen, die nicht zertifiziert sind, kann sich nicht auf den Angemessenheitsbeschluss stützen.

Sofern sich eine Übermittlung in die USA oder ein anderes Drittland, nicht auf einen Angemessenheitsbeschluss stützen kann, sind **weitere zusätzliche Garantien i.S.d. Art. 46 DSGVO** einzurichten, die ein angemessenes Schutzniveau für die betroffenen Personen gewährleisten. Solche Maßnahmen können technischer, vertraglicher oder organisatorischer Natur sein. Eine vertragliche Maßnahme kann der Abschluss von Standardvertragsklauseln im Sinne von Art. 46 Abs. 2 Buchstabe c DSGVO sein, wobei diese – in Abhängigkeit der Eingriffsbefugnisse des Drittlandes – aufgrund ihrer bilateralen Natur nicht immer genügen.

4.2.3 Ergänzende Anforderungen des § 22 BDSG

§ 27 Abs. 1 S. 2 BDSG stellt folgende ergänzende Anforderung: „Der Verantwortliche sieht angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person gemäß § 22 Abs. 2 S. 2 vor." § 22 Abs. 2 S. 1 BDSG schreibt für die Verarbeitung von Gesundheitsdaten zusätzlich vor, dass „*angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person*" vorzusehen sind. Gemäß § 22 Abs. 2 S. 2 BDSG können unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen dazu insbesondere gehören:

- technisch organisatorische Maßnahmen, um sicherzustellen, dass die Verarbeitung gemäß der Verordnung (EU) 2016/679 erfolgt (§ 22 Abs. 2 Nr. 1 BDSG),
- Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt worden sind, (§ 22 Abs. 2 Nr. 2 BDSG)
- Sensibilisierung der an Verarbeitungsvorgängen Beteiligten (§ 22 Abs. 2 Nr. 3 BDSG),
- Benennung einer oder eines Datenschutzbeauftragten (§ 22 Abs. 2 Nr. 4 BDSG),
- Beschränkung des Zugangs zu den personenbezogenen Daten innerhalb der verantwortlichen Stelle und von Auftragsverarbeitern (§ 22 Abs. 2 Nr. 5 BDSG),

[15] Siehe für die Microsoft Corporation: https://www.dataprivacyframework.gov/s/participant-search/participant-detail?id=a2zt0000000KzNaAAK&status=Active.

- Pseudonymisierung personenbezogener Daten (§ 22 Abs. 2 Nr. 6 BDSG),
- Verschlüsselung personenbezogener Daten (§ 22 Abs. 2 Nr. 7 BDSG),
- 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 (§ 22 Abs. 2 Nr. 8 BDSG),
- zur Gewährleistung der Sicherheit der Verarbeitung die Einrichtung eines Verfahrens zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen (§ 22 Abs. 2 Nr. 9 BDSG) oder
- spezifische Verfahrensregelungen, die im Fall einer Übermittlung oder Verarbeitung für andere Zwecke die Einhaltung der Vorgaben dieses Gesetzes sowie der Verordnung (EU) 2016/679 sicherstellen (§ 22 Abs. 2 Nr. 10 BDSG).

Die Verarbeitung zu einem anderen Zweck als dem Zweck, zu dem die Daten erhoben wurden, ist gemäß § 24 Abs. 2 nur zulässig, wenn ein Ausnahmetatbestand nach Art. 9 Abs. 2 DSGVO vorliegt.
Hierzu wird im Abschnitt „Vereinbarkeit bei Zweckänderung“ ausgeführt (4.4.3.)

4.3 Verarbeitungsbefugnis für Forschungszwecke

Für klinische Prüfungen kommt insbesondere die **Verarbeitungsbefugnis für Forschungszwecke** nach Art. 9 Abs. 2 lit. j DSGVO i.V.m.§ 27 Abs. 1 BDSG in Betracht. § 27 Abs. 1 S. 1 BDSG gestattet die Verarbeitung für Forschungszwecke,

> *„wenn die Verarbeitung zu diesen Zwecken erforderlich ist und die Interessen des Verantwortlichen an der Verarbeitung die Interessen der betroffenen Person an einem Ausschluss der Verarbeitung erheblich überwiegen*“.

Im Rahmen der gemäß der Rechtsgrundlage in § 27 Abs. 1 BDSG erforderlichen **Interessenabwägung** stehen sich die Interessen des Verantwortlichen an der Verarbeitung den Interessen der betroffenen Personen an einem Ausschluss der Verarbeitung gegenüber. Der **Begriff der Forschung** in der DSGVO wird von der juristischen Literatur teilweise sehr **weit** ausgelegt.[16] Unter Berufung auf ErwG 159 DSGVO sollen unter anderem die technische **Entwicklung**, die **Grundlagenforschung**, die **angewandte Forschung** und die **privat finanzierte Forschung** umfasst sein.[17] Je konkreter das Forschungsvorhaben beschrieben werden kann, desto einfacher lässt sich ein Interesse (und auch ein überwiegendes Interesse) hieran begründen. Relevanz haben hierfür nicht bloß die grundrechtlich gewährleistete Forschungsfreiheit (vgl. Art. 5 Abs. 3 GG), sondern das konkrete Ziel des Forschungsvorhabens und dessen Bedeutung für das Gemeinwohl.[18] Im Rahmen der Interessenabwägung spielen auch die Umstände der Datenverarbeitung eine Rolle. So nimmt insbesondere die Schutzbedürftigkeit der betroffenen

[16] BeckOK DatenschutzR/Koch, 42. Ed. 1.11.2022, BDSG § 27 Rn. 15a; Louven, in: Taeger/Gabel, 4. Aufl. 2022, BDSG § 27 Rn. 5.
[17] BeckOK DatenschutzR/Koch, 42. Ed. 1.11.2022, BDSG § 27 Rn. 15a.
[18] BeckOK DatenschutzR/Koch, 42. Ed. 1.11.2022, BDSG § 27 Rn. 31.

Personen ab, wenn ihre Daten in pseudonymisierter Form verarbeitet werden.[19] Wird sichergestellt, dass keine Zuordnung zu den betroffenen Personen erfolgt, kann dies ein Aspekt sein, der das Überwiegen der Interessen des Verantwortlichen begründen kann.[20] Die Eingriffe in das Persönlichkeitsrecht lassen sich also reduzieren, indem die Daten nur in pseudonymisierter oder anonymisierter Form verarbeitet werden. Wir vertreten zudem die Auffassung, dass je weniger die Betroffeneninteressen von einer Verarbeitung berührt werden, desto geringere Anforderungen an die Bestimmtheit des Forschungsvorhabens zu stellen sind. § 27 Abs. 3 S. 1 BDSG verlangt, dass die Daten zu anonymisieren sind, sobald dies nach dem Forschungsvorhaben möglich ist. Teile der Literatur sehen hierin die Rechtsgrundlage für Anonymisierung besonderer Kategorien personenbezogener Daten unabhängig von einem konkreten Forschungsvorhaben.[21]

Außerdem ist strittig, ob § 27 Abs. 1 BDSG als Rechtsgrundlage für die Datenverarbeitung angesehen werden darf.[22] Die gewichtigen Stimmen, die dem widersprechen, stützen sich insbesondere auf die Gesetzesbegründung zum Datenschutz-Anpassungs-und-Umsetzungsgesetz (EU–DSAnpUG-EU)[23] Mithin bestehen **erhebliche Rechtsunsicherheiten**, wenn keine weitere Rechtsgrundlage zur Verarbeitung der Daten im Rahmen der klinischen Prüfung ersichtlich ist.

Soweit die Verarbeitung von personenbezogenen Daten zu Forschungszwecken nicht auf eine den Anforderungen nach Art. 7 DSGVO genügenden Einwilligung gestützt werden kann, ist Art. 9 Abs. 2 lit. j DSGVO i.V.m. § 27 Abs. 1 BDSG als alleinige Rechtsgrundlage umstritten und deshalb nur mit Rechtsunsicherheiten heranziehbar.

4.4 Die Einwilligung der Studienteilnehmer und deren Limitationen

Diese Unsicherheiten geben Anlass zu prüfen, ob die Rechtsgrundlage für die Verarbeitung von Daten bei Forschung und Entwicklung sich daraus ergeben könnte, dass die betroffene Person, deren Daten verarbeitet werden, hierin **einwilligt** (vgl. Art.6 Abs. 1 lit. a und Art. 9 Abs. 2 lit. a DSGVO). Rechtlich ist dies ein gangbarer Weg, dem in Deutschland auch eine Präferenz eingeräumt wird, weil dem Recht auf informationelle Selbstbestimmung (zu Unrecht) ein Vorrang von Einwilligungslösungen entnommen wird.

4.4.1 Die im *broad consent* abgebildeten Datenflüsse einer klinischen Prüfung

Ob eine Einwilligung die Verarbeitungsprozesse legitimiert, ist in erster Linie von deren Formulierung abhängig. Um einerseits sicherzustellen, dass alle für das Forschungsprojekt erforderlichen Verarbeitungsprozesse von der Einwilligung gedeckt sind und andererseits unterschiedliche Einwilligungen zu vermeiden, wurde von der Arbeitsgruppe Consent der Medizininformatik-Initiative ein Patienteneinwilligung Mustertext entwickelt (sog **broad consent**), welcher in Version 1.6d (Stand 16.04.2020)

[19] Krohm, in: Gola/Heckmann, DSGVO, 3. Aufl. 2022, § 27 BDSG Rn. 26.
[20] Krohm, in: Gola/Heckmann, DSGVO, 3. Aufl. 2022, § 27 BDSG Rn. 26.
[21] Hornung/Wagner, ZD 2020, 223, 226.
[22] Zum Streitstand vgl. BeckOK DatenschutzR/Koch, 46. Ed. 1.11.2023, BDSG § 27 Rn. 4-6.
[23] RegE DSAnpUG-EU, BT-Drs. 18/11325, S. 99.

vorliegt.[24] Aufgrund der Beteiligungen wesentlicher Forschungseinrichtungen an der Erstellung dieses Einwilligungsformulars,[25] ist die Annahme berechtigt, dass mit der auf Grundlage des Formulars ergehenden Patienten-Einwilligung alle relevanten datenschutzrechtlichen Verarbeitungsvorgänge abgedeckt werden sollen:

	Voraussetzungen/ Bedingungen	Patienteneinwilligung gem. broad consent Version 1.6d
1. Patientendaten		
Zweckbestimmung	Medizinische Forschung	1.1
Pseudonymisierung	Durch Codierung in getrennter Verwaltung (Datentreuhänder)	1.1
Verarbeitung durch	Behandelnde Einrichtung (und Datentreuhänder)	
Weitergabe an Dritte	Zur Analyse und Nutzung auch an Forschungsobjekte im Ausland (unter bestimmten Bedingungen)	1.2
Zusammenführung von Daten	Mit Daten anderer Forschungspartner (mit gesonderter Einwilligung)	1.3
2. Krankenkassendaten		
Übermittlung der Krankenversicherungsnummer	an „zuständige Stelle“ (mit gesonderter Einwilligung)	2.1
Umfang der Krankenkassendaten	über in Anspruch genommene ärztliche Leistungen der letzten 5 Jahre (mit gesonderter Einwilligung) an behandelnde Einrichtung	2.2
3. Biomaterial		
Entnahme von Biomaterial	Geringe Mengen anlässlich Routine Entnahme	3.3
Lagerung und Verarbeitung von Biomaterialien	Für medizinische Forschungszwecke	3.1/3.3
Pseudonymisierung	Durch Codierung in getrennter Verwaltung (Datentreuhänder)	3.1
Weitergabe an Dritte	Zur Analyse und Nutzung auch an Forschungsobjekte im Ausland (unter bestimmten Bedingungen)	3.2

[24] Abzurufen unter: www.medizininformatik-initiative.de/sites/default/files/2020-04/MII_AG-Consent_Einheitlicher-Mustertext_v1.6d.pdf (Abruf am 17.12.2023)

[25] Vgl. https://www.medizininformatik-initiative.de/de/ueber-die-initiative

Zusammenführung von Daten	Mit Daten anderer Forschungspartner (mit gesonderter Einwilligung)	3.2
Eigentum	Übertragung an Biobank/Archiv	3.3

4.4.2 Voraussetzungen und Limitationen der Einwilligung

Gleichwohl zeigt auch diese, möglichst breit angelegte Einwilligung als Rechtsgrundlage für Verarbeitungsprozesse in der Forschung einige Voraussetzungen und Limitationen:

- Die Einwilligung muss **vor** der Verarbeitung der Daten eingeholt werden. Praktisch bedeutet das, dass bevor die Behandlung eines Patienten beginnt, dieser über die (weiteren) Zwecke, für die seine Daten verwendet werden sollen, aufgeklärt werden und er seine Einwilligung entsprechend erteilen muss.
- Aufgrund des **Kopplungsverbots** darf die Einwilligung nicht an die Behandlung des Patienten gebunden werden, vgl. Art. 7 Abs. 2 und 4 DSGVO. Dem Patienten steht es daher frei, nein zu sagen.
- Gleichzeitig ist es möglich, dass zum Zeitpunkt der Datenerhebung noch **nicht alle Zwecke** der Datenverarbeitung bekannt sind, sodass über diese nicht aufgeklärt werden kann mit der Folge, dass die Einwilligung für weitere, mit den ursprünglichen nicht vereinbare Zwecke[26] keine Geltung entfaltet.[27]
- Schließlich würde eine einwilligungsbasierte Verarbeitung erfordern, dass ggf. eine **Kontaktaufnahme mit Altpatienten** erforderlich ist, um für bereits vorhandene Daten eine Einwilligung abzufragen. Eine solche Kontaktaufnahme ist nicht in jedem Fall zulässig und hat in der Regel auch nur sehr geringe Rücklaufquoten.
- Soweit eine Einwilligung vorliegt, muss auch dafür Sorge getragen werden, dass der Patient durch einen **Widerruf der Einwilligung** die Datenverarbeitung und die Löschung der Daten erreichen kann. Dies erfordert spezifische Prozesse zur differenzierten Verarbeitung der entsprechenden Daten.

Soweit eine Legitimierung der Verarbeitung personenbezogener Daten über eine Einwilligung erfolgen soll, ist streng darauf zu achten, dass **sämtliche Datenverarbeitungsvorgänge** bei allen mit personenbezogenen Daten arbeitenden **Stellen** mit der **konkreten Zwecksetzung** der Verarbeitung von der Einwilligung umfasst sind.

Insgesamt betrachtet bietet die Einwilligung von Studienteilnehmern in die Verarbeitung ihrer Daten bei prospektiven klinischen Prüfungen einen probaten Weg zur Erreichung einer Rechtsgrundlage, weil Art. 7 Abs. 1 lit. a CTR für diese ohnehin eine Einwilligung (in die Studienteilnahme) vorsieht, welche zeitgleich erfolgen kann. Gleichwohl kann auch hier der Teilnehmer die Einwilligung verweigern oder

[26] Zur Vereinbarkeitsprüfung gem. Art. 6 Abs. 4 DSGVO vgl. 4.4.3.
[27] Vgl. Gutachten des Sachverständigenrates aus 2021 (Digitalisierung für Gesundheit), Rn. 460.

später widerrufen; eine unzureichende Aufklärung oder die fehlende Abbildung von Verarbeitungsvorgängen und-Zwecken kann diese (in Teilen) unwirksam machen. Da auch die Zusammenführung von Daten als Verarbeitung anzusehen ist, stellt die Einwilligung in diese dann eine besondere Herausforderung dar, wenn sogenannte Real World Data mit Studiendaten abgeglichen werden sollen. Keinesfalls kann die Einwilligung bindende gesetzliche Bestimmungen aufheben.

Verlangt die Forschung keine Einwilligung (insbesondere bei nicht interventionellen Studien und klinischer Forschung außerhalb von Studien) wäre die Erforderlichkeit einer datenschutzrechtlichen Einwilligung eine erhebliche Barriere zur Durchführung des Projekts. So führte bereits das Gutachten des Sachverständigenrates aus 2021 (Digitalisierung für Gesundheit, Rn. 454) wie folgt aus:

> *„Die Regelungen für die einwilligungsunabhängige Nutzung von Gesundheitsdaten für Forschungszwecke verteilen sich in Deutschland auf zahlreiche Gesetze. Dazu gehören die allgemeinen Datenschutzgesetze und darin enthaltene Forschungsklauseln des Bundes und der Länder, spezifische Regelungen in Spezialgesetzen[28], die Landeskrankenhausgesetze und das Kirchenrecht, das auf Gesundheitseinrichtungen in kirchlicher Trägerschaft anwendbar ist. Der gesetzliche Rahmen einer Nutzung von Daten durch die Forschung variiert daher je nach Art und ursprünglichem Erhebungszweck der Daten. Dadurch entsteht eine unübersichtliche Rechtslage, die die Umsetzung von Forschungsprojekten erschwert.“*

Im Ergebnis muss die Einwilligung außerhalb prospektiver klinischer Studien als unrealistische Verarbeitungsgrundlage betrachtet werden. Innerhalb von klinischen Prüfungen ist sie aufgrund der oben dargestellten Einwilligungserfordernisse leicht erreichbar. Probleme können auftreten, wenn Forschungszwecke zu Beginn der Studien nicht erkennbar und deshalb im weiteren Verlauf im Vergleich zur Einwilligung verändert werden müssen. Die Zweckänderung muss deshalb vertieft untersucht werden, um die Geeignetheit der Einwilligung bei klinischen Prüfungen sachgerecht einschätzen zu können.

4.4.3 Vereinbarkeit bei Zweckänderung aufgrund Einbeziehung der Daten in andere Forschungsprojekte nach DSGVO

Eine Schwierigkeit der Einwilligung, nämlich die Unvorhersehbarkeit der Verarbeitungszwecke, könnte überwunden werden, wenn auch eine spätere Zweckänderung zulässig wäre.

4.4.3.1 Zweckbindungsgebot

Das Zweckbindungsgebot nach Art. 5 Abs. 1 lit b) DSGVO scheint dem zu widersprechen, denn es lautet:

---

[28] Arzneimittelgesetz, das Medizinproduktegesetz, das Strahlenschutzgesetz, das Gendiagnostikgesetz, das Transfusionsgesetz, Regelungen zum Umgang mit Daten im ersten, fünften und zehnten Sozialgesetzbuch sowie im Strafgesetzbuch, s. u. 8.2 und 8.3.

„Personenbezogene Daten müssen … für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden.“

Lässt sich der Zweck der Forschung nicht in dem der ursprünglichen Einwilligung abbilden, bedarf es deshalb grundsätzlich einer ergänzenden Einwilligung des Studienteilnehmers, wenn keine andere Rechtsgrundlage für die Verarbeitung seiner Daten zu den Zwecken der eigenen Forschung besteht. Eine Datenverarbeitung kann nach DSGVO aber andererseits auch rechtmäßig sein, wenn der Zweck der Verarbeitung von dem Zweck, zu dem die Daten ursprünglich erhoben und verarbeitet wurden, abgedeckt wird.

4.4.3.2 Vereinbarkeitsprüfung nach Art. 6 Abs. 4 DSGVO

Um dies zu prüfen, muss bei der Weiterverarbeitung für andere Zwecke der Verantwortliche eine **Vereinbarkeitsprüfung** nach Art. 6 Abs. 4 DSGVO unter Berücksichtigung der folgenden Aspekte vornehmen:

- *„jede Verbindung zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung,*
- *den Zusammenhang, in dem die personenbezogenen Daten erhoben wurden, insbesondere hinsichtlich des Verhältnisses zwischen den betroffenen Personen und dem Verantwortlichen,*
- *die Art der personenbezogenen Daten, insbesondere ob besondere Kategorien personenbezogener Daten gemäß Artikel 9 verarbeitet werden oder ob personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 verarbeitet werden,*
- *die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen,*
- *das Vorhandensein geeigneter Garantien, wozu Verschlüsselung oder Pseudonymisierung gehören kann.“*

Jede Weiterverarbeitung muss anhand dieser Maßstäbe geprüft, begründet und dokumentiert werden. Die Weiterverarbeitung bedarf ebenfalls einer Rechtsgrundlage, vgl. Art. 5 Abs. 1 lit. a DSGVO.

Mit Blick auf **nicht-besondere Kategorien** von Daten kann die Weiterverarbeitung ggf. auf ein berechtigtes Interesse (z.B. Auswertungen zu Qualitätssicherung oder Produktverbesserung) i.S.d. Art. 6 Abs. 1 lit. f DSGVO gestützt werden. Hierfür ist das Vorliegen des berechtigten Interesses und die Abwägung der Interessen (Verarbeitungsinteresse des Verantwortlichen der klinischen Prüfung vs. Interesse der Betroffenen an der Nichtverarbeitung ihrer Daten) zu dokumentieren.

Eine Erhebung zu Behandlungszwecken erfolgt (ohne ausdrückliche separate Einwilligung) nicht auch zum Zweck der Forschung. Da die Forschung der behandelten Person praktisch bisher kaum zugute kam, weil die Ergebnisse derselben erst dann vorlagen, wenn diese nicht mehr therapiert wird, bestand bislang keine oder allenfalls eine geringe Verbindung der Zwecke im Sinne des ersten Aspekts. Dies wird sich in naheliegender Zukunft ändern, wenn Versorgung und Forschung mehr in ein Kontinuum übergehen. Auch ein „Zusammenhang“ zwischen den Zwecken ist eher fernliegend, da der Patient

nicht damit zu rechnen braucht, dass seine Daten auch zu Forschungszwecken verwendet werden. Soweit Behandlungsdaten zu Forschungszwecken genutzt werden sollen, ist deshalb in aller Regel nicht von einer zulässigen Zweckänderung auszugehen.

Eine Zweckänderung könnte allerdings darin liegen, dass die Daten, welche ursprünglich für eine klinische Prüfung zulässig verarbeitet wurden, für andere Forschungszwecke an Dritte weitergeleitet worden (unter Umständen zur Verbindung mit weiteren Daten). Auch in diesem Fall sind die Voraussetzungen im Einzelfall nach **Vereinbarkeitsprüfung** gem. Art. 6 Abs. 4 DSGVO zu belegen.

4.4.3.3 Forschungsprivileg nach Art. 5 Abs. 1 lit b) DSGVO

Jenseits einer Vereinbarkeit mit dem ursprünglichen Verarbeitungszweck könnte aber eine zulässige Verarbeitung der Studiendaten zu Forschungszwecken auch von dem Forschungsprivileg nach Art. 5 Abs. 1 lit b) DSGVO ermöglicht werden.

Art. 5 Abs. 1 lit b) DSGVO eröffnet nämlich eine **Weiterverarbeitung zu wissenschaftlichen Zwecken**, indem er bestimmt, dass

> "[…] *eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für **wissenschaftliche** oder historische **Forschungszwecke** oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken („Zweckbindung“);*“
>
> (Hervorhebung durch Verfasser)

Auch wenn die Regelung zum Teil kritisiert wird,[29] wird sie doch überwiegend als durch das öffentliche Interesse an der Forschung begründet und durch die besonderen Garantien nach Art. 89 Abs. 1 DSGVO hinreichend geschützt angesehen.[30]

4.4.4 Zusammenfassung zur Einwilligung als Rechtsgrundlage bei klinischen Prüfungen

Die Einwilligung bietet bei prospektiven klinischen Studien, die ohnehin eine Einwilligung der Studienteilnahme bedürfen, **eine Rechtsgrundlage** für die Verarbeitungsprozesse im Rahmen der klinischen Forschung.

Schwierigkeiten ergeben sich aber immer dann, wenn die ursprüngliche Studienplanung sich verändert und dadurch weitere Module oder Verarbeitungsprozesse mit einbezogen werden müssen. Die verarbeitenden Stellen und die dort verarbeitenden personenbezogenen Daten sind zuweilen bei Beginn der Studie nicht hinreichend klar zu bestimmen. Sollen Daten zur Validierung der Ergebnisse etwa mit vorhandenen Krankenkassendaten abgeglichen werden, ist dies nur zulässig, wenn die Einwilligung diesen Verarbeitungsprozess bereits umfasst. Dies ist im Einzelfall durch Vereinbarkeitsprüfung gem. Art. 6 Abs. 4 DSGVO zu bestimmen, die aber rechtlichen Unsicherheiten verbunden ist. Zwar enthält

[29] So BeckOK DatenschutzR/Schantz DS-GVO Art. 5 Rn. 22.
[30] Vgl. statt aller: Kühling/Buchner/Herbst, 4. Aufl. 2024, DS-GVO Art. 5 Rn. 52.

Art. 5 Abs. 1 lit b) DSGVO ein Forschungsprivileg, welches in seiner Bedeutung aber rechtlich umstritten ist.

4.5 Zwischenergebnis

Soweit die Verarbeitung von personenbezogenen Daten zu Forschungszwecken sowie die Auftragsverarbeitung und die Drittlandsübermittlung nicht auf eine den Anforderungen nach Art. 7 DSGVO genügende Einwilligung gestützt werden kann, ist Art. 9 Abs. 2 lit. j DSGVO i.V.m.§ 27 Abs. 1 BDSG als alleinige Rechtsgrundlage heranziehbar, welche aber umstritten und deshalb nur mit erheblichen Rechtsunsicherheiten genutzt werden kann.

Die Einbeziehung von Behandlungsdaten in Forschungsprojekte wird ohne gesonderte Einwilligung regelmäßig an der fehlenden Vereinbarkeit gem. Art. 6 Abs. 4 DSGVO der neuen Zwecksetzung im Vergleich zum Behandlungszweck scheitern.

Eine (Unter-) Auftragsverarbeitung muss den Anforderungen des Art. 28 DSGVO genügen; eine Drittlandsübermittlung, welche sich nicht auf einen Angemessenheitsbeschluss stützen kann, erfordert weitere zusätzliche Garantien i.S.d. Art. 46 DSGVO.

Die DSGVO enthält für die klinische Forschung immer noch Rechtsunsicherheiten.

5. Kirchliches Datenschutzrecht

Öffentlich-rechtliche Religionsgemeinschaften sind berechtigt, ihre Angelegenheit innerhalb der Schranken der für alle geltenden Gesetze selbständig zu ordnen und zu verwalten (Art. 140 GG iVm Art 137 Abs. 3 Weimarer Reichsverfassung). Die evangelische Kirche (s. 5.1) und die katholische Kirche (s. 5.25.2) haben von diesem Recht Gebrauch gemacht.

5.1 Vorgaben aus DSG-EKD

Für Einrichtungen in evangelischer Trägerschaft gilt das Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD).[31]

5.1.1 Verarbeitung für Forschungszwecke

§ 7 Abs. 1 Nr. 9 DSG-EKD gestattet ausdrücklich die zweckveränderte Verarbeitung für Forschungszwecke, wenn sie „*zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse der betroffenen Person an dem Ausschluss der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann*“. Es gelten die Ausführungen zu § 27 BDSG entsprechend (vgl. oben unter Abschnitt „Vereinbarkeit bei Zweckänderung“; 4.4.3).

[31] Vom 15. November 2017 (ABl. EKD S. 353, 2018 S. 35, S. 215) geändert am 24. Juni 2021 (ABl. EKD S. 158), zuletzt geändert am 9. November 2022 (ABl. EKD S. 156)

Gemäß § 13 Abs. 2 Nr. 10 DSG-EKD müssen die Interessen außerdem durch angemessene Maßnahmen gewahrt werden. Dies wird bei Einhaltung des Art. 32 DSGVO der Fall sein.

5.1.2 Einsatz von Auftragsverarbeitung

Die Vorgaben zur Auftragsverarbeitung der Evangelischen Kirche gemäß § 30 DSG-EKD entsprechen im Wesentlichen denen des Art. 28 DSGVO. Gemäß § 30 Abs. 5 Satz 3 DSG-EKD muss sich der Auftragsverarbeiter aber der kirchlichen Datenschutzaufsicht unterwerfen. Hierfür muss der Auftragsverarbeiter einen Vertragszusatz für Einrichtungen in evangelischer Trägerschaft vorhalten.

5.1.3 Zwischenergebnis

Das Datenschutzrecht der evangelischen Kirche nach DSG-EKD sieht keine wesentlichen Änderungen gegenüber dem durch DSGVO und BDSG gesetzten Rechtsrahmen vor. Allerdings muss ein Auftragsverarbeiter einen Vertragszusatz für Einrichtungen in evangelischer Trägerschaft vorhalten und erforderliche Abstimmungen mit den jeweiligen kirchlichen Datenschutzbeauftragten nach § 39 DSG-EKD vornehmen.

5.2 Vorgaben des KDG

Für Einrichtungen in katholischer Trägerschaft gilt das Gesetz über den kirchlichen Datenschutz der Katholischen Kirche in Deutschland (KDG), [32] welches in den jeweiligen Diözesen adaptiert Anwendung findet.[33]

5.2.1 Verarbeitung für Forschungszwecke

§ 11 Abs. 2 lit. j KDG entspricht Art. 9 Abs. 2 lit. j DSGVO und ermöglicht die Verarbeitung für Forschungswecke, sofern eine Rechtsvorschrift dies gestattet. § 6 Abs. 2 lit. i) KDG enthält eine § 7 Abs. 1 Nr. 9 DSG-EKD entsprechende Regelung. Es gelten daher auch hier die Ausführungen zu § 27 BDSG (vgl. oben im Abschnitt „Vereinbarkeit bei Zweckänderung“ 4.4.3). § 54 Abs. 2 KDG gestattet ausdrücklich die Offenlegung personenbezogener Daten für Forschungszwecke an Stellen außerhalb der Kirche, sofern diese sich verpflichten, die Daten nicht für andere Zwecke zu verwenden.

5.2.2 Einsatz von Auftragsverarbeitung

Die Vorgaben zur Auftragsverarbeitung der Katholischen Kirche gemäß § 29 KDG entsprechen im Wesentlichen denen des Art. 28 DSGVO. Allerdings beschränkt § 29 Abs. 11 KDG den Einsatz von Auftragsverarbeitern mit Drittlandsbezug. Die Verarbeitung in einem Drittland ist zulässig, *„wenn ein Angemessenheitsbeschluss der Europäischen Kommission […] vorliegt oder wenn die Datenschutzaufsicht selbst oder eine andere Datenschutzaufsicht festgestellt hat, dass dort ein angemessenes*

[32] Vom 29. Dezember 2017.

[33] So z.B. Gesetz über den Kirchlichen Datenschutz (KDG) für die Diözese Aachen vom 15. Februar 2018 veröffentlicht im Amtsblatt 3 vom 01. März 2018.

Datenschutzniveau besteht“. Der Einsatz Dienstleistern in Drittländern ist daher nur unter strengeren Einschränkungen als nach dem DSG-EKD möglich.

5.2.3 Zwischenergebnis

Die Verarbeitung für Forschungszwecke kann bei Vorliegen einer positiven Interessenabwägung auf § 6 Abs. 2 lit. i) i.V.m. § 11 Abs. 2 lit. j und § 54 KDG gestützt werden. Stellen außerhalb der Kirche müssen sich verpflichten, die Daten nicht für andere Zwecke zu verwenden.

Der Auftrag von Auftragsverarbeitern in Drittländern ohne Angemessenheitsbeschluss ist nur zulässig, wenn eine Datenschutzaufsicht festgestellt hat, dass ein angemessenes Datenschutzniveau vorliegt.

Zuständig für die Datenschutzaufsicht in den katholischen Diözesen ist der nach § 42 KGG zu benennende Diözesandatenschutzbeauftragte.

6. Vorgaben aus Landesgesetzen

6.1 Rechtsgrundlage für eine Übermittlung zu Forschungszwecken

Die folgenden Ausführungen beschreiben, unter welchen Voraussetzungen medizinische Einrichtungen gemäß etwaig einschlägigen Landesdatenschutz- oder Landeskrankenhausgesetzen i.V.m. Art. 9 Abs. 2 lit. j) DSGVO i.V.m. § 27 Abs. 1 Satz 1 BDSG personenbezogene Daten zum Zwecke der Verarbeitung für Forschungszwecke zur Verfügung stellen können.

6.1.1 Baden-Württemberg

Gemäß dem Wortlaut des § 43 Abs. 3 LKHG BW finden die besonderen datenschutzrechtlichen Vorschriften für die Datenverarbeitung in Krankenhäusern in §§ 43 ff. LKHG BW auf die Datenverarbeitung für Zwecke wissenschaftlicher Lehre oder Forschung keine Anwendung. Gleichwohl ist nach § 46 Abs. 1 Satz 1 Nr. 2a LKHG BW die Übermittlung, Offenlegung oder anderweitige Zugänglichmachung der Patientendaten an Personen und Stellen außerhalb des Krankenhauses zur Durchführung medizinischer Forschungsvorhaben des Krankenhauses erlaubt. Die im offenen Widerspruch zum § 43 Abs. 3 LKHG BW stehende Vorschrift des § 46 Abs. 1 Satz 1 Nr. 2a LKHG BW wurde in das LKHG BW mit Gesetz vom 23.05.2000 nachträglich eingefügt und verdrängt aufgrund des Grundsatzes „*lex posterior derogat legi priori*“ die ältere am 28.07.1999 beschlossene Regelung des § 43 Abs. 3 LKHG BW. Soweit gemäß § 46 Abs. 1 Satz 2 LKHG BW die Ziele des Forschungsvorhabens nicht mit anonymisierten Daten erreicht werden können und dem Forschungsvorhaben keine überwiegenden schutzwürdigen Interessen des Betroffenen entgegenstehen, kann die Übermittlung der Patientendaten an Personen und Stellen außerhalb des Krankenhauses zur Durchführung medizinischer Forschungsvorhaben somit auf § 46

Abs. 1 Satz 1 Nr. 2a LKHG BW gestützt werden. Im Umkehrschluss dürfen anonymisierte Daten uneingeschränkt Dritten zur Verfügung gestellt werden.

Für die Verarbeitung (hier noch in der alten Terminologie: „Erhebung, Speicherung, Veränderung und Nutzung“) der Patientendaten wird in § 45 LKHG BW keine Ausnahme für die Durchführung wissenschaftlicher Forschungsvorhaben von dem Grundsatz des § 43 Abs. 3 LKHG BW vorgesehen. Die Rechtsgrundlage für die Verarbeitung personenbezogener Daten zu einem wissenschaftlichen Forschungszweck in einem Krankenhaus (in öffentlicher Trägerschaft) ergibt sich somit aus § 13 Abs. 1 Landesdatenschutzgesetz Baden-Württemberg (LDSG BW), vgl. § 2 Abs. 3 Satz 1 LDSG BW. Auf § 13 Abs. 1 LDSG BW kann die Verarbeitung personenbezogener Daten durch öffentliche Stellen zu einem wissenschaftlichen Forschungszweck gestützt werden, wenn „*die Zwecke auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden können*“ und die Interessen der öffentlichen Stelle an der Durchführung des Forschungsvorhabens „*die Interessen der betroffenen Person an einem Ausschluss der Verarbeitung überwiegen*“. Gemäß § 13 Abs. 2 LDSG BW sind die Daten zu anonymisieren, oder zumindest zu pseudonymisieren, sobald dies nach dem Forschungszweck möglich ist.

Hieraus ergibt sich die Diskrepanz, dass das Krankenhaus Daten für wissenschaftliche Forschungszwecke nach § 13 Abs. 1 LDSG BW verarbeiten kann, die Daten gemäß § 46 Abs. 1 Satz 1 Nr. 2a LKHG BW jedoch nur für Forschungszwecke *des Krankenhauses* an Dritte – die nicht Auftragsverarbeiter sind – übermitteln darf.

Die Regelung des § 13 Abs. 1 LDSG BW entspricht der des § 27 BDSG. Wir gehen daher davon aus, dass das Krankenhaus eine Anonymisierung der Daten auch auf § 13 Abs. 1 LDSG BW stützen darf, sofern es nicht bereits durch das implizite Anonymisierungserfordernis aus § 46 Abs. 1 Satz 1 a.E. LKHG BW hierzu berechtigt ist. Das Krankenhaus kann sich unter den Bedingungen von § 48 LKHG BW auch eines Auftragsverarbeiters bedienen.

In Baden-Württemberg sind Krankenhäuser gesetzlich legitimiert, Daten für Forschungszwecke zu anonymisieren und die anonymisierten Daten Dritten zur Verfügung zu stellen.

Die Übermittlung nicht-anonymisierter Daten an Dritte und nachfolgende Speicherung und Verarbeitung durch diese sind nur für Forschungsvorhaben des Krankenhauses gestattet. Für die Verarbeitung für Forschungsvorhaben Dritter ist eine Einwilligung erforderlich.

6.1.2 Bayern

In Bayern dürfen gemäß Art. 27 Abs. 4 S. 1 BayKrG die Krankenhausärzte die Patientendaten nutzen, soweit dies zu Forschungszwecken im Krankenhaus oder im Forschungsinteresse des Krankenhauses erforderlich ist. Sie können gemäß Art. 27 Abs. 4 S.2 a.E. BayKrG anderen Personen die Nutzung der Patientendaten gestatten, soweit dies zur Durchführung des Forschungsvorhabens erforderlich ist und die Patientendaten im Gewahrsam des Krankenhauses verbleiben. Gemäß Art. 27 Abs. 2 Satz 1 BayKrG dürfen die Patientendaten nur erhoben und aufbewahrt werden, soweit dies zur Erfüllung der

Aufgaben des Krankenhauses oder im Rahmen des krankenhausärztlichen Behandlungsverhältnisses erforderlich ist oder die betroffene Person eingewilligt hat.

In Ermangelung einer Rechtsgrundlage für die Verarbeitung zu Forschungszwecken, die nicht des Krankenhauses eigene Zwecke sind, kann weder eine Anonymisierung noch die Übermittlung an eine Stelle außerhalb ihrer Tätigkeit als Auftragsverarbeiterin auf eine gesetzliche Grundlage gestützt werden. Die Verarbeitung für diese Zwecke bedarf daher einer Einwilligung der betroffenen Personen.

In Bayern dürfen Patientendaten nur für krankenhauseigene Zwecke verarbeitet werden. Auch eine Anonymisierung darf nur für krankenhauseigene Zwecke erfolgen.

Die Übermittlung nicht-anonymisierter Daten an Dritte und nachfolgende Speicherung und Verarbeitung durch diese sind nur für Forschungsvorhaben des Krankenhauses gestattet. Für die Verarbeitung für Forschungsvorhaben Dritter ist eine Einwilligung erforderlich.

6.1.3 Berlin

Die Datenverarbeitung zu Forschungszwecken ist für Berliner Krankenhäuser in § 25 BlnLKG geregelt. Dieser wurde im Rahmen des BlnDSAnpG-EU neugefasst. In seiner Begründung bezieht sich der Gesetzgeber auf die „*erforderlichen Anpassungen an die Begriffsbestimmungen und Regelungen*“[34] der DSGVO. Diese Formulierung legt nahe, dass der § 25 BlnLKG (neu) nur begriffliche, jedoch keine inhaltlichen Änderungen zu seiner Vorgängerfassung enthält.

Die Zulässigkeit von der Übermittlung von Daten für „*einrichtungsübergreifende Forschungsvorhaben, Forschungsregister oder Probensammlungen*“ richtet sich nach § 25 Abs. 3 BlnLKG. Genetische Daten und Gesundheitsdaten im Sinne des Art. 9 DSGVO dürfen gemäß § 25 Abs. 3 BlnLKG jedoch nur „*unter den Voraussetzungen des Absatzes 1*“ übermittelt werden. Eine Übermittlung von Daten betroffener Personen an den Verantwortlichen ist also „*unter den Voraussetzungen*“ des § 25 Abs. 1 BlnLKG zulässig. Wie auch die Altfassung enthält § 25 Abs. 1 BlnLKG vier Fälle, in denen die Verarbeitung zu Forschungszwecken ohne die Einwilligung der betroffenen Person zulässig ist:

(i) Ärztinnen und Ärzte, die an der Behandlung beteiligt waren, nutzen die Daten für eigene wissenschaftliche Forschungsvorhaben, § 25 Abs. 1 Nr. 1 BlnLKG,

(ii) das Einholen der Einwilligung ist nicht zumutbar, § 25 Abs. 1 Nr. 2 BlnLKG,

(iii) es besteht ein überwiegendes berechtigtes Interesse der Allgemeinheit, § 25 Abs. 1 Nr. 3 BlnLKG, oder

(iv) die Daten sind anonymisiert worden, § 25 Abs. 1 Nr. 4 BlnLKG.

[34] Berliner Abgeordnetenhaus Drs. 18/2598, S. 119, abrufbar unter: https://www.parlament-berlin.de/ados/18/IIIPlen/vorgang/d18-2598.pdf.

Damit das Krankenhaus sich auf § 25 Abs. 3 Satz 1 BlnLKG berufen können, muss sichergestellt werden, dass pseudonymisierte Daten nicht wieder mit den identifizierenden Daten zusammengeführt werden können.

In Berlin dürfen Krankenhäuser personenbezogene Daten für eigene Forschungszwecke verarbeiten und u.a. auch anonymisieren. Krankenhäuser dürfen außerdem pseudonymisierte Daten für Forschungsregister an Dritte übermitteln.

Die Verarbeitung pseudonymisierter Daten durch Stellen außerhalb des Krankenhauses bedarf der gesonderten gesetzlichen Grundlage oder Einwilligung.

6.1.4 Brandenburg

Gemäß § 25 Abs. 1 BbgDSG dürfen bei überwiegendem Forschungsinteresse personenbezogene Daten für Forschungszwecke verwendet werden. Die Vorschrift entspricht in diesem Punkt § 27 Abs. 1 BDSG. Nach ihr ist also grundsätzlich auch eine Übermittlung der Daten an Dritte gestattet. Dieser Grundsatz wird allerdings durch § 31 BbgKHEG eingeschränkt. Danach ist eine Offenlegung nur zulässig, wenn die zuständige Rechtsaufsichtsbehörde das Vorliegen der Voraussetzungen des § 25 Abs. 1 BbgDSG bestätigt hat.

In Brandenburg dürfen Krankenhäuser personenbezogene Daten für eigene Forschungszwecke verarbeiten.

Krankenhäuser dürfen Daten nur an Dritte übermitteln, wenn die zuständige Rechtsaufsicht das Vorliegen der Voraussetzungen des § 25 Abs. 1 BbgDSG (überwiegendes Forschungsinteresse) bestätigt hat.

6.1.5 Bremen

§ 39 Abs. 1 BremKrhG gestattet zunächst die Eigenforschung mit Patientendaten durch die Krankenhausärzte. § 39 Abs. 2 BremKrhG regelt, dass die Übermittlung an Dritte ohne Einwilligung des Patienten zulässig ist, *„wenn es nicht zumutbar ist, die Einwilligung einzuholen, und der Zweck eines bestimmten Forschungsvorhabens nicht auf andere Weise erfüllt werden kann*.“ In diesem Fall bedarf die Übermittlung der Patientendaten der Zustimmung der zuständigen Behörde. Die Zustimmung darf nur erteilt werden, wenn das berechtigte Interesse der Allgemeinheit an der Durchführung des Forschungsvorhabens das Geheimhaltungsinteresse des Patienten erheblich überwiegt.

In Bremen dürfen Krankenhäuser personenbezogene Daten für eigene Forschungszwecke verarbeiten.

Krankenhäuser dürfen Daten nur an Dritte übermitteln, wenn es nicht zumutbar ist, die Einwilligung einzuholen und die zuständige Behörde ihre Zustimmung erteilt hat, wobei die Zustimmung nur bei überwiegendem Forschungsinteresse erteilt werden darf.

6.1.6 Hamburg

§ 12 Abs. 1 S. 1 HmbKHG privilegiert die Eigenforschung von Krankenhäusern und Krankenhausgruppen, einschließlich von Kooperationsvorhaben mit anderen, externen Forschungseinrichtungen.[35] Die Privilegierung greift jedoch nur, wenn diese Verarbeitung zu Forschungszwecken durch Krankenhäuser in Hamburg erfolgt.[36] § 12 Abs. 1 S. 2 HmbKHG regelt als Ausnahmetatbestand von dem Verbot des Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 die Verarbeitung zu Forschungszwecken für den Fall des überwiegenden Interesses. Hierunter kann auch die Weitergabe der Daten zu Forschungszwecken fallen. Gestattet ist die Weitergabe sogar für (nicht konkretisierte) Datensammlungen, wenn die Daten zuvor anonymisiert wurden, § 12 Abs. 1 S. 4 HmbKHG. Mit einem Verweis auf die nach § 22 Abs. 2 BDSG zu treffenden Maßnahmen wird der Anforderung Rechnung getragen, dass geeigneten Garantien für die Rechte und Freiheiten für betroffenen Person bestehen.[37]

In Hamburg dürfen Krankenhäuser personenbezogene Daten für eigene Forschungszwecke verarbeiten, wenn das Forschungsinteresse überwiegt.

6.1.7 Hessen

In Hessen ist die Verarbeitung von personenbezogenen Gesundheitsdaten bei überwiegendem Forschungsinteresse zulässig (§ 12 Abs. 3 Hessisches Krankenhausgesetz, HKHG, i.V.m. § 24 Hessisches Datenschutz und Informationsfreiheitsgesetz, HDSIG). Insoweit kann auf die Ausführungen zu § 27 BDSG verwiesen werden. Neben den Maßnahmen nach § 20 Abs. 2 HDSIG muss außerdem ein **Datenschutzkonzept** vorgehalten werden.

In Hessen dürfen Krankenhäuser personenbezogene Daten für Forschungszwecke verarbeiten und übermitteln, wenn das Forschungsinteresse überwiegt. Es ist ein Datenschutzkonzept zu erstellen.

6.1.8 Mecklenburg-Vorpommern

Gemäß § 37 Abs. 2 LKHG M-V dürfen die Patientendaten nach „*nur für bestimmte, im öffentlichen Interesse liegende Forschungsvorhaben verarbeitet werden, soweit*

> *1. schutzwürdige Belange der Patientinnen und Patienten wegen der Art der Daten, ihrer Offenkundigkeit oder der Art ihrer Nutzung nicht beeinträchtigt werden oder*

[35] BÜRGERSCHAFT DER FREIEN UND HANSESTADT HAMBURG, Drs 31/14828, S. 25, abrufbar unter https://www.hamburg.de/contentblob/11795284/a300f8388b74051acd8cb9218a69e886/data/gesetzesentwurf-fixierung.pdf.
[36] BÜRGERSCHAFT DER FREIEN UND HANSESTADT HAMBURG, Drs 31/14828, S. 25.
[37] BÜRGERSCHAFT DER FREIEN UND HANSESTADT HAMBURG, Drs 31/14828, S. 25f.

2. das für die Aufsicht für das Krankenhaus zuständige Ministerium festgestellt hat, dass das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Belange der Patientinnen und Patienten erheblich überwiegt und der Zweck des Forschungsvorhabens auf andere Weise, insbesondere mit anonymisierten Daten, nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann."

Werden z.B. nur anonymisierte Daten verarbeitet, sind schutzwürdige Belange nicht beeinträchtig. Nach unserer Einschätzung lässt sich dies auch bei der Verwendung pseudonymisierter Daten begründen. Andernfalls ist die Feststellung des überwiegenden Forschungsinteresses durch das zuständige Ministerium einzuholen. Liegen die Voraussetzungen für die Forschungsverarbeitung vor, ist gemäß § 37 Abs. 4 LKHG M-V auch die Übermittlung zulässig, wenn „der Empfänger bereit und in der Lage ist, diese Vorschriften einzuhalten". Der Empfänger muss sich gemäß § 37 Abs. 6 LKHG M-V der Kontrolle des Landesbeauftragten für den Datenschutz unterwerfen.

In Mecklenburg-Vorpommern dürfen Krankenhäuser personenbezogene Daten für Forschungszwecke verarbeiten und übermitteln, wenn Belange der Betroffenen nicht beeinträchtigt werden oder das zuständige Ministerium bestätigt hat, dass das Forschungsinteresse überwiegt. Der Empfänger muss sich der Kontrolle der Datenschutzaufsichtsbehörde unterwerfen.

6.1.9 Niedersachsen

Das neue niedersächsische Krankenhausgesetz, NKHG, vom 01.01.2023 enthält keine Regelungen zur Forschung. Für Krankenhäuser in Trägerschaft des Landes Niedersachsen gilt daher § 13 des niedersächsischen Datenschutzgesetzes, NDSG.

Gemäß § 13 Abs. 1 NDSG dürfen bei überwiegendem Forschungsinteresse personenbezogene Daten für Forschungszwecke verwendet werden. Die Vorschrift entspricht im Wesentlichen § 27 Abs. 1 BDSG. Das Ergebnis der Interessenabwägung und seine Begründung sind aufzuzeichnen und der bestellte Datenschutzbeauftragte zu informieren. Hiernach ist grundsätzlich auch eine Übermittlung der Daten an Dritte gestattet, wenn diese die Vorgaben des § 13 NDSG einhalten und die Übermittlung der Landesdatenschutzbehörde frühzeitig angezeigt wird.

In Niedersachen dürfen Krankenhäuser personenbezogene Daten für Forschungszwecke verarbeiten und auch an Dritte übermitteln, wenn das Forschungsinteresse überwiegt und die Übermittlung der Landesdatenschutzbehörde angezeigt wird.

6.1.10 Nordrhein-Westfalen

In Nordrhein-Westfalen gilt für Krankenhäuser eine Regelung zur Verarbeitung zu Forschungszwecken, § 6 Gesundheitsdatenschutzgesetz Nordrhein-Westfalen, GDSG NW. Im Anwendungsbereich des § 6 GDSG NW kommen die Landesregelung § 17 Datenschutzgesetz, DSG NRW, oder die Bundesregelung aus § 27 BDSG lediglich ergänzend zur Anwendung. Gemäß dem in § 6 Abs. 1 GDG NW geregelten

Grundsatz ist die Verarbeitung zu Forschungszwecken, einschließlich der Übermittlung, nur mit Einwilligung möglich. Hiervon macht § 6 Abs. 2 Satz 1 GDSG NW eine Ausnahme für das behandelnde medizinische Personal, dass aufgrund seiner Tätigkeit ohnehin Zugriff auf die Daten hat.

Weiterhin ist die Verarbeitung für Forschungszwecke auch gemäß der in § 6 Abs. 2 Satz 2 GDSG NW genannten Ausnahme zulässig. So bedarf es gemäß § 6 Abs. 2 Satz 2 GDSG NW keiner Einwilligung, wenn

(i) *„der Zweck eines bestimmten Forschungsvorhabens nicht auf andere Weise erreicht werden kann*“,

(ii) *„das berechtigte Interesse der Allgemeinheit an der Durchführung des Forschungsvorhabens das Geheimhaltungsinteresse des Patienten erheblich überwiegt“* **und**

(iii) *„es entweder nicht möglich ist oder dem Patienten aufgrund seines derzeitigen Gesundheitszustandes nicht zugemutet werden kann, ihn um seine Einwilligung zu bitten*“.

Liegen diese drei Voraussetzungen (kumulativ) vor, ist auch eine Übermittlung zulässig. Aufgrund des Rechtfertigungserfordernisses für die Voraussetzungen des § 6 Abs. 2 Satz 2 GDSG NW wird diese Ausnahmevorschrift nicht greifen, wenn nicht alle Anforderungen durch das Forschungsvorhaben erfüllt sind. Die Übermittlung nicht anonymisierter Daten wird daher regelmäßig die Einwilligung erfordern.

Im Falle einer Übermittlung gilt – ungeachtet auf welcher Grundlage die Übermittlung erfolgt – außerdem Folgendes:

§ 6 Abs. 3 GDSG NW verpflichtet die übermittelnde Stelle, also das Krankenhaus, „*den Empfänger, die Art der übermittelten Daten, den Namen des Patienten und das Forschungsvorhaben*“ aufzuzeichnen. Gemäß § 6 Abs. 4 GDSG NW müssen die Patientendaten, wenn der Forschungszweck es gestattet, so bald wie möglich pseudonymisiert und dann anonymisiert werden.

§ 6 Abs. 6 GDSG NW regelt schließlich zusätzliche Anforderungen bei der Übermittlung an Dritte. Bei der Übermittlung an Dritte, muss sich der Dritte schriftlich verpflichten,

- die Daten nur für das von ihm genannte Forschungsvorhaben zu verwenden,
- die Bestimmungen der § 6 Abs. 4 (Pseudonymisierung) und Abs. 5 (Einschränkung der Veröffentlichung) einzuhalten und
- der für die übermittelnde Stelle zuständigen Datenschutzkontroll- oder Aufsichtsbehörde, auf Verlangen Einsicht zu gewähren.

Neben den Vorschriften des § 6 GDSG NW verlangt § 5 Abs. 2 GDSG NW, dass Personen oder Stellen, denen Patientendaten übermittelt werden, diese nur zu dem Zweck verwenden dürfen, zu dem sie ihnen zulässigerweise übermittelt worden sind, und sie die Daten unbeschadet sonstiger Datenschutzvorschriften in demselben Umfang geheim zuhalten zu haben wie die übermittelnde Einrichtung oder öffentliche Stelle selbst.

In Nordrhein-Westfalen darf medizinisches Personal Patientendaten für eigene Forschungszwecke verwenden. Dies schließt die Anonymisierung mit ein.

Die Übermittlung nicht-anonymisierter Daten an Dritte und nachfolgende Speicherung und Verarbeitung durch diese sind nur unter engen Voraussetzungen gestattet. Im Regelfall ist eine Einwilligung erforderlich. Das Krankenhaus treffen zusätzliche Dokumentationspflichten. Der Empfänger der Daten muss sich zur Einhaltung konkreter datenschutzrechtlicher Vorgaben verpflichten.

6.1.11 Rheinland-Pfalz

In Rheinland-Pfalz dürfen Patientendaten im Rahmen von Forschungsvorhaben ohne Einwilligung verarbeitet werden, wenn die Einholung der Einwilligung nicht zumutbar ist, das Forschungsinteresse der Allgemeinheit überwiegt, oder die Daten anonymisiert wurden, § 37 Abs. 1 Landeskrankenhausgesetz Rheinland-Pfalz, LKG RP. Anonymisierte Daten dürfen an Dritte übermittelt werden. Es dürfen auch nicht-anonymisierte Daten an Dritte übermittelt werden, wenn das Ziel des Forschungsvorhabens nicht anders erreicht werden kann. Die übermittelnde Stelle hat den Empfänger, die Art der zu übermittelnden Daten, die betroffenen Patienten und das Forschungsvorhaben aufzuzeichnen. Der Empfänger muss sich gemäß § 37 Abs. 5 LKG RP verpflichten,

- die Daten nur für das genannte Forschungsvorhaben zu verwenden,
- die personenbezogenen Daten zu anonymisieren oder, solange eine Anonymisierung noch nicht möglich ist, zu pseudonymisieren, sobald es der Forschungszweck erlaubt und dies nachzuweisen,
- der oder dem Landesbeauftragten für den Datenschutz und die Informationsfreiheit auf Verlangen Einsicht und Auskunft zu gewähren.

In Rheinland-Pfalz dürfen Krankenhäuser personenbezogene Daten für Forschungszwecke verarbeiten und auch an Dritte übermitteln, wenn der Forschungszweck dies erfordert und das Forschungsinteresse überwiegt. Das Krankenhaus und den Empfänger treffen verschiedene Dokumentationspflichten.

6.1.12 Saarland

Im Saarland ist die Übermittlung von Patientendaten an Dritte ohne Einwilligung gestattet, „*wenn das Interesse der Allgemeinheit an der Durchführung des Forschungsvorhabens das Geheimhaltungsinteresse der Patientin oder des Patienten erheblich überwiegt, die Einholung der Einwilligung der Patientin oder beim Patienten nicht zugemutet werden kann und ihre oder seine schutzwürdigen Belange nicht beeinträchtigt werden.*“ (§ 14 Abs. 2 S. 2 Saarländisches Krankenhausgesetz, SKHG). Die Krankenhäuser haben die Empfänger, die Art der zu übermittelnden Daten, den Kreis der betroffenen Patienten, das vom Empfänger genannte Forschungsvorhaben sowie das Vorliegen Übermittlungsvoraussetzungen aufzuzeichnen.

Im Saarland dürfen Krankenhäuser personenbezogene Daten für Forschungszwecke verarbeiten und auch an Dritte übermitteln, wenn der Forschungszweck dies erfordert, das Forschungsinteresse überwiegt und Patienteninteressen nicht beeinträchtigt werden. Das Krankenhaus treffen verschiedene Dokumentationspflichten.

6.1.13 Sachsen

Die Verarbeitung für Forschungszwecke ist für Krankenhäuser in Sachsen in § 29 Sächsisches Krankenhausgesetz, SächsKHG, geregelt. In Regelungsinhalt und -systematik ist die Norm dem § 6 GDSG NW sehr ähnlich. § 29 Abs. 1 SächsKHG regelt das Eigenforschungsprivileg des Personals der medizinischen Einrichtung. Die Übermittlung von Patientendaten an Dritte und die Verarbeitung durch diese erfordert gemäß § 29 Abs. 2 SächsKHG die Einwilligung der Patienten. Eine Ausnahme hiervon ist in § 29 Abs. 3 S. 1 SächsKHG geregelt. Hiernach bedarf es der Einwilligung nicht, *„soweit der Zweck eines bestimmten Forschungsvorhabens nicht auf andere Weise erfüllt werden kann“* und (i) *„das berechtigte Interesse der Allgemeinheit an der Durchführung des Forschungsvorhabens das Geheimhaltungsinteresse der Patientin oder des Patienten erheblich überwiegt“* oder (ii) *„es nicht zumutbar ist, die Einwilligung einzuholen und anderweitige schutzwürdige Belange der Patientin oder des Patienten nicht beeinträchtigt werden.“*

Ausweislich der Gesetzesbegründung ist die Ausnahmeregelung sehr restriktiv zu verstehen.[38] Auch hier gehen wir aufgrund der engen Voraussetzungen, insbesondere des Nachweises, dass die Einholung der Einwilligung nicht zumutbar ist, davon aus, dass Ausnahmen von dem Einwilligungserfordernis schwierig zu begründen sind. Die Übermittlung und Verarbeitung nicht anonymisierter Daten wird daher bei fehlendem Nachweis der Voraussetzungen die Einwilligung erfordern.

Im Falle einer Übermittlung hat das Krankenhaus gemäß § 29 Abs. 3 Satz 2 SächsKHG *„die empfangende Stelle einschließlich der Empfängerin oder dem Empfänger, eine detaillierte Beschreibung der zu übermittelnden Daten, die betroffenen Patientinnen und Patienten und das betreffende Forschungsvorhaben zu dokumentieren.“* Die Daten sind gemäß § 29 Abs. 4 SächsKHG zu anonymisieren oder, soweit dies nicht möglich ist, zu pseudonymisieren.

§ 29 Abs. 5 SächsKHG regelt schließlich, dass sich der Empfänger der Daten verpflichten muss,

- die Daten nur für das genannte Forschungsvorhaben zu verwenden,
- die Bestimmungen des § 29 Abs. 4 SächsKHG einzuhalten und die entsprechenden Maßnahmen nachzuweisen,
- der oder dem Sächsischen Datenschutzbeauftragten auf Verlangen Einsicht und Auskunft zu gewähren.

[38] Sächsischer Landtag, Drs 7/10501, S. 78.

In Sachsen darf medizinisches Personal Patientendaten für eigene Forschungszwecke verwenden. Dies schließt die Anonymisierung mit ein.

Die Übermittlung nicht-anonymisierter Daten an Dritte und nachfolgende Speicherung und Verarbeitung durch diese sind nur unter engen Voraussetzungen gestattet. Im Regelfall ist deshalb eine Einwilligung erforderlich. Das Krankenhaus treffen zusätzliche Dokumentationspflichten. Der Empfänger der Daten muss sich zur Einhaltung konkreter datenschutzrechtlicher Vorgaben verpflichten.

6.1.14 Sachsen-Anhalt

Die Verarbeitung für Forschungszwecke ist für Krankenhäuser in Sachsen-Anhalt in § 17 KHG LSA geregelt. § 17 Abs. 1 Satz 1 KHG LSA regelt, dass das behandelnde Personal der medizinischen Einrichtung im Grundsatz nur mit Einwilligung des Patienten die Daten für Forschungszwecke verwenden darf. Eine Verwendung von Patientendaten durch Krankenhausärzte, Krankenhausärztinnen oder sonstiges wissenschaftliches Personal der Einrichtung ohne Einwilligung des Patienten ist nur unter den einschränkenden Voraussetzungen des § 17 Abs. 1 Satz 2 KHG LSA erlaubt. Der sachsen-anhaltinische Gesetzgeber hat sich hierbei an einschränkenden Regelungen in anderen Bundesländern orientieren wollen.[39] Eine Einwilligung für die Forschung ist nicht erforderlich, wenn

- im Rahmen der Krankenhausbehandlung erhobene und gespeicherte Patientendaten vor ihrer weiteren Verarbeitung anonymisiert werden,
- die Einholung der Einwilligung des Patienten unzumutbar ist, der Forschungszweck auf andere Weise nicht erreicht werden kann und schutzwürdige Interessen des Patienten nicht betroffen sind oder
- das berechtigte Interesse der Allgemeinheit an der Durchführung des Forschungsvorhabens das Geheimhaltungsinteresse des Patienten erheblich überwiegt.

Auch eine Übermittlung von Patientendaten ist gemäß § 17 Abs. 2 Satz 1 KHG LSA nur mit schriftlicher Einwilligung zulässig. Gemäß § 17 Abs. 2 Satz 2 KHG LSA bedarf es der Einwilligung nicht, *„wenn es nicht zumutbar ist, die Einwilligung einzuholen, und der Zweck eines bestimmten Forschungsvorhabens nicht auf andere Weise erfüllt werden kann“.* In diesem Fall *„bedarf die Übermittlung der Patientendaten der Zustimmung der zuständigen Behörde;* [40] *die Zustimmung darf nur erteilt werden, wenn das berechtigte Interesse der Allgemeinheit an der Durchführung des Forschungsvorhabens das Geheimhaltungsinteresse des Patienten erheblich überwiegt.“*

Die Ausnahmevoraussetzungen des § 17 Abs. 2 KHG LSA sind strenger als die des § 17 Abs. 1 KHG LSA. Mit diesen erhöhten Anforderungen wollte der Gesetzgeber dem Umstand Rechnung tragen, dass die Übermittlung der Daten an Dritte einen höheren Eingriff in die Selbstbestimmung des Patienten

[39] Landtag von Sachsen-Anhalt Drs. 7/3383, S. 35.

[40] Die Genehmigung der Aufsichtsbehörde enthält (i) den Dritten, an den die Daten übermittelt werden, (ii) die Art der zu übermittelnden Daten und (iii) das bestimmte wissenschaftliche Forschungsvorhaben, vgl. Landtag von Sachsen-Anhalt Drs. 7/3383, S. 35.

darstellt.[41] Aufgrund der gesetzgeberischen Entscheidung, die einwilligungsfreie Forschung sowohl im Falle der Eigenforschung durch das Krankenhaus als auch im Falle der Übermittlung an Dritte zum Ausnahmefall zu machen, gehen wir davon aus, dass eine Übermittlung von nicht-anonymisierten Daten an verarbeitende Stellen zu deren Verarbeitung nicht ohne Einwilligung zu rechtfertigen ist. § 17 Abs. 4 KHG LSA enthält weitere Vorgaben zur Pseudonymisierung und Anonymisierung der Daten.

In Sachsen-Anhalt ist für die Verarbeitung personenbezogener Daten für Forschungszwecke, einschließlich der Übermittlung und subsequenten Verarbeitung und Speicherung durch Dritte, im Regelfall eine Einwilligung erforderlich. Eine Übermittlung ohne Einwilligung bedarf der Zustimmung der Behörde.

6.1.15 Schleswig-Holstein

Die Verarbeitung für Forschungszwecke ist für Krankenhäuser in Schleswig-Holstein in § 38 LKHG SH geregelt. Gemäß § 38 Abs. 1 Satz 1 LKHG SH dürfen Patientendaten für Forschungszwecke nur mit Einwilligung verarbeitet werden. Eine Ausnahme von diesem Grundsatz ist nicht vorgesehen. Die Einwilligung ist gemäß § 26 Abs. 2 LKHG SH revisionssicher zu dokumentieren. Um dem Grundsatz der Datensparsamkeit Rechnung zu tragen, verlangt der Gesetzgeber mit § 38 Abs. 2 LKHG SH, dass die Daten sobald möglich anonymisiert werden, und regelt in § 38 Abs. 3 LKHG SH die Pseudonymisierung der Daten.[42]

Gemäß § 38 Abs. 4 i.V.m. § 36 Abs. 3 LKHG SH dürfen die Empfänger die Daten nur zu dem Zweck verwenden, zu dem sie in zulässiger Weise übermittelt wurden, und müssen die Daten in demselben Umfang geheim halten wie das Krankenhaus; das Krankenhaus hat sicherzustellen, dass der Empfänger die Vorschriften des LKHG SH entsprechend anwendet. Das Krankenhaus muss außerdem den Kreis der betroffenen Personen und das Forschungsvorhaben dokumentieren.

Hoffnung gibt der Entwurf eines Gesetzes zur Änderung des Landeskrankenhausgesetzes[43], mit dem Abs 1 in § 38 LKHG wie folgt gefasst werden soll:

> „(1) Für die Durchführung von Forschungsvorhaben dürfen Patientendaten gemäß den Regelungen der Datenschutz-Grundverordnung, insbesondere Artikel 5, 9 Absatz 2 Buchstabe j, Artikel 12 bis 14, 32, 89, sowie gemäß dem Landesdatenschutzgesetz vom 2. Mai 2018 (GVOBl. Schl.-H. S. 162), insbesondere seiner §§ 12 und 13, verarbeitet werden. Für Krankenhäuser in privatwirtschaftlicher Trägerschaft sind abweichend von Satz 1 die Regelungen des Bundesdatenschutzgesetzes vom 30. Juni 2007 (BGBl. I S. 2097, zuletzt geändert durch Artikel 10 des Gesetzes vom 23.

[41] Landtag von Sachsen-Anhalt Drs. 7/3383, S. 35.
[42] Schleswig-Holsteinischer Landtag, Drs. 19/2042, S. 57.
[43] Gesetzesentwurf der Landesregierung zur Änderung des Landeskrankenhausgesetzes mit Stand 19.12.2023; Schleswig-Holsteinischer Landtag, Drs. 20/1764

Juni 2021 (BGBl. I S. 1858, ber. 2022 I S. 1045), insbesondere seines § 27, anzuwenden."

Mit Inkrafttreten wäre eine Patienteneinwilligung nicht mehr zwingend erforderlich und zu begrüßen wäre auch die Anpassung an die Regelungen von DSGVO, LDSG und BDSG (für private Häuser).

In Schleswig-Holstein ist für die Verarbeitung für Forschungszwecke, einschließlich der Übermittlung und nachfolgenden Speicherung und Verarbeitung durch Dritte, eine Einwilligung erforderlich.

6.1.16 Thüringen

§ 27a ThürKHG gestattet die Verarbeitung von Patientendaten für Forschungszwecke ohne Einwilligung, wenn keine Belange des Patienten beeinträchtigt werden und die oberste Aufsichtsbehörde (das Thüringer Landesverwaltungsamt) festgestellt hat, dass das Forschungsinteresse überwiegt. Unter diesen Voraussetzungen ist auch eine Übermittlung an Dritte gestattet. Das Krankenhaus muss den Empfänger, die Art der zu übermittelnden Daten, den Kreis der betroffenen Personen, das vom Empfänger genannte Forschungsvorhaben sowie das Vorliegen der Verarbeitungsvoraussetzungen aufzeichnen. Der Datenschutzbeauftragte des Krankenhauses ist zu beteiligen.

In Thüringen dürfen Krankenhäuser personenbezogene Daten für Forschungszwecke verarbeiten und auch an Dritte übermitteln, wenn der Forschungszweck dies erfordert, das Forschungsinteresse überwiegt, Patienteninteressen nicht beeinträchtigt werden und dies von der Aufsichtsbehörde bestätigt wurde. Das Krankenhaus treffen verschiedene Dokumentationspflichten.

6.1.17 Zwischenergebnis

Das Datenschutzrecht der Länder zeigt für die Befugnis zu Übermittlung von personenbezogenen Daten zu Forschungszwecken **ein sehr heterogenes Bild**: Zwar zeigen sich gewisse Grundmuster (überwiegendes Forschungsinteresse, fehlende Beeinträchtigung von betroffenen Belangen, Unzumutbarkeit der Einholung einer Einwilligung). Diese werden aber unterschiedlich kombiniert und zum Teil mit Verfahrensanforderungen ergänzt. Vielfach sind Abwägungen durch die zuständige Behörde zu bestätigen. Viele Bundesländer verlangen darüber hinaus die Erstellung von Datenschutzkonzepten, die Unterwerfung der Kontrolle der Datenschutzaufsicht, Anzeigen von Übermittlungen an Behörden, Dokumentationspflichten sowie Selbstverpflichtungen zur Einhaltung von Datenschutz-Anforderungen, etc. Einzelne Länder verlangen stets eine Einwilligung des Patienten oder setzen diese faktisch voraus, weil die Anforderungen an die Nutzung von nicht-anonymisierten Daten zu Forschungszwecken an enge Voraussetzungen geknüpft wird.

Die Durchführung multizentrischer Studien unter Beteiligung von verantwortlichen Stellen in mehreren Bundesländern wird durch diese Heterogenität erheblich erschwert. Sie muss nicht zuletzt wegen der Einholung von Zustimmungen verschiedener Datenschutzbeauftragten **als erhebliches Hindernis** für die klinische Forschung in Deutschland angesehen werden.

6.2 Einsatz von Auftragsverarbeitern und Drittlandsübermittlung

Im Rahmen von klinischen Prüfungen kann es sich aus verschiedenen Gründen anbieten, dritte Stellen mit der Verarbeitung von Daten in der Verantwortung der Auftraggeber zu betrauen. (Auftragsverarbeitung; vgl. oben 3.2.3). Die folgenden Ausführungen zeigen, welche Voraussetzungen landesrechtliche Vorschriften an die Auftragsbearbeitung und die Drittlandsübermittlung stellen.

6.2.1 Baden-Württemberg

Die Auftragsverarbeitung für Krankenhäuser in Baden-Württemberg war bis zum 05.07.2022 in § 48 Landeskrankenhausgesetz BW (LKHG BW) geregelt. Durch Art. 3 des Gesetzes zur Anpassung des bereichsspezifischen Datenschutzrechts an die VO (EU) 2016/679 vom 28.06.2022 wurde § 48 LKHG BW ersatzlos aufgehoben. Auch das Landesdatenschutzgesetz BW enthält keine spezifischen Sonderregelungen zur Auftragsverarbeitung, sodass Krankenhäuser sich beim Einsatz von Auftragsverarbeitern nur noch an die Vorgaben der DSGVO zu halten haben.

In Baden-Württemberg gibt es keine besonderen Vorschriften zum Einsatz von Auftragsverarbeitern oder zur Drittlandsübermittlung durch ein Krankenhaus.

6.2.2 Bayern

Auch in Bayern wurden zum 01.06.2022 durch Art. 32c des Gesundheitsdienst-Gesetzes vom 10.05.2022 die für Krankenhäuser geltenden Vorschriften zum Einsatz von Auftragsverarbeitern geändert. Gemäß Art. 27 Abs. 4 Satz 5 Bayerisches Landeskrankenhausgesetz (BayKrG) kann ein Krankenhaus sich *„zur Verarbeitung und Mikroverfilmung von Patientendaten anderer Personen oder Stellen bedienen, wenn es sicherstellt, dass beim Auftragnehmer die besonderen Schutzmaßnahmen nach [Art. 27 Abs. 6 BayKrG] eingehalten werden, und solange keine Anhaltspunkte dafür bestehen, dass durch die Art und Ausführung der Auftragsdatenverarbeitung schutzwürdige Belange von Patienten beeinträchtigt werden*“. Der ehem. Art. 27 Abs. 4 Satz 6 BayKrG *„Zur Verarbeitung oder Mikroverfilmung von Patientendaten, die nicht zur verwaltungsmäßigen Abwicklung der Behandlung der Patienten erforderlich sind, darf sich das Krankenhaus jedoch nur anderer Krankenhäuser bedienen.*“ wurde gestrichen., um den Weg für ein IT-Outsourcing zu ebnen und es Krankenhäusern zu ermöglichen „die Verarbeitung von Patientendaten auch außerhalb des Krankenhauses durch Auftragsverarbeiter vornehmen zu lassen, die keine Krankenhäuser sind“.[44]

Auch wenn Art. 27 Abs. 4 Satz 5 BayKrG weiterhin nur von der „Verarbeitung und Mikroverfilmung“ spricht, so ist klar, dass die Verarbeitung von Patientendaten nunmehr auf externe Dienstleister ausgelagert werden darf. So hat auch der bayerische Gesetzgeber erkannt: *„Mit Blick auf die gestiegenen*

[44] Bayrischer Landtag, Drucksache 18/19685, S. 53.

Anforderungen an die IT-Sicherheit sind für die Zukunft vor allem die Möglichkeiten der Externalisierung von Gesundheitsdaten von Patientinnen und Patienten zu berücksichtigen.“[45]

Beim Outsourcing müssen gem. Art. 27 Abs. 6 BayKrG insbesondere Art. 28 und 32 DSGVO eingehalten werden. Insbesondere müssen besondere Schutzmaßnahmen technischer und organisatorischer Art getroffen werden, damit Patientendaten nicht unberechtigt verwendet oder übermittelt werden können.

In Bayern gibt es beim Einsatz von Auftragsverarbeitern in Krankenhäusern keine Anforderungen, die über Art. 28 DSGVO hinausgehen und keine spezifischen Regelungen zur Drittlandsübermittlung.

6.2.3 Berlin

Auch der Berliner Gesetzgeber hat erkannt, dass Krankenhäuser „*einen immer höheren Bedarf hinsichtlich externer Produkte und Dienstleistungen zur Datenverarbeitung haben [werden] (denkbar ist dies insbesondere bei Cloudlösungen, Wartungsarbeiten der Krankenhaus-IT und der E-Akte). […] Es ist inzwischen in Forschung und Praxis anerkannt, dass insbesondere Cloud-Betreiber effektive IT-Sicherheitsvorkehrungen realisieren, die den datenschutzrechtlich unabdingbaren Schutz hochsensibler Daten gewährleisten.*“.[46] Durch die Änderung des § 24 Abs. 7 Berliner Krankenhausgesetz (BlnLKG) zum 13.11.2022 durch das Dritte Gesetz zur Änderung des Landeskrankenhausgesetzes wollte der Berliner Gesetzgeber mit den Gesetzesänderungen anderer Bundesländer gleichziehen und einen Wettbewerbsnachteil für Berliner Krankenhäuser vermeiden, gleichzeitig aber ein hohes Datenschutzniveau für die Verarbeitung von Gesundheitsdaten sichergestellt wissen.[47]

Seit der Änderung des § 24 Abs. 7 BlnLKG dürfen Krankenhäuser daher auch (externe) Auftragsverarbeiter i.S.d. Art. 28 DSGVO gem. § 24 Abs. 7 Satz 2 BlnLKG u.a. beauftragen, wenn

1. der Auftragsverarbeiter sicherstellt, dass die Verarbeitung in einem *Mitgliedstaat* der *Europäischen Union, des Europäischen Wirtschaftsraums*, der *Schweiz* oder, sofern ein *Angemessenheitsbeschluss* (Art. 45 DSGVO) vorliegt, in einem Drittstaat erfolgt und die Daten darüber hinaus nicht in Drittstaaten offengelegt werden,
2. gewährleistet ist, dass die Verarbeitung *ausschließlich durch Personen* erfolgt, die nach dem jeweils anwendbaren Recht in Bezug auf den Schutz der Geheimnisse einer *strafbewährten Verschwiegenheitspflicht* und einem Zeugnisverweigerungsrecht, das dem Schutz im Inland vergleichbar ist, unterliegen, und
3. der Verantwortliche der für Gesundheit *zuständigen Senatsverwaltung* rechtzeitig vor der Auftragserteilung
   a) den Auftragsverarbeiter, die bei diesem vorhandenen technischen und organisatorischen Maßnahmen sowie ergänzenden Weisungen,

[45] Bayrischer Landtag, Drucksache 18/19685, S. 2.
[46] Abgeordnetenhaus von Berlin, Drs. 19/0529, S. 2f.
[47] Abgeordnetenhaus von Berlin, Drs. 19/0529, S. 2f.

b) die Art und Menge der im Auftrag verarbeiteten Daten,
c) den Zweck, zu dessen Erfüllung die Auftragsverarbeitung erfolgen soll,
schriftlich oder elektronisch *anzeigt*.

Darüber hinaus dürfen Daten im Auftrag des Krankenhauses gem. § 24 Abs. 7 Satz 3 BlnLKG nur verarbeitet werden, wenn durch *technische Schutzmaßnahmen* sichergestellt ist, dass *der Auftragnehmer keine Möglichkeit hat, beim Zugriff auf Patientendaten den Personenbezug herzustellen.*

Durch die Weitergabe entsprechender Verschwiegenheitsverpflichtungen kann auch die Anforderung des § 24 Abs. 7 Satz 3 Nr. 2 BlnLKG erfüllt werden. Schließlich obliegt es dem beauftragenden Krankenhaus als Verantwortlicher die Anzeigepflicht ggü. der Senatsverwaltung gem. § 24 Abs. 7 Satz 3 Nr. 3 BlnLKG zu erfüllen.

Für die Drittlandsübermittlung gilt: Als Verarbeitungsstandort für die Auftragsverarbeitung kann ein Standort innerhalb der EU, der EWR oder der Schweiz vereinbart werden. Darüber hinaus wäre eine etwaige Übermittlung an Unternehmen in den USA nur durch einen Angemessenheitsbeschluss i.S.d. Art. 45 DSGVO legitimiert.

In Berlin dürfen Krankenhäuser Auftragsverarbeiter einsetzen, wenn die Einhaltung der Verschwiegenheitsverpflichtung sichergestellt ist. Das Krankenhaus muss die Auftragsverarbeitung der Senatsverwaltung anzeigen. Krankenhäuser müssen außerdem sicherstellen, dass die personenbezogenen Daten nicht in Drittländer außerhalb Europas oder ohne Angemessenheitsbeschluss nach Art. 45 DSGVO übermittelt werden.

6.2.4 Brandenburg

Das brandenburgische Krankenhausgesetz enthält keine Vorschriften zur Auftragsverarbeitung. Es gelten daher die allgemeinen Bestimmungen, die auf den Träger des Krankenhauses anzuwenden sind. Für Krankenhäuser in Trägerschaft des Landes Brandenburg gilt das BbgDSG. Gemäß § 24 BbgDSG sind Maßnahmen zur Wahrung der Betroffeneninteressen zu treffen. Diese entsprechen § 22 BDSG (vgl. oben 4.2.3).

In Brandenburg gibt es keine besonderen Vorschriften zum Einsatz von Auftragsverarbeitern oder zur Drittlandsübermittlung.

6.2.5 Bremen

§ 41 Abs. 1 BremKrhG gestattet die Auftragsverarbeitung von Patientendaten, wenn

> *„1. Störungen im Betriebsablauf insbesondere in der Patientenversorgung sonst nicht vermieden werden können, oder*
>
> *2. die Datenverarbeitung dadurch erheblich kostengünstiger gestaltet werden kann, oder*

3. die Datenverarbeitung vom Krankenhaus nicht oder nur mit einem großen Aufwand geleistet werden könnte, oder

4. Patientenakten oder ähnliche Unterlagen in Papierform einzuscannen und zu digitalisieren sind."

Gemäß § 41 Abs. 2 BremKrhG hat der Auftragsverarbeiter (entsprechend Art. 32 DSGVO) die geltende Schweigepflicht nach § 203 und den Art. 28 DSGVO einzuhalten.

In Bremen dürfen Auftragsverarbeiter eingesetzt werden. Krankenhäuser müssen die Beauftragung jedoch begründen (insbes. mit der Vermeidung von Betriebsablaufstörungen oder Kostenersparnissen). Die Anforderungen an Verschwiegenheit und den Auftragsverarbeitungsvertrag werden bereits durch die Einhaltung der Art. 28, 32 DSGVO erfüllt. Es gibt hier keine spezifischen Regelungen zur Drittlandsübermittlung.

6.2.6 Hamburg

Die Regelungen zur Auftragsverarbeitung für Krankenhäuser in Hamburg wurden aufgehoben. Auch das Hamburgische Datenschutzgesetz enthält keine besonderen Bestimmungen. Es gelten daher keine landesspezifischen Regelungen zur Auftragsverarbeitung oder Drittlandsübermittlung.

In Hamburg gibt es keine besonderen Vorschriften zum Einsatz von Auftragsverarbeitern oder zur Drittlandsübermittlung.

6.2.7 Hessen

Das hessische Krankenhausgesetz enthält keine Vorschriften zur Auftragsverarbeitung. Es gelten daher die allgemeinen Bestimmungen, die auf den Träger des Krankenhauses anzuwenden sind. Gemäß § 20 Abs. 2 HDSIG sind Maßnahmen zur Wahrung der Betroffeneninteressen zu treffen. Diese entsprechen § 22 BDSG (vgl. oben 4.2.3).

In Hessen gibt es keine besonderen Vorschriften zum Einsatz von Auftragsverarbeitern oder zur Drittlandsübermittlung.

6.2.8 Mecklenburg-Vorpommern

Das Landeskrankenhausgesetz gestattet Krankenhäusern in Mecklenburg-Vorpommern die Auftragsverarbeitung zum Beispiel zur Vermeidung von Betriebsablaufstörungen und zur Kostenersparnis. § 38 Abs. 2 LKHG M-V verlangt jedoch, dass eine über drei Monate hinausgehende Speicherung von Patientendaten durch einen Auftragnehmer außerhalb des Krankenhauses nur zulässig ist, wenn die Patientendaten auf getrennten Datenträgern gespeichert sind, die der Auftragnehmer für den

Krankenhausträger verwahrt. Gemäß § 38 Abs. 3 LKHG M-V ist zusätzlich die Einhaltung der Schweigepflicht nach § 203 StGB sicherzustellen.

Weiterhin schreibt § 38 Abs. 5 LKHG M-V vor: 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*“.

In Mecklenburg-Vorpommern dürfen Auftragsverarbeiter eingesetzt werden, wenn die Krankenhäuser die Beauftragung (z.B. mit der Vermeidung von Betriebsablaufstörungen oder mit Kostenersparnissen) begründen können. Die Anforderungen an Verschwiegenheit werden bereits durch die Einhaltung des Art. 32 DSGVO erfüllt. Spezielle Anforderungen gelten für eine über drei Monate hinausgehende Speicherung von Patientendaten durch einen Auftragnehmer außerhalb des Krankenhauses.

Eine Drittlandsübermittlung ist nur mit ausdrücklicher Einwilligung des Patienten oder mit gesetzlicher Geheimhaltungspflicht im Drittland möglich.

6.2.9 Niedersachsen

Das neue NKHG vom 01.01.2023 enthält keine Regelungen zur Auftragsverarbeitung. Es gelten daher die allgemeinen Bestimmungen, die auf den Träger des Krankenhauses anzuwenden sind. Für Krankenhäuser in Trägerschaft des Landes Niedersachen gilt das Niedersächsische Datenschutzgesetz, NDSG. Gemäß § 17 NDSG sind Maßnahmen zur Wahrung der Betroffeneninteressen zu treffen. Diese entsprechen im Wesentlichen § 22 BDSG (vgl. oben 4.2.3).

In Niedersachen gibt es keine besonderen Vorschriften zum Einsatz von Auftragsverarbeitern oder zur Drittlandsübermittlung.

6.2.10 Nordrhein-Westfalen

Die Auftragsverarbeitung für Krankenhäuser in NRW ist im Gesundheitsdatenschutzgesetz (GDSG NW) geregelt. Unbeschadet des Grundsatzes, dass Patientendaten grundsätzlich in „der Einrichtung“ zu verarbeiten sind (§ 7 Abs. 1 GDSG NW), ist die Auftragsverarbeitung gemäß § 7 Abs. 2 GDSG NW zulässig, *„wenn sonst Störungen im Betriebsablauf nicht vermieden oder Teilvorgänge der automatischen Datenverarbeitung hierdurch erheblich kostengünstiger vorgenommen werden können*“. Durch § 7 GDSG NW soll *„unabhängig von den spezifischen Übermittlungsregelungen*“ im GDSG NW *„sichergestellt werden, dass bei der Verarbeitung von Patientendaten durch Dritte der gleiche Datenschutz gewährleistet wird, wie bei der Verarbeitung der Daten durch die jeweilige Einrichtung selbst*“[48].

[48] Landtag NRW Drs 11/5705 S. 31.

§ 7 GDSG NW gestattet die Auslagerung von Verarbeitungstätigkeiten auf externe Dienstleister, nicht zuletzt aus Gründen der *„Kostendämpfung“*[49] im Gesundheitswesen. Insbesondere im Hinblick auf den damit verbundenen Kosten- und Personalaufwand ist unter Gesichtspunkten der Vermeidung erhöhter Kosten sinnvoll, die Aufbereitung von Daten zu Zwecken wie z.B. der Qualitätssicherung durch eine andere Stelle als das Krankenhaus wahrnehmen zu lassen. Zusätzlich müssen die technischen und organisatorischen Voraussetzungen der § 7 Abs. 3 und 4 GDSG NW eingehalten werden.

§ 7 Abs. 3 GDSG NW verlangt beim Einsatz von Auftragsverarbeitern:

- Beim Auftragsverarbeiter sind die Wahrung der Datenschutzbestimmungen des GDSG NW und der ärztlichen Schweigepflicht sicherzustellen;
- Patientendaten aus dem ärztlichen Bereich sind vom Auftragsverarbeiter auf *„physisch getrennten Dateien“* zu verarbeiten, wobei wir davon ausgehend, dass eine logische Mandantentrennung nach dem Stand der Technik dieser Anforderung genüge tut;
- der Auftragsverarbeiter darf Patientendaten nur im Rahmen der Weisungen des Auftraggebers verarbeiten;
- erforderlichenfalls sind dem Auftragsverarbeiter Weisungen zur Ergänzung seiner technischen und organisatorischen Einrichtungen und Maßnahmen zu erteilen.

Das GDSG NW enthält keine spezialgesetzlichen Regelungen zu technisch-organisatorischen Maßnahmen, sodass im Hinblick auf die letzte Anforderung des § 7 Abs. 3 GDSG NW die Anforderungen des nordrhein-westfälischen Datenschutzgesetzes (§ 17 Abs. 2 DSG NRW i.V.m. § 15 DSG NRW) zu erfüllen (Garantien zum Schutz personenbezogener Daten und anderer Grundrechte).

§ 7 Abs. 4 Satz 1 GDSG NW regelt zusätzliche Anforderungen, wenn es sich bei dem Auftragsverarbeiter nicht um eine öffentliche Stelle handelt. In diesem Fall hat der Auftraggeber sicherzustellen, dass der Auftragsverarbeiter sich der Kontrolle durch den Landesbeauftragten für den Datenschutz NRW unterwirft. Bei einer Auftragsdurchführung außerhalb des Geltungsbereichs des GDSG NW ist die zuständige Datenschutzkontrollbehörde zu unterrichten.

Da § 7 GDSG NW keine abschließenden Regelungen im Hinblick auf den Auftragsverarbeitungsvertrag enthält, gelten insoweit die allgemeinen Vorschriften. Es sind daher auch die Anforderungen des Art. 28 DSGVO zu beachten.

In Nordrhein-Westfahlen müssen Krankenhäuser die Auftragsverarbeitung begründen (z.B. mit der Vermeidung von Betriebsablaufstörungen oder mit Kostenersparnissen). Die Anforderungen an Verschwiegenheit, Weisungsgebundenheit, Mandantenfähigkeit und Datensicherheit werden z.T. durch die Einhaltung der Art. 28, 32 DSGVO erfüllt. Nicht-öffentliche Auftragsverarbeiter in NRW müssen sich der Aufsicht durch den Landesbeauftragten für den Datenschutz NRW unterwerfen.

[49] Innenministerium NRW, Vorlage 11/2578, S. 3.

Sofern die Auftragsverarbeitung außerhalb von NRW erfolgt, muss die dort zuständige Datenschutzaufsichtsbehörde unterrichtet werden.

6.2.11 Rheinland-Pfalz

Das rheinland-pfälzische Landeskrankenhausgesetz regelt in § 36 Abs. 8 LKG RLP, dass für die Auftragsverarbeitung für Krankenhäuser der Art. 28 DSGVO gilt.

Gemäß § 19 LDSG RLP sind Maßnahmen zur Wahrung der Betroffeneninteressen zu treffen. Diese entsprechen im Wesentlichen § 22 BDSG (vgl. oben 4.2.3).

In Rheinland-Pfalz gibt es keine besonderen Vorschriften zum Einsatz von Auftragsverarbeitern oder zur Drittlandsübermittlung.

6.2.12 Saarland

§ 13a Abs. 1 des saarländischen Krankenhausgesetzes (SKHG) gestattet die Auftragsverarbeitung zur Vermeidung von Betriebsablaufstörungen und zur Kostenersparnis. § 13a Abs. 2 SKHG verlangt, dass eine Speicherung, die länger als drei Monate andauert, beim Auftragsverarbeiter auf getrennten Datenträgern zu erfolgen hat. Gemäß § 13a Abs. 3 SKHG muss der Krankenhausträger eine Abschrift der Vereinbarung dem Unabhängigen Datenschutzzentrum Saarland und der Krankenhausaufsichtsbehörde unverzüglich übersenden. § 13a Abs. 3 SKHG verlangt, dass sich der Auftragsverarbeiter der Kontrolle des Landesbeauftragten für Datenschutz und Informationsfreiheit unterwirft.

Im Saarland müssen Krankenhäuser die Auftragsverarbeitung begründen (z.B. mit Vermeidung von Betriebsablaufstörungen oder mit Kostenersparnissen). Der Krankenhausträger muss dem Unabhängigen Datenschutzzentrum Saarland und der Krankenhausaufsichtsbehörde eine Kopie des Auftragsverarbeitungsvertrags übersenden. Der Auftragsverarbeiter muss sich der Kontrolle des Landesbeauftragten für Datenschutz und Informationsfreiheit unterwerfen. Speicherung, die länger als drei Monate andauert, hat beim Auftragsverarbeiter auf getrennten Datenträgern zu erfolgen. Es gibt keine spezifischen Regelungen zur Drittlandsübermittlung.

6.2.13 Sachsen

Das Sächsische Krankenhausgesetz (SächsKHG) vom 15.12.2022 trat am 01.01.2023 in Kraft. Gemäß § 28 Abs. 9 SächsKHG hat das Krankenhaus beim Einsatz von Auftragsverarbeitern für die Verarbeitung von Patientendaten „*insbesondere sicherzustellen, dass [der Auftragsverarbeiter] die Geheimhaltungspflicht nach § 203 des Strafgesetzbuches einhält. Der Auftragsverarbeiter hat eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten zu ernennen.*“ Auf das Erfordernis der Zustimmung durch die zuständige Aufsichtsbehörde hat der Sächsische Gesetzgeber bewusst verzichtet, da die in der

Vorgängernorm enthaltene Zustimmungsbedürftigkeit *„aufgrund des zwischenzeitlich eingetretenen stark erhöhten Schutzstandards insbesondere aus der [DSGVO] entfallen [ist].“*[50]

In Sachsen sind Auftragsverarbeiter zur Geheimhaltung zu verpflichten und haben einen Datenschutzbeauftragten zu bestellen. Es gibt hier keine spezifischen Regelungen zur Drittlandsübermittlung.

6.2.14 Sachsen-Anhalt

Mit mehreren Gesetzesänderungen wurden in Sachsen-Anhalt mit Wirkung vom 14.05.2019 u.a. die datenschutzrechtlichen Vorschriften des Krankenhausgesetz Sachsen-Anhalt (KHG LSA) aktualisiert. Gemäß § 16 Abs. 4 KHG LSA kann sich ein Krankenhaus

> *„zur Verarbeitung von Patientendaten im Wege der Datenverarbeitung im Auftrag anderer Personen oder Stellen bedienen, die an Tätigkeiten des Krankenhauses mitwirken und dafür Daten verarbeiten, soweit*
>
> - *dies für die Inanspruchnahme der Tätigkeit der anderen Personen oder Stellen erforderlich ist und*
> - *soweit keine Anhaltspunkte bestehen, dass durch die Auftragsdatenverarbeitung schutzwürdige Belange des Patienten oder des Betroffenen beeinträchtigt werden.*
>
> *Jede bei der Auftragsdatenverarbeitung nach Satz 1 beteiligte Person ist zur Geheimhaltung zu verpflichten, soweit sie nicht infolge ihrer sonstigen Tätigkeit bereits einer strafrechtlich sanktionierten Schweigepflicht unterliegt.*
>
> *Der Patient ist vorab über die Auftragsdatenverarbeitung nach Satz 1 zu informieren; der Patient kann der Verarbeitung der ihn betreffenden Daten nach Satz 1 widersprechen.“*

In seiner Begründung führt der Landesgesetzgeber aus, dass Krankenhäuser sich der Auftragsverarbeiter bedienen dürfen, *„sofern die in den Sätzen 1 bis 3 aufgeführten Voraussetzungen vorliegen. Die datenschutzrechtliche Grundlage für die Weitergabe der Daten vom Verantwortlichen auf den Auftragsverarbeiter ergibt sich bereits aus Artikel 28 DSGVO; die vorliegende Regelung dient jedoch der Klarstellung.“*[51] Leider lässt der Landesgesetzgeber offen, woraus sich ein Widerspruchsrecht der Patienten gegen die Auftragsverarbeitung ergeben soll, da die für die Auftragsverarbeitung einschlägige Regelung in Art. 28 DSGVO ein solches Recht nicht kennt. Offen ist ebenfalls, wie Krankenhäuser mit einem Widerspruch eines Patienten umgehen sollen, insbesondere wenn ein solcher Widerspruch gar nicht umsetzbar ist – z.B. wenn das KIS im Rahmen einer Auftragsverarbeitung eingesetzt wird und es nicht möglich ist, die Daten eines einzelnen Patienten nicht in dem vom Krankenhaus gewählten System zu verarbeiten. In (analoger) Anwendung des Art. 21 Abs. 1 Satz 2 DSGVO wird daher das Krankenhaus die Daten trotz Widerspruchs weiterverarbeiten dürfen, wenn es zwingende schutzwürdige

[50] Sächsischer Landtag, Drs. 7/10501, S. 77.
[51] Landtag von Sachsen-Anhalt Drs. 7/3383, S. 34.

Gründe für die Verarbeitung nachweisen kann, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen.

Beauftragende Krankenhäuser müssen daher die Erforderlichkeit der Tätigkeit begründen und dokumentieren, dass keine Belange der betroffenen Personen beeinträchtigt werden. Das Krankenhaus muss überdies einen Prozess etablieren, wie es Patienten einen Widerspruch ermöglicht und dessen Umsetzung prüft, und gegebenenfalls darüber informiert, wenn eine solche Auftragsverarbeitung trotzdem erfolgt.

In Sachsen-Anhalt dürfen Krankenhäuser Auftragsverarbeiter einsetzen, wenn die Inanspruchnahme von Auftragsverarbeitern erforderlich ist und schutzwürdige Belange der betroffenen Personen nicht beeinträchtigt werden. Auftragsverarbeiter sind zur Verschwiegenheit zu verpflichten. Krankenhäuser müssen die Patienten über die Auftragsverarbeitung vorab informieren und ihnen die Möglichkeit geben, der Verarbeitung zu widersprechen. Es gibt hier keine spezifischen Regelungen zur Drittlandsübermittlung.

6.2.15 Schleswig-Holstein

Das neue Landeskrankenhausgesetz Schleswig-Holstein (LKHG SH) vom 10.12.2020 trat zum 01.01.2021 in Kraft. Gemäß dem nun geltenden § 37 Abs. 1 LKHG SH sind Patientendaten *„grundsätzlich im Krankenhaus zu verarbeiten. Das Krankenhaus kann sich zur Verarbeitung von Patientendaten anderer Personen oder Stellen bedienen.“* § 37 Abs. 2 LKHG SH konkretisiert die Anforderungen an Auftragsverarbeiter wie folgt:

> *„Dem Auftragsverarbeiter dürfen 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.“*

Mit der Vorschrift wollte der Landesgesetzgeber regeln, „ob und wie das Krankenhaus sich bei eigenen Datenverarbeitungsvorgängen durch Dritte unterstützen lassen darf“, wobei an dem Grundsatz der Verarbeitung im Krankenhaus festgehalten wurde.[52] Der Gesetzgeber stellt klar, dass es für die Auftragsverarbeitung keiner Einwilligung des Patienten bedarf. [53] Mit der Regelung des § 37 Abs. 2 LKHG SH wollte der Gesetzgeber dem „Grundsatz der Datensparsamkeit“ Rechnung tragen.[54] Hierbei hat er übersehen, dass auch im Krankenhaus häufig eine Auftragsverarbeitung nicht nur mit pseudonymisierten Daten durchgeführt werden kann, etwa wenn das KIS durch einen Auftragsverarbeiter betrieben wird. Die Daten der Patienten müssen daher auch durch andere – mindestens gleichwertige – Maßnahmen geschützt werden können. Denkbar ist z.B. eine technische Verschlüsselung der Daten.

[52] Schleswig-Holsteinischer Landtag, Drs. 19/2042, S. 56.
[53] Schleswig-Holsteinischer Landtag, Drs. 19/2042, S. 56.
[54] Schleswig-Holsteinischer Landtag, Drs. 19/2042, S. 56.

Eine weitere Voraussetzung für die Verarbeitung personenbezogener Daten im Auftrag ist, dass diese nicht oder jedenfalls nicht in der Art und Weise durch das Krankenhaus selbst durchgeführt werden kann.

In Schleswig-Holstein dürfen Krankenhäuser ihrem Auftragsverarbeiter Daten nur offenlegen, soweit dies erforderlich ist. Weil die Daten zumindest zu pseudonymisieren sind, ist eine Auftragsbearbeitung mit identifizierbaren Daten nicht zulässig. Zur Drittlandsübermittlung gibt es keine spezifischen Regelungen.

6.2.16 Thüringen

In Thüringen ist den Krankenhäusern der Einsatz von Auftragsverarbeitung zur Vermeidung von Störungen im Betriebsablauf und aus Kostengründen gestattet (§ 27 Abs. 1 ThürKHG). Weitere Voraussetzung ist, dass die Einhaltung der Schweigepflicht sichergestellt ist und das Krankenhaus die beabsichtigte Auftragsverarbeitung vorab schriftlich bei der Aufsichtsbehörde anzeigt.

§ 27 Abs. 2 ThürKHG verlangt zudem, dass im Auftragsverarbeitungsvertrag sicherzustellen ist, dass vom Verantwortlichen oder von dessen Datenschutzkontrollbehörde veranlasste Kontrollen vom Auftragsverarbeiter jederzeit zu ermöglichen sind.

In Thüringen müssen Krankenhäuser die Auftragsverarbeitung begründen (z.B. mit der Vermeidung von Betriebsablaufstörungen oder mit Kostenersparnissen). Die Anforderungen an die Schweigepflicht werden bereits durch die Einhaltung der Art. 28, 32 DSGVO erfüllt. Das Krankenhaus muss der Aufsichtsbehörde die Auftragsverarbeitung vorab anzeigen. Der Auftragsverarbeiter muss Kontrollen jederzeit ermöglichen. Es gibt hier keine spezifischen Regelungen zur Drittlandsübermittlung.

6.2.17 Zwischenergebnis

Das Datenschutzrecht der Länder zeigt für die Auftragsverarbeitung und Drittlandsübermittlung ebenfalls **ein sehr heterogenes Bild**. Die Durchführung multizentrischer Studien unter Beteiligung verantwortlicher Stellen in mehreren Bundesländern wird durch diese Heterogenität erheblich erschwert. Sie muss **als erhebliches Hindernis** für die klinische Forschung in Deutschland angesehen werden.

6.3 Matrix zu Rechtsgrundlagen für Auftragsverarbeitung und Verarbeitung zur Forschung

Die folgende Matrix zeigt eine Übersicht der maßgeblichen Regelungen zur Verarbeitung von Gesundheitsdaten in der Forschung sowie für Auftragsverarbeitung und Drittlandsübermittlung:

	Auftragsverarbeitung und Drittlands-übermittlung	Verarbeitung zur Forschung
Allgemein (DSGVO)	• Art. 28-Anforderungen können erfüllt werden • Bei Übermittlung in Drittländer ohne Angemessenheitsbeschluss: zusätzliche Garantien erforderlich	• Möglich, wenn Forschungsinteresse erheblich überwiegt (§ 27 BDSG)
BDSG	• Ggf. zusätzliche Maßnahmen nach § 22 Abs. 2 BDSG erforderlich	• Möglich, wenn Forschungsinteresse erheblich überwiegt
Evangelische Kirche (DSG-EKD)	• Auftragsverarbeiter muss sich kirchlicher Datenschutzaufsicht unterwerfen	• Möglich, wenn Forschungsinteresse überwiegt
Katholische Kirche	• Verarbeitung in Drittländern nur zulässig, wenn Datenschutzaufsicht ein angemessenes Datenschutzniveau feststellt	• Möglich, wenn Forschungsinteresse überwiegt • Verpflichtung, Daten nicht für andere Zwecke zu verwenden
Berufsgeheimnisträger (Ärzte) (§ 203 StGB)	• Dienstleister müssen über Strafbarkeit aufgeklärt und zur Verschwiegenheit verpflichtet werden	• Verwendung anonymisierter oder hinreichend pseudonymisierter Daten verstößt nicht gegen Schweigepflicht
Krankenhausspezifische Regeln		
Baden-Würtemberg	• Es gelten die Anforderungen der DSGVO	• Möglich mit nicht anonymisierten Daten nur für Forschungszwecke des Krankenhauses
Bayern	• Es gelten die Anforderungen der DSGVO	• Möglich mit nicht anonymisierten Daten nur für Forschungszwecke des Krankenhauses
Berlin	• Keine Übermittlung an außereuropäische Drittländer ohne Angemessenheitsbeschluss • Auftragsverarbeitung muss angezeigt werden	• Möglich mit pseudonymisierten Daten bei überwiegendem Forschungsinteresse
Brandenburg	• Es gilt DSGVO sowie Maßnahmen entsprechend § 22 Abs. 2 BDSG	• Möglich mit nicht-anonymisierten Daten, wenn das Forschungsinteresse überwiegt und die zuständige Behörde dies bestätigt hat
Bremen	• Begründungspflicht für Auftragsverarbeitung	• Möglich mit nicht-anonymisierten Daten, wenn das Forschungsinteresse überwiegt und die zuständige Behörde dies bestätigt hat

	• Es gelten keine wesentlich über Art. 28, 32 DSGVO hinausgehenden Anforderungen	
Hamburg	• Es gelten die Anforderungen der DSGVO	• Möglich mit nicht-anonymisierten Daten, für eigene Forschungszwecke wenn das Forschungsinteresse überwiegt
Hessen	• Es gilt DSGVO sowie Maßnahmen entsprechend § 22 Abs. 2 BDSG	• Möglich mit nicht-anonymisierten Daten, wenn das Forschungsinteresse überwiegt • Es ist ein Datenschutzkonzept zu erstellen
Mecklenburg-Vorpommern	• Auftragsverarbeitung muss begründet werden • Anforderungen an Verschwiegenheit und Mandantenfähigkeit (idR erfüllt durch Art. 28, 32 DSGVO) • Spezielle Anforderungen gelten für eine über drei Monate hinausgehende Speicherung von Patientendaten durch einen Auftragnehmer außerhalb des Krankenhauses • Drittlandsübermittlung ist nur mit ausdrücklicher Einwilligung des Patienten oder mit gesetzlicher Geheimhaltungspflicht im Drittland möglich.	• Möglich mit nicht-anonymisierten Daten, wenn Betroffenenbelange nicht beeinträchtigt werden oder das Forschungsinteresse überwiegt und die zuständige Behörde dies bestätigt hat • Empfänger muss sich Kontrolle der Datenschutzaufsicht unterwerfen
Niedersachsen	• Es gilt DSGVO sowie Maßnahmen entsprechend § 22 Abs. 2 BDSG	• Möglich mit nicht-anonymisierten Daten, wenn das Forschungsinteresse überwiegt • Übermittlung ist der Behörde anzuzeigen
Nordrhein-Westfalen	• Auftragsverarbeitung muss begründet werden • Anforderungen an Weisungsgebundenheit, Verschwiegenheit, Mandantenfähigkeit und Datensicherheit (idR erfüllt durch Art. 28, 32 DSGVO) • Nicht-öffentlicher Auftragsverarbeiter muss sich der Aufsicht des Landes NRW unterwerfen	• Möglich mit nicht-anonymisierten Daten nur unter engen Voraussetzungen gestattet • Der Empfänger der Daten muss sich zur Einhaltung konkreter datenschutzrechtlicher Vorgaben verpflichten.

	• Bei Auftragsverarbeitung außerhalb NRW ist die zuständige Aufsichtsbehörde zu informieren	
Rheinland-Pfalz	• Es gilt DSGVO sowie Maßnahmen entsprechend § 22 Abs. 2 BDSG	• Möglich mit nicht-anonymisierten Daten, wenn das Forschungsinteresse überwiegt • Es bestehen Dokumentationspflichten
Saarland	• Auftragsverarbeitung muss begründet werden • Anforderungen an Mandantenfähigkeit (idR erfüllt durch Art. 28 DSGVO) • Krankenhaus muss Kopie des Vertrags an die Aufsichtsbehörden und dem dem Unabhängigen Datenschutzzentrum Saarland übersenden • Der Auftragsverarbeiter muss sich der Kontrolle des LfDI unterwerfen. • Speicherung, die länger als drei Monate andauert, hat beim Auftragsverarbeiter auf getrennten Datenträgern zu erfolgen	• Möglich mit nicht-anonymisierten Daten, wenn das Forschungsinteresse überwiegt und Betroffenenbelange nicht beeinträchtigt werden • Es bestehen Dokumentationspflichten
Sachsen	• Der Auftragsverarbeiter ist zur Geheimhaltung zu verpflichten und muss einen Datenschutzbeauftragen bestellen	• Möglich mit nicht-anonymisierten Daten nur unter engen Voraussetzungen gestattet
Sachsen-Anhalt	• Auftragsverarbeitung muss geprüft/begründet werden: keine Beeinträchtigung schutzwürdiger Belange • Verpflichtung zur Verschwiegenheit • Patienten haben Widerspruchsrecht	• Möglich mit Zustimmung der Behörde, wenn das Forschungsinteresse erheblich überwiegt und die Einholung der Einwilligung nicht zumutbar ist
Schleswig-Holstein	• Offenbarung von Patientendaten an den Auftragsverarbeiter nur, soweit dies erforderlich ist	• Möglich nur mit Einwilligung (betrifft alle Datentypen)
Thüringen	• Auftragsverarbeitung muss begründet werden	• Möglich mit nicht-anonymisierten Daten, wenn das Forschungsinteresse überwiegt und

	• Anforderungen an die Schweigepflicht (idR erfüllt durch Art. 28 DSGVO) • Krankenhaus muss die Auftragsverarbeitung bei der Aufsichtsbehörde anzeigen • Auftragsverarbeiter muss Kontrollen ermöglichen • Daten müssen zumindest pseudonymisiert sein	Betroffenenbelange nicht beeinträchtigt werden und dies von der Behörde festgestellt wurde

7. Vorgaben des ärztlichen Berufsrechts

Ärzte und Angehörige anderer staatlich anerkannter Heilberufe unterliegen der Berufsgeheimnispflicht gemäß § 203 Abs. 1 Nr. 1 StGB. Demnach macht sich strafbar, wer unbefugt ein fremdes Geheimnis offenbart, das ihm im Rahmen der Tätigkeitsausübung bspw. als Arzt bekannt geworden ist. Offenbaren heißt, dem Empfänger der Erklärung ein Wissen zu vermitteln, das diesem noch verborgen ist oder von dem dieser jedenfalls noch keine sichere Kenntnis hat.[55] Offenbaren setzt nach überwiegender Auffassung in der Literatur voraus, dass die Mitteilung den Schluss auf die betroffene Person zulässt.[56] Diese Auffassung wird auch unter Nennung von Beispielen in der juristischen Literatur vertreten:

- Demnach ist die wissenschaftliche Erörterung praktischer Fälle in Veröffentlichungen und Vorträgen in anonymisierter oder pseudonymisierter Form möglich, weil es dann nicht zu einer Individualisierung des Betroffenen kommt.[57]
- Hinreichend verfremdete oder anonymisierte Behandlungsfälle können z.B. im Rahmen einer psychotherapeutischen Supervision beraten werden, ohne dass es einer zusätzlichen gesetzlichen Erlaubnis oder einer Entbindung von der Schweigepflicht bedarf.[58]
- Ebenso liegt keine Offenbarung vor, wenn z.B. die geschützten Daten von Versicherungsnehmern entweder anonymisiert oder pseudonymisiert oder technisch verschlüsselt übermittelt werden.[59]

Die Verwendung, Übermittlung und Weitergabe anonymisierter oder hinreichend pseudonymisierter Daten ist kein Offenbaren fremder Geheimnisse i.S.d. § 203 StGB, denn das Geheimhaltungsinteresse einer Person ist erst dann verletzt, wenn ein Geheimnis dieser Person auch zugeordnet werden kann.

---

55 Cierniak/Niehaus, in: MüKo StGB, 4. Auflage 2021, § 203 Rn. 54 m.w.N., u.a. unter Verweis auf BGH Urt. v. 9.2.1977 – 3 StR 498/76.
56 Cierniak/Niehaus, in: MüKo StGB, 4. Auflage 2021, § 203 Rn. 54, m.w.N.
57 Cierniak/Niehaus, in: MüKo StGB, 4. Auflage 2021, § 203 Rn. 54.
58 Dochow, MedR 2019, 363, 367.
59 Wolf, in: Bürkle, Compliance in Versicherungsunternehmen, 3. Auflage 2020, § 18 Rn. 41.

Die berufsrechtlichen Anforderungen weichen von den datenschutzrechtlichen Vorgaben in diesem Punkt ab.

8. Exkurs und Ausblick

Im Rahmen ihrer Datenstrategie[60] hat die EU verschieden Rechtsakte erlassen, um einen Binnenmarkt für Daten zu schaffen und die EU-weite und branchenübergreifende Datenweitergabe zu ermöglichen.

8.1 Data Governance Act

Mit dem seit dem 24.09.2023 geltenden Data Governance Act (**DGA**) soll die Verfügbarkeit von Daten für die Nutzung gefördert werden, indem das Vertrauen in Datenvermittler gestärkt und die Mechanismen für den Datenaustausch in der gesamten EU ausgebaut werden. Der DGA regelt u.a. die Weiterverwendung von Daten im Besitz öffentlicher Institutionen durch natürliche oder juristische Personen für kommerzielle und nicht-kommerzielle Zwecke, legt Anforderungen und einschränkende Bedingungen für die Erbringung von Datenvermittlungsdienstleistungen fest, führt die die Figur der datenaltruistischen Organisation ein, die Daten auf einfache Weise zum Wohle der Gesellschaft teilen. Darüber hinaus wird mit dem DGA ein Europäischer Dateninnovationsrat geschaffen.

Mit dem DGA werden die Rechte und Pflichten von Datentreuhändern (als Datenvermittlungsdienst und als datenaltruistische Organisation) stärker geregelt, sodass (über den Erlass der Durchführungsakte) mit einer europaweiten Vereinheitlichung der Anforderungen an diese gerechnet werden kann. Die neuen Regelungen müssen bei der Entwicklung deutscher gesetzlicher und untergesetzlicher Vorgaben für die Forschung im Blick behalten werden.

8.2 Data Act

Mit dem derzeit in der Finalisierung befindlichen Data Act (**DA**) sollen Inhaber von Daten angeregt werden, Daten zu teilen und so die Entwicklung innovativer Produkte und verbundener Dienste gefördert und die Innovationen auf den Anschlussmärkten vorangetrieben werden. Der DA soll Fairness gewährleisten, indem Regeln für den Zugang zu und die Nutzung von Daten festgelegt werden, die u.a. von Internet of Things (IoT)-Geräten generiert werden. Neben Zugangsrechten und-pflichten und Regelungen zur Entwicklung von Interoperabilitätsstandards enthält der DA Maßnahmen zur Verhinderung des Missbrauchs vertraglicher Ungleichgewichte. Die hierzu insbesondere in Art. 13 und Art. 34 DA enthaltenen Regelungen sind vergleichbar mit den Vorschriften zur AGB-Kontrolle im deutschen Recht.

Aus dem DA ergeben sich für die Verarbeitung von Daten zunächst keine weiteren Beschränkungen, sondern Regeln, die ggf. zu beachten sind, wenn Produkte, Dienste oder Daten bereitstellt werden.

[60] Siehe https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_de.

Gleichwohl sollten auch diese neuen Regelungen bei der Entwicklung deutscher gesetzlicher und untergesetzlicher Vorgaben für die Forschung im Blick behalten werden

8.3 EHDS-VO

Mit dem Entwurf der Verordnung über den europäischen Gesundheitsdatenraum (European Health Data Space) (**EHDS-VO**) soll ein gesundheitsspezifisches Ökosystem geschaffen werden, das aus Vorschriften, gemeinsamen Standards und Verfahren, Infrastrukturen und einem Governance-Rahmen besteht. Ziel der EHDS-VO ist die Stärkung der Kontrolle der Einzelpersonen über ihre eigenen Gesundheitsdaten, die Förderung der Nutzung von Gesundheitsdaten für eine bessere medizinische Versorgung, für **Forschung**, Innovation und Politikgestaltung sowie die Ermöglichung innerhalb der EU das Potenzial von Austausch, Nutzung und Weiterverwendung von Gesundheitsdaten unter gesicherten Bedingungen voll auszuschöpfen.

Hierfür enthalt die EHDS-VO Regelungen zur sog. Primärnutzung von Daten, mit denen die Handlungskompetenz der Einzelpersonen durch besseren digitalen Zugang zu ihren personenbezogenen elektronischen Gesundheitsdaten gestärkt und ein echter Binnenmarkt für elektronische Patientendatensysteme, relevante Medizinprodukte und Hochrisikosysteme gefördert werden sollen. Mit den Regelungen zur Sekundärnutzung von Daten soll ein kohärentes, vertrauenswürdiges und effizientes Umfeld für Forschung, Innovation, Politikgestaltung und Regulierungstätigkeiten geschaffen werden. In diesem Zusammenhang ist es denkbar, dass forschende Stellen als Organisation im Gesundheitssektor und gleichzeitiger Inhaber von Gesundheitsdaten u.U. als **Dateninhaber** zur Bereitstellung dieser Daten verpflichtet werden. Sofern diese unter den Dateninhaber-Begriff der EHDS-VO fallen, könnten sie zukünftig verpflichtet sein, die Art der vorhandenen Daten (Metadaten) an eine einzurichtende Zugangsstelle zu melden. Sofern Datennutzer erfolgreich die Nutzung der Daten beantragen, sind sie dann verpflichtet diese Daten – gegen eine Aufwandsentschädigung – bereitzustellen. Gleichzeitig ist es denkbar, dass forschende Stellen als **Datennutzer** von den Daten anderer Dateninhaber profitieren kann. Die nationale Ausgestaltung des EHDS erfolgt durch das Gesundheitsdatennutzungsgesetz (**GDNG**).

Aus der EHDS-VO ergeben sich keine Einschränkungen für die Verarbeitung der Daten, sondern vielmehr potentielle Melde- und Bereitstellungspflichten sowie ggf. Möglichkeiten zur Datennutzung von Daten aus anderen Quellen.

8.4 Gesundheitsdatennutzungsgesetz (GDNG)

Das zum 26.03.2024 in Kraft getretene GDNG dient in erster Linie der Umsetzung des EHDS und errichtet zu diesem Zweck eine „zentrale Datenzugangs- und Koordinierungsstelle für Gesundheitsdaten“ beim BfArM, § 3 GDNG.

Es enthält in § 5 auch weiterhin eine Zuständigkeitsbündelung für die Datenschutzaufsicht bei länderübergreifenden Gesundheitsforschungsvorhaben, dessen Absatz 1 wie folgt lautet:

„Sind an einem Vorhaben der Versorgungs- oder Gesundheitsforschung, bei dem Gesundheitsdaten verarbeitet werden, eine oder mehrere öffentliche oder nicht öffentliche Stellen als Verantwortliche derart beteiligt, dass mehr als eine Datenschutzaufsichtsbehörde des Bundes oder der Länder nach Kapitel 6 der Verordnung (EU) 2016/679 zuständig ist und sind diese Stellen nicht gemeinsam Verantwortliche gemäß Artikel 26 der Verordnung (EU) 2016/679, so kann dieses Vorhaben den Datenschutzaufsichtsbehörden zur federführenden Datenschutzaufsicht angezeigt werden."

Nach Abs. 4 kann die Bündelung auch durch die betroffenen Landesdatenschutzbeauftragten selbst gemeinsam angezeigt werden.

Diese Bündelung der Zuständigkeiten ist vor dem Hintergrund der auch hier kritisierten Probleme aufgrund der heterogenen Zuständigkeiten von Datenschutzbeauftragten (9.2.2) zu begrüßen. Sie wird aber keine zufriedenstellende Lösung bieten, weil

- sie nur die unterschiedlichen Landesdatenschützer bündelt und damit nicht eine ebenfalls parallel bestehende Zuständigkeit des BfDI und der kirchlichen Datenschützer umfasst und weil
- sie keine stringente Verfahrensbestimmung besorgt, durch die Forschende innerhalb kurzer Zeit Gewissheit über die Datenschutzkonformität ihres Forschungsprojekts erlangen können.

Die Regelung nach § 5 GDNG ist somit zu begrüßen. Sie kann auch im Ansatz den Schwierigkeiten aus heterogenen Anforderungen an Inhalte und Verfahren des Datenschutzes in der medizinischen Forschung begegnen.

Interessant und hilfreich ist weiterhin die Regelung in § 6 GDNG, die besagt:

„Datenverarbeitende Gesundheitseinrichtungen dürfen die bei ihnen gemäß Artikel 9 Absatz 2 Buchstabe h und i der Verordnung (EU) 2016/679 rechtmäßig gespeicherten Daten weiterverarbeiten, soweit dies erforderlich ist,

…

2. zur medizinischen, zur rehabilitativen und zur pflegerischen Forschung oder…"

Kontrolliert und eingeschränkt wird diese Weiterverarbeitungsbefugnis allerdings durch Bestimmungen nach Absatz 1 S.3 ff., die lauten:

„Sind mehrere natürliche Personen in der datenverarbeitenden Gesundheitseinrichtung tätig, hat die Gesundheitseinrichtung ein Rechte- und Rollenkonzept zu erstellen, das gewährleistet, dass nur befugte Personen die in Satz 1 genannten Daten

weiterverarbeiten können sowie Weiterverarbeitungen protokolliert und unbefugte Verarbeitungen geahndet werden können.“

und insbesondere Abs. 3 S. 1, der lautet

„Die Weitergabe der personenbezogenen Daten an Dritte ist im Rahmen der Weiterverarbeitung nach Absatz 1 untersagt. Abweichend von Satz 1 ist die Weitergabe von personenbezogenen Daten im Rahmen der Weiterverarbeitung nach Absatz1 zulässig, soweit die betroffene Person eingewilligt hat oder eine andere gesetzliche Vorschrift des Bundesrechts, des Landesrechts oder unmittelbar geltender Rechtsakte der Europäischen Union dies vorsieht.“

Zwar wurde im parlamentarischen Verfahren noch folgende Aufweichung des Weitergabeverbots in Satz 4 des gleichen Absatzes erreicht:

„Abweichend von Satz 1 ist eine gemeinsame Nutzung und Verarbeitung der in Absatz 1 Satz 1 genannten Daten zu den in Absatz 1 Satz 1 genannten Zwecken durch öffentlich geförderte Zusammenschlüsse von datenverarbeitenden Gesundheitseinrichtungen einschließlich Verbundforschungsvorhaben und Forschungspraxennetzwerken zulässig, wenn

1. die Verarbeitung zu den in Absatz 1 Satz 1 genannten Zwecken erforderlich ist,

2. die Anforderungen nach den Absätzen 1, 2 und 4 hinsichtlich der Verarbeitung eingehalten werden,

3. die Interessen des datenschutzrechtlich Verantwortlichen an der Verarbeitung die Interessen der betroffenen Person an einem Ausschluss der Verarbeitung erheblich überwiegen und

4. die zuständige Datenschutzaufsichtsbehörde der gemeinsamen Nutzung und Verarbeitung der Daten zugestimmt hat.“

Bemerkenswert ist immerhin die in dem folgenden Satz zu findende Fristbindung:

„Die Datenschutzaufsichtsbehörde soll innerhalb eines Monats über die Zustimmung nach Satz 4 Nummer 4 entscheiden.“

welche allerdings Ausnahmen (weil nur „soll“) zulässt.

Im Ergebnis sind die Regelungen des § 6 GDNG erfreulich und hilfreich, zwar auch von vielen Voraussetzungen abhängig, aber doch eine spürbare Verbesserung für die Forschung, die es weiter zu entwickeln gilt.

9. Legislative Handlungsoptionen zur Verbesserung der rechtlichen Rahmenbedingungen für klinische Forschung

9.1 Zusammenfassung der Analyse

Die Analyse der geltenden krankenhausspezifischen Regelungen der Länder und der konfessionellen Datenschutzbestimmungen zur Übermittlung von personenbezogenen Daten zu Forschungszwecken sowie zur Auftragsbearbeitung und Drittlandsübermittlung ergab zum Teil erhebliche Abweichungen von den Grundregelungen der DSGVO und des BDSG.

9.1.1 Übermittlung von personenbezogenen Daten zu Forschungszwecken

Die Übermittlung von personenbezogenen Daten zu Forschungszwecken ist nach Art. 9 Abs. 2 lit. j) DSGVO i.V.m. § 27 BDSG möglich, wenn Forschungsinteressen erheblich überwiegen. Zwar findet sich dieser Grundgedanke auch in den meisten Regelung der Landeskrankenhausgesetze und der konfessionellen Datenschutzbestimmungen wieder. Doch sehen eine Reihe von Ländern eine Prüfung dieser Interessenabwägung und Feststellung durch Behörden vor, die maßgeblich den Datenschutz zur Aufgabe haben (und deswegen befürchten lassen, dass das Forschungsinteresse dort institutionell geringere Bedeutung hat). In anderen Ländern bestehen zusätzliche Pflichten zur Dokumentation und oder zur Unterwerfung unter die Aufsicht des Landesdatenschutzes. Ausgerechnet im bevölkerungsreichsten Bundesland Nordrhein-Westfalen sind die Voraussetzungen insgesamt betrachtet so eng, dass die Forschung mit personenbezogenen Daten ohne entsprechende Einwilligung faktisch ausgeschlossen ist; in Schleswig-Holstein ist dies sogar gänzlich durch Gesetz untersagt.[61]

9.1.2 Auftragsbearbeitung und Drittlandsübermittlung

Die Auftragsbearbeitung ist nach den allgemeinen Regelungen der DSGVO und des BDSG unter bestimmten Anforderungen möglich (Art. 28 DSGVO und § 22 Abs. 2 BDSG). Kann der Dienstleister personenbezogene Gesundheitsdaten einsehen, ist er zur Verschwiegenheit nach § 203 StGB zu verpflichten. Auch hier finden sich aber weitergehenden Anforderungen in konfessionellen und länderspezifischen Datenschutzregelungen: Das Datenschutzgesetz der evangelischen Kirche etwa verpflichtet den Auftragsverarbeiter zur Unterwerfung unter die kirchliche Datenschutzaufsicht. Die Regelungen der Landeskrankenhausgesetze sehen zum Teil Begründungspflichten für Auftragsverarbeitung vor (so z.B. in Nordrhein-Westfalen, Saarland, in Sachsen-Anhalt und Thüringen). Sachsen-Anhalt räumt darüber hinaus ein spezifisches Widerspruchsrecht für Patienten gegen die Auftragsbearbeitung ein. Die strengste Regelung aber hat wiederum Schleswig-Holstein, welches allenfalls pseudonymisierte Daten

[61] Beachte allerdings den Vorschlag der Landesregierung die entsprechende Regelung in § 38 LKG zu streichen.

auf Auftrag verarbeiten lässt und damit etwa der Einrichtung einer Vertrauensstelle in Auftragsbearbeitung faktisch ausschließt.

Die Vermittlung von Daten in Drittländer des europäischen Auslands ist nach der DSGVO an keine weiteren Voraussetzungen geknüpft. Länder außerhalb der EU bedürfen eines sogenannten Angemessenheitsbeschlusses oder zusätzlicher Garantien, Art. 46 DSGVO. Die Landeskrankenhausgesetze enthalten keine darüber hinausgehenden Anforderungen; jedoch fordert das Datenschutzrecht der katholischen Kirche, dass ihre Datenschutzaufsicht ein angemessenes Datenschutzniveau in dem Drittland festgestellt hat.

9.2 Kernforderung

9.2.1 Einheitliche Grundregeln

Die Forschung mit personenbezogenen Daten braucht eindeutige und einheitliche Grundregeln. Insbesondere bei multizentrischen Studien, die für spezielle Fragestellungen und Therapien für seltene Erkrankungen unabdingbar sind, stellen landesspezifische und kirchliche Datenschutzregelungen zum Teil erhebliche Hindernisse und Verzögerungen für die Forschungsprojekte dar. Für multinationale Projekte innerhalb Europas wäre es stark förderlich, wenn die Nationalstaaten möglichst wenig zusätzliche Anforderungen gegenüber der DSGVO aufgestellt haben.

Forschung, welche auf die Verarbeitung von Personen bezogenen Daten angewiesen ist, braucht einheitliche Regelungen; zumindest in Deutschland, aber nach Möglichkeit auch für Europa. Zusätzliche Anforderungen des landesrechtlichen und kirchlichen Datenschutzes sind dürfen deshalb nicht für die Verarbeitung von Gesundheitsdaten zu Forschungszwecken gelten.

9.2.2 Einheitliche Zuständigkeit

Derzeit können multizentrische Studien unter Beteiligung von Krankenhäusern mit konfessionellen und kommunalen Trägern verschiedener Länder nur mit einer Vielzahl von Genehmigungen verschiedener Datenschutzaufsichtsbehörden durchgeführt werden. Da mit der Patientenrekrutierung erst begonnen werden kann, wenn auch die letzte Genehmigung vorliegt, stellt diese Heterogenität der Zuständigkeiten ein erhebliches Verzögerungsrisiko für die Forschungsprojekte dar. Darüber hinaus kann die unterschiedliche Zuständigkeit selbst dort, wo einheitliche Anforderungen bereits bestehen, unterschiedliche Auffassungen der beteiligten Aufsichtsbehörden auslösen. Die Schaffung von einheitlichen und effizienten Strukturen (z.B. die Einrichtung einer gemeinsamen Vertrauensstelle in Auftragsbearbeitung) wird aber verunmöglicht, wenn auch nur eine der zuständigen Datenschutzbeauftragten die Anforderungen (z.B. von Art. 28 DSG VO) als nicht erfüllt ansieht und Anpassungen verlangt, welche dann wiederum von allen anderen beteiligten Datenschutzbehörden zu genehmigen sind.

Zuständigkeiten, insbesondere für die Zulässigkeit der Auftragsverarbeitung und die Feststellung eines den Datenschutz überwiegenden Forschungsinteresses, sind bei einer zentralen Ethik-Kommission zu

bündeln, welche regelhaft den Bundesbeauftragten für den Datenschutz und Informationsfreiheit anzuhören hat und abschließend auch über die erforderlichen datenschutzrechtlichen Fragen entscheidet.

10. Gesetzesvorschläge

Die Analyse der heterogenen gesetzlichen Regelungen für die Verarbeitung von personenbezogenen Daten in der Forschung hat zu den beiden folgenden Kernforderungen geführt:

1. Die Forschung mit personenbezogenen Daten braucht eindeutige und einheitliche Grundregeln.

2. Bündelung der Zuständigkeiten für sämtliche nationalen datenschutzrechtlichen Genehmigungen im Zusammenhang mit medizinischer Forschung.

Dieses Kapitel befasst sich mit konkreten Vorschlägen zur Umsetzung der Kernforderungen in gesetzliche Neuregelungen.

Ein Regelungsbedarf besteht dabei sowohl für solche Forschungsvorhaben, bei denen eine Einwilligung der Studienteilnehmer ohnehin erforderlich ist (und deshalb auch den Datenschutz umfassen kann). Er besteht aber insbesondere für solche medizinische Forschung, welche eine gesetzliche Rechtsgrundlage braucht, weil die Einwilligungen der Betroffenen nur mit enormen Aufwand und vielfach nicht vollständig erreicht werden können (z.B. weil der aktuelle Wohnort des Betroffenen nicht ermittelbar ist).

10.1 Harmonisierung der LKG

Eine Möglichkeit zum Erreichen der Kernforderungen wäre die Harmonisierung der Regelungen der Länder und der Konfessionen, um sowohl einheitliche Rahmenbedingungen als auch übergeordnete Zuständigkeiten zu erreichen. So erscheint denkbar, dass Länder und Kirchen von der Sinnhaftigkeit des Vorhabens überzeugt werden können und sich in einem gemeinsamen Staatsvertrag verpflichten, datenschutzrechtliche Befugnisse für Kliniken in ihrem Zuständigkeitsbereich nach einem gemeinsamen gesetzlichen Muster zu regeln.

Für diesen Fall ist zu empfehlen, dass die Regelungen des BDSG als Muster genutzt werden, weil diese für Kliniken mit privater Trägerschaft ohnehin maßgeblich sind. Im Übrigen kann darauf gesetzt werden, dass bei einer entsprechenden Gestaltung der vertraglichen Verpflichtung auch zukünftige Anpassungen der Regelungen des BDSG von den Ländern daraufhin zu prüfen sind, ob gewichtige Gründe gegen deren Übernahme sprechen, sodass auch für die Zukunft eine einheitliche Regelung gewährleistet wäre.

Es erscheint jedoch aus den unten genannten Gründen (s.u. 10.2) fraglich, ob eine solche Initiative tatsächlich von allen Ländern und den Kirchen unterstützt werden würde.

10.2 Neue spezifische Gesetzesgrundlage für Datenverarbeitung in der Forschung

Vorzugswürdig gegenüber der Harmonisierung der landesrechtlichen Bestimmungen ist deshalb die Schaffung von speziellen bundesgesetzlichen Rechtsgrundlagen für die Datenverarbeitung im Rahmen der medizinischen Forschung. Diese Rechtsgrundlagen haben zur Erfüllung der Kernforderungen die Unsicherheiten und Hindernisse zu beseitigen:

1. Es bedarf einer eindeutigen und klaren Ermächtigung zur Verarbeitung medizinischer Daten zum Zwecke der Forschung, welche den Anforderungen von Art. 9 Abs. 2 lit. j DSGVO entspricht. Diese muss unabhängig von dem Träger der verantwortlichen Stelle die Voraussetzungen zur rechtlichen Verarbeitung von patientenbezogenen Gesundheit Daten regeln.

2. Entsprechend der Logik von § 27 Abs. 1 BDSG (und einer Reihe von landesgesetzlichen Bestimmungen) muss durch die Regelung klargestellt sein, dass die Verarbeitung von Gesundheitsdaten *„auch ohne Einwilligung für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke zulässig [ist], wenn die Verarbeitung zu diesen Zwecken erforderlich ist und die Interessen des Verantwortlichen an der Verarbeitung die Interessen der betroffenen Person an einem Ausschluss der Verarbeitung erheblich überwiegen*“. Regelbeispiele sollen dabei konturieren, wann von einem Überwiegen des Forschungsinteresses auszugehen ist.

3. Bei klinischen Prüfungen, welche das Votum einer Ethik-Kommission erfordern, ist die Feststellung über das Überwiegen des Forschungsinteresses durch die zuständige Ethik-Kommission und der Beteiligung des BfDI zu treffen. Die bereits vom BMG mit Ankündigung des Medizinforschungsgesetzes angekündigten Maßnahmen, nämlich Einrichtung einer Bundes-Ethik-Kommission beim Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) sowie Bestimmung von Bearbeitungsfristen und Musterformularen, ergänzt um Beratungsmöglichkeiten werden die Genehmigungsverfahren erleichtern und beschleunigen.

4. Bei Forschungsvorhaben, welche außerhalb von klinischen Prüfungen Gesundheitsdaten verarbeiten wollen, kann der Verantwortliche im Sinne von Art. 4 Nr. 7 DSGVO einen Antrag auf Feststellung des Überwiegens des Forschungsinteresses bei der Bundes-Ethik-Kommission stellen.

5. Auftragsbearbeitung und Drittlandsübermittlung erhalten eine eigene, den Anforderungen von Art. 28 DSGVO entsprechende Regelung. Auch diese tritt vollständig als speziellere Bestimmung anstelle von landesgesetzlichen und konfessionellen Datenschutzregelungen.

6. Der Verantwortliche im Sinne von Art. 4 Nr. 7 DSGVO kann bei der Bundes-Ethik-Kommission einen Antrag auf Feststellung stellen, dass die vorgesehene Auftragsbearbeitung und Drittlandsübermittlung den gesetzlichen Anforderungen entspricht.

7. Es wird gesetzlich klargestellt, dass eine Weiterverarbeitung für wissenschaftliche Forschungszwecke im Einklang mit dem Forschungsprivileg nach Art. 5 Abs. 1 lit b) DSGVO nicht der

Zweckbindung unterliegt und deshalb auch zu anderen Forschungszwecken verarbeitet werden dürfen, selbst wenn die Daten aufgrund einer Einwilligung verarbeitet wurden.

10.3 Regelungsvorschlag

Konkrete Umsetzung könnten diese Ziele durch den folgenden Paragrafen in einem Bundesgesetz erhalten:

§ X Verarbeitung von Gesundheitsdaten

(1) Die Rechtmäßigkeit der Verarbeitung von Gesundheitsdaten im Rahmen von medizinischer Forschung richtet sich unabhängig von dem Sitz oder der Trägerschaft der verantwortlichen nach § 27 Abs. 1 BDSG. Von einem Überwiegen der Interessen des Verantwortlichen an der Verarbeitung gegenüber den Interessen der betroffenen Person an einem Ausschluss der Verarbeitung ist auszugehen, wenn

- nur ein Datentreuhänder über Informationen verfügt, die eine Re-Identifizierung ermöglichen, und sämtliche weitere im Rahmen des Forschungsprojekts verarbeitende Stellen auch keine andere Möglichkeit haben, rechtmäßig an solche Informationen zu gelangen,

- das Forschungsprojekt durch öffentliche Mittel gefördert wird oder in öffentlich zugänglichen Registern aufgeführt ist.

(2) Bei Forschungsvorhaben, welche eine Genehmigung des Bundesinstituts für Arzneimittel und Medizinprodukte erfordern, ist die Feststellung über das Überwiegen des Forschungsinteresses durch das Bundesinstitut für Arzneimittel und Medizinprodukte unter der Beteiligung der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit und nach Stellungnahme der zuständigen Bundes-Ethik-Kommission innerhalb der für eine Genehmigung maßgeblichen Fristen zu treffen. Auf Antrag ist die Feststellung nach Satz 1 auch außerhalb eines Votums zu treffen; die Bearbeitungszeit darf nach Vorliegen des vollständigen Antrags einen Monat nicht überschreiten. Das Bundesinstitut für Arzneimittel und Medizinprodukte stellt Musterformulare zur Verfügung und berät auf Antrag zu den datenschutzrechtlichen Anforderungen des Forschungsvorhabens. Die Genehmigung nach Satz 1 und die Feststellung nach Satz 3 kann mit Nebenbestimmungen versehen werden.

(3) Die Anforderungen an die Auftragsverarbeitung bestimmen sich ausschließlich nach Artikel 28 Verordnung (EU) 2016/679 und die an die Drittlandsübermittlung von Gesundheitsdaten ausschließlich nach dem 5. Kapitel der Verordnung (EU) 2016/679.

(4) Eine Weiterverarbeitung für wissenschaftliche Forschungszwecke unterliegt nicht, auch nicht wenn die Daten aufgrund einer Einwilligung verarbeitet wurden, der Zweckbindung nach Artikel 5 Abs. 1 lit b) Unterabsatz 1 Verordnung (EU) 2016/679 und dürfen deshalb unter den Voraussetzungen nach Absatz 1 und Artikel 5 Absatz 1 lit b) Unterabsatz 2 Verordnung (EU) 2016/679 auch zu anderen Forschungszwecken verarbeitet werden.

(5) Liegt eine Einwilligung vor, welche aber nicht sämtliche Verarbeitungsvorgänge umfasst, können diese auch auf gesetzliche Grundlagen gestützt werden.

Dieser Vorschlag versteht sich als eine Arbeitsgrundlage, welche im Gespräch mit Forschenden und zu deren Schwierigkeiten bei der Nutzung von Gesundheitsdaten zu validieren und zu überarbeiten ist.

11. Zusammenfassung

1. Die Vielfalt landesrechtlicher und konfessioneller Bestimmungen mit unterschiedlichen Anforderungen an die Verarbeitung von Gesundheitsdaten in der medizinischen Forschung und divergierenden verfahrensrechtlichen Anforderungen mit heterogenen Zuständigkeiten sind ein erhebliches Hindernis für die medizinische Forschung.

2. Auch eine Einwilligung, welche bei prospektiven klinischen Prüfungen und Leistungsstudien ohnehin nach dem deutschen Recht erforderlich ist, kann selbst bei einer breiten und einheitlichen Formulierung als *broad consent* die vielfältigen Erfordernisse, weitere verarbeitende Stellen in das Forschungsprojekt mit einzubeziehen, den Verarbeitungszweck zu ändern oder die Daten zur Validierung mit anderen Daten zusammenzuführen, keine für die Forschungsarbeit hinreichende datenschutzrechtliche Grundlage bilden. Sie muss deshalb um gesetzliche Ermächtigungen erweiterbar und rechtssicher auch andere Zwecke (im Sinne des Forschungsprivilegs nach Art 5 Abs. lit b) DSGVO) der Verarbeitung umfassen.

3. Die Zuständigkeiten sind (weitergehend als von § 5 GDNG vorgesehen) datenschutzrechtlich, und in Bezug auf die Feststellung des (erheblichen) Überwiegens der Forschungs- gegenüber den Patienteninteressen bei der von dem Medizinforschungsgesetz vorgesehenen Bundes-Ethik-Kommission zu bündeln.

4. Das Verfahren muss den Forschenden schnelle Gewissheit bieten, dass ihr Forschungsvorhaben den geltenden datenschutzrechtlichen Anforderungen genügt. Die Bundes-Ethik-Kommission muss deshalb gesetzlich beauftragt werden, innerhalb einer vorgegebenen Bearbeitungszeit die abschließende Entscheidung über das Vorliegen sämtlicher datenschutzrechtlichen Anforderungen zu treffen und die forschenden Stellen mit Musterformularen und Beratung bei der Vorbereitung ihrer Eingaben zu unterstützen.

5. Diese Forderungen lassen sich insgesamt und umfassend nur durch eine neue und zentrale Ermächtigung zur Verarbeitung von Gesundheitsdaten zu Forschungszwecken im Medizinforschungsgesetz umsetzen, welche eindeutige und klare Anforderungen an die Verarbeitung der Daten und der Voraussetzungen für Auftragsverarbeitung und Drittlandsübermittlung stellt und eine rasche und abschließende Entscheidung über die datenschutzrechtliche Zulässigkeit des Forschungsprojekts gewährleistet.

***

Unterzeichnet von den folgenden Personen:

Joachim Maurice Mielert
Generalsekretär

Dr. Michael Meyer
Generalsekretär

Dr. Alexander Unger
Head of Innovation and Business Excellence

Finn Dierks
Senior Director, Legal, International

Prof. Dr. Markus Schwaiger
Präsident

Christian Thams
Head of Government Affairs & Policy Germany und Mitglied der Geschäftsleitung Johnson & Johnson Innovative Medicine

Prof. Dr. Sylvia Thun
Direktorin für Digitale Medizin und Interoperabilität

Mi-Young Miehler
Chief Operating Officer

Dr. Barbara Jonischkeit
Geschäftsführung, Leiterin strategische Kommunikation und Innovation

Maro Bader
Excellence Lead Digital Transformation

Dr. Claudia Luther
Geschäftsführung, Leiterin Branchenanalyse und Standortentwicklung

Prof. Dr. Dr. Frederik Wenz
Leitender Ärztlicher Direktor und Vorstandsvorsitzender Universitätsklinikum Freiburg

Dr. Andreas Jäcker
Associate Director, Government Affairs

Prof. Dr. Jochen Werner
Vorstandsvorsitzender und Ärztlicher Direktor der Universitätsmedizin Essen

Prof. Dr. Dr. Felix Balzar
Kommissarischer CIO

Dr. Georg Ralle
Generalsekretär