# RECHTSGUTACHTEN

## Lösungsvorschläge für ein neues Gesundheitsforschungsdatenschutzrecht in Bund und Ländern

**ERSTELLT AM**

**15.09.2019**

**FÜR DAS**

**Bundesministerium für Gesundheit**

**DURCH**


**Dierks + Company Rechtsanwaltsgesellschaft**

**RA Prof. Dr. med. Dr. iur. Christian Dierks**

Unter Mitarbeit von

RA Dr. iur. Philipp Kircher, RAin Charlotte Husemann, MLE

RA Dr. iur. Karsten Engelke, RAin Julia Pirk, Maîtrise en Droit

Dr. iur. Martin Haase, LL.M., LL.M. MLE



**Dierks+Company**
**Rechtsanwaltsgesellschaft mbH**

HELIX HUB
Invalidenstraße 113
D-10115 Berlin

T +49 30 586 930-000
F +49 30 586 930-099
info@dierks.company
**www.dierks.company**

SteuerNr. 30/261/50055
USt-IdNr. DE313860752
Amtsgericht Charlottenburg
HRB 190063 B

**Geschäftsführer**
Prof. Dr. med. Dr. iur.
Christian Dierks

Deutsche Apotheker- und Ärztebank
IBAN DE24 3006 0601 0008 0611 05
SWIFT DAAEDEDDXXX

# INHALTSÜBERBLICK

# Teil 1: Sachverhalt und Fragestellungen

Das Datenschutzrecht durchdringt – entsprechend seiner Natur als Querschnittsmaterie – weite Teile des deutschen Rechts. Nachdem sich in Deutschland seit den 1970er Jahren zunächst auf Initiative einzelner Bundesländer datenschutzrechtliche Gewährleistungen als Abwehrrechte gegen den Staat im Bereich der Eingriffsverwaltung entwickelt hatten, die infolge der Rechtsprechung des Bundesverfassungsgerichts zur Volkszählung (BVerfGE 65, 1) zunehmend bereichsspezifisch ausdifferenziert wurden, wurde zuletzt mit der Datenschutz-Grundverordnung (DS-GVO) der Europäischen Union ein neuer supranationaler Rahmen für die Verarbeitung personenbezogener Daten geschaffen. Unter diesem existieren nationale und regionale Normen, die sich aus unterschiedlichen Gesetzgebungskompetenzen und Öffnungsklauseln speisen.

In der medizinischen Forschung stellt sich die Regulierung der Verarbeitung personenbezogener Daten oft als Forschungshindernis dar, wenn Gesundheitsdaten oder Bioproben für medizinische Erkenntnisse qualitätsgesichert verarbeitet werden müssen und dies durch landesrechtliche Vorgaben von unterschiedlichen Voraussetzungen abhängig ist oder unterschiedliche Rechtsfolgen nach sich zieht. Die verteilten Strukturen der unabhängigen Datenschutzaufsichtsbehörden führen zusätzlich zu erhöhtem Abstimmungsbedarf, bürokratischem Aufwand und Rechtsunsicherheit.

Die DS-GVO adressiert öffentliche wie nicht-öffentliche Stellen gleichermaßen und präsentiert sich mit einigen Sonderklauseln bezüglich der Verarbeitung personenbezogener Daten zum Zweck der wissenschaftlichen Forschung als forschungsfreundliches Sekundärrecht mit unmittelbarer Wirkung in allen EU-Mitgliedstaaten. Anders als andere Verordnungen der Europäischen Union beinhaltet die DS-GVO jedoch sehr viele und teilweise sehr weit reichende Öffnungsklauseln, die es den Mitgliedstaaten ermöglichen oder sie verpflichten, bestehendes Datenschutzrecht aufrechtzuerhalten oder neue datenschutzrechtliche Regelungen zu erlassen. Dies betrifft auch die Verarbeitung der besonderen Kategorien personenbezogener Daten zu wissenschaftlichen Forschungszwecken, wovon insbesondere Gesundheitsdaten umfasst sind. In diesem Bereich ist daher auch mitgliedstaatliches Recht zu beachten.

In Ermangelung einer ausschließlichen Gesetzgebungskompetenz des Bundes für die Materie des Datenschutzes trifft die Idee der Zentralisierung und Vereinheitlichung des Datenschutzrechts in der EU allerdings in der Forschung mit Gesundheitsdaten auf einen föderal zersplitterten Umsetzungsrechtsrahmen innerhalb der Bundesrepublik Deutschland. Neben allgemeinen Forschungsklauseln des BDSG finden sich bundesrechtliche Spezialnormen etwa im SGB X hinsichtlich des Umgangs mit Sozialdaten, im SGB V hinsichtlich des Umgangs mit personenbezogenen Daten in der gesetzlichen Krankenversicherung, im Arzneimittelgesetz (AMG), Medizinproduktegesetz (MPG), Strahlenschutzgesetz (StrlSchG) hinsichtlich der Verarbeitung in klinischen Prüfungen sowie landesrechtlich in den 16 Landesdatenschutzgesetzen. 13 Länder haben zusätzlich Regelungen

in bereichsspezifischen Landesdatenschutzgesetzen (z.B. in elf Ländern in Landeskrankenhausgesetzen, in Nordrhein-Westfalen im Gesundheitsdatenschutzgesetz (GDSG NRW), in Bremen im Krankenhausdatenschutzgesetz (BremKHDSG) implementiert.

Während das BDSG, das SGB I i.V.m. dem SGB X sowie die allgemeinen Landesdatenschutzgesetze bereits an die DS-GVO angepasst wurden, gilt dies für das bereichsspezifische Datenschutzrecht nicht gleichermaßen. Nur in wenigen Spezialgesetzen ist eine Anpassungs- und Umsetzungsgesetzgebung erfolgt. So sind beispielsweise die fachspezifischen Bücher des SGB noch nicht an die DS-GVO angepasst und in fünf Bundesländern stehen Anpassungen der krankenhausspezifischen Gesetze noch aus.

Zusätzlich zu den oben genannten Datenschutzgesetzen kann das Datenschutzrecht der öffentlich-rechtlichen Religionsgemeinschaften anzuwenden sein, was insbesondere dann der Fall ist, wenn Krankenhäuser in kirchlicher Trägerschaft an Forschungsvorhaben teilnehmen. Das Recht der öffentlich-rechtlichen Religionsgemeinschaften folgt aus Art. 140 GG i.V.m. Art. 136, 137 Abs. 3 Satz 1 WRV und kann auch auf eine Öffnungsklausel in Art. 91 DS-GVO gestützt werden.

Moderne Forschungsvorhaben können als Big-Data-Analysen zunehmend datengestützt sein und sich neuer wissenschaftlicher Methoden wie etwa Künstlicher Intelligenz bedienen. Um einen ausreichend großen Datenpool zu generieren und die für ein Forschungsvorhaben erforderlichen Ressourcen zur Verfügung zu stellen, sind bundeslandübergreifende Forschungsvorhaben in Forschungsverbünden die Regel. Dabei kommt (nicht nur) nach Ansicht der Datenschutzkonferenz (DSK) eine gemeinsame Verantwortlichkeit im Sinne des Art. 26 DS-GVO in Betracht, sodass für jeden an einem Forschungsvorhaben Beteiligten ein anderes Datenschutzregime Anwendung findet. Aus der Pluralität der anwendbaren Datenschutznormen entstehen Gesetzeskonkurrenzen, Inkonsistenzen und Widersprüche.

Durch dieses nicht vereinheitlichte Datenschutzrecht im Bund und in den Ländern entsteht, auch vor dem Hintergrund der mit der DS-GVO erheblich gesteigerten Geldbußenbewehrung für unrechtmäßige Datenverarbeitungen, insbesondere in Fällen, in denen personenbezogene Gesundheitsdaten verarbeitet werden, ein erhebliches Forschungshindernis.

Hinzu treten weitere Beschränkungen durch Verschwiegenheitspflichten, wie sie aus den jeweiligen Berufsordnungen der Landesärztekammern sowie aus § 203 StGB folgen.

Der Schutz der informationellen Selbstbestimmung durch das Datenschutzrecht steht in verfassungsrechtlicher Dimension im Spannungsverhältnis mit der grundrechtlich garantierten Forschungsfreiheit. Um diese Grundrechtskollision in schonenden Ausgleich zu bringen und ungewollte Hindernisse für dem Allgemeinwohl dienende Forschungsvorhaben zu beseitigen, möchte das BMG die bestehenden datenschutzrechtlichen

Regelungen analysieren, Friktionen erkennen und Lösungen entwickeln. Dabei sind aktuelle Konzepte wie „Broad Consent“ und „Datenspenden“ sowie deren Vereinbarkeit mit dem datenschutzrechtlichen Rechtsrahmen zu berücksichtigen.

# Teil 2: Executive Summary

Der in der Bundesrepublik Deutschland gegenwärtig bestehende rechtliche Rahmen für die Verarbeitung personenbezogener Daten zu Forschungszwecken ist gekennzeichnet durch ein Normengeflecht von DS-GVO, Bundesdatenschutzgesetz, Landesdatenschutzgesetzen und Landeskrankenhausgesetzen mit eigenständigen Regelungen zur Forschung mit Patientendaten. Diese Zersplitterung mag für ein einzelnes Krankenhaus zwar anspruchsvoll, doch in der täglichen Praxis abbildbar sein. Für den Regelfall eines Forschungsverbunds mit Krankenhäusern in unterschiedlicher Trägerschaft über Landesgrenzen hinweg führt der legislative Flickenteppich zu einer schwer übersehbaren Regelungsvielfalt. Hieraus resultieren erhebliche Rechtsunsicherheiten und Nachteile für die Attraktivität des Forschungsstandortes Deutschland. Zusätzlich kompliziert wird die länderübergreifende Forschung durch die parallele Zuständigkeit der Landes- und des Bundesdatenschutzbeauftragten, der Datenschutzbeauftragten der evangelischen Landeskirchen und der Diözesandatenschutzbeauftragten. Die jeweils zuständigen Behörden nehmen ihre Aufgaben parallel und ohne Konzentrationsmöglichkeit oder ein formal geregeltes Verfahren zur Gewährleistung einer kohärenten Aufsichtstätigkeit wahr. Dies führt zu redundanten Verfahren, widersprüchlichen Ergebnissen und ist unwirtschaftlich.

Vor dem Hintergrund dieser Problembeschreibung erörtert das Gutachten potenzielle Handlungsoptionen zur Vereinfachung der Nutzung von Gesundheitsdaten zu Forschungszwecken. Unter Berücksichtigung der Gesetzgebungskompetenzen des Bundes zur Schaffung eines einheitlichen Rechtsrahmens für die länderübergreifende Forschung mit Patientendaten empfiehlt das Gutachten eine Ergänzung des Bundesdatenschutzgesetzes. Des Weiteren werden die dem Bund zur Verfügung stehenden Möglichkeiten beschrieben, Krankenhäuser in Trägerschaft der evangelischen und katholischen Kirche einzubeziehen. Zur Gewährleistung einer kohärenten Aufsichtstätigkeit aus einer Hand empfiehlt das Gutachten die Einrichtung einer federführenden Aufsichtsbehörde analog dem Beispiel der DS-GVO für Kontexte zwischen den Mitgliedstaaten. Ergänzend wird die legislative Kompetenz des Bundes zur Gestaltung einer sogenannten Datenspende geprüft und ein entsprechender Vorschlag unterbreitet.

Abschließend wird auf die Verpflichtung und Möglichkeit des Ministeriums hingewiesen, die Ausbildung und Vorlage von Verhaltensregeln nach Art. 40 DS-GVO zu fördern („Codes of Conduct“). Dieses Instrument bietet die Möglichkeit, auf europäischer Ebene ein einheitliches Verständnis darüber zu erarbeiten, wie zwischen dem Forschungsinteresse der Allgemeinheit und dem Schutzinteresse der betroffenen Personen abgewogen werden soll. Darüber hinaus können Vorgaben für die Pseudonymisierung in Forschungsvorhaben herausgearbeitet werden. Aus den entsprechenden Regelwerken können sich auch für die Fortentwicklung der Rechtssituation in Deutschland vielfältige Impulse ergeben.

# Teil 3: Europa- und verfassungsrechtlicher Rahmen

Das Datenschutzrecht speist sich zunächst aus dem supranationalen Primärrecht der Europäischen Union, das als „Verfassungsrecht der Union“ bezeichnet werden kann.[1] Neben dem Primärrecht der EU besteht das nationale Verfassungsrecht mit seinen grundrechtlichen Gewährleistungen und staatsorganisatorischen Vorgaben fort, auch wenn es infolge der supranationalen Überformung einem Deutungswandel unterzogen ist.[2] Jedenfalls insoweit als ein deutscher Gesetzgeber unionsrechtliche Vorgaben umsetzt, kommt es zur vorrangigen Anwendung supranationalen Verfassungsrechts – insbesondere also primärrechtlicher Grundrechtsgewährleistungen – vor nationalem Verfassungsrecht in diesem sog. unionsrechtlich determinierten Bereich.

## A. Primärrechtlicher Regelungsrahmen in der Europäischen Union

Das Primärrecht der Europäischen Union besteht aus dem Vertrag über die Europäische Union (EUV) [3] und dem Vertrag über die Arbeitsweise der Europäischen Union (AEUV)[4], den zugehörigen Protokollen und Anhängen sowie der Charta der Grundrechte der Europäischen Union (GRCh)[5], vgl. Art. 1 Abs. 3 Satz 2 EUV, Art. 51 EUV, Art. 6 Abs. 1 Hs. 2 EUV.[6]

Hinsichtlich datenschutzrechtlicher Gewährleistungen ergibt sich ein „Rechtsquellenpluralismus“[7] bereits auf unionsrechtlicher Ebene, da insbesondere Art. 7, 8 GRCh sowie Art. 16 AEUV rechtsverbindliche Grundrechtsgewährleistungen gewähren.[8] Ebenfalls beleuchtet werden soll die in Artikel 13 GRCh verbürgte Forschungsfreiheit.

### I. Vertrag über die Arbeitsweise der Europäischen Union (AEUV)

Zunächst ist festzuhalten, dass sich seit dem Vertrag von Lissabon in Art. 16 AEUV sowohl ein Datenschutzgrundrecht als auch eine datenschutzrechtliche Gesetzgebungskompetenz der Europäischen Union findet. Das damit in Art. 16 Abs. 1 AEUV neben Art. 8 GRCh (hierzu siehe sogleich) zweifach im Primärrecht der

---

1 *Ruffert* in: Callies/Ruffert (Hrsg.), EUV/AEUV, 5. Aufl., 2016, Art. 1 AEUV Rn. 4, 9.
2 *Masing*, NJW 2006, 264.
3 Vertrag über die Europäische Union (konsolidierte Fassung), ABl. C 202 vom 7.6.2016, S. 363–368.
4 Vertrag über die Arbeitsweise der Europäischen Union (konsolidierte Fassung), ABl. C 202 vom 7.6.2016, S. 368–390
5 Charta der Grundrechte der Europäischen Union (konsolidierte Fassung), ABl. C 202 vom 7.6.2016, S. 391–407.
6 *Ruffert* in: Callies/Ruffert (Hrsg.), EUV/AEUV, 5. Aufl., 2016, Art. 1 AEUV Rn. 8.
7 *Bretthauer*, in: Specht/Mantz (Hrsg.), Handbuch Europäisches und deutschen Datenschutzrecht, 2019, Teil A Rn. 6.
8 Es sei auf die Regelung in Art. 39 EUV hingewiesen, die jedoch wegen des Bezug auf die gemeinsame Außen- und Sicherheitspolitik (GASP) im vorliegenden Kontext außer Betracht bleiben kann. Auf Art. 8 EMRK wird wegen des bisher nicht erfolgten Beitritts der EU zur EMRK nicht eingegangen; dieser wäre für eine unmittelbare Verbindlichkeit auf unionaler Ebene gemäß Art. 6 Abs. 2 EUV erforderlich. Die Grundrechte der EMRK sind als allgemeine Grundsätze neben den Verfassungsüberlieferungen der Mitgliedstaaten als Rechtserkenntnisquelle bedeutsam, vgl. *Kingreen*, in: Calliess/Ruffert, EUV/AEUV, 5. Auflage 2016, Art. 6 EUV Rn. 7.

EU verankerte Datenschutzgrundrecht hat aber keine eigenständige Bedeutung.[9] Der schrankenfrei formulierte Art. 16 Abs. 1 AEUV soll nicht die Schranken des Art. 8 GRCh unterminieren.[10] Art. 16 Abs. 1 AEUV bleibt daher in der weiteren Betrachtung außer Acht.

Anders hingegen der in Art. 16 Abs. 2 AEUV normierte Datenschutzgesetzgebungskompetenztitel der EU: Während die DS-RL in Ermangelung eines allgemeinen Kompetenztitels der EU im Bereich der Datenverarbeitung noch auf die Binnenmarktharmonisierungskompetenz (ex-Art. 100a EGV, jetzt Art. 114 AEUV) gestützt werden musste, wurde mit Art. 16 Abs. 2 AEUV ein spezieller Gesetzgebungskompetenztitel (neben der Kompetenz nach Art. 39 AEUV im Bereich der GASP) geschaffen, der einheitliches Datenschutzrecht ermöglicht, welches die Organe, Einrichtungen und sonstigen Stellen der Union sowie die Mitgliedstaaten bei datenverarbeitenden Tätigkeiten im Anwendungsbereich des Unionsrechts bindet. Als Querschnittsmaterie ist der Datenschutz unabhängig von spezifischen Kompetenzen in den übrigen unionalen Tätigkeitsfeldern. Art. 16 Abs. 2 AEUV knüpft aber gerade nicht an diesen Sektoren sondern an den Umgang mit Daten an und ist insofern spezieller.[11] Art. 16 Abs. 2 AEUV hat sich also von der Akzessorietät der Binnenmarktkompetenz nach Art. 114 AEUV emanzipiert und ermöglicht ein umfassendes europäisches Datenschutzrecht.[12]

## II. Charta der Grundrechte der Europäischen Union (GRCh)

Im Kontext der Verarbeitung personenbezogener Daten zu Forschungszwecken stehen sich regelmäßig kollidierende Grundrechtsgewährleistungen von unterschiedlichen Grundrechtträgern gegenüber, die in schonenden Ausgleich gebracht werden müssen. Das Forschungsdatenschutzrecht kleidet also das Spannungsverhältnis zwischen dem Schutz personenbezogener Daten einerseits und der Forschungsfreiheit auf der anderen Seite aus. Im Anwendungsbereich der Charta der Grundrechte der Europäischen Union ist daher der Fokus auf die Gewährleistung von Privatleben und Datenschutz (Art. 8 GRCh iVm Art. 7 GRCh) und Forschungsfreiheit (Art. 13 GRCh) zu legen.

### 1. Anwendungsbereich

Die GRCh enthält verbindliche Grundrechtsgewährleistungen, die für die Organe, Einrichtungen und sonstigen Stellen der Union unter Wahrung des Subsidiaritätsprinzips und für die Mitgliedstaaten **ausschließlich bei der Durchführung des Rechts der Union verbindlich sind** (Art. 52 Abs. 1 S. 1 GRCh). Sie dehnt den Geltungsbereich des Unionsrechts nicht über die Zuständigkeiten der Union hinaus aus und begründet weder neue Zuständigkeiten noch neue Aufgaben für die Union, noch ändert sie die in den Verträgen festgelegten

---

9 *Kircher*, Der Schutz personenbezogener Gesundheitsdaten im Gesundheitswesen, 2016, S. 55; *Kühling/Raab*, in: Kühling/Buchner (Hrsg.), DS-GVO / BDSG, 2. Aufl. 2018, Teil A. Einführung Rn. 35.

10 *Kingreen,* in: Callies/Ruffert (Hrsg.), EUV/AEUV, 5. Aufl., 2016, Art. 8 GRCh Rn. 3.

11 *Kühling/Raab*, in: Kühling/Buchner (Hrsg.), DS-GVO / BDSG, 2. Aufl. 2018, Teil A. Einführung Rn. 8.

12 Ehmann/Selmayr, DS-GVO vor Art. 1 Rn. 36, beck-online

Zuständigkeiten und Aufgaben (Art. 52 Abs. 2 GRCh). Bei der Frage, wann Unionsrecht durchgeführt wird, ist zu beachten, dass das Unionsrecht sowohl das Primär- als auch Sekundärrecht, sowie das auf dieser Grundlage von Unionsorganen und weiteren Unionseinrichtungen erlassene Tertiärrecht umfasst. Das in Umsetzung der Datenschutz-Richtlinie 95/46/EG (DS-RL) und nun auch der Datenschutz-Grundverordnung (EU) 2016/679 (DS-GVO) geschaffene oder angewendete Recht – unabhängig davon, ob es sich um unionales oder nationales Recht handelt, fällt in den Anwendungsgebereich der GRCh. Dabei ist es unerheblich, ob eine „Durchführungsabsicht“[13] bestand oder Regelungen des nationalen Rechts nachträglich in den Dienst unionsrechtlicher Ziele gestellt wurden. [14]

Die Gewährleistungen der GRCh stehen neben solchen Unionsgrundrechten, die der EuGH auf der Basis der Rechtserkenntnisquellen der gemeinsamen Verfassungsüberlieferungen der Mitgliedstaaten und der EMRK entwickelt hat und die ebenfalls verbindlich gelten (Art. 6 Abs. 3 EUV).[15]

## 2. Datenschutzgrundrecht – Art. 8 GRCh

Artikel 8 zum Schutz personenbezogener Daten lautet:

> *(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.*
>
> *(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.*
>
> *(3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.*

Anders als im Grundgesetz wurde in **Art. 8 GRCh ein eigenes Datenschutzgrundrecht** kodifiziert. Es handelt sich nicht um einen bloßen Grundsatz i.S.d. Art. 52 Abs. 5 GRCh.[16] Während Art. 8 Abs. 1 GRCh allgemein das Recht einer jeden Person auf Schutz der sie betreffenden personenbezogenen Daten „konstitutionalisiert“, beinhalten Abs. 2 und 3 Schutzelemente eines effektiven Datenschutzgrundrechts.[17] So werden materiell-rechtlich bereits der **Zweckbindungsgrundsatz** sowie die **Legitimationstatbestände** der Einwilligung oder einer sonstigen

---

13 *Ohler*, NVwZ 2013, 1433 (1434).
14 *EuGH*, Urt. V. 26.02.2013, Rs. C-617/10, Rn.28 – Åkerberg Fransson; a.A. noch GA Cruz Villalón, Schlussanträge v. 12.06.2012 zur Rs. C-617/10, Rn. 60.
15 *Streinz* in: Streinz (Hrsg.), EUV/AEUV, 3. Aufl. 2018, Art. 1 GRCh Rn. 13.
16 *Streinz* in: Streinz (Hrsg.), EUV/AEUV, 3. Aufl. 2018, Art. 8 GRCh Rn. 6.
17 *Kühling/Raab* in: Kühling/Buchner (Hrsg.), DS-GVO BDSG, 2. Auflage 2018, Einf. Rn. 26.

gesetzlich geregelten legitimen Grundlage festgeschrieben, prozedural wird das **Auskunfts-** und **Berichtigungsrecht** gewährleistet und institutionell das Erfordernis einer **unabhängigen Aufsichtsbehörde** formuliert.[18]

Die vorgenannten Anforderungen sind damit nicht mehr nur das Ergebnis von Auslegungen oder die Folge einfachrechtlicher Gesetzgebung, sondern müssen als **wesentliche Grundsätze des Primärrechts** – also mit europäischem Verfassungsrang, und somit auf normhierarchisch höchster Stufe – verstanden werden.

Der Schutzbereich ist auf personenbezogene Daten beschränkt, ohne dass Art. 8 GRCh eine Legaldefinition enthielte. Bei Art. 8 GRCh handelt es sich um ein normgeprägtes Grundrecht, sodass auf die sekundärrechtlichen Definitionen (vgl. Art. 4 Nr. 1 DS-GVO) hierzu herangezogen werden.[19] Nicht erfasst sind im Umkehrschluss anonyme Daten.[20] Eine Binnenmarktrelevanz der Daten ist nicht erforderlich.[21]

Ein Eingriff in den Schutzbereich kann entweder durch eine Einwilligung ausgeschlossen[22] oder im Fall des Eingreifens einer gesetzlich geregelten Grundlage gerechtfertigt werden. Eine solche Rechtsgrundlage muss ein legitimes Ziel verfolgen, verhältnismäßig sein und den Erforderlichkeitsgrundsatz wahren. Nach ständiger Rechtsprechung des EuGH erfordern Einschränkungen des Schutzes personenbezogener Daten eine Beschränkung auf das „absolut Notwendige".[23]

Art. 8 GRCh steht in engem Verhältnis zu Art. 7 GRCh, wonach jede Person das Recht **auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation** hat. Wegen der Überschneidungen des Schutzes von Privatleben und Datenschutz wird Art. 7 GRCH in der Rechtsprechung des Europäischen Gerichtshofs (EuGH) meist zusammen mit Art. 8 GRCh geprüft.[24] Dem EuGH zufolge besteht zwischen den beiden Grundrechten des Art. 7 GRCh und des Art. 8 GRCh Idealkonkurrenz; in der Literatur wird hingegen vertreten, dass Art. 8 GRCh *lex specialis* zu Art. 7 GRCh ist.[25] Der Begriff „Privatleben" ist offen und erfasst nicht nur die Ausschnitte des aktiven Lebens, sondern auch den Schutz der Persönlichkeit und das Für-sich-Sein des Menschen sowie die Entfaltung der eigenen Persönlichkeit auch im sozialen Umfeld.[26] Ein Auffanggrundrecht im Sinne einer

---

18 *Kühling/Raab* in: Kühling/Buchner (Hrsg.), DS-GVO BDSG, 2. Auflage 2018, Einf. Rn. 26.

19 Kritisch hierzu: Britz, EuGRZ 2009, 1 (7); *Kircher*, Der Schutz personenbezogener Gesundheitsdaten im Gesundheitswesen, 2016, S. 58; *Bretthauer*, in: Specht/Mantz (Hrsg.), Handbuch Europäisches und deutschen Datenschutzrecht, 2019, Teil A Rn. 13.

20 Wann eine Person im Sinne der Definition des Art. 4 Nr. 1 DS-GVO noch als identifizierbar gilt, sodass sie betreffende Informationen als personenbezogen anzusehen sind, ergibt sich aus Erwägungsgrund 26 der DS-GVO. Vgl. zum nahezu gleichlautenden Erwägungsgrund 26 der DS-RL auch die Rechtsprechung des *EuGH*, Urt. v. 19.10.2016 Rs. C-582/14 Rn. 43 ff. – Breyer. Zur Übertragbarkeit der Rechtsprechung auf die DS-GVO *Dierks/Kircher*, in: Trill (Hrsg.), Praxisbuch eHealth, 2. Aufl. 2018, S. 114 ff.

21 Jarass, Charta der Grundrechte der EU, 3. Auflage 2016, Art. 8 Rn. 6.

22 Jarass, Charta der Grundrechte der EU, 3. Auflage 2016, Art. 8 Rn. 9.

23 *EuGH*, Urt. v. 8.4.2014, verb. Rs. C-293/12 u. C-594/23, Rn. 52 – Digital Rights Ireland.

24 *Bretthauer*, in: Specht/Mantz (Hrsg.), Handbuch Europäisches und deutschen Datenschutzrecht, 2019, Teil A Rn. 10.

25 *Streinz* in: Streinz (Hrsg.), EUV/AEUV, 3. Aufl. 2018, Art. 8 GRCh Rn. 4a m.w.N.; *Kühling/Raab* in: Kühling/Buchner (Hrsg.), DS-GVO BDSG, 2. Auflage 2018, Einf. Rn. 26 m.w.N.; *Kingreen* in: Callies/Ruffert (Hrsg.), EUV/AEUV, 5. Aufl., 2016, Art. 8 GRCh Rn. 1a.

26 *Wolff*, in: Schantz/Wolff, Das neue Datenschutzrecht, 2017, Teil A. Rn. 31.

allgemeinen Handlungsfreiheit enthält Art. 7 GRCh hingegen nicht.[27] Art. 7 GRCh fällt insbesondere bei Abwägungen hinsichtlich der Intensität eines Eingriffs in das Datenschutzgrundrecht zusätzlich ins Gewicht.[28]

### 3. Forschungsfreiheit – Art. 13 GRCh

**Art. 13 GRCh** besagt, dass Kunst und Forschung frei sind und die akademische Freiheit geachtet wird. Die hier maßgebliche **Forschungsfreiheit** ist – soweit ersichtlich – bisher noch nicht Gegenstand der Rechtsprechung des *EuGH* gewesen, sodass eine Konturierung des Grundrechts durch die Judikative fehlt, obgleich wegen der Zielsetzungen der Forschungspolitik nach Art. 179 AEUV ein unionaler Handlungsspielraum besteht, der mit Eingriffen einhergehen könnte.[29]

Der Begriff der Forschung wird in Art. 13 GRCh nicht legaldefiniert. Aus den europäischen Verfassungsüberlieferungen ergeben sich unterschiedliche Auffassungen einer solchen Definition, weshalb vorgeschlagen wird, die Intention wissenschaftlicher Betätigung im Europarecht als „methodisch geleitetes Generieren neuen Wissens“ zu verstehen, wobei entsprechend dem Wortlaut der Norm keine Differenzierung zwischen Grundlagenforschung und angewandter Forschung erfolgen sollte.[30]

In der juristischen Literatur wird vertreten, dass von freier Wissenschaft zu erwarten sei, dass sie zu wissenschaftlichem Fortschritt führt und daher Nutzen für das Gemeinwesen haben kann, sodass mit der Forschungsfreiheit die Erwartung von Innovation verbunden wird; diese gesellschaftliche „Schlüsselfunktion“ gelte auch in der EU und wirke schutzverstärkend.[31]

Keine Einschränkungen soll es hinsichtlich der vom Schutzbereich erfassten Personen oder Tätigkeiten geben: Jedermann kann daher Träger der Wissenschaftsfreiheit sein, wobei alle forschungsbezogenen Tätigkeiten von der Vorbereitung über die Planung, Unterstützung und Durchführung bis hin zur Publikation und Verwertung umfasst sind.[32]

## B. Sekundärrechtlicher Regelungsrahmen in der Europäischen Union

Das Europäische Sekundärrecht sieht an verschiedenen Stellen datenschutzrechtliche Regelungen zu wissenschaftlicher Forschung vor. Ausgangspunkt ist hierbei die Datenschutz-Grundverordnung (DS-GVO).

---

27 *Jarass*, Charta der Grundrechte der EU, 3. Auflage 2016, Art. 7 Rn. 3.
28 *Wolff*, in: Schantz/Wolff, Das neue Datenschutzrecht, 2017, Teil A. Rn. 34.
29 *Ruffert*, in: Calliess/Ruffert (Hrsg.), 5. Aufl. 2016, EUV/AEUV, Art. 13 GRCh Rn. 2.
30 *Ruffert*, in: Calliess/Ruffert (Hrsg.), 5. Aufl. 2016, EUV/AEUV, Art. 13 GRCh Rn. 6.
31 *Ruffert*, in: Calliess/Ruffert (Hrsg.), 5. Aufl. 2016, EUV/AEUV, Art. 13 GRCh Rn. 7 m.w.N.
32 *Ruffert*, in: Calliess/Ruffert (Hrsg.), 5. Aufl. 2016, EUV/AEUV, Art. 13 GRCh Rn. 8.

Daneben bestehen im Kontext der medizinischen Forschung insbesondere arzneimittelrechtliche und medizinprodukterechtliche Regelungen.

## I. Datenschutz-Grundverordnung (DS-GVO)

Nachdem sich der Europäische Rat, das Europäische Parlament und die Europäische Kommission am 15. Dezember 2015 über die Inhalte der neuen Verordnung „zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)“ geeinigt hatten, und das Europäische Parlament die Verordnung am 14. April 2016 verabschiedet hatte, wurde diese am 27. April 2016 erlassen. Nach ihrer Veröffentlichung im Amtsblatt der Europäischen Union[33] am 04. Mai 2016 trat sie gemäß Art. 99 DS-GVO am 24. Mai 2016 in Kraft und erlangte am 25. Mai 2018 Wirkung.

### 1. Allgemeines

Während nach bisher geltender Rechtslage das allgemeine Datenschutzrecht lediglich unter Zuhilfenahme des Instruments der Richtlinie im Sinne des Art. 288 Abs. 3 AEUV durch die Richtlinie 95/46/EG (Datenschutz-Richtlinie, DS-RL) vorgegeben, sodass die Mitgliedstaaten hinsichtlich der Wahl der Form und der Mittel der Umsetzung der Richtlinie im nationalen Recht frei waren, prägt die DS-GVO das Datenschutzrecht nun wesentlich stärker vor. Der starke Einfluss der DS-GVO ergibt sich aus ihrer Rechtsnatur. Die DS-GVO ist eine Verordnung im Sinne des Art. 288 Abs. 2 AEUV und hat daher allgemeine Geltung. Sie ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedsstaat.

Mit dem Ziel der weitgehenden Vollharmonisierung des europäischen Datenschutzrechts wurde bewusst die Abkehr vom bisherigen Regelungsinstrument der Richtlinie beschlossen. Als „Grund“-Verordnung sah sie allerdings schon nach dem Entwurf der Kommission Ermächtigungsgrundlagen für delegierte Rechtsakte und Durchführungsakte von Parlament und Rat vor. Die Wirkung der Vollharmonisierung wurde dadurch eingeschränkt. Anstelle der ursprünglich geplanten delegierten Rechtsakte und Durchführungsakte enthält die DS-GVO nunmehr an die Mitgliedstaaten gerichtete Öffnungsklauseln, die punktuell Elemente einer Richtlinie nach Art. 288 Abs. 3 AEUV implementieren, indem sie **Regelungsbefehle und -spielräume für die mitgliedstaatlichen Gesetzgeber** schaffen. Die DS-GVO ist daher ein „Hybrid“[34] zwischen Verordnung und Richtlinie und kann sogar als ein Novum im Kanon der sekundärrechtlichen Rechtsakte der Europäischen Union begriffen werden.

---

[33] Verordnung (EU) 2016/679, Abl. L 119 vom 04.05.2016, 1; korrigiert durch Abl. L 314 vom 22.11.2016, 72.

[34] *Kühling/ Martini* et al., Die DSGVO und das nationale Recht, 2016, S. 1, die auch von einer "Richtlinie im Verordnungsgewand“ sprechen.

Im Ergebnis ist daher bei der Rechtsanwendung zunächst zu prüfen, ob die DS-GVO Anwendung findet, diese selbst eine Datenverarbeitung zur Forschungszwecken reguliert und eine Verarbeitung erlaubt, oder aber eine Öffnungsklausel besteht, in deren Rahmen der nationale Gesetzgeber regeln kann oder muss. Sodann wäre diese zu identifizieren und auf ihre Anwendbarkeit zu prüfen.

## 2. Sachlicher Anwendungsbereich der DS-GVO

Die DS-GVO gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung von personenbezogenen Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen (Art. 2 Abs. 1 DS-GVO).

### a) Personenbezogene Daten

Der Begriff der **personenbezogenen Daten** ist in Art. 4 Nr. 1 HS. 1 DS-GVO definiert als

> *„alle Informationen, die sich auf eine identifizierte oder **identifizierbare** natürliche Person (im Folgenden „betroffene Person“) beziehen;“*[35]

Die Neufassung unterstreicht, dass der Gesetzgeber auf eine breite Auslegung des Begriffes abzielt.[36] Lediglich beispielhaft und nicht abschließend werden in Art. 4 Nr. 1 HS. 2 DS-GVO Zuordnungen zu Kennungen wie Namen, Kennnummern, Standortdaten, Online-Kennungen oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, aufgeführt, anhand derer eine natürliche Person identifiziert werden kann.

Es muss also eine Information über eine natürliche Person und nicht nur ein bloßes Sachdatum vorliegen.[37] Außerdem muss die betreffende Person mindestens **identifizierbar** (oder sogar identifiziert) sein. Ab wann eine Person als identifizierbar gilt, wird im rechtsverbindlichen Normtext der DS-GVO nicht geregelt. Allerdings lassen sich wesentliche Anhaltspunkte aus Erwägungsgrund 26 gewinnen. Dort heißt es:

> *„Die Grundsätze des Datenschutzes sollten für alle Informationen gelten, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Einer Pseudonymisierung*

---

35 Hervorhebungen in Zitaten sind sämtlich nicht im Original
36 Ehmann/Selmayr/Klabunde, 2. Aufl. 2018, DS-GVO Art. 4 Rn. 7.
37 Kühling/Buchner/Klar/Kühling, 2. Aufl. 2018, DS-GVO Art. 4 Nr. 1 Rn. 12-14

> *unterzogene personenbezogene Daten, die durch Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden könnten, sollten als Informationen über eine identifizierbare natürliche Person betrachtet werden. Um festzustellen, ob eine natürliche Person* ***identifizierbar*** *ist, sollten* ***alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren****, wie beispielsweise das Aussondern. 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****. Die Grundsätze des Datenschutzes sollten daher nicht für anonyme Informationen gelten, d. h. für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann. (…)"*.

Hieraus ergibt sich, dass nicht alle erdenklichen Mittel, unter deren Zuhilfenahme eine natürliche Person identifiziert werden könnte, beachtlich sind, sondern nur solche, die nach allgemeinem Ermessen wahrscheinlich genutzt werden, wobei objektive Faktoren wie Kosten und Zeitaufwand und die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen beachtet werden müssen.

Aus Erwägungsgrund 26 der DS-GVO sowie aus der Rechtsprechung des Europäischen Gerichtshofs (EuGH) vom 19.10.2016 zum Personenbezug von dynamischen IP-Adressen[38] lässt sich folgern, dass keine absolute Anonymität erforderlich ist sondern **faktische Anonymität** ausreicht. Mit anderen Worten ist es zum Ausschluss eines Personenbezugs nicht erforderlich, dass Daten von niemandem in Bezug zu einer bestimmten Person gesetzt werden können, sondern es ausreicht,

> *„wenn die Identifizierung der betreffenden Person gesetzlich verboten oder praktisch nicht durchführbar wäre, z. B. weil sie einen unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskräften erfordern würde, so dass das Risiko einer Identifizierung de facto vernachlässigbar erschiene." (EuGH*, Urteil vom 19.10.2016, Rs. C-582/14 – Breyer, Rn. 46*)*

[38] *EuGH*, Urteil vom 19.10.2016, Rs. C-582/14 – Breyer.

Daraus folgt auch, dass nicht jedes bei einem Dritten vorliegende Wissen beachtlich ist, sondern nur solches, das mit legitimen (also rechtmäßigen) und mit nach allgemeinem Ermessen wahrscheinlich genutzten Mitteln erlangt werden kann. Ein Datum kann nach der Rechtsprechung des *EuGH* also für eine Stelle personenbezogen sein, während es für eine andere Stelle, die über erforderliches Zusatzwissen nicht verfügt, anonym sein kann (sog. **relativer Personenbezug**).[39]

Nach der Rechtsprechung des *EuGH* ist es für das Vorliegen eines Personenbezugs aber jedenfalls ausreichend, wenn das zur Identifikation erforderliche Zusatzwissen eines Dritten über ein legitimes Mittel erlangt werden kann.[40]

### b) Ausschluss der Anwendbarkeit

Der sachliche Anwendungsbereich der DS-GVO ist gemäß Art. 2 Abs. 2 DS-GVO hingegen nicht eröffnet, wenn die Verarbeitung personenbezogener Daten **nicht in den Anwendungsbereich des Unionsrechts** fällt, sie in den Rahmen von Tätigkeiten der **gemeinsamen Außen- und Sicherheitspolitik** fällt, sie durch natürliche Personen zur Ausübung **ausschließlich persönlicher oder familiärer Tätigkeiten** oder sie durch die zuständigen Behörden zum Zwecke der **Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit** erfolgt.

Weiterhin gilt die DS-GVO nicht für personenbezogene Daten **Verstorbener**, sie überlässt es jedoch den Mitgliedstaaten dies im nationalen Recht abweichend zu regeln, was teilweise auch geschehen ist.[41]

## 3. Verarbeitung personenbezogener Daten zu Forschungszwecken nach der DS-GVO

Die DS-GVO kann als forschungsfreundlich bezeichnet werden, ohne dass sie jedoch eine umfassende Privilegierung wissenschaftlicher Zwecke enthält.[42] Sie setzt für eine rechtmäßige Datenverarbeitung im Sinne einer Zulässigkeit („Ob“) stets voraus, dass eine **Einwilligung oder ein gesetzlicher Erlaubnistatbestand** die Verarbeitung legitimieren. Dieses Verbot mit Zulässigkeitsvorbehalt folgt bereits aus Art. 8 Abs. 2 S. 1 GRCh, der seinen Niederschlag in Art. 6 Abs. 1 S. 1 DS-GVO („nur rechtmäßig wenn“) gefunden hat.

Für **besondere Kategorien personenbezogener Daten**, also solche Daten, die nach Ansicht des Gesetzgebers per se besonders sensibel und daher schützenswert sind, besteht darüber hinaus ein ausdrückliches Verbot der Verarbeitung (Art. 9 Abs. 1 DS-GVO), welches nur in den Fällen des Art. 9 Abs. 2 DS-GVO nicht gilt. Zu den

---

39 *Kühling/Klar*, Anmerkung zu EuGH, Urt. V. 19.10.2016, C-582/14, ZD 2017, 24 (27).
40 *EuGH*, Urteil vom 19.10.2016, Rs. C-582/14 – Breyer.
41 Erwägungsgrund 27 der DS-GVO. Vgl. hierzu etwa § 35 Abs. 5 SGB I.
42 *Gola*, , in: Specht/Mantz (Hrsg.), Handbuch Europäisches und deutschen Datenschutzrecht, 2019, § 23 Rn. 4.

besonderen Kategorien personenbezogener Daten gehören neben solchen, aus denen die rassische und ethnische Herkunft, politischen Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, auch genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Daten zum Sexualleben oder der sexuellen Orientierung eine natürlichen Person und insbesondere auch **Gesundheitsdaten**.

Der Kanon der unmittelbar eingreifenden Ermächtigungsgrundlagen in Art. 6 und Art. 9 DS-GVO sieht nicht ohne Weiteres vor, dass personenbezogene Daten zu Forschungszwecken verarbeitet dürfen. Nicht-sensible personenbezogene Daten könnten aber grundsätzlich auf Basis einer Einwilligung (Art. 6 Abs. 1 lit. a) DS-GVO) oder auf gesetzlicher Basis in Wahrnehmung einer Aufgabe im öffentlichen Interesse verarbeitet werden (Art. 6 Abs. 1 lit. e) DS-GVO. Eine Verarbeitung von Gesundheitsdaten kann auf dieser Grundlage jedoch nicht erfolgen. Hierzu müsste ein Tatbestand nach Art. 9 Abs. 2 DS-GVO eingreifen. Eine Verarbeitung zu Forschungszwecken ist jedoch, ohne dass weitere Erlaubnistatbestände aus dem Recht der Europäischen Union oder dem Recht der Mitgliedstaaten eingreifen, nur auf Basis einer ausdrücklichen Einwilligung nach Art. 9 Abs. 2 lit. a) DS-GVO zulässig. Einen selbstständigen Forschungstatbestand kennt die DS-GVO insofern nicht.

## 4. Öffnungsklauseln

Die Öffnungsklauseln der DS-GVO sind die Einfallstore für die nationale Gesetzgebung. Nur in den Grenzen dieser Öffnungsklauseln und unter Beachtung der Vorgaben des unionsrechtlichen und des nationalen Verfassungsrechts kommt eine nationale Datenschutzgesetzgebung in Betracht. Öffnungsklauseln sind unterschiedlich gestaltet. In der juristischen Literatur ist bereits die Zahl der Öffnungsklauseln uneinheitlich beschrieben.[43] Für die sich daraus ergebenden Gesetzgebungsspielräume gilt das erst recht. Die Aufarbeitung der inhaltlichen Vorgaben ist daher eine wesentliche Vorarbeit für die Analyse des verbleibenden Gestaltungsspielraums der mitgliedstaatlichen Gesetzgeber.

Werden mit einer Öffnungsklausel Regelungen durch eine **mitgliedstaatliche Rechtsvorschrift** ermöglicht, meint die DS-GVO gemäß Erwägungsgrund 41 nicht nur formelle Gesetze (Parlamentsgesetze), sondern auch materielle Gesetze (z.B. Rechtsverordnungen). Ob diese ein taugliches Instrument im jeweiligen Mitgliedsstaat darstellen, bestimmt sich nach dem jeweiligen Verfassungsrecht.

[43] Von rund vier Dutzend ausgehend: *Kühling/ Martini* et. al., Die DSGVO und das nationale Recht, 2016, S. 1; mehr als 70 zählen *Buchner/ Schwichtenberg*, GuP 2016, 218 (219).

## a) Typologie der Öffnungsklauseln

### aa) Echte und unechte Öffnungsklauseln

Es können sog. „echte Öffnungsklauseln“ von „unechten Öffnungsklauseln“ unterschieden werden. Ergibt sich aus dem Wortlaut unzweideutig ein Regelungsauftrag oder eine Regelungsoption für die Mitgliedsstaaten („die Mitgliedsstaaten sehen vor“, „Mitgliedsstaaten können vorsehen“), so handelt es sich um „echte Öffnungsklauseln“. Wird hingegen nur auf das Recht der Mitgliedsstaaten verwiesen, so kann dies entweder als eigene (echte) Öffnungsklausel zu interpretieren sein, oder aber als bloßer Verweis auf eine an anderer Stelle der DS-GVO existierende Öffnungsklausel; in letzterem Fall läge eine „unechte Öffnungsklausel“ vor.[44] Im Ergebnis sind unechte Öffnungsklauseln also keine Öffnungsklauseln.

### bb) Fakultative und obligatorische Öffnungsklauseln

Öffnungsklauseln lassen sich weiter in zwei Kategorien unterscheiden. Zum einen gibt es fakultative Öffnungsklauseln, die den Mitgliedsstaaten die Option zur Gesetzgebung offenhalten und die entsprechenden Gestaltungsspielräume definieren, zum anderen gibt es obligatorische Öffnungsklauseln, die Ausfüllungspflichten beinhalten.[45]

### cc) Drei Handlungsmöglichkeiten bei fakultativen Öffnungsklauseln

Die Handlungsoptionen eines mitgliedstaatlichen Gesetzgebers ergeben sich aus den jeweiligen Öffnungsklauseln. Während obligatorische Öffnungsklauseln im Einzelnen festlegen, was ein Mitgliedsstaat tun muss, bestehen bei fakultativen Öffnungsklauseln drei Handlungsvarianten, die sowohl einzeln als auch kombiniert zur Anwendung kommen können.[46] Zunächst kommt eine nähere Bestimmung der Regelung in der DS-GVO in Betracht (Konkretisierung). Zweitens können Regelungen der DS-GVO vervollständigt werden (Ergänzung). Drittens können Öffnungsklauseln eine Abweichung von den Regelungen der DS-GVO zulassen (Modifikation). Wie diese Konkretisierungen, Ergänzungen oder Modifikationen ausgestaltet sind, ergibt sich durch Auslegung der jeweiligen Öffnungsklausel.

## b) Reichweite der Öffnungsklauseln

Der mitgliedstaatliche Handlungsspielraum für die Schaffung von Ermächtigungsgrundlagen im öffentlichen Bereich ist tendenziell größer als im nicht-öffentlichen Bereich. Zwar unterscheidet die DS-GVO nicht grundlegend zwischen öffentlichen und nicht-öffentlichen Stellen und regelt die Materie im Wesentlichen einheitlich, jedoch kommt der Begriff der öffentlichen Stellen oder der Behörde in der DS-GVO immerhin

---

44 Zu dieser Unterscheidung bereits *Kühling/ Martini* et. al., Die DSGVO und das nationale Recht, 2016, S. 11.
45 *Kühling/ Martini* et. al., Die DSGVO und das nationale Recht, 2016, S. 1.
46 Vgl. bereits *Kühling/ Martini,* EuZW 2016, 448 (449).

vereinzelt vor. Im öffentlichen Bereich verfolgt die DS-GVO das Ziel der Vollharmonisierung nicht im gleichen Maß wie im nicht-öffentlichen Bereich (vgl. Erwägungsgründe 9, 10). Dementsprechend bestehen im öffentlichen Bereich weitergehende Öffnungsklauseln, die den Erlass von Rechtsgrundlagen und Einzelheiten der Verarbeitung ermöglichen (vgl. Art. 6 Abs. 1 Abs. 1 lit. c), e), Abs. 2, 3 DS-GVO).[47] Im Übrigen ist die Reichweite der Öffnungsklauseln aber jeweils im Einzelnen zu ermitteln.

### c) Wesentliche Öffnungsklauseln

Aus der großen Zahl an Öffnungsklauseln in der DS-GVO kommt einigen wenigen besondere Bedeutung für den hier zu begutachtenden Bereich der Forschung zu. Diese Öffnungsklauseln sollen nachfolgend vorab dargestellt und erläutert werden.

#### aa) Art. 6 DS-GVO (Rechtmäßigkeit der Verarbeitung)

Art. 6 Abs. 2 und 3 DS-GVO sind allgemeine, fakultative Öffnungsklauseln.[48] Beide nehmen Bezug auf die Rechtfertigungstatbestände nach Art. 6 Abs. 1 lit. c) und e) DS-GVO. Art. 6 Abs. 2 DS-GVO ermöglicht spezifischere mitgliedstaatliche Regelungen, um die Bestimmungen der Art. 6 Abs. 1 lit. c) und e) DS-GVO anzupassen, indem entweder „spezifische Anforderungen für die Verarbeitung“ oder aber „sonstige Maßnahmen“ präziser bestimmt werden. Solche Anpassungen müssen dem Zweck dienen, eine rechtmäßig und nach Treu und Glauben erfolgende Verarbeitung zu gewährleisten. Jedenfalls ermöglicht die Norm eine **Konkretisierung**. Eine Erweiterung oder Ergänzung der Normen der DS-GVO kann wohl nicht auf Art. 6 Abs. 2 DS-GVO gestützt werden.[49]

Gemäß Art. 6 Abs. 3 Satz 1 DS-GVO muss eine Rechtsgrundlage für die Verarbeitung in Fällen der Art. 6 Abs. 1 lit. c) oder e) DS-GVO im Unionsrecht oder im Recht eines Mitgliedsstaats existieren. Diese kann eine **genaue Bestimmung der Voraussetzungen**, unter denen die Verarbeitung personenbezogener Daten rechtmäßig ist, beinhalten (vgl. Erwägungsgrund 10). Für beide Fälle des Art. 6 Abs. 1 lit. c) und e) DS-GVO ist ein öffentliches Interesse erforderlich, das mit der Rechtsgrundlage im Recht der Union oder der Mitgliedstaaten verfolgt werden soll. Auch wenn der Wortlaut dies in seiner zerfaserten Struktur nicht auf den ersten Blick klarstellt, ergibt sich dies einheitlich für beide Fälle entweder unmittelbar aus Art. 6 Abs. 1 lit. e) DS-GVO oder aber aus Art. 6 Abs. 3 Satz 2 und Satz 4 DS-GVO.[50] Das öffentliche Interesse kann in jedem Mitgliedsstaat einzeln festgelegt werden. Im deutschen Recht kann dies insbesondere die Bereiche der Ordnungs-, Leistungs-, und Lenkungsverwaltung betreffen.[51]

---

47 *Kühling/ Martini et. al.,* Die DSGVO und das nationale Recht, 2016, S. 13 f.
48 Vgl. *Kühling/ Martini et al.*, Die DSGVO und das nationale Recht, 2016, S. 28. Kritisch zum Begriff der „allgemeinen“ Öffnungsklausel: Ehmann/ Selmayr/ *Herberlein* 2017, DS-GVO , Art. 6 Rn. 33.
49 Ehmann/Selmayr/ *Herberlein*, 2017, DS-GVO, Art. 6 Rn. 33.
50 Vgl. *Kühling/Martini et al.*, Die DSGVO und das nationale Recht, 2016, S. 29.
51 *Kühling/ Martini et al.*, Die DSGVO und das nationale Recht, 2016, S. 32.

Art. 6 Abs. 3 Satz 3 DS-GVO nennt eine Vielzahl von Handlungsoptionen, welche „**spezifischen Bestimmungen zur Anpassung der Anwendung**“ der DS-GVO in einer mitgliedstaatlichen Rechtsgrundlage enthalten sein können. Geregelt werden können demnach jedenfalls Bestimmungen darüber,

- welche allgemeinen Bedingungen für die Regelung der Rechtmäßigkeit der Verarbeitung durch den Verantwortlichen gelten,
- welche Arten von Daten verarbeitet werden,
- welche Personen betroffen sind,
- an welche Einrichtungen und für welche Zwecke die personenbezogenen Daten offengelegt werden dürfen,
- welcher Zweckbindung sie unterliegen,
- wie lange sie gespeichert werden dürfen,
- welche Verarbeitungsvorgänge und -verfahren angewandt werden dürfen,
- welche Maßnahmen zur Gewährleistung einer rechtmäßig und nach Treu und Glauben erfolgenden Verarbeitung angewandt werden dürfen, wie solche für sonstige besondere Verarbeitungssituationen gemäß Kapitel IX (wovon insbesondere der forschungsspezifische Art. 89 DS-GVO umfasst ist).

Zur Auslegung kann weiterhin auf Erwägungsgrund 45 zurückgegriffen werden. Dieser bezieht sich ausdrücklich auf die Fälle des Art. 6 Abs. 1 lit. c) und e) DS-GVO. Demnach genügt eine Rechtsgrundlage im nationalen Recht auch für mehrere Verarbeitungsvorgänge. Außerdem formuliert Erwägungsgrund 45 verbindlicher, dass die oben genannten Aspekte nicht nur geregelt werden können, sondern vielfach „sollten“. Erwägungsgrund 45 fordert schließlich auch, dass geregelt wird, ob eine Behörde oder eine andere dem öffentlichen Recht unterfallende natürliche oder juristische Person oder juristische Person des Privatrechts eine Aufgabe im öffentlichen Interesse oder in Ausübung der öffentlichen Gewalt wahrnimmt. Erwägungsgrund 45 geht davon aus, dass **auch nicht-öffentliche Stellen** insbesondere im **Bereich der öffentlichen Gesundheit** oder der sozialen Sicherheit oder der Verwaltung von Leistungen der Gesundheitsfürsorge entsprechende Aufgaben wahrnehmen können, da dies im öffentlichen Interesse gerechtfertigt sein kann.

Art. 6 Abs. 3 DS-GVO eröffnet überaus weite Gestaltungsspielräume für die Fälle des Art. 6 Abs. 1 lit. c) und e) DS-GVO. In der juristischen Literatur wird angenommen, dass bereits die allgemeinen Regelungen des § 13 Abs. 1 BDSG a.F. aufrechterhalten werden können, sodass „sämtliche bereichsspezifischen Regelungen des deutschen Datenschutzrechts im öffentlichen Bereich, welche die Vorgaben des Art. 6 Abs. 1 UAbs. 1 lit. c) bzw. e) DS-GVO erfüllen, aufrechterhalten werden“ können.[52]

[52] *Kühling /Martini et al.*, Die DSGVO und das nationale Recht, 2016, S. 37 f.

Art 6 Abs. 4 DS-GVO betrifft Fälle der **Zweckänderung**. Ist ein neuer Verarbeitungszweck nicht mit dem ursprünglichen Zweck vereinbar, bedarf es ohne Einwilligung einer gesonderten Rechtsgrundlage zur Weiterverwendung. Diese kann sich auch aus dem mitgliedstaatlichen Recht ergeben, was den Mitgliedstaaten die Möglichkeit zum Erlass von Zweckänderungsvorschriften bei zweckinkompatibler Weiterverarbeitung geben soll.[53] Voraussetzung ist lediglich, dass notwendige und verhältnismäßige Maßnahmen zum Schutz der in Art. 23 Abs. 1 DS-GVO genannten Ziele getroffen werden, wobei eine Begrenzung auf eines der Ziele und Wahrung der Verhältnismäßigkeit ausreichen soll.[54]

### bb) Art. 9 DS-GVO (Besondere Kategorien personenbezogener Daten)

Für die medizinische Forschung ist im Regelfall die Verarbeitung von Gesundheitsdaten erforderlich. Im Hinblick auf die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 DS-GVO ergeben sich weiterhin Spielräume aus den Öffnungsklauseln des Art. 9 DS-GVO, der ebenfalls **fakultative Öffnungsklauseln** enthält.

#### aaa) Verhältnis zu Art. 6 DS-GVO

Neben Art. 6 DS-GVO enthält Art. 9 Abs. 2 DS-GVO eine Vielzahl von Öffnungsklauseln, nach denen die Verarbeitung besonders sensibler personenbezogener Daten auf Grundlage des Unionsrechts oder des nationalen Rechts ausnahmsweise rechtmäßig sein kann. Das Verhältnis des Art. 9 DS-GVO zu Art. 6 DS-GVO ist indessen weitgehend ungeklärt.[55] Art. 9 DS-GVO enthält gegenüber Art. 6 DS-GVO erhöhte Rechtmäßigkeitsvoraussetzungen, da die Eingriffsintensität bei sensiblen Daten in der Regel höher ist und an die Verhältnismäßigkeit der Verarbeitung daher strengere Anforderungen gestellt werden. Teilweise wird vertreten, dass die Voraussetzungen des Art. 6 DS-GVO auch im Rahmen des Art. 9 DS-GVO anzuwenden sind.[56] Dies dürfte aber nicht die Rechtmäßigkeitsvoraussetzungen des Art. 6 Abs. 1 DS-GVO umfassen, die im Verhältnis zu Art. 9 Abs. 2 DS-GVO unspezifisch sind. Außerdem wäre unklar in welcher Kombination aus Tatbestandsvoraussetzungen des Art. 6 Abs. 1 DS-GVO mit solchen des Art. 9 Abs. 2 DS-GVO eine wirksame Legitimation zu sehen ist. Überzeugender erscheint es, dass das Verbot des Art. 9 Abs.1 DS-GVO lediglich einen Rückgriff auf Art. 6 Abs. 1 DS-GVO sperren sollte und eine **Verarbeitung von besonderen Kategorien personenbezogener Daten ausschließlich nach Art. 9 Abs. 2 DS-GVO zu legitimieren** ist.

Richtig ist der Hinweis auf die Anwendbarkeit des Art. 6 DS-GVO aber insofern als es nicht um Zulässigkeitstatbestände sondern Vorschriften mit allgemeinem Regelungscharakter geht. So muss auch bei der

---

53 *Kühling/ Martini et al.*, Die DSGVO und das nationale Recht, 2016, S. 38.
54 *Kühling/ Martini et al.*, Die DSGVO und das nationale Recht, 2016, S. 39 f.
55 *Kühling/ Martini et al.*, Die DSGVO und das nationale Recht, 2016, S. 54.
56 Kühling/ Buchner/ *Weichert*, 2017, DS-GVO , Art. 9, Rn. 4.

Verarbeitung sensibler Daten beispielsweise der Zweckbindungsgrundsatz des Art. 6 Abs. 4 DS-GVO Beachtung finden, der für sensible personenbezogene Daten in Art. 6 Abs. 4 lit. c) DS-GVO sogar in verschärfter Form zu berücksichtigen ist.

### bbb) Art. 9 Abs. 2 lit. a) DS-GVO (Einwilligung)

Art. 9 Abs. 2 lit. a) DS-GVO sieht vor, dass die Mitgliedstaaten die Möglichkeit, eine Einwilligung zur Legitimation der Verarbeitung besonderer Arten personenbezogener Daten heranzuziehen, ausschließen können; für Einwilligungen nach Art. 6 Abs. 1 lit. a) DS-GVO besteht hingegen kein Regelungsspielraum.[57] Aus dem Recht der Mitgliedstaaten kann sich also ergeben, dass das grundsätzliche Verbot der Verarbeitung sensibler Daten – etwa von Gesundheitsdaten – durch eine Einwilligung nicht aufgehoben werden kann. Sofern eine nationale Vorschrift existiert, die die Einwilligungsmöglichkeit gemäß Art. 9 Abs. 2 lit. a) DS-GVO ausschließt, bleibt es zunächst beim Verbot nach Art. 9 Abs. 1 DS-GVO.[58]

Das bedeutet allerdings auch, dass das nationale Recht engere Voraussetzungen an die Einwilligung als Minus zum möglichen, vollständigen Ausschluss der Einwilligung vorgeben kann, als sie in der DS-GVO bestimmt sind.[59] Es ist daher zulässig, dass ein Mitgliedstaat anstelle eines vollständigen Ausschlusses der Einwilligung lediglich erhöhte Anforderungen – etwa bezüglich der Form – an diese stellt.

### ccc) Art. 9 Abs. 2 lit. b) DS-GVO (Recht der sozialen Sicherheit und Sozialschutz)

Art. 9 Abs. 2 lit. b) DS-GVO ermöglicht durch das Recht der Mitgliedstaaten oder durch Kollektivvereinbarungen (z.B. Tarifverträge), die Verarbeitung im Bereich des Arbeitsrechts und dem Recht der sozialen Sicherung und des Sozialschutzes zu regeln. Diese Öffnungsklausel ist weit gefasst und unkonditioniert.[60] Art. 9 Abs. 2 lit. b) DS-GVO setzt zudem die Erforderlichkeit der Verarbeitung voraus. Sie ist allgemeine Voraussetzung bei der Verarbeitung auf Grundlage einer gesetzlichen Ermächtigung.[61] Dem Begriff kommt im Rahmen von Art. 9 DS-GVO keine besondere Bedeutung zu. Weiterhin werden von Art. 9 Abs. 2 lit. b) DS-GVO geeignete Garantien für die Grundrechte und Interessen der betroffenen Person gefordert. Diese Anforderungen gehen nicht über ohnehin bestehende verfassungsrechtliche Anforderungen aus der GRCh und dem GG hinaus und entfalten daher keine weitergehende Bedeutung.

---

57 *Kühling/ Martini et al.*, Die DSGVO und das nationale Recht, 2016, S. 316 f.

58 Dies ungeachtet der Möglichkeit, dass gesetzliche Ermächtigungsbefugnisse eingreifen können.

59 Siehe auch: *Kühling/ Martini et al.*, Die DSGVO und das nationale Recht, 2016, S. 49 f.

60 Siehe auch: *Kühling/ Martini et al.*, Die DSGVO und das nationale Recht, 2016, S. 50 f.

61 Vgl. Art. 6 Abs. 1 UAbs. 1 lit. b) – f) und Art. 9 Abs. 2 lit. b), c), f) - j) DS-GVO. Im Fall einer Einwilligung formulieren die Art. 6 Abs. 1 UAbs. 1 lit. a) und Art. 9 Abs. 2 lit. a) DS-GVO die Erforderlichkeit nicht als Voraussetzung. Ebenso verzichtet die DS-GVO in den Fällen der Art. 9 Abs. 2 lit. d) und e) DS-GVO, also der Verarbeitung durch politisch, weltanschaulich, religiös oder gewerkschaftlich ausgerichtete Organisationen und bei offensichtlich öffentlich gemachten personenbezogenen Daten auf dieses Merkmal.

### ddd) Art. 9 Abs. 2 lit. g) DS-GVO (erhebliches öffentliches Interesse)

Art. 9 Abs. 2 lit. g) DS-GVO ermöglicht die Schaffung einer mitgliedstaatlichen Rechtsgrundlage zur Verarbeitung besonderer Kategorien personenbezogener Daten aus Gründen eines „erheblichen öffentlichen Interesses". Welche Anforderung an die ausdrücklich geforderte Erheblichkeit des öffentlichen Interesses gestellt werden muss, lässt sich nur tendenziell aus den Erwägungsgründen 46 und 112 entnehmen. Beispielhaft werden als „wichtige Gründe des öffentlichen Interesses" humanitäre Zwecke, die Überwachung von Epidemien, humanitäre Notfälle und Naturkatastrophen,[62] aber auch der internationale Datenaustausch zwischen Wettbewerbs-, Steuer-, oder Zollbehörden, zwischen Finanzaufsichtsbehörden oder zwischen für **Angelegenheiten der sozialen Sicherheit** oder für die **öffentliche Gesundheit zuständigen Diensten** genannt.[63] Im Ergebnis beinhaltet Art. 9 Abs. 2 lit. g) DS-GVO abermals eine weite – wenn nicht gar die weiteste[64] – Öffnungsklausel zur Ausnahme vom Verbot des Art. 9 Abs. 1 DS-GVO. Sie wäre insbesondere geeignet, die Fallgestaltungen der **gesetzlichen Krankenversicherung** weitgehend abzudecken, allerdings ist davon auszugehen, dass die spezifischeren Öffnungsklauseln nach Art. 9 Abs. 2 lit. h) und i) DS-GVO vorgehen, die zum einen das individuelle Interesse an der medizinischen Versorgung und zum anderen die Verarbeitung im öffentlichen Gesundheitsinteresse abdecken[65] (hierzu sogleich).

Die Anforderungen an die Erforderlichkeit, die Verhältnismäßigkeit und die Wahrung des Wesensgehalts des Rechts auf Datenschutz sowie angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person haben keine wesentliche, über die üblichen Anforderungen hinausgehende Bedeutung. Eine Klarstellung dahingehend, dass weitere Maßnahmen im nationalen Recht zulässig sind, lässt sich ihnen aber entnehmen.

### eee) Art. 9 Abs. 2 lit. h) DS-GVO (Maßnahmen der individuellen medizinischen Versorgung und Verwaltung)

Der Verordnungsgeber war sich des Umstandes bewusst, dass im Gesundheitsbereich ein enormer informationstechnischer Fortschritt wie bspw. die Verschmelzung von Gentechnik und Informationstechnik, die Vorverlagerung einer gesundheitsrelevanten Datenverarbeitung und Big Data im Medizinbereich zu erwarten ist.[66] Die Vorschrift des Art. 9 Abs. 2 lit. h) DS-GVO soll den Fortschritt und die medizinische Funktionalität durch Schaffung einer gesetzlichen Grundlage ermöglichen.

Die fakultative Öffnungsklausel des Art. 9 Abs. 2 lit. h) DS-GVO ermöglicht die Schaffung einer mitgliedstaatlichen Rechtsgrundlage, die neben eine solche im Unionsrecht oder aber neben einen Vertrag mit einem Angehörigen

---

62 Erwägungsgrund 46 zu Art. 6 Abs. 1 UAbs. 1 lit. d) DS-GVO.
63 Erwägungsgrund 112.
64 Ehmann/ Selmayr/ *Schiff*, 2017, DS-GVO , Art. 9, Rn. 44.
65 Kühling/ Buchner/ *Weichert*, 2017, DS-GVO, Art. 9, Rn. 93.
66 Kühling/ Buchner/ *Weichert*, 2017, , DS-GVO, Art. 9, Rn. 94 m.w.N.

eines Gesundheitsberufs treten kann. Art. 9 Abs. 2 lit. h) DS-GVO betrifft die Maßnahmen der **individuellen**[67] **medizinischen Versorgung** (konkret der Gesundheitsvorsorge, Arbeitsmedizin, Beurteilung der Arbeitsfähigkeit, medizinische Diagnostik, Versorgung oder Behandlung im Gesundheits- oder Sozialbereich) sowie der **Verwaltung** von Systemen und Diensten im Gesundheits- oder Sozialbereich. Durch die Ausrichtung auf die individuelle Gesundheit lässt sich Art. 9 Abs. 2 lit. h) DS-GVO von Art. 9 Abs. 2 lit. i) DS-GVO abgrenzen.[68]

Die Mitgliedstaaten können in diesem Bereich weitere Zulässigkeitstatbestände schaffen. Sie sollen die Zulässigkeit „näher (…) ausgestalten", wobei die DS-GVO stets voraussetzt, dass die Anforderungen des Art. 9 Abs. 3 DS-GVO eingehalten werden müssen.[69] So muss also eine Verarbeitung durch Fachpersonal oder unter dessen Verantwortung erfolgen und sichergestellt werden, dass dieses **Fachpersonal** nach dem Unionsrecht, dem Recht eines Mitgliedstaats oder durch Vorschriften nationaler zuständiger Stellen *„dem Berufsgeheimnis unterliegt"*.

Zu diesen Stellen zählen bspw. die Landesärztekammern. Nach den von diesen erlassenen Berufsordnungen besteht eine ärztliche **Schweigepflicht**.[70]

Auf bundesrechtlicher Ebene hat diese Schweigepflicht in § 203 Abs. 1 Nr. 1, Abs. 3 Satz 2 Strafgesetzbuch[71] ihren Niederschlag gefunden. Demnach sind Ärzte sowie ihre berufsmäßig tätigen Gehilfen und die Personen, die bei ihnen zur Vorbereitung auf den Beruf tätig sind, zur Datenverarbeitung berechtigte Personen im Sinne des Art. 9 Abs. 3 DS-GVO.

Unter der Verantwortung dieses Fachpersonals können auch weitere Personen tätig werden, sofern diese ebenfalls nach dem Unionsrecht oder dem Recht eines Mitgliedstaats oder den Vorschriften nationaler zuständiger Stellen einer Geheimhaltungspflicht unterliegen. Nach der Reform des § 203 StGB ist zukünftig eine Einbindung von externen Dienstleistern im Rahmen von Auftragsverarbeitungen möglich, während gleichzeitig die strafrechtliche Schweigepflicht auf diese „sonstigen Mitwirkenden" ausgedehnt wird. Auch diese erfüllen zukünftig also die Anforderungen des Art. 9 Abs. 3 DS-GVO.

Das Tatbestandsmerkmal der Erforderlichkeit in Art. 9 Abs. 2 lit. h) DS-GVO hat keine über die üblichen Anforderungen hinausgehende Bedeutung.

---

67 Paal/ Pauly/ *Frenzel*, 2017, DS-GVO, Art. 9, Rn. 41 ff.
68 Kühling/ Buchner/ *Weichert,* 2017, DS-GVO, Art. 9, Rn. 93.
69 *Kühling/ Martini et al.*, Die DSGVO und das nationale Recht, 2016, S. 51.
70 Vgl. § 9 Abs. 1 und 3 (Muster-)Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte in der Fassung des Beschlusses des 118. Deutschen Ärztetages 2015 in Frankfurt am Main; § 9 Abs. 1 Berufsordnung der Ärztekammer Berlin vom 26. November 2014, in der Fassung der Bekanntmachung vom 04. September 1978 (GVBl. S. 1937, 1980), zuletzt geändert durch Gesetz vom 27. März 2013 (GVBl. S. 70).
71 Strafgesetzbuch (StGB) in der Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S. 3322), zuletzt geändert durch Artikel 1 des Gesetzes vom 17. Juli 2017 (BGBl. I S. 2442).

### fff) Art. 9 Abs. 2 lit. i) DS-GVO (Verarbeitung von Gesundheitsdaten im öffentlichen Interesse)

Art. 9 Abs. 2 lit. i) DS-GVO ermöglicht als **fakultative Öffnungsklausel** eine mitgliedstaatliche Rechtsgrundlage zur Verarbeitung sensibler Daten aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit. Der Begriff der öffentlichen Gesundheit wird weit verstanden.[72] Nach Erwägungsgrund 54 Satz 3 ist der Begriff der **öffentlichen Gesundheit** im Sinne der Verordnung (EG) Nr. 1338/2008 des Europäischen Parlaments und des Rates[73] auszulegen. Nach Art. 3 lit. c) dieser Verordnung bezeichnet als öffentliche Gesundheit

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

Allerdings stellt Erwägungsgrund 54 Satz 4 klar, dass eine Verarbeitung von Gesundheitsdaten aus Gründen des öffentlichen Interesses nicht dazu führen darf, dass Dritte, wie Arbeitgeber oder Versicherungs- und Finanzunternehmen, solche personenbezogenen Daten zu anderen Zwecken verarbeiten. Daraus folgt, dass sich private Unternehmen nicht auf diesen Ausnahmetatbestand berufen können, es sei denn, das Unternehmen nimmt auf gesetzlicher Grundlage Aufgaben der öffentlichen Gesundheit wahr, bspw. als beliehenes Unternehmen.[74]

Beispielhaft für ein öffentliches Interesse im Bereich der öffentlichen Gesundheit nennt Art. 9 Abs. 2 lit. i) DS-GVO den Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren oder zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten. Von dieser Öffnungsklausel sind daher insbesondere die Regelungsbereiche des Arzneimittelgesetzes (AMG), des Medizinproduktegesetzes (MPG) und die Krebsregistergesetze sowie bereichsspezifische Normen zur Qualitätssicherung nach § 299 adressiert.[75]
Die Anforderungen an die Erforderlichkeit und an angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person, insbesondere die Wahrung des Berufsgeheimnisses, haben nur geringe Bedeutung.

---

[72] *Kühling/ Martini et al.*, Die DSGVO und das nationale Recht, 2016, S. 51.
[73] Verordnung (EG) Nr. 1338/2008 des Europäischen Parlaments und des Rates vom 16. Dezember 2008 zu Gemeinschaftsstatistiken über öffentliche Gesundheit und über Gesundheitsschutz und Sicherheit am Arbeitsplatz (ABl. L 354 vom 31. Dezember 2008, S. 70).
[74] Kühling/ Buchner/ *Weichert*, 2017, DS-GVO, Art. 9, Rn. 116.
[75] Kühling/ Buchner/ *Weichert*, 2017, DS-GVO, Art. 9, Rn. 119.

Art. 9 Abs. 2 lit. i) DS-GVO ist damit im Ergebnis eine weitreichende Öffnungsklausel, die es den Mitgliedstaaten ermöglicht, die Verarbeitung eigenständig zu gestalten. So soll es möglich sein, die Vorgaben der DS-GVO zu konkretisieren, zu modifizieren und dabei sowohl Erleichterungen als auch Verschärfungen vorzusehen, ohne dass besondere Konditionierungen erfolgen.[76]

### ggg) Art. 9 Abs. 2 lit. j) DS-GVO (Forschungszwecke)

Art. 9 Abs. 2 lit. j) DS-GVO ermöglicht den Mitgliedstaaten die Schaffung von gesetzlichen Ermächtigungsgrundlagen für im öffentlichen Interesse liegende Archivzwecke, für **wissenschaftliche** oder historische **Forschungszwecke** oder für statistische Zwecke gemäß Art. 89 Abs. 1 DS-GVO. Mit dem unbestimmten Rechtsbegriff des **öffentlichen Interesses** sind die Belange des Gemeinwohls gemeint. Von einem öffentlichen Interesse an der Durchführung eines Forschungsvorhabens kann wohl nur dann ausgegangen werden, wenn verlässliche wissenschaftliche Forschungsergebnisse zu erwarten sind und die schutzwürdigen Belange des Betroffenen, insbesondere sein Geheimhaltungsinteresse, überwiegen.[77]

Die Öffnungsklausel ermöglicht weitgehende Regelungen, die unter anderem erhöhte Anforderungen an die Zulässigkeit von Forschungsvorhaben stellen können. Die Anforderungen an die Erforderlichkeit, die Verhältnismäßigkeit und die Wahrung des Wesensgehalts des Rechts auf Datenschutz sowie angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person entsprechen im Wesentlichen den allgemeinen Anforderungen, wie sie verfassungsrechtlich ohnehin gefordert sind.

Angesichts der besonderen Bedeutung wissenschaftlicher Erkenntnisse für das Allgemeinwohl und der von der DS-GVO intendierten Forschungsförderung kommt den angemessenen und spezifischen Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person nach Art. 9 Abs. 2 lit. j) DS-GVO jedoch eine im Vergleich zu den anderen Tatbeständen des Art. 9 Abs. 2 DS-GVO besondere Bedeutung zu. Diese Anforderung verfolgt das Ziel, einen Interessenausgleich zwischen der Notwendigkeit der Verarbeitung und dem Grundrechts- und Interessenschutz der betroffenen Person herzustellen.[78] Im Rahmen der vorzunehmenden Abwägung wirkt es sich dabei positiv zugunsten der Verarbeitung aus, dass zusätzliche prozedurale und technische Maßnahmen als Kompensation für den Eingriff in die Sphäre des Betroffenen fungieren. Die Erforderlichkeit dieser prozeduralen, technischen und organisatorischen Maßnahmen ist auch in der deutschen höchstrichterlichen Rechtsprechung anerkannt.[79] Bei der Festlegung der Schutzmaßnahmen sind diese auf die Besonderheiten der sensiblen Daten auszurichten und über die allgemeinen Maßnahmen hinaus zu fassen,

---

[76] *Kühling/ Martini et al.*, Die DSGVO und das nationale Recht, 2016, S. 52.
[77] *Metschke/ Wellbrock*, Berliner Beauftragter für Datenschutz und Informationsfreiheit, Hessischer Datenschutzbeauftragter, Datenschutz in Wissenschaft und Forschung, 2002, S. 35.
[78] Kühling/ Buchner/ *Weichert*, 2017, DS-GVO, Art. 9, Rn. 132.
[79] *BVerfG*, Urteil vom 15.12.1983, Az. 1 BvR 209/83, juris-Rn. 185.

indem sie beispielsweise kumuliert oder in ihrer Garantiefunktion vertieft werden.[80] Im Bereich von Gesundheitsdaten ist eine typische Schutzmaßnahme das Patientengeheimnis. Als weitere Schutzmaßnahme kommt auch die Ausweitung der Betroffenenrechte oder die Umsetzung der Schutzziele, zum Beispiel Integrität, Vertraulichkeit und Transparenz, in Betracht. Im Sinne einer größtmöglichen Datensparsamkeit ist zudem eine frühestmögliche Löschung, Anonymisierung oder Pseudonymisierung denkbar. Schutzmaßnahmen im materiellen Sinne können auch ein Zweckänderungsverbot oder eine Zweckänderungsbeschränkung sein, wie es beispielsweise als Forschungsgeheimnis im wissenschaftlichen Bereich in Betracht kommt.[81]

### hhh) Art. 9 Abs. 4 DS-GVO (Bedingungen/Beschränkungen bei genetischen, biometrischen und Gesundheitsdaten)

Art. 9 Abs. 4 DS-GVO eröffnet den nationalen Gesetzgebern die Möglichkeit, weitere Bedingungen einschließlich Beschränkungen, einzuführen oder aufrechtzuerhalten, soweit die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten betroffen ist.

Die Öffnungsklausel ermöglicht zunächst – nach dem Wortlaut eindeutig – Be*schränkungen*, die den Umfang der Verarbeitung ein*schränken* oder aber höhere Hürden an die Zulässigkeit der Verarbeitung stellen. Diese können ohne Weiteres unter den Wortlaut „zusätzliche Bedingungen" gefasst werden. In der juristischen Literatur wird aber ebenfalls vertreten, dass unter zusätzlichen Bedingungen auch befugniserweiternde Anforderungen oder Erleichterungen verstanden werden könnten, da eine Beschränkung nur „lediglich als eine Möglichkeit" der Bedingungen genannt werde.[82] Nach anderer Ansicht sind ausschließlich Verschärfungen, also strengere Anforderungen, möglich und Erleichterungen ausgeschlossen.[83] Jedoch sollten nach Erwägungsgrund 53 Satz 4 die Bedingungen

> *„den freien Verkehr personenbezogener Daten innerhalb der Union nicht beeinträchtigen, falls die betreffenden Bedingungen für die grenzüberschreitende Verarbeitung solcher Daten gelten".*

Art. 9 Abs. 4 DS-GVO ist nach hier vertretener, vermittelnder Ansicht folglich dahingehend zu verstehen, dass unter Beachtung des Grundsatzes der Verhältnismäßigkeit und des Ziels der DS-GVO, den freien Verkehr personenbezogener Daten nicht zu beeinträchtigen, Erleichterungen jedenfalls insoweit erlaubt sein müssen,

---

80 Kühling/ Buchner/ *Weichert*, 2017, DS-GVO, Art. 9, Rn. 134.

81 Netzwerk Datenschutzexpertise, Datenschutzrechtlicher Handlungsbedarf für die deutsche Politik nach Verabschiedung der EU-DS-GVO, 2016, S. 3.

82 *Dochow*, GesR 2016, 401 (407); Kühling/ Buchner/ *Weichert*, 2017, DS-GVO, Art. 9, Rn. 150. Auch Kühling/ Martini et al., Die DSGVO und das nationale Recht, 2016, S. 52 sehen die Möglichkeit, Zulässigkeitstatbestände und Modifikationen zu schaffen.

83 Ehmann/ Selmayr/ Schiff, 2017, DS-GVO, Art. 9, Rn. 56; Plath/ ders., 2. Aufl., 2016, DSGVO, Art. 9, Rn. 30.

wie sie erforderlich sind, mögliche andere Verschärfungen im Sinne einer zu wahrenden Verhältnismäßigkeit auszugleichen.

### cc) Art. 23 DS-GVO (Beschränkung der Betroffenenrechte)

Mit der allgemeinen, **fakultativen Öffnungsklausel** des Art. 23 DS-GVO erhalten die Mitgliedstaaten die Möglichkeit, Beschränkungen von Pflichten und Rechten nach den Art. 12 – 22 und 34 DS-GVO (Betroffenenrechte) und den Grundsätzen der Verarbeitung nach Art. 5 DS-GVO (sofern dessen Bestimmungen denen der Art. 12 – 22 DS-GVO entsprechen) im nationalen Recht zu regeln. Solche Beschränkungen sind nur zulässig, wenn mindestens eines der enumerierten Schutzziele nach Art. 23 Abs. 1 lit. a) bis j) DS-GVO verfolgt wird. Der Hinweis darauf, dass diese Beschränkungen den Wesensgehalt der Grundrechte und Grundfreiheiten achten und in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellen müssen, ist eine verfassungsrechtliche Selbstverständlichkeit, der keine gesonderte Bedeutung zukommt. Wichtig sind hingegen die Voraussetzungen nach Art. 23 Abs. 2 DS-GVO. Demnach muss jede beschränkende Gesetzgebungsmaßnahme im Sinne des Art. 23 Abs. 1 DS-GVO spezifische Vorschriften in Bezug auf alle enumerierten Fälle in Absatz 2 lit. a) bis h) enthalten (Zwecke, Datenkategorien, Umfang der Beschränkung, Garantien gegen Missbrauch, unrechtmäßige Datenzugänge, unrechtmäßige Übermittlung, Angaben zum Verantwortlichen, Speicherfristen, geltende Garantien, Risiken für die betroffene Person, Recht auf Unterrichtung der betroffenen Person über die Beschränkung). Der eigenwilligen Formulierung („insbesondere gegebenenfalls (…) zumindest“) lässt sich immerhin entnehmen, dass die genannten Fälle des Art. 23 Abs. 2 DS-GVO nicht abschließend sind. Im vorliegenden Kontext dürften Ziele nach Art. 23 Abs. 1 lit. e) – j) DS-GVO in Betracht kommen, wobei der Schwerpunkt auf Art. 23 Abs. 1 lit. e) DS-GVO liegen wird.

Art. 23 Abs. 1 lit. e) DS-GVO setzt voraus, dass der Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses der EU oder eines Mitgliedsstaats, insbesondere eines wichtigen wirtschaftlichen oder finanziellen Interesses beabsichtigt ist. Beispielhaft nennt die Norm neben Währungs-, Haushalts- und Steuerbereichen den Bereich der öffentlichen Gesundheit und der sozialen Sicherheit. Art. 23 Abs. 1 lit. e) DS-GVO wird zudem von Art. 23 Abs. 1 lit. h) DS-GVO, neben lit. a) – d) und g), referenziert, der Ziele der Kontroll-, Überwachungs- und Ordnungsfunktionen betrifft. Weiterhin kommen nach Art. 23 Abs. 1 lit. i) DS-GVO Schutzziele der Rechte und Freiheiten anderer Personen und nach Art. 23 Abs. 1 lit. j) DS-GVO die Durchsetzung zivilrechtlicher Ansprüche als Ziele in Betracht. Im Ergebnis liegt eine „weite Freiheit“ vor, von der Öffnungsklausel sowohl im allgemeinen Datenschutzrecht als auch im bereichsspezifischen Datenschutzrecht Gebraucht zu machen.[84]

[84] *Kühling/ Martini et al.*, Die DSGVO und das nationale Recht, 2016, S. 74.

### dd) Art. 89 DS-GVO (Forschung)

Art. 89 Abs. 2, 3 DS-GVO ermöglicht als Öffnungsklausel bei der Verarbeitung zu wissenschaftlichen oder historischen Forschungszwecken Ausnahmen von den Rechten aus Art. 15, 16, 18 und 21 DS-GVO oder bei der Verarbeitung zu statistischen Zwecken von den Rechten aus Art. 15, 16, 18, 19, 20 und 21 DS-GVO durch mitgliedstaatliches Recht. Dabei müssen die Bedingungen und Garantien gem. Art. 89 Abs. 1 DS-GVO eingehalten sein und ansonsten die Verwirklichung der spezifischen Zwecke durch die Wahrnehmung dieser Rechte unmöglich oder ernsthaft beeinträchtigt werden. Die Ausnahmen müssen für die Erfüllung der Zwecke notwendig sein.

# C. Verfassungsrechtlicher Rahmen in Deutschland

## I. Bedeutung des nationalen Verfassungsrechts

Im Bereich der Durchführung von Unionsrecht ist hinsichtlich der grundrechtlichen Gewährleistungen eine Bedeutungsverlagerung von der nationalen auf die unionale Ebene erfolgt. Zwar gibt es im nationalen Verfassungsrecht entsprechende Gewährleistungen insbesondere hinsichtlich des Datenschutzes (sog. Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 iVm Art. 1 Abs. 1 GG)[85] und der Forschungsfreiheit (Art. 5 Abs. 3 GG). Allerdings ist nicht absehbar, dass ein effektiver Grundrechtsschutz auf unionaler Ebene unzureichend wäre, sodass infolge des Anwendungsvorrangs des Unionsrechts maßgeblich auf dieses und nicht mehr auf nationales Recht abzustellen ist.[86] Dieser Vorrang hat freilich keine Implikationen für die innerstaatliche Verteilung der Gesetzgebungskompetenzen.

## II. Gesetzgebungskompetenzen

Die Öffnungsklauseln der DS-GVO sowie die daraus resultierenden Handlungspflichten und -spielräume richten sich an die jeweilige mitgliedstaatliche Legislative. In der Bundesrepublik Deutschland ist hierbei die Kompetenzverteilung des Grundgesetzes zu beachten.

Im Grundgesetz ist keine spezifische Gesetzgebungsbefugnis für das Datenschutzrecht vorgesehen. Für diesen Bereich werden daher verschiedene Befugnisse herangezogen. Die jeweilige Gesetzgebungskompetenz folgt dabei stets derjenigen für die Regelung einer übergeordneten Sachmaterie.[87] Aus Art. 70 Abs. 1 GG folgt der Grundsatz der Länderzuständigkeit, wonach der Bund nur dann gesetzgebungskompetent ist, wenn ihm das

---

85 BVerfGE 65, 1.

86 Vgl. hierzu *Kircher*, Der Schutz personenbezogener Gesundheitsdaten im Gesundheitswesen, 2016, S. 60 ff.; BVerfGE 118, 79 (95); E 122, 1 (20); E 125, 260 (306 f.); E 129, 78 (90); E 129, 186 (198 ff.); E 130, 151 (177 f.).

87 *Kircher*, Der Schutz personenbezogener Gesundheitsdaten im Gesundheitswesen, 2016, S. 81 f. Es handelt sich hierbei um eine Kompetenz kraft Sachzusammenhangs oder eine sog. Annexkompetenz.

Grundgesetz („ausnahmsweise“) eine solche Kompetenz zuweist. Dies kann entweder im Rahmen von Art. 71 i.V.m. Art. 73 GG (ausschließliche Gesetzgebungskompetenz des Bundes) oder im Rahmen von Art. 72 i.V.m. Art. 74 GG (konkurrierende Gesetzgebungskompetenz) der Fall sein.[88]

## 1. Gesetzgebungskompetenzen des Bundes

Aus den folgenden Gesetzgebungskompetenzen des Bundes lassen sich Gesetzgebungsbefugnisse hinsichtlich des Datenschutzrechtes im Gesundheitswesen ableiten, soweit ein Zusammenhang mit der jeweiligen Materie besteht:

- Recht der **Sozialversicherung** (Art. 74 Abs. 1 Nr. 12 GG)
- Recht des privatrechtlichen Versicherungswesens (Art. 74 Abs. 1 Nr. 1 und 11 i.V.m. Art. 72 Abs. 2 GG)
- Zulassung zu ärztlichen und anderen Heilberufen sowie zum Heilgewerbe (Art. 74 Abs. 1 Nr. 19 GG)
- Recht des Apothekenwesens (Art. 74 Abs. 1 Nr. 19 GG)
- Recht der **Arzneien** (Art. 74 Abs. 1 Nr. 19 GG)
- Recht der **Medizinprodukte** (Art. 74 Abs. 1 Nr. 19 GG)
- Recht der Heilmittel (Art. 74 Abs. 1 Nr. 19 GG)
- Recht der Betäubungsmittel und Gifte (Art. 74 Abs. 1 Nr. 19 GG)
- Recht der wirtschaftlichen Sicherung der Krankenhäuser (Art. 74 Abs. 1 Nr. 19a GG i.V.m. Art. 72 Abs. 2 GG)
- Recht der medizinisch unterstützten Erzeugung menschlichen Lebens (Art. 74 Abs. 1 Nr. 26 GG i.V.m. Art. 72 Abs. 2 GG)
- Recht der Untersuchung und der künstlichen Veränderung von Erbinformationen (Art. 74 Abs. 1 Nr. 26 GG i.V.m. Art. 72 Abs. 2 GG)
- Recht der Transplantation von Organen, Geweben und Zellen (Art. 74 Abs. 1 Nr. 26 GG i.V.m. Art. 72 Abs. 2 GG)
- Recht der Telekommunikation und Telemedien (Art. 73 Abs. 1 Nr. 7 GG)
- Recht der Bundeswehrkrankenhäuser (Art. 73 Abs. 1 Nr. 1 GG)
- Strafrecht (Art. 74 Abs. 1 Nr. 1 GG i.V.m. Art. 72 Abs. 2 GG)
- Recht der öffentlichen Stellen des Bundes als Annex zum Verwaltungsverfahren kraft Sachzusammenhangs

Die vorgenannten Gesetzgebungskompetenzen werden in der juristischen Literatur sowie in den Gesetzgebungsunterlagen herangezogen.

[88] Daneben gibt es auch ungeschriebene Gesetzgebungskompetenzen „kraft Natur der Sache“. Diese Kategorie kann hier aber außer Betracht bleiben. Gleiches gilt für die Kompetenzen zur Steuergesetzgebung aus Art. 105 GG.

Weitgehend unbeachtet blieb – soweit ersichtlich – bisher hingegen die konkurrierende Gesetzgebungskompetenz des Bundes gemäß **Art. 74 Abs. 1 Nr. 13** i.V.m. Art. 72 Abs. 2 **GG auf dem Gebiet der Förderung der wissenschaftlichen Forschung**. Nach dieser Systematik ist es denkbar, dass Datenverarbeitungen, die im Sachzusammenhang mit Forschung stehen, bundeseinheitlich geregelt werden können. Der Begriff der Forschungsförderung umfasst neben finanziellen Fördermaßnahmen auch organisatorische und planerische Maßnahmen zur Förderung von Forschungsprojekten und Forschungseinrichtungen.[89] Infolge des Wegfalls der Rahmenkompetenz im Hochschulwesen (Art. 75 Abs. 1 Nr. 1a G a.F.) erfährt Art. 74 Abs. 1 Nr. 13 GG seine Grenze nunmehr in der „Umgestaltung des Hochschulwesens“, [90] die hier nicht in Rede steht. Der Bund kann auf der Grundlage dieser Vorgabe Forschungsförderungsmaßnahmen der Länder organisatorischer oder planerischer Art vorschreiben.[91] Es ist ihm durchaus möglich, zum Abbau datenschutzrechtlicher Hemmnisse gesetzliche Grundlagen für organisatorische Maßnahmen zur Förderung der Forschung im länderübergreifenden Kontext zu erlassen.

Die zusätzlichen Voraussetzungen des Art. 72 Abs. 2 GG für die Gesetzgebungskompetenz des Art. 74 Abs. 1 Nr. 13 GG sind notwendig zu berücksichtigen. Nach dieser Norm setzt die Ausübung der Gesetzeskompetenz voraus, dass zur Wahrung der Rechts- oder Wirtschaftseinheit im gesamtstaatlichen Interesse (2. Alt. des Art. 72 Abs. 2 GG) eine bundesgesetzliche Regelung erforderlich ist. Letzteres soll hier kursorisch betrachtet werden. Die Wahrung der Wirtschaftseinheit ist dahingehend zu verstehen, dass ein gesamtwirtschaftlicher Kontext, wie beispielsweise ein multizentrisches Forschungsvorhaben nicht vor den Grenzen eines einzelnen Bundeslandes „halt machen“ darf und dass wissenschaftliche Studien, die in mehreren Bundesländern gleichzeitig stattfinden, nicht binnenstaatlichen Hindernissen ausgesetzt sein sollen. Eine bundeslandesspezifische Heterogenität der rechtlichen Regelungsrahmen steht der wissenschaftlichen Forschung der Krankenhäuser einer „gesamtstaatlichen Wirtschaftseinheit“ jedenfalls entgegen. Hieraus lässt sich, wenn auch in den Grenzen des den Ländern zugewiesenen Hochschulrechts, eine Bundeskompetenz zur Gestaltung eines einheitlichen Datenschutzrechts der bundeslandübergreifenden wissenschaftlichen Forschung ableiten. Freilich ist dieses Instrument behutsam einzusetzen, da die Väter der Verfassung hierfür die Formulierung „wenn und soweit“ verwendet haben, sodass hohe Maßstäbe an die Notwendigkeit einer solchen Regelung anzulegen sind. Die sich daraus ergebenden Optionen werden im Teil 3 C., Lösungsmodelle, näher zu untersuchen sein.

## 2. Gesetzgebungskompetenzen der Länder

Die Gesetzgebungskompetenzen der Länder resultieren aus Art. 70 Abs. 1 GG. Sie umfassen insbesondere das

- Recht der **Berufsausübung bei ärztlichen und anderen Heilberufen** sowie beim Heilgewerbe (Ausnahme etwa bei sozialversicherungsrechtlichem Bezug, s.o.)

---

89 BeckOK Grundgesetz/Seiler, 41. Ed. 15.2.2019, GG Art. 74 Rn. 54.
90 BeckOK Grundgesetz/Seiler, 41. Ed. 15.2.2019, GG Art. 74 Rn. 54.
91 Maunz/Dürig, Grundgesetz-Kommentar Werkstand: 86. EL Januar 2019, Rn. 180

- Recht der **Krankenhausorganisation und -planung**
- Recht der **öffentlichen Stellen der Länder** als Annex zum Verwaltungsverfahren kraft Sachzusammenhangs.

## 3. Ergebnis

Sowohl für das Datenschutzrecht als auch für das Gesundheitswesen und die Forschung ist die Gesetzgebungskompetenz des Bundes nicht vollumfassend. Je nachdem welche Materien betroffen sind und welche Stellen im Rahmen der erforderlichen Datenverarbeitungen eingebunden werden sollen, können sich aber zusätzliche Gesetzgebungsbefugnisse ergeben. Vergleichsweise weitgehend ist bisher eine Gesetzgebung im Rahmen der Sozialversicherung gemäß Art. 74 Abs. 1 Nr. 12 GG möglich. Aus der Gesetzgebungskompetenz zur Förderung der wissenschaftlichen Forschung gem. Art. 74 Abs. 1 Nr. 13 GG könnten sich weitergehende Kompetenzen ableiten, die sich daraus ergeben, dass die wissenschaftliche Forschung in länderübergreifenden Zusammenhängen einer einheitlichen Rechtsgrundlage bedarf.

# Teil 4: Nationaler Rechtsrahmen

In Ermangelung einer ausschließlichen Gesetzgebungskompetenz des Bundes für die Materie des Datenschutzes trifft die Idee der Zentralisierung und Vereinheitlichung des Datenschutzrechts in der EU allerdings im Bereich der Forschung mit Gesundheitsdaten auf einen föderal zersplitterten Umsetzungsrechtsrahmen innerhalb der Bundesrepublik Deutschland. Neben allgemeinen Forschungsklauseln des BDSG finden sich bundesrechtliche Spezialnormen etwa im SGB X hinsichtlich des Umgangs mit Sozialdaten, im SGB V hinsichtlich des Umgangs mit Sozialdaten im Bereich der gesetzlichen Krankenversicherung, im Arzneimittelgesetz (AMG), Medizinproduktegesetz (MPG), Strahlenschutzgesetz (StrlSchG) hinsichtlich der Verarbeitung in klinischen Prüfungen sowie landesrechtlich in den 16 Landesdatenschutzgesetzen. 13 Länder haben zusätzlich datenschutzrechtliche Regelungen in bereichsspezifischen Landeskrankenhausgesetzen (z.B. in elf Ländern in (Landes-)Krankenhausgesetzen, in Nordrhein-Westfalen im Gesundheitsdatenschutzgesetz (GDSG NRW), in Bremen im Krankenhausdatenschutzgesetz (BremKHDSG)) implementiert.

## A. Normanalyse

Die intensive Auseinandersetzung mit den bereichsspezifischen Datenschutzvorschriften auf Bundes- und Landesebene mit besonderer Relevanz für Forschungstätigkeiten im Gesundheitswesen zeigt deren komplexe Struktur und zahlreiche Unterschiede. Im Folgenden wird ein Überblick über die Rechtslage gegeben. Beachtung finden dabei auch Fassungen, wie sie in aktuellen Gesetzgebungsvorhaben geplant sind.[92]

### I. Analyse der Landeskrankenhaus- und Landesdatenschutzgesetze

Ein Großteil der Forschung im Gesundheitswesen findet in Krankenhäusern sowie in Kooperation mit Krankenhäusern statt. Die folgende Analyse konzentriert sich daher auf die für die Forschung besonders relevanten datenschutzrechtlichen Regelungen der Landeskrankenhausgesetze. Im Fokus stehen

- die verschieden ausgestalteten Anwendungsbereiche,
- die spezifischen Vorgaben für die Verarbeitung zu Forschungszwecken sowie
- die Zuständigkeitszuweisungen hinsichtlich der Aufsichtsbehörden.

Die folgende Übersicht zeigt, welche speziellen Forschungsklauseln für die Verarbeitung von personenbezogenen Daten in Krankenhäusern eines öffentlich-rechtlichen Trägers gelten. Darüber hinaus gelten fast alle Datenschutzvorschriften der LKHG auch für die Verarbeitung zu Forschungszwecken.

[92] Berücksichtigt werden aktuelle Gesetzgebungsvorhaben, wie sie bis zum Zeitpunkt der Auftragserteilung in einer Drucksache des Bundestages oder des Bundesrates veröffentlicht sind.

| Bundesland | Krankenhausspezifische landesrechtliche Vorschriften | Landesdatenschutzgesetz |
|---|---|---|
| **Baden-Württemberg** | § 46 LKHG BW | § 13 LDSG |
| **Bayern** | Art. 27 BayKrG | |
| **Berlin** | § 25 BlnLKG | |
| **Brandenburg** | § 31 BbgKHEG | |
| **Bremen** | § 7 BremKHDSG | |
| **Hamburg** | § 12 HmbKHG | |
| **Hessen** | § 12 Abs. 3 HKHG | § 24 HDSIG |
| **Mecklenburg-Vorpommern** | §§ 34 Abs. 1 Nr. 4 i.V.m. 37 LKHG M-V | |
| **Niedersachsen** | | § 13 NDSG |
| **Nordrhein-Westfalen** | § 6 GDSG NW | |
| **Rheinland-Pfalz** | § 37 LKG | |
| **Saarland** | § 24 SKHG | |
| **Sachsen** | § 34 SächsKHG | |
| **Sachsen-Anhalt** | § 17 KHG LSA | |
| **Schleswig-Holstein** | | § 13 LDSG |
| **Thüringen** | §§ 27, 27a ThürKHG | |

*Übersicht 1: Bereichsspezifische Vorschriften für die Verarbeitung personenbezogener Daten durch Krankenhäuser zu Forschungszwecken*

## 1. Anwendungsbereich

Vorgaben zum Umgang mit personenbezogenen Daten im Zusammenhang mit der medizinischen Forschung in Krankenhäusern lassen sich den Landeskrankenhausgesetzen der Länder entnehmen.

Soweit es in einem Land keine bereichsspezifischen Vorschriften gibt, ist für Krankenhäuser in Trägerschaft einer juristischen Person des privaten Rechts oder des Bundes auf das Bundesdatenschutzrecht, für Krankenhäuser in Trägerschaft der nicht-öffentlichen Stellen der Länder auf das allgemeine Landesdatenschutzrecht zurückzugreifen. In all diesen Fällen (siehe oben Übersicht 1) findet das Landesdatenschutzrecht oder jedenfalls die entsprechende Forschungsklausel allerdings keine Anwendung, soweit öffentliche Stellen als Unternehmen mit eigener Rechtspersönlichkeit **am Wettbewerb teilnehmen**.[93] Für diese sind dann die für nicht-öffentliche Stellen geltenden datenschutzrechtlichen Vorschriften anzuwenden. Eine öffentliche Stelle muss nicht in jeder Hinsicht am Wettbewerb teilnehmen, dies kann sich für unterschiedliche Tätigkeitsbereiche durchaus unterschiedlich darstellen.[94] Der Bayerische Landesbeauftragte für den Datenschutz (BayLfD) vertritt mittlerweile auch für Universitätskliniken die Auffassung, dass sie insoweit am Wettbewerb teilnehmen als sie Aufgaben der Krankenversorgung wahrnehmen, denn diese können auch von privaten oder gemeinnützigen Krankenhäusern erbracht werden.[95] Dies muss auch für die Forschung in Krankenhäusern gelten, denn auch damit stehen Krankenhäuser des Landes klar im Wettbewerb zu anderen Krankenhäusern. Deutlich wird der Wettbewerb im Zusammenhang mit vom Bund geförderten Drittmittelprojekten. Jährlich werden viele Millionen Euro öffentlicher Gelder zur Durchführung von medizinischen Forschungsvorhaben zur Verfügung gestellt, um die viele Forschungskonsortien mit ihren Projektanträgen konkurrieren.

Aus diesem Grund liegt der **Fokus im Folgenden auf dem Anwendungsbereich der Landeskrankenhausgesetze**, denn den Landesdatenschutzgesetzen verbleibt mit Blick auf die medizinische Forschung kein eigener Anwendungsbereich, wenn ein Landeskrankenhaus den Datenschutz in Forschungsvorhaben regelt.

Im Datenschutzrecht kann zwischen sachlichen, persönlichen und räumlichen **Anwendungsbereichen** differenziert werden.

### a) Sachlicher Anwendungsbereich der Landeskrankenhausgesetze

Zentraler Anknüpfungspunkt der Datenschutzvorschriften in den Landeskrankenhausgesetzen ist das Vorliegen von „Patientendaten“. Dieser Begriff basiert auf dem Merkmal der „personenbezogenen Daten“ (vgl. Art. 4 Nr. 1 DS-GVO).

Patientendaten stellen einen Unterfall von personenbezogenen Daten dar. Auch wenn sich die Definitionen des Begriffs „Patientendaten“ der einzelnen Landeskrankenhausgesetze im Kern überschneiden, sind hinsichtlich der

---

93 § 2 Abs. 6 KDSG BW; § 2 Abs. 2 HDSIG; § 1 Abs. 4 NDSG; § 2 Abs. 5 LDSG SH.
94 Der Bayerische Landesbeauftragte für den Datenschutz, 26. Tätigkeitsbericht 2014, Kap. 7.2.5.
95 Der Bayerische Landesbeauftragte für den Datenschutz, 26. Tätigkeitsbericht 2014, Kap. 7.2.5.

Details diverse Unterschiede festzustellen. Dies betrifft insbesondere die einbezogenen Personengruppen sowie den Kontext der Verarbeitung. Wegen der besonderen Bedeutung des Begriffs „Patientendaten“ soll dieser genutzt werden, um die Unterschiede zwischen den Landeskrankenhausgesetzen besonders umfassend aufzeigen. Dabei ist zu erkennen, dass die Unterschiede zwischen den Landeskrankenhausgesetzen i.d.R. in der „Tiefe des Gesetzes“ zu finden sind, d.h. häufig in den Details liegen.

### aa) Patientendaten

Der sachliche Anwendungsbereich sämtlicher in den Landeskrankenhausgesetzen existierender bereichsspezifischer Datenschutzvorschriften wird durch das Vorliegen personenbezogener Daten von Patientinnen und Patienten[96] (sog. „Patientendaten“) eröffnet. Die Anknüpfung des sachlichen Anwendungsbereiches an Patientendaten ergibt sich in Baden-Württemberg aus § 43 Abs. 4 S. 1 i.V.m. §§ 45 ff. LKHG BW, in Bayern aus Art. 27 Bay KHG, in Berlin aus §§ 24 ff. LKHG Bln, in Brandenburg aus § 27 Abs. 2 i.V:m. §§ 28 ff.BbGKHG, in Bremen aus § 1 Abs. 1 S. 2, 3 i.V.m. §§ 2 ff. BremKHDSG, in Hamburg aus § 7 Abs. 1 S. 1 i.V.m. §§ 8 ff. HmbKHG, in Hessen aus § 12 HKHG; in Mecklenburg-Vorpommern aus §§ 33 ff. LKHG M-V, in Nordrhein-Westfalen aus § 2 Abs. 1 S. 1 i.V.m. § 5 ff. GDSG NRW, in Rheinland-Pfalz aus §§ 36 f. LKG RP, im Saarland aus § §§ 13 ff. SKHG, in Sachsen aus §§ 33 f. SächsKHG, in Sachsen-Anhalt aus §§ 16 f. KHG LSA, in Thüringen aus §§ 27 ff. ThürKHG. Innerhalb dieser Vorschriften finden sich auch die Legaldefinitionen zu dem Begriff „Patientendaten“ (§ 43 Abs. 4 S. 1, S. 2 LKHG BW, Art. 27 Abs. 1 Bay KHG, § 24 Abs. 2 LKHG Bln, § 27 Abs. 2 BbGKHG, § 1 Abs. 1 S. 2, 3 BremKHDSG, § 7 Abs. 1 S. 1 u. 2 HmbKHG, § 12 Abs. 2 HKHG; § 33 Abs. 1 LKHG M-V, § 2 Abs. 1 S. 1 GDSG NRW, § 36 Abs. 1 S. 4 LKG RP, § 13 Abs. 1 S. 1 SKHG, § 33 Abs. 1 S. 2 SächsKHG, § 16 Abs. 1 KHG LSA, § 27 Abs. 2 S. 2 ThürKHG).

Soweit der Begriff der „Patientendaten“ in den Landeskrankenhausgesetzen definiert wird, können ehebliche Unterschiede zwischen den jeweiligen Vorschriften festgestellt werden.

In manchen Landeskrankenhausgesetzen ist keine Definition zu finden. So setzen die Landeskrankenhausgesetze von Hessen und Mecklenburg-Vorpommern den Begriff weitgehend ohne Definition voraus. Und das niedersächsische Krankenhausgesetz (NKHG) enthält im wortmächtigen § 16 zum Patientenfürsprecher in Absatz 3 Satz 2 NKHG lediglich eine spezifische Regelung zur Übermittlung von Betroffenendaten an die Patientenfürsprecherin, aber keine weiteren bereichsspezifischen Vorschriften zum Umgang mit personenbezogenen Daten.

[96] teilweise mit der Ergänzung: „des Krankenhauses“, „im Krankenhaus“, „aus dem Bereich der Krankenhäuser“ bzw. „im Krankenhaus verarbeitete“.

### aaa) Einzelangaben über persönliche und sachliche Verhältnisse

In den Ländern Baden-Württemberg (§ 43 Abs. 4 S. 1 LKHG BW), Bayern (Art. 27 Abs. 1 S. 1 Bay KHG), Berlin (§ 24 Abs. 2 S. 1 LKG Bln), Brandenburg (§ 27 Abs. 2 BbgKHEG), Bremen (§ 1 Abs. 1 S. 2 BremKDSG), Sachsen (§ 33 Abs. 1 S. 2 SächsKHG), Sachsen-Anhalt (§ 16 Abs. 1 KHG LSA), Thüringen (§ 27 Abs. 2 S. 2 ThürKHG) beziehen sich die Legaldefinitionen für den Begriff „Patientendaten" in den Landeskrankenhausgesetzen derzeit noch auf „Einzelangaben über persönliche oder sachliche Verhältnisse bestimmter oder bestimmbarer (Patientinnen und) Patienten". Die Voraussetzungen „Einzelangabe", „persönliche oder sachliche Verhältnisse" sowie „Bestimmtheit oder Bestimmbarkeit" stammen aus dem (alten) Datenschutzrecht der Bundesrepublik Deutschland vor dem 25. Mai 2018. Der Begriff „Einzelangabe" sowie der Bezug zu „persönlichen oder sachlichen Verhältnissen" ist in Art. 4 Nr. 1 DS-GVO nicht enthalten. Die „Bestimmbarkeit" kann als gleichbedeutend mit „Identifizierbarkeit" angesehen werden.[97]

### bbb) Einbeziehung von Angehörigen, Begleitpersonen und sonstigen Bezugspersonen

Teilweise umfasst der Begriff „Patientendaten" nicht nur Informationen über Personen, die im Sinne des Behandlungsverhältnisses tatsächlich Patientin oder Patient sind, sondern darüber hinaus weitere Personengruppen:

#### (1) Angehörige

In Baden-Württemberg (§ 43 Abs. 4 S. 1 LKHG BW), Berlin (§ 24 Abs. 2 S. 1 LKHG Bln), Brandenburg (§ 27 Abs. 2 BbgKHG), Bremen (§ 1 Abs. 1 S. 3 BremKHDSG), Hamburg (§ 7 Abs. 1 S. 2 HmbKHG), (wohl auch) Nordrhein-Westfalen (§ 2 Abs. 1 S. 2 GDSG NRW), Rheinland-Pfalz (§ 36 Abs. 1 S. 4 LKG RP), Saarland (§ 13 Abs. 1 S. 2 SKHG), Sachsen (§ 33 Abs. 1 S. 3 SächsKHG), Sachsen-Anhalt (§ 16 Abs. 1 Nr. 2 KHG LSA) und Thüringen (§ 27 Abs. 2 S. 3 ThürKHG) gehören zu den Patientendaten auch personenbezogene Daten über Angehörige. So werden in Baden-Württemberg Angehörige einbezogen, „die im Krankenhaus im Zusammenhang mit der stationären Versorgung des Patienten bekannt werden" (§ 43 Abs. 4 S. 1 LKHG BW). Auf das „bekannt werden im Krankenhaus" wird auch in den meisten anderen Bundesländern abgestellt.

> Baden -Württemberg*: „sowie ihrer **Angehörigen**, Begleitpersonen und sonstigen Bezugspersonen (Betroffene), **die im Krankenhaus** im Zusammenhang mit der stationären Versorgung des Patienten **bekannt werden**"* (§ 43 Abs. 4 S. 1 LKHG BW).
>
> Brandenburg*: „Patientendaten sind alle Einzelangaben über persönliche oder sachliche Verhältnisse bestimmter oder bestimmbarer Patientinnen oder Patienten aus dem Bereich der*

[97] Ähnlich: Krügel, in: ZD 2017, 455, 455.

*Krankenhäuser (Nr. 1), von deren **Angehörigen** und anderen Bezugspersonen (Nr. 2) und sonstiger Dritter (Nr. 3), **die dem Krankenhaus** im Zusammenhang mit einer stationären, teilstationären oder ambulanten Behandlung **bekannt werden**."* (§ 27 Abs. 2 BbgKHG).

Bremen*: „Als Patientendaten gelten auch personenbezogene Daten von **Angehörigen** oder anderen Bezugspersonen des Patienten oder der Patientin sowie sonstiger Dritter, **die dem Krankenhaus** im Zusammenhang mit der Behandlung **bekannt werden**."* (§ 1 Abs. 1 S. 3 BremKHDSG).

Hamburg*: „Zu den Patientendaten gehören auch die personenbezogenen Daten von **Angehörigen** einer Patientin oder eines Patienten oder von sonstigen Dritten, wenn die Daten **dem Krankenhaus** im Zusammenhang mit der Behandlung der Patientin oder des Patienten **bekannt werden.**"* ( § 7 Abs. 1 S. 2 HmbKHG).

Nordrhein-Westfalen*: „Den Patientendaten sind gleichgestellt personenbezogene Daten **Dritter**, die bei Tätigkeiten nach Satz 1 (§ 2 Abs. 1 S. 1 GDSG NRW) den dort **genannten Stellen bekannt werden**."* (§ 2 Abs. 1 S. 2 GDSG NRW).

Rheinland-Pfalz*: „Patientendaten im Sinne der folgenden Bestimmungen sind auch personenbezogene Daten von **Angehörigen** oder anderen Bezugspersonen der Patientin oder des Patienten sowie sonstiger Dritter, **die dem Krankenhaus** im Zusammenhang mit der Behandlung **bekanntwerden**."* (§ 36 Abs. 1 S. 4 LKG RP).

Saarland*: „Patientendaten sind auch personenbezogene Daten von **Angehörigen** oder anderen Bezugspersonen der Patientin oder des Patienten sowie sonstiger Dritter, die **dem Krankenhaus** im Zusammenhang mit der Behandlung **bekannt werden**."* (§ 13 Abs. 1 S. 2 SKHG).

Sachsen*: „Patientendaten sind auch die personenbezogenen Daten von **Angehörigen**, anderen Bezugspersonen des Patienten sowie sonstiger Dritter, die dem Krankenhaus im Zusammenhang mit der Behandlung **bekannt werden**."(*§ 33 Abs. 1 S. 3 SächsKHG).

Sachsen-Anhalt*: „Patientendaten sind alle Einzelangaben über persönliche oder sachliche Verhältnisse bestimmter oder bestimmbarer Patienten aus dem Bereich des Krankenhauses (Nr. 1) sowie der **Angehörigen** des Patienten, anderer Bezugspersonen und sonstiger Dritter (Nr. 2) (Betroffene), die im Krankenhaus im Zusammenhang mit einer Behandlung **bekannt werden**."* (§ 16 Abs. 1 KHG LSA).

Thüringen*: „Patientendaten sind auch personenbezogene Daten von **Angehörigen** oder anderen Bezugspersonen der Patienten sowie sonstiger Dritter, die dem Krankenhaus im Zusammenhang mit der Behandlung **bekannt werden**.",* (§ 27 Abs. 2 S. 3 ThürKHG).

In Berlin werden Angehörige pauschal mit in das Merkmaal „Patientendaten“ einbezogen

> *„Patientendaten sind alle Einzelangaben über persönliche oder sachliche Verhältnisse bestimmter oder bestimmbarer Patientinnen und Patienten und **deren Angehörigen**.“* (§ 24 Abs. 2 S. 1 LKHG Bln).

In Bayern, Hessen und Mecklenburg-Vorpommern findet sich im Wortlaut des Gesetzes hingegen nur ein Bezug zu Patientinnen und Patienten.[98]

### (2) Weitere Personengruppen

In Baden-Württemberg, Brandenburg, Bremen, Hamburg, Nordrhein-Westfalen, Rheinland-Pfalz, Saarland, Sachsen, Sachsen-Anhalt und Thüringen werden allgemein weitere Personengruppen (Begleitpersonen, Bezugspersonen, Dritte) mit einbezogen (siehe oben).

> Baden-Württemberg*: „sowie ihrer Angehörigen, **Begleitpersonen und sonstigen Bezugspersonen** (Betroffene), die im Krankenhaus im Zusammenhang mit der stationären Versorgung des Patienten bekannt .werden“* (§ 43 Abs. 4 S. 1 LKHG BW)

> Brandenburg*: „Patientendaten sind alle Einzelangaben über persönliche oder sachliche Verhältnisse bestimmter oder bestimmbarer Patientinnen oder Patienten aus dem Bereich der Krankenhäuser, von deren Angehörigen und anderen **Bezugspersonen und sonstiger Dritter**, die dem Krankenhaus im Zusammenhang mit einer stationären, teilstationären oder ambulanten Behandlung bekannt werden“* (§ 27 Abs. 2 BbgKHG).

> Bremen*: „Als Patientendaten gelten auch personenbezogene Daten von Angehörigen oder anderen **Bezugspersonen** des Patienten oder der Patientin sowie **sonstiger Dritter**, die dem Krankenhaus im Zusammenhang mit der Behandlung bekannt werden“* (§ 1 Abs. 1 S. 3 BremKHDSG*).*

> Hamburg*: „Zu den Patientendaten gehören auch die personenbezogenen Daten von Angehörigen einer Patientin oder eines Patienten oder von **sonstigen Dritten**, wenn die Daten dem Krankenhaus im Zusammenhang mit der Behandlung der Patientin oder des Patienten bekannt werden“* (§ 7 Abs. 1 S. 2 HmbKHG).

[98] Bayern: Art. 27 Bay KHG; Hessen: § 12 Abs. HKHG; Mecklenburg-Vorpommern: § 33 Abs. 1 LKHG M-V.

Nordrhein-Westfalen*: „Den Patientendaten sind gleichgestellt **personenbezogene Daten Dritter**, die bei Tätigkeiten nach Satz 1 den dort genannten Stellen bekannt werden“* (§ 2 Abs. 1 S. 2 GDSG NRW).

Rheinland-Pfalz*: „Patientendaten im Sinne der folgenden Bestimmungen sind auch personenbezogene Daten von Angehörigen **oder anderen Bezugspersonen** der Patientin oder des Patienten sowie sonstiger Dritter, die dem Krankenhaus im Zusammenhang mit der Behandlung bekanntwerden“* (§ 36 Abs. 1 S. 4 LKG RP).

Saarland*: „Patientendaten sind auch personenbezogene Daten von Angehörigen oder **anderen Bezugspersonen** der Patientin oder des Patienten sowie **sonstiger Dritter**, die dem Krankenhaus im Zusammenhang mit der Behandlung bekannt werden“* (§ 13 Abs. 1 S. 2 SKHG*).*

Sachsen*: „Patientendaten sind auch die personenbezogenen Daten von Angehörigen, **anderen Bezugspersonen** des Patienten sowie **sonstiger Dritter**, die dem Krankenhaus im Zusammenhang mit der Behandlung bekannt werden“* (§ 33 Abs. 1 S. 3 SächsKHG).

*Sachsen-Anhalt: „Patientendaten sind alle Einzelangaben über persönliche oder sachliche Verhältnisse 1. bestimmter oder bestimmbarer Patienten aus dem Bereich des Krankenhauses sowie 2. der Angehörigen des Patienten, **anderer Bezugspersonen und sonstiger Dritter** (Betroffene), die im Krankenhaus im Zusammenhang mit einer Behandlung bekannt werden“* (§ 16 KHG LSA).

*Thüringen: „Patientendaten sind auch personenbezogene Daten von Angehörigen oder **anderen Bezugspersonen** der Patienten sowie **sonstiger Dritter**, die dem Krankenhaus im Zusammenhang mit der Behandlung bekannt werden“* (§ 27 Abs. 2 S. 3 ThürKHG).

### bb) Kontext der Verarbeitung

Der sachliche Anwendungsbereich der Landeskrankenhausgesetze bezieht sich auf den Vorgang der Verarbeitung. Vielfach spielt der Kontext der Verarbeitung eine Rolle. Innerhalb der Vorschriften findet häufig eine Differenzierung zwischen Erhebung, (Weiter-)verarbeitung und Übermittlung statt.

Baden-Württemberg*: „Personenbezogene Daten im Sinne dieses Gesetzes sind Einzelangaben über persönliche oder sachliche Verhältnisse bestimmter oder bestimmbarer Patienten **des Krankenhauses** sowie ihrer Angehörigen, Begleitpersonen und sonstigen Bezugspersonen (Betroffene), **die im Krankenhaus im Zusammenhang mit der stationären Versorgung des Patienten bekannt werden** (Patientendaten)“* (§ 43 Abs. 4 S. 1 LKHG BW).

Bayern*: „Patientendaten sind alle Einzelangaben über persönliche oder sachliche Verhältnisse bestimmter oder bestimmbarer Patienten* ***aus dem Bereich der Krankenhäuser****"* (Art. 27 BayKHG).

Brandenburg*: „Patientendaten sind alle Einzelangaben über persönliche oder sachliche Verhältnisse bestimmter oder bestimmbarer Patientinnen oder Patienten* ***aus dem Bereich der Krankenhäuser****, von deren Angehörigen und anderen Bezugspersonen und sonstiger Dritter,* ***die dem Krankenhaus im Zusammenhang mit einer stationären, teilstationären oder ambulanten Behandlung bekannt werden****"* (§ 27 BbgKHEG).

Bremen*: „Patientendaten sind alle Einzelangaben über persönliche oder sachliche Verhältnisse bestimmter oder bestimmbarer Patienten und Patientinnen* ***des Krankenhauses****. Als Patientendaten gelten auch personenbezogene Daten von Angehörigen oder anderen Bezugspersonen des Patienten oder der Patientin sowie sonstiger Dritter,* ***die dem Krankenhaus im Zusammenhang mit der Behandlung bekannt werden****"* (§ 1 Abs. 1 S. 2, 3 BremKHDSG).

Hamburg*: „In diesem Abschnitt wird der Schutz von personenbezogenen Daten der Patientinnen und Patienten* ***im Krankenhaus*** *geregelt. Zu den Patientendaten gehören auch die personenbezogenen Daten von Angehörigen einer Patientin oder eines Patienten oder von sonstigen Dritten,* ***wenn die Daten dem Krankenhaus im Zusammenhang mit der Behandlung der Patientin oder des Patienten bekannt werden****"* (§ 7 Abs. 1 S.1, S. 2 HmbKHG).

Nordrhein-Westfalen*: „Dieses Gesetz gilt für die Verarbeitung der personenbezogenen Daten 1.von Personen,* ***die, auch aufgrund eines gesonderten ärztlichen Behandlungsvertrages, in einem zugelassenen Krankenhaus*** *im Sinne von § 107 Abs. 1, § 108 und in einer V****orsorge- und Rehabilitationseinrichtung*** *gemäß § 107 Abs. 2, § 111 des Sozialgesetzbuches, Fünftes Buch – Gesetzliche Krankenversicherung – (SGB V) vom 20. Dezember 1988 (BGBl. I S. 2477) in der jeweils geltenden Fassung, deren Träger nicht der Bund oder eine bundesunmittelbare Körperschaft gemäß Artikel 87 Abs. 2 des Grundgesetzes ist,* ***(Einrichtung) ambulant oder stationär untersucht oder behandelt werden****, 2.von Personen,* ***für die Maßnahmen aufgrund des*** *Gesetzes über Hilfen und Schutzmaßnahmen bei psychischen Krankheiten (****PsychKG****) vom 17. Dezember 1999 (GV. NRW. S. 622) in der jeweils geltenden Fassung* ***getroffen werden****, 3.von Personen,* ***die vom Gesundheitsamt untersucht oder von dessen Maßnahmen getroffen werden****. (Patientendaten). … 3Den Untersuchungen nach Nummer 3 gleichgestellt sind Untersuchungen, die von Vollzugsärztinnen und Vollzugsärzten im Rahmen von § 118 Absatz 3 des Landesbeamtengesetzes vom 21. April 2009 (GV. NRW. S. 224), das zuletzt durch Artikel 1 des Gesetzes vom 9. Dezember 2014 (GV. NRW. S. 874) geändert worden ist, durchgeführt werden."* (§ 2 Abs. 1 S. 1, 3 GDSG NRW)

Rheinland-Pfalz*: „Patientendaten im Sinne der folgenden Bestimmungen sind auch personenbezogene Daten von Angehörigen oder anderen Bezugspersonen der Patientin oder des Patienten sowie sonstiger Dritter**, die dem Krankenhaus im Zusammenhang mit der Behandlung bekanntwerden**"* (§ 36 Abs. 1 S. 4 LKG RP).

Saarland*: „Alle Daten von Patientinnen und Patienten (Patientendaten)* ***im Krankenhaus*** *unterliegen* ***unabhängig von der Art ihrer Verarbeitung*** *dem Datenschutz. Patientendaten sind auch personenbezogene Daten von Angehörigen oder anderen Bezugspersonen der Patientin oder des Patienten sowie sonstiger Dritter,* ***die dem Krankenhaus im Zusammenhang mit der Behandlung bekannt werden.**"* (§ 13 Abs. 1 S. 1, 2 SKHG).

Sachsen*: „Patientendaten sind alle Einzelangaben über persönliche oder sachliche Verhältnisse bestimmter oder bestimmbarer Patienten* ***aus dem Bereich der Krankenhäuser****. Patientendaten sind auch die personenbezogenen Daten von Angehörigen, anderen Bezugspersonen des Patienten sowie sonstiger Dritter,* ***die dem Krankenhaus im Zusammenhang mit der Behandlung bekannt werden.**"* (§ 33 Abs. 1 S. 2, 3 SächsKHG).

Sachsen-Anhalt*: „Patientendaten sind alle Einzelangaben über persönliche oder sachliche Verhältnisse 1. bestimmter oder bestimmbarer Patienten* ***aus dem Bereich des Krankenhauses*** *sowie 2. der Angehörigen des Patienten, anderer Bezugspersonen und sonstiger Dritter (Betroffene),* ***die im Krankenhaus im Zusammenhang mit einer Behandlung bekannt werden**"* (§ 16 Abs. 1 KHG LSA).

Anders ist es hingegen in Berlin:

*„Patientendaten sind alle Einzelangaben über persönliche oder sachliche Verhältnisse bestimmter oder bestimmbarer Patientinnen und Patienten und deren Angehörigen."* (§ 24 Abs. 2 S. 1 LKHG Bln).

### cc) Ambulante Behandlung

In manchen Krankenhausgesetzen wird im Rahmen der Begriffsbestimmung für „Patientendaten" explizit auf die ambulante Behandlung und weitere Bereiche der Krankenhäuser eingegangen. Beispiele finden sich in Baden-Württemberg und Nordrhein-Westfalen:

Baden-Württemberg: „*Patientendaten in diesem Sinne sind auch Daten, die im Zusammenhang mit einer ambulanten Behandlung stehen, die das Krankenhaus im Rahmen einer Institutsambulanz oder einer institutionellen Ermächtigung erbringt."* (§ 43 Abs. 4 S. 2 LKHG BW).

Nordrhein-Westfalen*: „Dieses Gesetz gilt für die Verarbeitung der personenbezogenen Daten 1.von Personen, die, auch aufgrund eines gesonderten ärztlichen Behandlungsvertrages, in einem zugelassenen Krankenhaus im Sinne von § 107 Abs. 1, § 108 und in einer Vorsorge- und Rehabilitationseinrichtung gemäß § 107 Abs. 2, § 111 des Sozialgesetzbuches, Fünftes Buch – Gesetzliche Krankenversicherung – (SGB V) vom 20. Dezember 1988 (BGBl. I S. 2477) in der jeweils geltenden Fassung, deren Träger nicht der Bund oder eine bundesunmittelbare Körperschaft gemäß Artikel 87 Abs. 2 des Grundgesetzes ist, (Einrichtung) ambulant oder stationär untersucht oder behandelt werden,…"* (§ 2 Abs. 1 S. 1 Nr. 1 GDSG NRW*).*

### dd) Postmortaler Schutz

In Hamburg geht der Schutz der bereichsspezifischen Datenschutzvorschriften explizit über den Tod hinaus.[99]

### ee) Gesetzliche Ausnahmen

In Einzelfällen existieren im Gesetzeswortlaut Ausnahmen von der sachlichen Anwendbarkeit:

#### aaa) Forschung

In Baden-Württemberg normiert § 43 Abs. 3 LKHG BW eine Ausnahme vom Anwendungsbereich. Demnach gelten die Vorschriften des 7. Abschnitts, in dem die krankenhausspezifischen Vorschriften zum Datenschutz geregelt sind, nicht für Datenverarbeitungen für Zwecke wissenschaftlicher Forschung.

Gleichwohl enthält dieser Abschnitt, der für Datenverarbeitungen zu Zwecken der wissenschaftlichen Forschung nicht gilt, eine Erlaubnis zur Datenübermittlung zu eben diesen Zwecken. § 46 Abs. 1 S. 1 Nr. 2a LKHG BW normiert, dass Patientendaten an Personen und Stellen außerhalb des Krankenhauses übermittelt werden dürfen, soweit dies erforderlich ist

*„zur Durchführung medizinischer Forschungsvorhaben des Krankenhauses".*

Diese Vorschrift ist mit Gesetz vom 23.05.2000 (GBl. S. 450) offenbar unter Verkennung des Anwendungsbereichs der Vorschriften zum Datenschutz im Krankenhausgesetz eingefügt worden. Dieser **Normenwiderspruch** lässt sich nicht durch Auslegung auflösen, sodass auf allgemeine Kollisionsregeln zurückgegriffen werden muss. Vorliegend kommt der Grundsatz „*lex posterior derogat legi priori*" zum Tragen, wonach das zeitlich jüngere das ältere Gesetz verdrängt[100]. Diese Kollisionsregel kann vorliegend angewendet werden, denn es handelt sich um eine Normenkollision auf derselben normenhierarchischen Stufe – ja sogar innerhalb desselben Gesetzes.

---

[99] Vgl. Hamburg: „Der Datenschutz endet nicht mit dem Tode der Patientin oder des Patienten.", § 7 Abs. 1 S. 3 HmbKHG.
[100] *Dederer*, in: Maunz/Dürig (Hrsg.), Grundgesetz-Kommentar, 84. EL 2018, Art. 100 GG, Rn. 96.

Während der Anwendungsbereich seit der Einführung des Gesetzes mit Wirkung vom 28.07.1999 nicht geändert wurde, ist die Übermittlungserlaubnis im Jahr 2000 nachträglich in das Landeskrankenhausgesetz Baden-Württemberg eingefügt worden. Demnach gilt der § 46 Abs. 1 S. 1 Nr. 2a LKHG BW trotz der grundsätzlich im Bereich der wissenschaftlichen Forschung nicht anwendbaren bereichsspezifischen Vorschriften.

### bbb) Gefangene und Sicherheitsverwahrte

In Nordrhein-Westfalen gibt es eine Ausnahme im Hinblick auf personenbezogene Daten von Gefangenen und Sicherheitsverwahrten.[101]

### ff) Verweise auf die Datenschutz-Grundverordnung

In einigen Landeskrankenhausgesetzen, die bereits an die DS-GVO angepasst worden sind, sind Verweise auf die DS-GVO zu finden. Beispiele finden sich in Brandenburg, Hessen, Mecklenburg-Vorpommern und Rheinland-Pfalz.

> Brandenburg*: „Ergänzend zu der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates von 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (**Datenschutz-Grundverordnung)** (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72; L 127 vom 23.5.2018, S. 2) gilt das Brandenburgische Datenschutzgesetz, soweit in diesem Gesetz oder anderen Spezialgesetzen, die Regelungen über die Datenverarbeitung von Patientendaten durch Krankenhäuser treffen, nichts anderes bestimmt ist“* (§ 27 Abs. 1 BbgKHEG*).*
>
> Hessen*: „Für Krankenhäuser gelten die Bestimmungen der Verordnung (EU) Nr. 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (**Datenschutz-Grundverordnung**) (ABl. EU Nr. L 119 S. 1, Nr. L 314 S. 72) in der jeweils geltenden Fassung sowie des Hessischen Datenschutz- und Informationsfreiheitsgesetzes in der jeweils geltenden Fassung abweichend von dessen § 2 Abs. 2 uneingeschränkt nach Maßgaben der Abs. 2 bis 5“* (§ 12 HKHG).
>
> *Mecklenburg-Vorpommern: „Im Krankenhaus verarbeitete personenbezogene Daten unterliegen unabhängig von der Art ihrer Verarbeitung der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG*

[101] Nordrhein-Westfalen: „Dieses Gesetz gilt, soweit nichts anderes bestimmt ist, nicht für die Verarbeitung von personenbezogenen Daten von Gefangenen und Sicherungsverwahrten sowie von Personen, die nach §§ 63, 64 des Strafgesetzbuches, nach §§ 81, 126a der Strafprozeßordnung oder nach § 73 des Jugendgerichtsgesetzes untergebracht sind.“, § 2 Asb. 2 GDSG NRW.

*(**Datenschutz-Grundverordnung**; ABl. LEU 119 vom 4.5.2016, S. 1, L 314, S. 72) und ergänzend den datenschutzrechtlichen Bestimmungen dieses Abschnitts"* (§ 32 S. 1 LKHG M-V).

Rheinland-Pfalz*: „Die datenschutzrechtlichen Vorschriften dieses Gesetzes finden keine Anwendung, soweit das Recht der Europäischen Union, im Besonderen die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (**Datenschutz-Grundverordnung**) (ABl. EU Nr. L 119 S. 1) in der jeweils geltenden Fassung, unmittelbar gilt"* (§ 36 Abs. 1 S. 1 LKG RP).

Die DS-GVO gilt jedoch immer unmittelbar und für bzw. neben allen bereichsspezifischen Datenschutzgesetzen, unabhängig davon, ob dies im Gesetz explizit erwähnt wird. Der Verweis kann also nur klarstellende Wirkung haben.

#### gg) Art der Verarbeitung

Darüber hinaus finden sich verschiedene Klarstellungen in den Gesetzen. Hierzu gehört auch der Verweis auf eine Anwendbarkeit unabhängig von der Art der Verarbeitung.[102]

### b) Persönlicher Anwendungsbereich

Der persönliche Anwendungsbereich beschreibt einerseits die geschützten Personen. Diese werden auch (von der Datenverarbeitung) „Betroffene" genannt. In erster Linie gehören hierzu die Patientinnen und Patienten, deren personenbezogene Daten verarbeitet werden. Darunter können auch Angehörige und sonstige Personen fallen (s.o.).

Andererseits bezieht sich der persönliche Anwendungsbereich auf das verpflichtete Rechtssubjekt, also die verantwortliche Stelle. In erster Linie adressieren die Landeskrankenhausgesetze die **Krankenhäuser**, die damit in der Terminologie des Datenschutzrechts als „verantwortliche Stellen" anzusehen sind. In manchen Bundesländern richten sich die Vorschriften auch an die **Ärztinnen und Ärzte**.

### c) Räumlicher Anwendungsbereich

Der räumliche Anwendungsbereich der Vorschriften über die Datenverarbeitung zu Forschungszwecken leitet sich i.d.R. direkt aus dem jeweiligen räumlichen Anwendungsbereich des Landeskrankenhausgesetzes ab.

---

[102] Beispiele: Bremen: „unabhängig von der Art ihrer Verarbeitung", § 1 S. 1 BremKrhG; § 32 S. 1 LKHG M-V; Saarland: „unabhängig von der Art ihrer Verarbeitung", § 13 Abs. 1 SKHG.

## 2. Verhältnis der Landeskrankenhausgesetze zu anderen Gesetzen

Auch wenn die Krankenhäuser dem jeweiligen Landesdatenschutzgesetz unterliegen, gehen die Vorschriften der Landeskrankenhausgesetze den Regelungen der Landesdatenschutzgesetze als ***leges speciales*** in allen Bundesländern vor.[103] Das ist aber nur dann der Fall, wenn tatsächlich eine Konfliktlage existiert: wenn die bereichsspezifischen Vorschriften keine Regelung enthalten, kommt das allgemeine Datenschutzrecht zum Tragen.[104]

Im Hinblick auf das Verhältnis zwischen Landeskrankenhausgesetzen und Bundesdatenschutzgesetz, welches für Krankenhäuser des Bundes und Krankenhäuser in privater Trägerschaft relevant ist, stellt sich die Situation anders dar. Gemäß § 1 Abs. 2 S. 1 BDSG hat das Bundesdatenschutzgesetz den Charakter eines **subsidiären Auffanggesetzes** gegenüber bereichsspezifischen Spezialregelungen, die vorrangig anzuwenden sind.[105] Das gilt allerdings nach dem Wortlaut der Norm nur für andere Rechtsvorschriften des Bundes, die die Verarbeitung personenbezogener Daten regeln. Das Verhältnis zum Landesrecht wird von Art. 31 GG bestimmt, sodass das BDSG für Krankenhäuser des Bundes und Krankenhäuser in nicht-öffentlicher Trägerschaft grundsätzlich vorginge. Dieses Ergebnis ist schon deshalb nicht sachgerecht, weil der Gesetzgeber ausdrücklich davon ausgeht, dass es sich bei dem BDSG um ein Auffanggesetz handelt.[106] Im Ergebnis besteht daher weitgehend Einigkeit darüber, dass eine Korrektur dieses Vorrangs notwendig ist.[107] Unabhängig von der jeweiligen Trägerschaft gilt deshalb für Krankenhäuser bei der Verarbeitung von Patientendaten das **bereichsspezifische Landesrecht**, sofern ein solches existiert.

## 3. Verarbeitung von Patientendaten zu Forschungszwecken nach den Landeskrankenhaus- und Landesdatenschutzgesetzen

Im Folgenden werden die voneinander abweichenden landesrechtlichen Vorgaben im Hinblick auf verschiedene thematische Aspekte untersucht.

### a) Zulässigkeit der Datenverarbeitung

Die Verarbeitung personenbezogener Daten ist zulässig, wenn ein Gesetz die Verarbeitung erlaubt oder die betroffene Person in die Datenverarbeitung eingewilligt hat.[108] Im Hinblick auf personenbezogene Daten, die zu Forschungszwecken verarbeitet werden, ergibt sich die Besonderheit, dass es sich häufig um Daten handelt, die etwa zum Zweck der Durchführung des Behandlungsverhältnisses erhoben wurden und sodann zu Forschungszwecken weiterverarbeitet werden sollen. Insofern ist daher zwischen der **Primär- und der**

---

[103] Sosna, Daten- und Geheimnisschutz bei Outsourcing-Projekten im Krankenhausbereich, 1. Aufl. 2015, S. 44.
[104] Sosna, Daten- und Geheimnisschutz bei Outsourcing-Projekten im Krankenhausbereich, 1. Aufl. 2015, S. 44.
[105] Gusy/Eichenhofer, in: Wolff/Brink, BeckOK Datenschutzrecht, 29. Ed., Stand 01.05.2018, Rn. 78.
[106] BT-Drs. 18/11325, 79.
[107] Sosna, Daten- und Geheimnisschutz bei Outsourcing-Projekten im Krankenhausbereich, 1. Aufl. 2015, S. 45 f. m.w.N.
[108] Vgl. Art. 5 Abs. 1, 6 Abs. 1, 9 Abs. 2 DS-GVO.

**Sekundärnutzung** (auch -verarbeitung) der Daten zu unterscheiden. Da die Datenverarbeitung stets zweckgebunden ist, bedarf die Weiterverarbeitung zu einem anderen als dem ursprünglichen Zweck daher auch einer eigenen Rechtsgrundlage. Nach dem gegenwärtig vorherrschenden Verständnis ersetzt die **Kompatibilitätsprüfung** des Art. 6 Abs. 4 DS-GVO jedenfalls nicht die notwendige Rechtsgrundlage für eine Datenverarbeitung mit einem geänderten Zweck.[109] Dies vorausgeschickt, sollen nun die Vorgaben im Hinblick auf die Zulässigkeit der Verarbeitung personenbezogener Daten zu Forschungszwecken dargestellt werden.

### aa) Erhebung von Patientendaten zu Forschungszwecken nach dem jeweiligen Landesrecht

In den meisten Landeskrankenhausgesetzen existieren neben den „allgemeinen" Regelungen zur Verarbeitung von Patientendaten besondere Regeln zur Verarbeitung von Patientendaten für Forschungszwecke.

#### aaa) Erhebung von Patientendaten zu sonstigen Zwecken

Fast alle Landeskrankenhausgesetze enthalten zunächst (explizit) Erlaubnisnormen für die Erhebung (bzw. Verarbeitung)[110] von Patientendaten.[111] Ein großer Teil der Landeskrankenhausgesetze enthält jedoch keine explizite Erlaubnis für die **Erhebung** von Patientendaten **zu Forschungszwecken**. So sehen die Erlaubnisnormen der Landeskrankenhausgesetze zur Erhebung von Patientendaten in Baden-Württemberg (§ 45 LKHG BW), Bayern (Art. 24 Abs. 2 BayKrG), Brandenburg (§ 28 BbgKHEG), Bremen (§ 2 BremKHDSG), Hamburg (§ 8 HmbKHG), Nordrhein-Westfalen (§§ 10, 13 GDSG NW), (wohl auch) Saarland (§ 13 SKHG); (wohl auch) Sachsen (§ 34 SächsKHG); (wohl auch) Sachsen-Anhalt (§ 16 KHG LSA) keine ausdrückliche Befugnis zu der **Erhebung** von Patientendaten für **Forschungszwecke** vor.

#### bbb) Verarbeitung von Patientendaten zu Forschungszwecken

Die Regelungen der Landeskrankenhausgesetze in Baden-Württemberg, Bayern, Brandenburg, Bremen, Mecklenburg-Vorpommern, Nordrhein-Westfalen, Saarland, Sachsen und Sachsen-Anhalt zur Verarbeitung von Patientendaten zu Forschungszwecken[112] beziehen sich lediglich auf die **(Weiter-)verarbeitung (oder Nutzung) bereits erhobener und gespeicherter (d.h. „vorhandener") Patientendaten**. Es herrscht eine große Vielfalt von gesetzlichen Anknüpfungspunkten:

In Bayern bezieht sich die Erlaubnis auf das „***Nutzen***" (Art. 27 Abs. 4 BayKrG).

---

[109] Vgl. statt vieler Kühling/Buchner/Buchner/Petri, 2. Aufl. 2018, DS-GVO Art. 6 Rn. 181-185

[110] Teilweise sind die Landeskrankenhausgesetze an die Terminologie der Datenschutz-Grundverordnung angepasst worden. Verarbeitung i.S.v. Art. 4 Nr. 2 DS-GVO umfasst die Erhebung personenbezogener Daten.

[111] § 45 LKHG BW, Art. 27 Abs. 2 BayKrG, § 24 Abs. 4 LKHG Bln, § 28 ,BbgKHEG („Verarbeitung"), § 2 BremKHDSG, § 8 HmbKHG, § 33 Abs. 1 LKHG M-V („Verarbeitung"); § 10 GDSG NW; § 36 Abs. 2 LKHG RP; § 13 SKHG, § 33 Abs. 2 SächsKHG; § 16 Abs. 2, 3 KHG LSA; § 27 Abs. 3 ThürKHG; Ausnahmen: Hessen und Niedersachsen; In Hessen wird lediglich auf die Datenschutz-Grundverordnung (DS-GVO) sowie das Hessische Datenschutz- und Informationsfreiheitsgesetz verwiesen (§ 12 Abs. 1 HKHG).

[112] In Nordrhein-Westfalen „Datenverarbeitung für wissenschaftliche Zwecke", § 6 GDSG NW.

In Baden-Württemberg wird im Wortlaut der Begriff "***übermitteln***" verwandt (§ 46 Abs. 1 S. 1 Nr. 2a. LKHG BW).

Das Brandenburgische Krankenhausentwicklungsgesetz spricht von: „***Offenlegung*** *von Patientendaten*" (§ 31 BbgKHEG; § 31 BbgKHEG verweist jedoch auf § 25 LDSG Bbg. Dieser bezieht sich auf die „**Verarbeitung**").

In Bremen bezieht sich die Erlaubnis auf die *„Verarbeitung von Patientendaten, die im Rahmen von § 2 Abs. 1* ***gespeichert*** *worden sind"* (§ 7 BremKHDSG).

In Mecklenburg-Vorpommern findet sich im Gesetzestext die Formulierung *„Verarbeitung und Nutzung von personenbezogenen Daten von Patientinnen und Patienten, die im Rahmen des § 33 Absatz 1 (LKHG M-V)* ***erhoben*** *worden sind"* (§ 37 Abs. 1 LKHG M-V).

In Nordrhein-Westfalen enthät das Gesetz die Einschränkungen: *„Übermittlung von Patientendaten und die Verarbeitung"* (§ 6 Abs. 1 GDSG NW) sowie „***nutzen***" (§ 6 Abs. 2 GDSG NW).

Im Saarland wird die Verarbeitung auf *„die innerhalb ihrer Fachabteilung zu Behandlungszwecken* ***aufgezeichneten*** *Patientendaten für eigene medizinische wissenschaftliche Forschung nutzen*" beschränkt (§ 14 Abs. 1 SKHG).

Das sächsische Krankenhausgesetz bezieht sich im Wortlaut auf die **Weitergabe** ( § 14 Abs. 2 SKHG) sowie die Speicherung, Verarbeitung und Nutzung (§ 14 Abs. 3 SKHG).

Das Sächsiche Gesetz enthält folgende Formulierung: *„Ärzte dürfen Patientendaten, die innerhalb ihrer Fachabteilung oder bei Hochschulen innerhalb ihrer medizinischen Einrichtungen, in den Universitätsklinika oder in sonstigen medizinischen Einrichtungen* ***gespeichert*** *sind, für eigene wissenschaftliche Forschungsvorhaben verarbeiten*", § 34 Abs. 1 SächsKHG.

Darüber hinaus bezieht sich das sächsische Gesetz auf die „***Übermittlung***", § 34 Abs. 2 SächsKHG;

In Sachsen-Anhalt lautet der Gesetzestext: *„Patientendaten, die innerhalb ihrer Fachabteilung oder bei Hochschulen innerhalb ihrer Klinik oder in sonstigen medizinischen Einheiten eines Universitätsklinikums* ***verarbeitet*** *worden sind, für eigene wissenschaftliche Forschungsvorhaben verwenden*", § 17 Abs. 1 KHG LSA und „Übermittlung" (§ 17 Abs. 2 KHG LSA).

Im Landeskrankenhausgesetz Thüringens wird zwischen der Verarbeitung zu Forschungszwecken von Patientendaten *„durch die Krankenhausärzte*" (§ 27 Abs. 4 ThürKHG) und der Verarbeitung „für *Forschungszwecke außerhalb des Krankenhauses*" (§ 27a ThürKHG) differenziert. § 27a Abs. 1 ThürKHG bezieht sich auf „*Patientendaten, die im Rahmen des § 27 Abs. 3* ***gespeichert*** *worden sind*".

### ccc) Erhebung von Patientendaten zu Forschungszwecken

Das Landeskrankenhausgesetz in Berlin sieht hingegen (auch) eine explizite Ermächtigung zur **Erhebung** von Patientendaten **für Forschungszwecke** vor (§ 25 LKHG Bln).

Die Landeskrankenhausgesetze in Rheinland-Pfalz[113] und Thüringen sind bereits an die DS-GVO angepasst worden, so dass der in diesen Landeskrankenhausgesetzen gewählte Begriff der Verarbeitung im Lichte der Begriffsdefinition der DS-GVO weit zu verstehen ist. Nach Art. 4 Nr. 2 DS-GVO bezeichnet der Begriff „Verarbeitung" jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten, worunter auch das Erheben fällt. Vor diesem Hintergrund erlauben die Vorschriften auch eine Erhebung zu Forschungszwecken (Rheinland-Pfalz: § 37 Abs. 1 LKHG RP; § 27 Abs. 4 ThürKHG).

In Thüringen gilt dies scheinbar nur für die Verarbeitung zu Forschungszecken durch die Krankenhausärzte (vgl. § 27 Abs. 4 ThürKHG und § 27a Abs. 1 ThürKHG).

### ddd) Rückgriff auf die allgemeinen Datenschutzvorschriften

Soweit nun die Datenverarbeitung von Patientendaten aus Krankenhäusern durch die Landeskrankenhausgesetze geregelt wird, sind diese Regelungen als spezifischer gegenüber dem allgemeinen Datenschutzrecht anzusehen. Für die Praxis bedeutet dies, dass ein Krankenhaus in einem Bundesland zunächst zu prüfen hat, ob der Verarbeitungsprozess im entsprechenden Landeskrankenhausgesetz geregelt ist. Für Krankenhäuser in Trägerschaft einer öffentlich-rechtlichen Einrichtung des Landes ist zusätzlich zu prüfen, ob die Regelungen des Landesdatenschutzrechts ergänzend heranzuziehen sind oder das Landeskrankenhausgesetz den Sachverhalt vollständig regelt. Für Krankenhäuser in privater Trägerschaft ist ein entsprechender Abgleich mit dem Bundesdatenschutzgesetz erforderlich. Das Landesdatenschutzgesetz ist daher anzuwenden, wenn das Krankenhaus in Trägerschaft einer öffentlich-rechtlichen Körperschaft des Landes steht und soweit das Landeskrankenhausgesetz keine Regelung für den Sachverhalt enthält.[114] Bei alledem ist zusätzlich zu beachten, dass die Landesdatenschutzgesetze den klarstellenden Hinweis enthalten, dass im Falle wettbewerblichen Handelns einer öffentlichen Stelle zumindest teilweise das Bundesrecht anzuwenden ist.[115]

Die Regelungen der Landeskrankenhausgesetze verhalten sich jedoch zu der Frage der Anwendbarkeit allgemeiner datenschutzrechtlicher Vorschriften unterschiedlich:

So heißt es etwa im Bundesland Bayern:

---

[113] § 36 Abs. 1 LKHG RP.
[114] Vgl. zur alten Rechtslage: Karaalp, Der Schutz von Patientendaten für die medizinische Forschung in Krankenhäusern, 2017. S. 72 ff.
[115] Vgl. z.B. § 2 Abs. 3 BlnDSG

> *„Patientendaten dürfen **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."* (Art. 27 Abs. 2 S. 1 BayKrG).

Im selben Gesetz sogleich danach:

> *„Soweit in diesem Gesetz nichts anderes bestimmt ist, sind auf Patientendaten die jeweils geltenden Vorschriften über den Schutz personenbezogener Daten anzuwenden."* (Art. 27 Abs. 1 S. 2 BayKrG)

Das Hessische Krankenhausgesetz verweist zunächst auf die DS-GVO sowie das Hessische Datenschutz- und Informationsfreiheitsgesetz (§ 12 Abs. 1 HKHG) und befasst sich sodann mit der „Übermittlung" von Patientendaten (§ 12 Abs. 2 HKHG). Die Übermittlung für Forschungszwecke taucht nicht explizit auf. Das Niedersächsisches Krankenhausgesetz (NKHG) enthält keine bereichsspezifischen Datenschutzvorschriften und in Schleswig-Holstein existiert kein Landeskrankenhausgesetz.

### bb) Weiterverarbeitung zu Forschungszwecken nach Landesrecht

Die Landeskrankenhausgesetze sehen in unterschiedlichem Umfang die Möglichkeit vor, Patientendaten, die ohnehin im Krankenhaus erhoben worden sind, zu Forschungszwecken **weiterzuverarbeiten**.

#### aaa) Anforderungen an die Einwilligung

Betroffene Personen können grundsätzlich in die Verarbeitung der sie betreffenden personenbezogenen Daten zu Forschungszwecken einwilligen. Die Einwilligung wird als originärer Ausdruck informationeller Selbstbestimmung verstanden,[116] ja sogar als eigenes Grundrecht auf Einwilligung, das sich aus Art. 8 Abs. 2 S. 1 GRCh ergibt.[117] Während das Grundrecht auf informationelle Selbstbestimmung die rechtliche und faktische Möglichkeit umfasst, einer anderen Person gegenüber das Einverständnis zu einer bestimmten Verarbeitung zu geben, schützt das Grundrecht auf Einwilligung auch den rechtlichen Erfolg der Erklärung, der darin besteht, einer anderen Person die Verarbeitung zu erlauben und diese von an die Verarbeitung rechtlich anknüpfenden negativen Sanktionen freizustellen.[118] Vorgaben für die Rechtmäßigkeit der Einwilligung ergeben sich aus Art. 6 Abs. 1 S. 1 lit. a und Art. 9 Abs. 2 lit. a) DS-GVO jeweils in Verbindung mit Art. 7 DS-GVO. Dies wird von einigen Landesgesetzen aufgenommen[119] oder präzisiert. Soweit es sich hier um Wiederholungen der Vorgaben der

---

116 *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, 2001, 15.
117 *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 1. Aufl. 2019, Art. 7 DSGVO, Rn. 20.
118 *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 1. Aufl. 2019, Art. 7 DSGVO, Rn. 20.
119 Vgl. § 37 Abs. 1 und 5 LKHG M-V, § 37 Abs. 1 LKG.

Datenschutzgrundverordnung handelt, liegt möglicherweise ein **Verstoß gegen das EU-rechtliche Wiederholungsverbot** vor.

In Bremen beschränkt § 7 Abs. 1 BremKHDSG die Einwilligung in die Verarbeitung von rechtmäßig gespeicherten Patientendaten auf wissenschaftliche medizinische Forschungsvorhaben der

- Angehörigen eines Heilberufs oder Gesundheitsfachberufs der Behandlungseinrichtung im Krankenhaus,
- durch Hochschulen oder
- andere mit wissenschaftlicher Forschung beauftragte Stellen.

### bbb) Datenspende

Der Begriff der „Datenspende“ wird in erster Linie im politischen Kontext verwandt, um Forderungen an die Ausgestaltung und Umsetzung des Datenschutzrechts zu formulieren.[120] So empfiehlt der deutsche Ethikrat in einer Stellungnahme aus dem Jahr 2017, eine „(r)echtliche Möglichkeit für Individuen (zu) schaffen, die umfassende Nutzung ihrer Daten für die medizinische Forschung zu erlauben („Datenspende“).[121]

Der Begriff findet sich nicht in den Gesetzestexten des Datenschutzes (DS-GVO, BDSG, LDSG, LKHG). Auch wird der Begriff in der Literatur nur vereinzelt verwandt.[122]

Aus den genannten Gründen existiert weder eine einheitliche Definition noch ein einheitliches Verständnis zum Begriff „Datenspende“. Aus datenschutzrechtlicher Perspektive steht der Begriff insbesondere im Zusammenhang mit der Einwilligung.

#### (1) Begriff

Der Begriff „Datenspende“ setzt sich aus den Wortbestandteilen „Daten“ und „Spende“ zusammen.

---

[120] Deutscher Ethikrat, Big Data und Gesundheit – Datensouveränität als informationelle Freiheitsgestaltung – Stellungnahme 2017 (abrufbar unter: https://www.ethikrat.org/fileadmin/Publikationen/Stellungnahmen/deutsch/stellungnahme-big-data-und-gesundheit.pdf)); Digitalisierung – CDU-Politiker Sorge spricht sich für Datenspende aus, BibliomedManager 12.12.2018, abrufbar unter: https://www.bibliomedmanager.de/news-des-tages/detailansicht/37041-cdu-politiker-sorge-spricht-sich-fuer-datenspende-aus/ (zuletzt abgerufen am: 26.07.2019); Politik – CDU-Politiker wirbt für Datenspende, aerzteblatt.de, 11.12.2018, abrufbar unter: https://www.aerzteblatt.de/nachrichten/99767/CDU-Politiker-wirbt-fuer-Datenspende (zuletzt abgerufen am: 26.07.2019); Politik – Hecken plädiert für verpflichtende Datenspende, aerzteblatt.de, 18.12.2018, abrufbar unter: https://www.aerzteblatt.de/nachrichten/99900/Hecken-plaediert-fuer-verpflichtende-Datenspende (zuletzt abgerufen am: 26.07.2019); Politik & Wirtschaft – Gesundheitsdaten für Forschung freigeben, Pharmazeutische Zeitung, 11.04.2019, abrufbar unter: https://www.pharmazeutische-zeitung.de/gesundheitsdaten-fuer-forschung-freigeben/ (zuletzt abgerufen am: 26.07.2019); Vernetzung . Brauchen wir die Datenspende?, EHealthCOM, abrufbar unter: https://e-health-com.de/details-news/brauchen-wir-die-datenspende/ (zuletzt abgerufen am: 26.07.2019)..

[121] Deutscher Ethikrat, Big Data und Gesundheit – Datensouveränität als informationelle Freiheitsgestaltung – Stellungnahme 2017 (abrufbar unter: https://www.ethikrat.org/fileadmin/Publikationen/Stellungnahmen/deutsch/stellungnahme-big-data-und-gesundheit.pdf)), S. 43.

[122] Ausnahmen sind z.B.: Heldt, Transparenz bei algorithmischen Entscheidungen – Food for Thoughts, Ein vergleichender Blick auf Kennzeichnungspflichten im Lebensmittelrecht, CR 2018, 494.

Im Zusammenhang mit der Verarbeitung von Patientendaten zu Forschungszwecken geht es stets um den Umgang mit **personenbezogenen Daten**. Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (Art. 4 Nr. 1 DS-GVO). Sollte unter einer Datenspende doch die Aufgabe von Rechten an anonymisierten Daten verstanden werden (im Sinne einer „Dereliktion"), ist eine Diskussion über die rechtlichen Voraussetzungen entbehrlich, da auf anonymisierte Daten das Datenschutzrecht jedenfalls keine Anwendung findet. In diesem Kontext wäre aber zu diskutieren, ob eine Anonymisierung tatsächlich dergestalt erfolgen kann, dass auch in Zukunft eine (Re-)Identifikation unter Ausschöpfung aller technischen Möglichkeiten von *Data Linkage*, Verkettung und *Big Data* dennoch möglich wäre. Die zu anonymisierenden Datensätze müssten um aussagefähige Parameter reduziert werden, wodurch sie für die Forschung an Aussagekraft und Bedeutung verlieren. Aus diesem Grund scheint die Diskussion über die Datenspende tatsächlich nur sinnvoll führbar, wenn es sich dabei um spezifische, aussagekräftige und damit letztlich personenbezogene aber oder zumindest personenbeziehbare Datensätze handelt.

Eine „**Spende**" ist nach einer allgemeinen Erläuterung „etwas, was zur Hilfe, Unterstützung, Förderung einer Sache oder Person gegeben wird, beitragen soll".[123] In der datenschutzrechtlichen Diskussion wird „Datenspende" als das „freiwillige Herausgeben von Nutzerdaten zu Forschungszwecken (…)" beschrieben.[124] Sie ist unwiderruflich, ähnlich der endgültigen Aufgabe des Eigentums an einem Grundstück gem. § 928 BGB, der „Dereliktion".

### (2) Zulässigkeit – Wirksamkeitsvoraussetzungen der datenschutzrechtlichen Einwilligung

Es stellt sich die Frage, ob, basierend auf den Vorgaben der Datenschutz-Grundverordnung, eine „Datenspende" zulässig ist. Hierzu sollten folgende Überlegungen angestellt werden: Die Datenschutz-Grundverordnung räumt dem Betroffenen einerseits Rechte ein, andererseits verpflichtet sie die verantwortliche Stelle, bestimmte Vorkehrungen zu treffen, die die Einhaltung dieser Rechte möglich macht. Bezüglich der Rechte ist zu prüfen, ob es sich dabei um dispositive Rechte handelt, mit anderen Worten, ob der Betroffene auf die Ausübung dieser Rechte wirksam im Außenverhältnis **verzichten** kann. Dabei ist zu bedenken, dass nicht nur nach den Grundsätzen des deutschen Rechts eine gesetzliche Beschränkung der Ausübung einseitig rechtsgestaltender Willenserklärungen in einem intensiven Spannungsfeld mit der grundgesetzlich verankerten **Handlungsfreiheit** stehen wird. Ein Gleiches ist anzunehmen für den Rechtsmaßstab des Artikels 8 der Grundrechte-Charta der EU. Des Weiteren ist zu überlegen, ob ein Verzicht auf die Ausübung dieser Rechte auch so erklärt werden kann, dass eine verantwortliche Stelle (die dann beispielsweise über die gespendeten Daten verfügt), die **Einhaltung dieser Betroffenen-Rechte auch nicht mehr gewährleisten** muss.

---

[123] Dudenredaktion (o.J.),„Spende" auf Duden online. URL: https://www.duden.de/node/169759/revision/169795 (zuletzt abgerufen am: 15.08.2019).

[124] Heldt, CR 2018, 494, 496, Fn. 4.

Auch ist zu untersuchen, ob eine Datenspende bereits im bisher bestehenden rechtlichen Kontext möglich ist, oder einer eigenständigen Rechtsgrundlage, entweder im Europarecht oder im nationalen Recht bedarf. Für die Verankerung im deutschen Recht ist erforderlich, dass dies unter Berücksichtigung der Vorgaben der DS-GVO erfolgen muss.

Ausgehend davon, dass eine Spende stets als etwas „Freiwilliges" angesehen wird, kommt eine Rechtfertigung über eine gesetzliche Erlaubnis nicht in Betracht, weil bei dieser Art der Rechtfertigung die Entscheidung der betroffenen Person nicht ausschlaggebend ist. Die datenschutzrechtliche Zulässigkeit kann sich daher **nur aus einer wirksamen Einwilligung** ergeben (vgl. Art. 5 Abs. 1 lit. a), 6 Abs. 1, 9 Abs. 1, 2 DS-GVO).

Nach Art. 4 Nr. 11 DS-GVO ist „Einwilligung" jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

Nach Art. 7 Abs. 3 S. 1 DS-GVO hat die betroffene Person aber das Recht, ihre Einwilligung zu widerrufen. Das widerspricht einer Spende im herkömmlichen Sinne insofern als unter einer Spende in der Regel eine endgültige und damit unwiderrufliche Überlassung verstanden wird. Wird die verantwortliche Stelle von der Verpflichtung zur Löschung im Fall eines Widerrufs freigestellt, wenn der Betroffene auf sein Widerrufsrecht verzichtet hat? Eine im nationalen Kontext verankerte Regelung zur Datenspende müsste jedenfalls vorsehen, dass der **Betroffene auf sein Widerrufsrecht ausdrücklich und unwiderruflich verzichtet**, und, damit korrespondierend, **der Verantwortliche von der Verpflichtung zur Löschung** gemäß Art. 17 Abs. 1b DS-GVO **befreit** wird.

Eine weitere Herausforderung für die Datenspenden liegt darin, dass personenbezogene Daten nach Art. 5 DS-GVO nur für festgelegte, eindeutige und legitime Zwecke erhoben und nur in einer mit diesen Zwecken zu vereinbarenden Weise weiterverarbeitet werden dürfen. Dementsprechend ist die Rechtmäßigkeit der Verarbeitung auf den Zweck beschränkt, zu dem die Einwilligung des Betroffenen, also hier des Spenders, beruht. Soll die Verarbeitung zu einem anderen Zweck erfolgen, besteht nach Art. 6 Abs. 4 DS-GVO die Verpflichtung des Verantwortlichen, eine Kompatibilitätsprüfung durchzuführen, die allerdings das Erfordernis einer Rechtsgrundlage für die weitere Verarbeitung nicht ersetzen kann.

In der bisherigen Diskussion um die Festlegung des Zwecks wurde deutlich, dass nach der DS-GVO eine Einwilligung zu mehreren Zwecken, aber auch zu weniger spezifischen Zwecken erklärt werden kann (*broad consent*). Hierzu sind die Datenschutzbehörden des Bundes und der Länder im Gespräch mit Mitgliedern der

Medizininformatik-Initiative. Ein entsprechendes Positionspapier befindet sich im Abstimmungsprozess.[125] Bei einer Datenspende ist zu diskutieren, ob ein in diesem Sinne „breiter Zweck" ausreichend ist. Soweit bei einer Datenspende angenommen wird, dass der Betroffene sich schon im Vorfeld der Verarbeitung mit jedweder Verarbeitung zu allen möglichen Zwecken einverstanden erklärt, geht dies jedenfalls erheblich über das gegenwärtige Verständnis der Zweckbindung hinaus. Die Einwände aus Sicht des Datenschutzes fußen darauf, dass der Betroffene im Moment einer solchen Verzichtserklärung noch nicht vorhersehen kann, welche in der Zukunft möglichen Verarbeitungsprozesse dann doch Nachteile für den Datenbestände mit sich bringen können. Das hieraus resultierende Schutzbedürfnis für den Bürger, eine solche unbedingte und inhaltlich noch nicht abschätzbar Erklärung nicht abgeben zu dürfen, ist erklärlich, steht aber gleichwohl im Konflikt mit der allgemeinen Handlungsfreiheit. Um diesen Vorbehalt nicht gänzlich aufzugeben, erscheint eine Datenspende möglich, wenn der Betroffene seine Rechte an den Daten zwar **zeitlich unbefristet** aufgibt, aber eine zweckmäßige **Beschränkung auf die Forschung** erklärt. Dies könnte weiter eingegrenzt werden auf bestimmte Verantwortliche, etwa **private oder staatliche Forschungseinrichtungen**, die für die Verarbeitungsprozesse möglicherweise auch bestimmte Voraussetzungen erfüllen müssten, wie etwa ein **Verbot der Weitergabe** an unbefugte Dritte einzuhalten. Eine solche, sehr weitreichende Zweckerklärung wäre dann ein **Auslegungskriterium für den Kompatibilitätstest** nach Art. 6 Abs. 4 der DS-GVO.

**Insgesamt verbleiben Zweifel, ob angesichts der fehlenden Öffnungsklausel zum Gebot der Zweckbindung und der Löschungsverpflichtung bei Widerruf in der DS-GVO eine praktikable Datenspende im deutschen Recht abbildbar ist.**

### ccc) Gesetzliche Erlaubnistatbestände

Sowohl der europäische Gesetzgeber als auch der Bundes- und Landesgesetzgeber haben für eine Reihe von bestimmten Verarbeitungssituationen vorgesehen, dass diese auch ohne Einwilligung der betroffenen Person erlaubt sind und insofern selbst die Verwirklichungsbedingungen der informationelle Selbstbestimmung mit anderen Grundrechten in Ausgleich gebracht. Dies gilt in einigen Konstellationen auch für die Verarbeitung von personenbezogenen Daten zu Forschungszwecken.

#### (1) Nutzung durch Krankenhausärzte zur Eigenforschung

Einige Landeskrankenhausgesetze ermöglichen die Nutzung von Patientendaten zu eigenen wissenschaftlichen Forschungszwecken. So etwa § 25 Abs. 1 Nr. 1 BlnLKG, der die Erlaubnis auf Ärztinnen und Ärzte erstreckt, die die Patientendaten im Rahmen der Krankenhausbehandlung innerhalb ihrer Fachrichtung erhoben und gespeichert haben, sofern schutzwürdige Belange der Patientin oder des Patienten nicht entgegenstehen und

[125] https://www.medizininformatik-initiative.de/de/mustertext-zur-patienteneinwilligung

eine gewerbliche Nutzung ausgeschlossen ist. Gleiches gilt gemäß § 34 Abs. 1 SächsKHG in Sachsen, allerdings ohne die Einschränkungen des Entgegenstehens schutzwürdiger Belange des Patienten oder des Ausschlusses der gewerblichen Nutzung. In Bremer Krankenhäusern dürfen Angehörige eines Heilberufs oder Gesundheitsfachberufs gemäß § 8 S. 1 BremKHDSG für eigene Forschungszwecke Dateien „anlegen". Auch im Saarland dürfen Krankenhausärzte die innerhalb ihrer Fachabteilung zu Behandlungszwecken aufgezeichneten Patientendaten für eigene wissenschaftliche Forschung nutzen. § 24 Abs. 1 SKHG stellt die Rechtmäßigkeit dieser Verarbeitung allerdings unter den Vorbehalt, dass der Zweck der Forschung auf andere Weise nicht erreicht werden kann und die Patientin oder der Patient entweder nach Unterrichtung über Art, Umfang und Zweck des Forschungsvorhabens nicht widersprochen hat oder schutzwürdige Belange nicht beeinträchtigt werden und nachträglich die Möglichkeit zum Widerspruch nicht oder nur mit unverhältnismäßigem Aufwand eingeräumt werden kann.

### (2) Nutzung durch Krankenhausärzte für Forschung des Krankenhauses

Nach dem Bayerischen und dem Thüringischen Krankenhausgesetz dürfen Krankenhausärzte Patientendaten nutzen, soweit dies **zu Forschungszwecken im Krankenhaus oder im Forschungsinteresse des Krankenhauses erforderlich** ist (Art. 27 Abs. 4 S. 1 und § 27 Abs. 4 ThürKHG). Das Hamburgische Krankenhausgesetz enthält einen ähnlichen Erlaubnistatbestand: Nach § 12 S. 1 HmbKHG darf ein Krankenhaus oder eine Krankenhausgruppe, die dort im Zusammenhang mit der Behandlung der Patientin oder des Patienten erhobene Patientendaten für **eigene wissenschaftliche Forschung** weiterverarbeiten. Damit ist der persönliche Anwendungsbereich weiter gefasst als der des Bayerischen Krankenhausgesetzes. Gleichzeitig bedarf es in Hamburg des zusätzlichen **Überwiegens des öffentlichen Interesses** an der Durchführung des Forschungsvorhabens gegenüber den schützenswerten Interessen der betroffenen Person. § 6 Abs. 2 GDSG NW erlaubt es dem wissenschaftlichen Personal, Patientendaten zu Zwecken der wissenschaftlichen Forschung zu nutzen, auf die es in der Einrichtung aufgrund seiner Tätigkeit ohnehin Zugriff hat. Eine Einschränkung auf Eigenforschung des jeweiligen Arztes oder auf Forschung im Interesse des Krankenhauses kennt das Gesundheitsdatenschutzgesetz NRW nicht.

### (3) Unzumutbarkeit der Einholung der Einwilligung

Nach § 25 Abs. 1 Nr. 2 BlnLKG dürfen Krankenhäuser Patientendaten für krankenhausinterne Forschungsvorhaben verarbeiten, wenn es **nicht zumutbar ist, die Einwilligung einzuholen** und schutzwürdige Belange der Patientin oder des Patienten nicht beeinträchtigt werden. Dies gilt gemäß § 37 Abs. 1 Nr. 1 LKG auch für Krankenhäuser in Rheinland-Pfalz und gemäß § 34 Abs. 3 Nr. 2 SächsKG für Krankenhäuser in Sachsen. § 17 Abs. 1 Nr. 2 KHG LSA normiert ebenfalls eine Erlaubnis der Datenverarbeitung zu Forschungszwecken im Fall der Unzumutbarkeit der Einholung der Einwilligung, allerdings unter der zusätzlichen Voraussetzung, dass der Forschungszweck auf andere Weise nicht erreicht werden kann.

### (4) Öffentliches Interesse

Einige Landeskrankenhausgesetze erlauben die Verarbeitung von Patientendaten zu Forschungszwecken, wenn ein **öffentliches Interesse an dem Forschungsvorhaben** besteht. Gemäß § 25 Abs. 1 Nr. 3 BlnLKG muss das berechtigte Interesse der Allgemeinheit an der Durchführung des Forschungsvorhabens das Geheimhaltungsinteresse der Patientin oder des Patienten erheblich überwiegen, damit Krankenhäuser Patientendaten für krankenhausinterne Forschungsvorhaben verarbeiten dürfen. Gleiches gilt gemäß § 37 Abs. 1 Nr. 2 LKG für Krankenhäuser in Rheinland-Pfalz, nach § 34 Abs. 3 Nr. 1 SächsKHG für Krankenhäuser in Sachsen sowie gemäß § 17 Abs. 1 Nr. 3 KHG LSA für Krankenhausärzte in Sachsen-Anhalt. Ebenso dürfen Krankenhäuser im Anwendungsbereich des Bremer Krankenhausgesetzes Patientendaten verarbeiten, wenn das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Belange des Patienten oder der Patientin erheblich überwiegt (§ 7 Abs. 2 S. 1 BremKHDSG). Außerdem darf der Zweck der Forschung nicht auf andere Weise oder nur mit unverhältnismäßigem Aufwand erreicht werden. So formuliert es auch § 13 Abs. 1 LDSG SH. Das Gesundheitsdatenschutzgesetz NRW normiert neben diesen beiden Voraussetzungen in § 16 Abs. 2 S. 2 Nr. 3 GDSG NW die Unzumutbarkeit der Einholung der Einwilligung aufgrund **des Gesundheitszustands des Patienten**. Auch § 37 Abs. 2 LKHG M-V normiert, dass Patientendaten für im öffentlichen Interesse liegende Forschungsvorhaben verarbeitet werden dürfen, allerdings nur unter zwei Voraussetzungen: Die schutzwürdigen Belange der Patientinnen und Patienten dürfen nicht beeinträchtigt werden und das für das Krankenhaus zuständige **Ministerium hat festgestellt**, dass das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Belange der Patientinnen und Patienten erheblich überwiegt.

### (5) Anonymisierte Daten

Die Verarbeitung anonymer Daten fällt mangels Personenbezug nicht in den Anwendungsbereich der Datenschutzgesetze. Gleichwohl wird die Möglichkeit der Verarbeitung anonymisierter Daten von einigen Landeskrankenhausgesetzen explizit erwähnt. § 25 Abs. 1 Nr. 4 BlnLKG etwa erlaubt die Verarbeitung von im Rahmen der Krankenhausbehandlung erhobenen und gespeicherten Patientendaten, wenn diese **vor der weiteren Verarbeitung anonymisiert** werden. Gleiches gilt gemäß § 37 Abs. 1 Nr. 3 LKG für Krankenhäuser in Rheinland-Pfalz und gemäß § 17 Abs. 1 Nr. 1 KHG LSA für Krankenhäuser in Sachsen-Anhalt.

### (6) Genehmigung der Aufsichtsbehörde

In Thüringer Krankenhäusern dürfen Patientendaten ohne Einwilligung des Patienten verarbeitet werden, wenn kumulativ die folgenden drei in § 27a Abs. 2 ThürKHG normierten Voraussetzungen vorliegen:

- Schutzwürdige Belange des Patienten werden nicht beeinträchtigt,
- die für das Krankenhaus zuständige Aufsichtsbehörde hat festgestellt, dass das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Belange des Patienten erheblich überwiegt und

- der Zweck des Forschungsvorhabens kann auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden.

### cc) Datenübermittlung

#### aaa) Im Eigeninteresse des Krankenhauses

Krankenhäuser, die in den Geltungsbereich des Landeskrankenhausgesetzes Baden-Württemberg fallen, dürfen Patientendaten gemäß § 46 Abs. 1 Nr. 2a LKHG BW **an Stellen außerhalb des Krankenhauses** übermitteln, soweit dies erforderlich ist zur Durchführung medizinischer Forschungsvorhaben des Krankenhauses und sofern der Zweck nicht mit anonymisierten Daten erreicht werden kann und nicht überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen.

#### bbb) Zu Behandlungszwecken

Gemäß Art. 27 Abs. 5 BayKHG ist die **Übermittlung von Patientendaten an Dritte** zulässig im Rahmen des Behandlungsverhältnisses oder dessen verwaltungsmäßiger Abwicklung.

#### ccc) Zu Forschungszwecken

Die Übermittlung von Patientendaten **an Personen und Stellen außerhalb des Krankenhauses** ist in Bremen gem. § 4 Abs. 1 Nr. 6 BremKHDSG nach Maßgabe von § 7 BremKHDSG zulässig, soweit dies zu Forschungszwecken erforderlich ist. Aus Absatz 2 ergeben sich folgende Vorgaben:

1. Schutzwürdige Belange des Patienten (insb. wegen der Art der Daten, wegen ihrer Offenkundigkeit oder wegen der Art der Verarbeitung) werden nicht beeinträchtigt **oder**
2. das öffentliche Interesse an der Durchführung des Forschungsvorhabens überwiegt die schutzwürdigen Belange des Patienten erheblich **und**
3. der Zweck der Forschung kann auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden **und**
4. Aufzeichnung von
    - empfangender Stelle,
    - Art der zu übermittelnden Daten,
    - Kreis der betroffenen Patienten,
    - das von der empfangenden Stelle genannte Forschungsvorhaben und
    - Vorliegen von Punkt 1. bis 3.

    durch das übermittelnde Krankenhaus **und**
5. Beteiligung des Datenschutzbeauftragten des Krankenhauses.

Die empfangende Stelle muss sich nach § 4 Abs. 2 und 3 BremKHDSG außerdem zur Geheimhaltung verpflichten. Gemäß § 6 Abs. 6 GDSG NW muss sich die empfangende Stelle noch umfangreicher verpflichten. Folgende Verpflichtungen müssen schriftlich eingegangen werden:

- Verwendung der Daten nur für das von dem Dritten genannte Forschungsvorhaben.
- Pseudonymisierung oder Anonymisierung muss so früh wie möglich durchgeführt werden.
- Keine Möglichkeit der Identifizierbarkeit von Personen bei Veröffentlichung von Forschungsergebnissen.
- Gewährung von Einsicht gegenüber der für die übermittelnde Stelle zuständigen Datenschutzkontroll- oder Aufsichtsbehörde.

### ddd) Pseudonymisierte Daten

Das Berliner Krankenhausgesetz ermöglicht in § 25 Abs. 3 die Übermittlung pseudonymisierter Daten an einrichtungsübergreifende Forschungsvorhaben, Forschungsregister oder Probensammlungen. Die Norm erlaubt dabei die Übermittlung der nach § 25 Abs. 1 BlnLKG verarbeiteten Daten – also solcher Patientendaten, die rechtmäßig für krankenhausinterne Forschungsvorhaben im für das Forschungsvorhaben erforderlichen Umfang erhoben, gespeichert oder genutzt wurden.

### eee) Genehmigung durch eine Behörde

Nach § 31 S. 1 BbgKHEG bedarf die Offenlegung von Patientendaten an andere Stellen oder Personen für Forschungszwecke ohne Einwilligung der vorherigen Bestätigung der nach § 11 BbgKHEG zuständigen Rechtsaufsichtsbehörde, dass die Voraussetzungen für eine zulässige Datenübermittlung nach § 25 Abs. 1 S. 1 BbgDSG vorliegen.

### fff) Keine andere Möglichkeit der Zweckerreichung

§ 37 Abs. 3 LKG RP sieht vor, dass Patientendaten zu Forschungszwecken an Dritte übermittelt werden dürfen, wenn der Zweck eines Forschungsvorhabens **nicht auf andere Weise erfüllt werden kann** und die Einholung der Einwilligung nicht zumutbar ist und schutzwürdige Belange der Patientin oder des Patienten nicht beeinträchtigt werden und das berechtigte Interesse der Allgemeinheit an der Durchführung des Forschungsvorhabens das Geheimhaltungsinteresse des Patienten erheblich überwiegt. Die übermittelnde Stelle muss außerdem aufzeichnen, an wen sie Daten übermittelt, welche Daten übermittelt werden, welche Patienten von der Übermittlung betroffen sind und für welches Forschungsvorhaben die Daten übermittelt werden. Einen ähnlichen Regelungsgehalt hat § 17 Abs. 2 KHG LSA, der zusätzlich zur **Unmöglichkeit der Zweckerreichung** eines bestimmten Forschungsvorhabens die Unzumutbarkeit der Einholung der Einwilligung sowie die Zustimmung der zuständigen Behörde fordert. Die Zustimmung darf nach § 17 Abs. 2 S. 3 SächsKHG nur erteilt werden, wenn das berechtigte Interesse der Allgemeinheit an der Durchführung des Forschungsvorhabens das Geheimhaltungsinteresse des Patienten erheblich überwiegt.

#### ggg) Interesse der Allgemeinheit überwiegt

Saarländische Krankenhäuser dürfen Patientendaten gemäß § 24 Abs. 2 S. 2 SKHG an andere Stellen für bestimmte Forschungsvorhaben weitergeben, wenn das Interesse der Allgemeinheit an der Durchführung des Forschungsvorhabens das Geheimhaltungsinteresse des Patienten erheblich überwiegt, die Einholung der Einwilligung dem Patienten nicht zugemutet werden kann und seine schutzwürdigen Belange nicht beeinträchtigt werden.

### b) Auftragsverarbeitung

Die Zulässigkeit Auftragsverarbeitung für Krankenhäuser wird in den Landeskrankenhausgesetzen an sehr unterschiedliche Bedingungen geknüpft.

Nach § 24 Abs. 7 BlnLKG dürfen Patientendaten grundsätzlich nur im Auftrag **durch ein anderes Krankenhaus** verarbeitet werden. Etwas anderes gilt nur dann, wenn der Auftragnehmer keine Möglichkeit hat, beim Zugriff auf Patientendaten den Personenbezug herzustellen, was durch technische Schutzmaßnahmen sichergestellt werden muss.

Eine Auftragsverarbeitung für Bremer Krankenhäuser ist nach Maßgabe des § 10 Abs. 1 BremKHDSG nur zulässig, wenn die Wahrung der Datenschutzbestimmungen dieses Gesetzes bei der verarbeitenden Stelle sichergestellt ist und diese sich insoweit der **Kontrolle des Landesbeauftragten für den Datenschutz unterwirft**. Auch in Sachsen ist die Mitwirkung der zuständigen Behörde erforderlich. Die Auftragserteilung bedarf nach § 33 Abs. 8 SächsKHG der **Zustimmung** zuständigen Behörde. Verantwortliche, die in den Anwendungsbereich des Thüringischen Krankenhausgesetzes fallen, haben demgegenüber **Berichtspflichten gegenüber dem Landesverwaltungsamt**. Gemäß § 27b Abs. 1 Nr. 3 ThürKHG muss der Verantwortliche rechtzeitig vor Auftragserteilung Art, Umfang und die technischen und organisatorischen Maßnahmen der beabsichtigten Datenverarbeitung im Auftrag **schriftlich anzeigen**, da die Auftragsverarbeitung anderenfalls unzulässig ist. Zusätzlich müssen die Voraussetzungen des § 27b Abs. 1 Nr. 1 und 2 ThürKHG erfüllt sein.

Derweil dürfen Verantwortliche in Mecklenburg-Vorpommern und im Saarland die Verarbeitung von personenbezogenen Patientendaten einem Auftragnehmer gemäß § 38 Abs. 1 LKHG M-V bzw. § 13a Abs. 1 SKHG nur übertragen, wenn eine der folgenden Voraussetzungen vorliegt:

- Störungen im Betriebsablauf können sonst nicht vermieden werden.
- Die Datenverarbeitung kann dadurch erheblich kostengünstiger gestaltete werden.
- Das Krankenhaus stellt seinen Betrieb ein.

Die Vorgaben im Hinblick auf die Auftragsverarbeitung weichen daher nicht nur untereinander erheblich voneinander ab, sondern auch von der europarechtlichen Bestimmung des Art. 28 DS-GVO. Insbesondere Vorschriften, die wie § 24 Abs. 7 BlnLKG eine Ungleichbehandlung von unterschiedlichen Auftragnehmern vorsehen und die Auftragsverarbeitung, die nicht durch ein Krankenhaus erfolgt, an zusätzliche Bedingungen knüpfen, sind aus unserer Sicht **europarechtswidrig**. Das Landeskrankenhausgesetz Berlin erlaubt die Datenverarbeitung im Auftrag durch eine Stelle, die nicht Krankenhaus ist, nur dann, wenn der Auftragnehmer keine Möglichkeit hat, beim Zugriff auf Patientendaten den Personenbezug herzustellen. Im Übrigen sind gleichwohl die allgemeinen Anforderungen an die Auftragsverarbeitung zu beachten.[126] Das bedeutet, dass Datenschutzvorschriften zu beachten sind, obwohl der Auftragnehmer ohnehin keinen Personenbezug herstellen können darf. Dieser Regelungsansatz steht im Widerspruch zu europäischem Datenschutzrecht.[127] Zum einen besteht keine Notwendigkeit, Datenschutzgesetze anzuwenden, wenn keine personenbezogenen Daten verarbeitet werden und zum anderen unterscheidet die Datenschutz-Grundverordnung gerade nicht zwischen der Verarbeitung von „normalen“ personenbezogenen Daten im Auftrag und der Verarbeitung von Gesundheitsdaten im Auftrag. Es gibt zwar strengere Anforderungen an die Zulässigkeit der Verarbeitung von Gesundheitsdaten und auch an anderen Stellen höhere Anforderungen bei der Verarbeitung von Gesundheitsdaten, die aber nicht das Instrument der Auftragsverarbeitung betreffen. Mangels einer europarechtlichen Öffnungsklausel **hat der nationale Gesetzgeber** (und auch nicht der Landesgesetzgeber) hier aber **keinen Handlungsspielraum**, der den Erlass einer abweichenden Regelung legitimieren würde.

Die Berliner Datenschutzbeauftragte hielt § 24 Abs. 7 BlnLKG für uneingeschränkt anwendbar, räumte aber ein, dass nach einer Änderung des § 203 StGB, die Vorgabe, dass Auftragsverarbeitung nur durch ein anderes Krankenhaus durchgeführt werden darf, nicht mehr tragbar sei. Da der § 203 StGB nunmehr geändert wurde und die Verarbeitung im Auftrag von Berufsgeheimnisträgern gerade ermöglicht werden sollte, ist das Berliner Landeskrankenhausgesetz nicht nur europarechtswidrig, sondern auch im **Dissens mit nationalem Recht**.

Aus diesen Gründen kann § 24 Abs. 7 BlnLKG daher nicht mehr angewendet werden, die Norm verstößt gegen das Europarecht und spiegelt nicht die gesetzgeberische Absicht des Bundesgesetzgebers in Deutschland wieder. Stattdessen muss in diesen Fällen Art. 28 DS-GVO angewendet werden.[128] Die Unionsrechtswidrigkeit von landeskrankenhausrechtlichen Normen führt zu einer zusätzlichen Rechtsunsicherheit.

---

126 § 24 Abs. 7 BlnLKG verweist auf § 11 BDSG a.F., was nunmehr als Verweis auf Art. 28 DS-GVO verstanden werden muss.

127 Sosna, Daten- und Geheimnisschutz bei Outsourcing-Projekten im Krankenhausbereich, 1. Aufl. 2015, S. 186.

128 So in Bezug auf die Datenschutz-Richtlinie auch Sosna, Daten- und Geheimnisschutz bei Outsourcing-Projekten im Krankenhausbereich, 1. Aufl. 2015, S. 187.

### c) Genehmigungserfordernisse

Das Thüringische Krankenhausgesetz stellt die Erlaubnis der Verarbeitung und Nutzung von Patientendaten ohne Einwilligung unter den **Vorbehalt der Feststellung der für das Krankenhaus zuständigen obersten Aufsichtsbehörde,**[129] dass das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Belange des Patienten erheblich überwiegt und der Zweck des Forschungsvorhabens auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

### d) Offenbarungsbefugnisse

Neben den datenschutzrechtlichen Befugnisnormen enthalten einige Landeskrankenhausgesetze Offenbarungsbefugnisse im Sinne des § 203 StGB. Das gilt etwa für Bestimmungen in bereichsspezifischen Gesetzen, die explizit die Auftragsdatenverarbeitung von im Krankenaus anfallenden Patientendaten regeln.[130] Der Landesgesetzgeber begründet dies mit dem Interesse der betroffenen Patienten an einer kostengünstigen und effektiven Dokumentation. Unter den Voraussetzungen der im Landeskrankenhausgesetz Mecklenburg-Vorpommern näher geregelten Sicherungen sei es daher gerechtfertigt, auf die sonst erforderlich werdende Einwilligung jedes einzelnen Patienten zu verzichten. Der Landesdatenschutzbeauftragte Mecklenburg-Vorpommern formuliert es wie folgt:

> *„Die in der Datenübermittlung liegende Offenbarung der Daten erfolgt bei Einhaltung dieser Voraussetzungen dann ‚befugt' im Sinne von § 203 Abs. 1 StGB."*[131]

In Bundesländern ohne bereichsspezifische Erlaubnisnorm kann eine Auftragsbearbeitung von Patientendaten hingegen nur nach Einholung einer Schweigepflichtentbindungserklärung durchgeführt werden.

### e) Zwischenergebnis

Die bereichsspezifischen Datenschutzvorschriften weichen von Land zu Land ganz erheblich voneinander ab. Sowohl die Ersterhebung von personenbezogenen Daten zu Forschungszwecken als auch die Sekundärnutzung bereits vorhandener Daten unterliegen divergierenden Vorgaben. Für länderübergreifende Forschungsvorhaben bedeutet das, dass sich die **Schnittmenge zulässiger Datenverarbeitungen verringert**. Hinzu kommt eine nicht unerhebliche **Rechtsunsicherheit** in Bezug auf die mögliche Unionsrechtswidrigkeit des Landesrechts.

---

[129] Nach § 32 Abs. 1 ThürKHG ist das für das Krankenhauswesen zuständige Ministerium zuständige Landesbehörde.
[130] Conrad/Strittmatter, in: Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, 2. Aufl. 2016, § 22, Rn. 198.
[131] Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern, Datenschutz im Krankenhaus, 2011, S. 35.

## II. Analyse des Bundesrechts

Auf Bundesebene ist die Verarbeitung von personenbezogenen Daten im Gesundheitsbereich trotz Geltung der Datenschutz-Grundverordnung nach wie vor in sehr unterschiedlichen Gesetzen geregelt und damit höchst komplex.[132] Dies gilt insbesondere auch für die Verarbeitung personenbezogener Daten zu Forschungszwecken. Ursächlich hierfür sind die unterschiedlichen Akteure, die verteilten Gesetzgebungskompetenzen sowie der divergierende Schutzbedarf.[133]

### 1. Bundesdatenschutzgesetz (BDSG)

Allgemeine Vorschriften zum Umgang mit personenbezogenen Daten in der Bundesrepublik Deutschland finden sich in dem Bundesdatenschutzgesetz (BDSG)

#### a) Anwendungsbereich

Das Bundesdatenschutzgesetz (BDSG) gilt für die Verarbeitung personenbezogener Daten durch **öffentliche Stellen des Bundes** (§ 1 Abs. 1 S. 1 Nr. 1 BDSG). Für öffentliche Stellen der Länder gilt es, soweit der Datenschutz nicht durch Landesgesetz geregelt ist und soweit sie Bundesrecht ausführen (§ 1 Abs. 1 S. 1 Nr. 2 a) BDSG) oder als Organe der Rechtspflege tätig werden, und es sich nicht um Verwaltungsangelegenheiten handelt (§ 1 Abs. 1 S. 1 Nr. 2 b) BDSG). Für **nichtöffentliche Stellen** gilt das Bundesdatenschutzgesetz (BDSG) für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie die nicht automatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen, es sei denn, die Verarbeitung durch natürliche Personen erfolgt zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten (§ 1 Abs. 1 S. 2 BDSG). Die Regelungen in § 1 BDSG gelten „einheitlich für das gesamte BDSG“.[134]

An der Gesundheitsforschung in der Bundesrepublik Deutschland beteiligen sich auch öffentliche Stellen des Bundes sowie nicht-öffentliche Stellen. Hierzu gehören beispielsweise Krankenhäuser, deren Träger ein Privatrechtssubjekt oder der Bund ist.[135] Für diese kann das BDSG zur Anwendung kommen.

#### b) Verhältnis zu anderen Vorschriften und Gesetzen

Das Verhältnis der Regelungen des Bundesdatenschutzgesetzes (BDSG) zu anderen Vorschriften und Gesetzen, die für die Verarbeitung personenbezogener Daten im Rahmen der Gesundheitsforschung relevant sind, ist in § 1 Abs. 2 BDSG und § 1 Abs. 5 BDSG normiert.

---

[132] Ähnlich: Paschke, in: Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, Teil B, § 13, Rn. 1, 18.
[133] Paschke, in: Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, Teil B, § 13, Rn. 1.
[134] Klar, in: Kühling/Buchner, DS-GVO BDSG, 2. Auflage, 2018, § 1, Rn. 2.
[135] Einzelheiten zum „Datenumgang im Krankenhaus“, siehe bei: Paschke, in: Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, 1. Auflage 2019, Teil B, § 13, Rn. .10, 34 f..

Gemäß § 1 Abs. 2 S. 1 BDSG gehen andere Rechtsvorschriften des Bundes über den Datenschutz den Vorschriften des BDSG vor. Regeln diese Rechtsvorschriften einen Sachverhalt, für den dieses Gesetz gilt, nicht oder nicht abschließend, finden die Vorschriften des BDSG Anwendung (§ 1 Abs. 2 S. 2 BDSG). Rechtsvorschriften können sowohl formelle als auch materielle Gesetze sein.[136] Hierzu gehören auch Rechtsverordnungen und Satzungen der bundesunmittelbaren Körperschaften, Anstalten und Stiftungen.[137] Damit kommt dem BDSG gegenüber bereichsspezifischen Datenschutzvorschriften eine „Auffangfunktion" zu.[138]

Für den Gesundheitsbereich weist die gesetzliche Schweigepflicht eine besondere Relevanz auf (vgl. insbesondere § 203 StGB). Die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, bleibt von den Vorschriften des BDSG unberührt (§ 1 Abs. 2 S. 3 BDSG).

§ 1 Abs. 5 BDSG stellt das Verhältnis zur DS-GVO klar. Die Vorschriften dieses Gesetzes finden keine Anwendung, soweit das Recht der Europäischen Union, im Besonderen die Verordnung (EU) 2016/679 in der jeweils geltenden Fassung, unmittelbar gilt (§ 1 Abs. 5 BDSG).

### c) Rechtmäßigkeit der Verarbeitung personenbezogener Daten zu Forschungszwecken

Aufgrund der unmittelbaren Wirkung der Datenschutz-Grundverordnung (DS-GVO) finden sich im BDSG in Bezug auf die DS-GVO in erster Linie Anpassungsvorschriften.[139] § 22 BDSG und § 27 BDSG weisen eine besondere Bedeutung für die rechtmäßige Verarbeitung personenbezogener Daten im Rahmen der **Gesundheitsforschung** auf.

§ 22 Abs. 1 BDSG enthält eine Regelung zur Zulässigkeit der Verarbeitung besonderer Kategorien personenbezogener Daten. Zu den besonderen Kategorien personenbezogener Daten gehören gemäß Art. 9 Abs. 1 i.V.m. Art. 4 Nr. 15 DS-GVO auch **Gesundheitsdaten**.

§ 27 BDSG bezieht sich auf die Datenverarbeitung zu **wissenschaftlichen** oder historischen **Forschungszwecken** und zu statistischen Zwecken. § 27 Abs. 1 S. 1 BDSG regelt die Zulässigkeit der Verarbeitung zu solchen Zwecken.

---

136 Klar, in: Kühling/Buchner, DS-GVO BDSG, 2. Auflage, 2018, § 1, Rn. 14.
137 Ebenda.
138 Ebenda.
139 Vgl. Kühling/Raab, in: Kühling/Buchner, DS-GVO BDSG, 2. Auflage 2018, Rn. 127 ff..

### aa) Besondere Anforderungen an die Einwilligung

Das BDSG enthält keine besonderen Anforderungen an die Einwilligung im Zusammenhang mit der Gesundheitsforschung. Besondere Regelungen zur Einwilligung finden sich lediglich im Beschäftigungskontext (§ 26 Abs. 2, 3 BDSG).

§ 46 Nr. 17 BDSG sowie § 51 BDSG befinden sich in Teil 3 des BDSG und gehören damit zu den Bestimmungen für Verarbeitungen zu Zwecken gemäß Artikel 1 Absatz 1 der Richtlinie (EU) 2016/680.[140] Für die Forschung im Gesundheitswesen haben sie kaum Relevanz.

### bb) Gesetzliche Erlaubnistatbestände

§ 27 BDSG regelt die Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken. Die Vorschrift stützt sich auf Art. 9 Abs. 2 lit. j und Art. 89 Abs. 2 DS-GVO.[141] Sie gilt für die öffentliche und private Forschung sowohl durch öffentliche als auch nichtöffentliche Stellen.[142]

Abweichend von Art. 9 Abs. 1 DS-GVO ist die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 DS-GVO auch ohne Einwilligung für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke zulässig, 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 (§ 27 Abs. 1 S. 1 BDSG). Der Verantwortliche sieht angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person gemäß § 22 Abs. 2 Satz 2 BDSG vor (§ 27 Abs. 1 S. 2 BDSG). Der Begriff der „wissenschaftlichen Forschung“ sei weit auszulegen.[143]

§ 22 BDSG regelt die Verarbeitung besonderer Kategorien personenbezogener Daten.

### cc) Übermittlung personenbezogener Daten im Rahmen der Gesundheitsforschung

Der in § 22 Abs. 1 und § 27 Abs. 1 S. 1 BDSG verwendete Begriff der „Verarbeitung“ umfasst auch die Übermittlung (vgl. Art. 4 Nr. 2 DS-GVO).

---

[140] Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates

[141] So auch: Buchner/Tinnefeld, in: Kühling/Buchner, DS-GVO BDSG, 2. Auflage 2018, BDSG, § 27, Rn. 1.

[142] Gesetzesbegründung, Drucksache 18/11325, S. 99.

[143] Buchner/Tinnefeld, in: Kühling/Buchner, DS-GVO BDSG, 2. Auflage 2018, BDSG, § 27, Rn. 5.

#### dd) Auftragsverarbeitung im Rahmen der Gesundheitsforschung

Auftragsverarbeiter werden nach § 22 Abs. 2 S. 2 Nr. 5 BDSG in die Maßnahmen zur Wahrung der Interessen der betroffenen Person (§ 22 Abs. 2 BDSG) einbezogen.

### d) Genehmigungserfordernisse

§ 22 BDSG und § 27 BDSG enthalten keine expliziten Genehmigungserfordernisse im Hinblick auf Forschungsvorhaben im Gesundheitswesen.

## 2. Arzneimittelgesetz

Das Gesetz über den Verkehr mit Arzneimitteln (AMG) regelt die „wesentlichen gesetzlichen Rahmenbedingungen für Arzneimittel“ in der Bundesrepublik Deutschland.[144] Kernziele des Arzneimittelrechts sind sowohl der Verbraucherschutz als auch die Arzneimittelsicherheit.[145] Zweck des AMG ist, im Interesse einer ordnungsgemäßen Arzneimittelversorgung von Mensch und Tier für die Sicherheit im Verkehr mit Arzneimitteln, insbesondere für die Qualität, Wirksamkeit und Unbedenklichkeit der Arzneimittel nach Maßgabe der Vorschriften des Arzneimittelgesetzes zu sorgen (§ 1 AMG). Im AMG finden sich unter anderem bereichsspezifische Datenschutzvorschriften für die Verarbeitung personenbezogener Daten im Rahmen von klinischen Prüfungen.

Durch die Geltung der DS-GVO bestand hinsichtlich der Regelungen im AMG zur Verarbeitung personenbezogener Daten Änderungs- und Anpassungsbedarf. Aus diesem Grund erfolgen mit dem zweiten Datenschutzanpassungs- und Umsetzungsgesetz EU (2. DSAnpUG-EU) Anpassungen des AMG an die DS-GVO.

Neben der Datenschutz-Grundverordnung wurde auf Ebene der EU zudem die Verordnung über klinische Prüfungen mit Humanarzneimitteln verabschiedet („Clinical Trials Regulation – CTR“).[146] Geltung erlangt die Verordnung in zeitlicher Hinsicht sechs Monate nachdem die Kommission eine Mitteilung über die Funktionsfähigkeit des EU-Portals und der EU-Datenbank veröffentlicht hat (Art. 99 VO (EU)).

### a) Anwendungsbereich

Der Anwendungsbereich des AMG bezieht sich auf Arzneimittel.[147] Der Begriff „Arzneimittel“ wird in § 2 AMG definiert.

---

144 Meier, in: Meier/von Czettritz/Gabriel/Kaufmann, Pharmarecht, 2. Auflage 2018, § 2, Rn. 1.
145 Ulsenheimer, in: Laufs/Kern, Handbuch des Arztrechts, 5. Auflage 2019, § 136, Rn. 1.
146 Verordnung (EU) Nr. 536/2014 des europäischen Parlamentes und des Rates vom 16. April 2014 über klinische Prüfungen mit Humanarzneimitteln und zur Aufhebung der Richtlinie 2001/20/EG.
147 Vgl. Meier, in: Meier/von Czettritz/Gabriel/Kaufmann, Pharmarecht, 2. Auflage 2018, § 2, Rn. 7.

§ 4a AMG enthält Ausnahmen vom Anwendungsbereich. Diese haben jedoch für die Forschung am Menschen eine geringe Relevanz.[148]

Vorschriften zum Umgang mit personenbezogenen Daten im Kontext der Forschung im Gesundheitswesen, existieren im AMG insbesondere im Zusammenhang mit klinischen Prüfungen.[149] So enthält der sechste Abschnitt des AMG Vorschriften zum Schutz des Menschen bei der klinischen Prüfung. Klinische Prüfung bei Menschen ist jede am Menschen durchgeführte Untersuchung, die dazu bestimmt ist, klinische oder pharmakologische Wirkungen von Arzneimitteln zu erforschen oder nachzuweisen oder Nebenwirkungen festzustellen oder die Resorption, die Verteilung, den Stoffwechsel oder die Ausscheidung zu untersuchen, mit dem Ziel, sich von der Unbedenklichkeit oder Wirksamkeit der Arzneimittel zu überzeugen (§ 4 Abs. 23 S. 1 AMG)[150]. § 40 AMG legt allgemeine Voraussetzungen der klinischen Prüfung fest. Hierzu gehört auch der Schutz personenbezogener Daten, da klinische Prüfungen i.d.R. mit der Verarbeitung von personenbezogenen Daten verbunden sind.

### b) Verhältnis zu anderen Vorschriften und Gesetzen

Im deutschen Recht ist das Verhältnis zwischen den Datenschutzvorschriften im AMG und BDSG klar geregelt. Soweit das AMG den Umgang mit personenbezogenen Daten regelt, gehen diese Regelungen denen des BDSG vor (vgl. § 1 Abs. 2 S. 1 § BDSG).

Auf europäischer Ebene existiert keine explizite Kollisionsnorm. Der Europäische Datenschutzausschuss (European Data Protection Board – EDPB) hat eine Stellungnahme zu dem Zusammenspiel der Verordnung über klinische Prüfungen und der DS-GVO angenommen.[151]

> *„Während die DSGVO den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und harmonisierte Vorschriften für den freien Verkehr solcher Daten gewährleistet, zielt die Verordnung über klinische Prüfungen auf eine stärkere Harmonisierung der Bestimmungen für die Durchführung klinischer Prüfungen in der EU ab."*[152]

---

[148] Nach § 2 S. 1 Nr. 3 AMG findet das AMG keine Anwendung auf Gewebe, die innerhalb eines Behandlungsvorgangs einer Person entnommen werden, um auf diese ohne Änderung ihrer stofflichen Beschaffenheit rückübertragen zu werden.

[149] Der Begriff „klinische Prüfung" wird in § 4 Abs. 23 AMG definiert. Der Begriff „klinische Studie" ist in Art. 2 Abs. 2 Nr. 1 VO (EU) 536/2014 definiert.

[150] Siehe auch § 4 Abs. 23 S. 2 und 3 AMG.

[151] EDPB, Stellungnahme 3/2019 zu den Fragen und Antworten zum Zusammenspiel der Verordnung über klinische Prüfungen und der Datenschutz-Grundverordnung (DSGVO), angenommen am 23. Januar 2019.

[152] EDPB, Stellungnahme 3/2019 zu den Fragen und Antworten zum Zusammenspiel der Verordnung über klinische Prüfungen und der Datenschutz-Grundverordnung (DSGVO), angenommen am 23. Januar 2019, S. 3.

### c) Rechtmäßigkeit der Verarbeitung personenbezogener Daten zu Forschungszwecken

§ 40 Abs. 1 S. 3 Nr. 3 AMG regelt im Zusammenhang mit klinischen Prüfungen die Einwilligung und Aufklärung der betroffenen Person. Die Erhebung und Verwendung personenbezogener Daten ist umfasst.[153]

#### aa) Rechtsgrundlage der Datenverarbeitung

§ 40 AMG legt allgemeine Voraussetzungen der klinischen Prüfung fest. Dabei wird ein Bezug zum Umgang mit personenbezogenen Daten hergestellt. Nach § 40 Abs. 1 S. 3 Nr. 3 b) und c) AMG darf die klinische Prüfung eines Arzneimittels bei Menschen nur durchgeführt werden, wenn und solange die betroffene Person nach § 40 Abs. 2 S. 1 AMG aufgeklärt worden ist und gemäß § 40 Abs. 1 S. 3 Nr. 3 lit. b AMG schriftlich in die Teilnahme an der klinischen Prüfung eingewilligt hat, soweit in § 40 Abs. 4 oder in § 41 AMG nichts Abweichendes bestimmt ist sowie nach § 40 Abs. 2a S. 1 und 2 AMG informiert worden ist und schriftlich [oder elektronisch][154] in die mit der klinischen Prüfung verbundene Verarbeitung personenbezogener Daten eingewilligt hat. Die Einwilligung muss sich ausdrücklich auch auf die [Erhebung und][155] Verarbeitung von Angaben über die Gesundheit beziehen (§ 40 Abs. 1 S. 3 Nr. 3 c) AMG).[156]

Rechtsgrundlage für die Verarbeitung personenbezogener Daten in der klinischen Prüfung ist damit nach geltendem Recht die Einwilligung der betroffenen Person. Für die Zukunft gibt es Bestrebungen, etwa von Seiten der Generaldirektion Gesundheit und Lebensmittelsicherheit der Europäischen Kommission, die Verarbeitung personenbezogener Daten mit Geltungsbeginn der Verordnung (EU) 536/2014 nicht mehr auf die Einwilligung, sondern auf eine gesetzliche Erlaubnis zu stützen. Dies liegt darin begründet, dass die Widerruflichkeit der Einwilligung eines Einzelnen dazu führen kann, dass das Studienprotokoll nicht mehr einzuhalten ist und Forschungshypothesen nicht mehr mit ausreichender Signifikanz bewiesen werden können. Wenn also in Zukunft die Verarbeitung personenbezogener Daten in klinischen Studien auf eine gesetzliche Verpflichtung gestützt wird, bringt dies mehr Rechtssicherheit für die an der klinischen Studie Beteiligten.

---

153 Listl-Nörr, in: Spickhoff, Medizinrecht, 3. Auflage 2018, AMG, § 40, Rn. 32.

154 Wird ersetzt durch die §§ 40 - 40d aufgrund des Artikel 2 des Vierten Gesetzes zur Änderungen arzneimittelrechtlicher und anderer Vorschriften.

155 Wird geändert durch Artikel 18 des Zweiten Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680, Gesetzentwurf der BReg vom 01.10.2018.

156 Kann die betroffene Person nicht schreiben, so kann in Ausnahmefällen statt der in § 40 Abs. 1 S. 3 Nr. 3 b) und c) AMG geforderten schriftlichen Einwilligung eine mündliche Einwilligung in Anwesenheit von mindestens einem Zeugen, der auch bei der Information der betroffenen Person einbezogen war, erteilt werden (§ 40 Abs. 1 S: 4 AMG). Der Zeuge darf keine bei der Prüfstelle beschäftigte Person und kein Mitglied der Prüfgruppe sein (§ 40 Abs. 1 S: 5 AMG). Die mündlich erklärte Einwilligung ist schriftlich zu dokumentieren, zu datieren und von dem Zeugen zu unterschreiben (§ 40 Abs. 1 S: 6 AMG).

## 3. Gendiagnostikgesetz (GenDG)

Der Verarbeitung von genetischen Gesundheitsdaten kommt im Rahmen der Gesundheitsversorgung und -forschung eine hohe Bedeutung zu.[157] Ziel des Gendiagnostikgesetzes ist es, „die mit der Untersuchung menschlicher genetischer Eigenschaften verbundenen möglichen Gefahren von genetischer Diskriminierung zu verhindern und gleichzeitig die Chancen des Einsatzes genetischer Untersuchungen für den einzelnen Menschen zu wahren."[158]„Mit dem Gesetz sollen Anforderungen an eine gute genetische Untersuchungspraxis verbindlich gemacht werden."[159] Das Gendiagnostikgesetz räumt „dem Recht auf informationelle Selbstbestimmung des Patienten einen hohen Stellenwert ein".[160]

Das Gendiagnostikgesetz gilt für genetische Untersuchungen und im Rahmen genetischer Untersuchungen durchgeführte genetische Analysen bei geborenen Menschen sowie bei Embryonen und Föten während der Schwangerschaft und den Umgang mit dabei gewonnenen genetischen Proben und genetischen Daten bei genetischen Untersuchungen zu medizinischen Zwecken, zur Klärung der Abstammung sowie im Versicherungsbereich und im Arbeitsleben (§ 2 GenDG). Nach § 2 Abs. 2 Nr. 1 GenDG gilt das Gendiagnostikgesetz allerdings nicht für genetische Untersuchungen und Analysen und den Umgang mit genetischen Proben und Daten zu Forschungszwecken. Der Begriff der Forschung ist weit zu verstehen, sodass auch klinische Prüfungen vom Anwendungsbereich des Gendiagnostikgesetzes ausgenommen sind.[161] Soweit das Gendiagnostikgesetz keine Anwendung findet, sind die allgemeinen Datenschutzvorschriften auf die Verarbeitung personenbezogener Daten anwendbar.[162] Insofern ist auf die Regelungen zum Schutz besonderer Kategorien personenbezogener Daten der DS-GVO und – in Abhängigkeit von dem jeweiligen Verantwortlichen – des BDSG sowie der landesrechtlichen Regelungen zurückzugreifen.

## 4. Medizinproduktegesetz

Zweck des Medizinproduktegesetzes ist gemäß § 1 MPG, den Verkehr mit Produkten zu regeln und dadurch für die Sicherheit, Eignung und Leistung der Medizinprodukte sowie die Gesundheit und den erforderlichen Schutz der Patienten, Anwender und Dritter zu sorgen. Dadurch sollen insbesondere die Ziele eines freien Warenverkehrs einerseits und die Gewährleistung der Produktsicherheit anderseits erreicht werden.[163]

---

[157] Zur Bedeutung für die individualisierte und personalisierte Medizin: Gräfin von Hardenberg, in: ZD 2014, 115, 115; Paschke, in: Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, 1. Auflage 2019, Teil B, § 13, Rn. 11.

[158] Deutscher Bundestag, Gesetzesentwurf der Bundesregierung, Drucksache 16/10532, S. 1.

[159] Ebenda.

[160] von Hardenberg, in: ZD 2014, 115, 116.

[161] Sosnitza/Op den Camp, in: MedR 2011, 401, 404.

[162] So auch: von Hardenberg, in: ZD 2014, 115, 117.

[163] Webel, in: Bergmann/Pauge/Steinmeyer, Gesamtes Medizinrecht, 3. Aufl. 2018, § 1 MPG, Rn. 1.

Das Medizinproduktegesetz gilt nach § 2 Abs. 1 MPG für Medizinprodukte und deren Zubehör. Zubehör wird als eigenständiges Medizinprodukt behandelt.

Rechtsgrundlage für die Verarbeitung personenbezogener Daten in klinischen Prüfungen von Medizinprodukten ist nach § 20 Abs. 1 S. 4 Nr. 2 MPG die Einwilligung der betroffenen Person. Die Person, bei der die klinische Prüfung durchgeführt werden soll, muss insofern erklären, dass sie mit der im Rahmen der klinischen Prüfung erfolgenden Aufzeichnung von Gesundheitsdaten und mit der Einsichtnahme zu Prüfungszwecken durch Beauftragte des Auftraggebers oder der zuständigen Behörde einverstanden ist.

Daneben gelten die Rechtsvorschriften über Geheimhaltung und Datenschutz, was § 2 Abs. 4 MPG explizit klarstellt, sodass sowohl die Datenschutz Grundverordnung als auch die allgemeinen und bereichsspezifischen nationalen Datenschutzvorschriften auf klinische Prüfungen von Medizinprodukten Anwendung finden.

## 5. Strahlenschutzgesetz und -verordnung

Das Strahlenschutzgesetz trifft Regelungen zum Schutz des Menschen und der Umwelt, sofern es um den langfristigen Schutz der menschlichen Gesundheit geht, vor der schädlichen Wirkung ionisierender Strahlung. Die Strahlenschutzverordnung hingegen enthält ergänzende Regelungen spezifischer und konkretisierender materieller Aspekte, um das Strahlenschutzgesetz vollzugsfähig zu machen.[164] Daten über berufliche Expositionen werden nach dem Strahlenschutzgesetz in einem beim Bundesamt für Strahlenschutz eingerichteten Strahlenschutzregister erfasst.

Die im Strahlenschutzregister gespeicherten personenbezogenen Daten dürfen gemäß § 170 Abs. 7 StrlSchG zu Forschungszwecken nach den Vorgaben des BDSG verarbeitet werden. Für eine Übermittlung der Daten an Dritte bedarf es grundsätzlich der Einwilligung der betroffenen Person, es sei denn, schutzwürdige Belange der betroffenen Person stehen der Übermittlung nicht entgegen oder wenn das öffentliche Interesse an der Forschungsarbeit das Geheimhaltungsinteresse der betroffenen Personen erheblich überwiegt.[165]

## 6. Sozialgesetzbücher (Erstes, fünftes und zehntes Sozialgesetzbuch)

Für Leistungsträger sowie die weiteren in § 35 Abs. 1 SGB aufgeführten Stellen findet bei der Erfüllung ihrer öffentlichen Aufgabe nach dem Sozialgesetzbuch das Rechtsregime des Sozialdatenschutzes gemäß § 35 Abs. 1 SGB I i.V.m. §§ 67 ff. SGB X Anwendung. Für die Gesetzliche Krankenversicherung sind die öffentlichen Aufgaben insbesondere im SGB V normiert. Während die Zulässigkeit der Verarbeitung von Sozialdaten in den §§ 67a ff. geregelt ist, ergibt sich die Zweckbindung aus den fachspezifischen Sozialgesetzbüchern. Ausgangspunkt des

[164] BR-Drs. 423/18, 1.
[165] § 170 Abs. 7 StrlSchG.

Sozialdatenschutzes ist das in § 35 Abs. 1 SGB I legaldefinierte Sozialgeheimnis, dessen Gegenstand der Schutz der Sozialdaten betroffener Personen ist. Ein personenbezogenes Datum kann nach § 67 Abs. 2 SGB X nur dann als Sozialdatum bezeichnet werden, wenn es durch einen Leistungsträger im Sinne des § 35 Abs. 1 SGB V verarbeitet wird. Leistungsträger sind die in den §§ 18 bis 29 SGB I genannten Körperschaften, Anstalten und Behörden, die für Sozialleistungen zuständig sind. Das Sozialdatenschutzrecht unterscheidet im Gegensatz zur DS-GVO und zu nationalen Datenschutzgesetzen nicht zwischen öffentlichen und nicht-öffentlichen Stellen, es gilt daher gleichermaßen für alle Sozialleistungsträger, unabhängig davon, ob sie Behörden des Bundes, eines Landes oder einer Kommune sind.[166]

Die Krankenkassen übernehmen die Abrechnung der Leistungen durch die Leistungsträger.[167] In Bezug auf diese Abrechnung sind Krankenkassen auf Informationen über Diagnosen und erbrachten Leistungen angewiesen.[168] Das SGB V eröffnet die Möglichkeit unter bestimmten Voraussetzungen mit diesen personenbezogenen Daten zu forschen. § 287 Abs. 1 SGB V etwa erlaubt den **Krankenkassen und den Kassenärztlichen Vereinigungen mit Erlaubnis der Aufsichtsbehörde die Datenbestände leistungserbringer- oder fallbeziehbar für zeitlich befristete und im Umfang begrenzte Forschungsvorhaben selbst auszuwerten**. Die Forschungszwecke werden vom Gesetzgeber vorgegeben, hierzu gehören die Gewinnung epidemiologischer Erkenntnisse, Erkenntnisse über Zusammenhänge zwischen Erkrankungen und Arbeitsbedingungen oder Erkenntnisse über örtliche Krankheitsschwerpunkte.

Das Sozialdatenschutzrecht ist als „**Vollregelung**“ konzipiert,[169] sodass das BDSG über keinen eigenen Anwendungsbereich verfügt – etwas anderes gilt ausnahmsweise dann, wenn das SGB als spezielle datenschutzrechtliche Regelung auf das BDSG verweist.[170] Auch für die Anwendbarkeit der Datenschutz-Grundverordnung verbleibt insofern kein Raum, als die Zulässigkeit der Datenverarbeitung in Frage steht.[171] Im Hinblick auf die **Landeskrankenhausgesetze** ergibt sich **keine Konkurrenz zum Sozialdatenschutzrecht**, da Adressaten der bereichsspezifischen Vorschriften für Krankenhäuser, die Leistungserbringer und nicht die Leistungsträger sind.

Im Hinblick auf Forschungsvorhaben, an denen beispielsweise ein Krankenhaus und eine gesetzliche Krankenkasse beteiligt sind, ergibt sich die Anwendbarkeit unterschiedlicher Normen zum Schutz personenbezogener Daten. Eine Harmonisierung der Vorschriften in diesem Verhältnis ist allerdings aus unserer Sicht nicht möglich und nicht erstrebenswert.

---

166 Kircher, Der Schutz personenbezogener Gesundheitsdaten im Gesundheitswesen, 1. Aufl. 2016, S. 2019.
167 Paschke, in: Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, 1. Auflage 2019, Teil B, § 13, Rn. 13.
168 Paschke, in: Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, 1. Auflage 2019, Teil B, § 13, Rn. 13.
169 Hoidn, in: Roßnagel, Das neue Datenschutzrecht, 1. Aufl. 2018, S. 300.
170 Kipker/Pollmann, in: Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, 1. Auflage 2019, Teil C, § 26, Rn. 3.
171 Kipker/Pollmann, in: Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, 1. Auflage 2019, Teil C, § 26, Rn. 34.

Das Bundessozialgericht hat in einem Urteil aus dem Jahr 2004 entschieden, dass auch bei der Vergütung von Pflegesätzen eine klare Trennung zwischen der normalen stationären Behandlung und der stationären Behandlung, bei der Arzneimittelstudien im Vordergrund stehen, vorzunehmen ist.[172]

Für die Zukunft plant die Bundesregierung die Einführung eines Forschungsdatenzentrums. Aus dem Kabinettsentwurf des Digitale-Versorgung-Gesetz (DVG)[173] geht hervor, dass eine bessere Nutzbarkeit von Gesundheitsdaten für Forschungszwecke ermöglicht werden soll. Bestehende gesetzliche Regelungen zur Datentransparenz im Kontext der Nutzung von Sozialdaten der Krankenkassen sollen erweitert und die Datenaufbereitungsstelle zu einem **Forschungsdatenzentrum** weiterentwickelt werden. Die Aufgaben des Forschungsdatenzentrums werden in § 303d SGB V n.F. konkretisiert. Hierzu gehören unter anderem die Aufbereitung der Daten für die Auswertung für in § 303e Abs. 2 SGB V n.F. normierte Zwecke (Abs. 1 Nr. 1), die Prüfung der Anträge auf Datennutzung (Abs. 1 Nr. 3), die Zurverfügungstellung der beantragten Daten an Nutzungsberechtigte (Abs. 1 Nr. 4), die Bewertung und unter Umständen die Minimierung des spezifischen Reidentifikationsrisikos in Bezug auf die durch Nutzungsberechtigte nach § 303e SGB V n.F. beantragten Daten sowie die Förderung der wissenschaftlichen Erschließung der Daten.

## 7. Strafgesetzbuch

§ 203 StGB stellt die unbefugte Offenbarung eines fremden Geheimnisses durch Ärzte (Abs. 1 Nr. 1) und durch Personen, die auf die gewissenhafte Erfüllung ihrer Geheimhaltungspflicht bei der Durchführung wissenschaftlicher Forschungsvorhaben auf Grund eines Gesetzes förmlich verpflichtet worden sind (Abs. 2 S. 1 Nr. 6) unter Strafe, soweit ihnen dieses im Rahmen ihrer beruflichen Tätigkeit anvertraut oder sonst bekanntgeworden ist. § 203 Abs. 2 S. 1 Nr. 6 StGB ist im Zusammenhang mit § 476 StPO und § 487 Abs. 4 StPO zu lesen, die normieren, unter welchen Voraussetzungen in einem Strafverfahren rechtmäßig erhobene personenbezogene Daten für Zwecke wissenschaftlicher Forschung an Forschungseinrichtungen übermittelt und von diesen verwendet werden dürfen.[174] Gemäß § 476 Abs. 3 StPO dürfen personenbezogene Daten nur an solche Personen übermittelt werden, die Amtsträger oder für den öffentlichen Dienst besonders Verpflichtete oder zur Geheimhaltung verpflichtet worden sind. § 203 Abs. 2 S. 1 Nr. 6 StGB kann daher tatbestandlich nur von solchen Personen erfüllt werden, die auf die gewissenhafte Erfüllung ihrer Geheimhaltungspflicht bei der Durchführung wissenschaftlicher Forschungsvorhaben aufgrund eines Gesetzes förmlich verpflichtet worden sind.[175] Dies trifft auf Forscher im Gesundheitswesen in der Regel nicht zu.

---

[172] BSG, Urteil vom 22.07.2004 – B 3 KR 21/03 R, BeckRS 2004, 41723.

[173] Gesetzentwurf der Bundesregierung, Entwurf eines Gesetzes für eine bessere Versorgung durch Digitalisierung und Innovation (Digitale-Versorgung-Gesetz – DVG), die nach dem Entwurf des DVG zu ändernden Normen des SGB V werden als „SGB V n.F." bezeichnet.

[174] Wittig, in: Graf, BeckOK StPO mit RiStBV und MiStra, 34. Ed., Stand 01.07.2019, § 476 StPO, Rn. 1.

[175] Eisele, in: Schönke/Schröder, Strafgesetzbuch, 30. Aufl. 2019, § 203 StGB, Rn. 95.

Dagegen ist § 203 Abs. 1 Nr. 1 StGB im Zusammenhang mit der medizinischen Forschung stets zu beachten. Sofern mit Patientendaten geforscht wird, werden diese von Ärzten oder berufsmäßig tätigen Gehilfen verarbeitet, die gemäß § 203 Abs. 4 StGB von der Verschwiegenheitspflicht erfasst werden. Tatbestandlich geschützt ist ein fremdes Geheimnis. Unter einem Geheimnis sind solche Tatsachen zu verstehen, die sich auf den Betroffenen beziehen und nur einem begrenzten Personenkreis bekannt sind.[176] Es ist zudem ein sachlich begründetes Geheimhaltungsinteresse des Betroffenen erforderlich.[177] Auf den Großteil der Daten, die für die medizinische Forschung relevant sind, trifft dies zu, denn es handelt sich ganz überwiegend um **Patientendaten**, die **im Rahmen eines Behandlungsverhältnisses** erhoben wurden. Werden diese Daten an eine andere Stelle übermittelt, so kann die Tathandlung des unbefugten Offenbarens eines Geheimnisses erfüllt sein. Ein Geheimnis ist offenbart worden, wenn es auf irgendeine Art einem Dritten mitgeteilt wurde, der von dem Geheimnis noch keine sichere Kenntnis hatte.[178] Das Offenbaren von Patientendaten ist allerdings nur strafbar, wenn der Arzt unbefugt handelt. Das Merkmal „unbefugt" kann sowohl als Tatbestandsmerkmal verstanden werden als auch die Rechtswidrigkeit indizieren.[179] Es hat mithin eine Doppelfunktion und kann einerseits den Tatbestand begrenzen und andererseits die Bedeutung des allgemeinen Deliktsmerkmals der Rechtswidrigkeit haben, je nachdem, ob die Befugnis zur Offenbarung tatbestandsausschließend oder rechtfertigend wirkt.[180] Die Befugnis der Offenbarung kann über die Zustimmung des Verfügungsberechtigten herbeigeführt werden, als ein Recht oder eine gesetzliche Pflicht.[181]

Die ärztliche Schweigepflicht steht neben dem Datenschutzrecht und bleibt von diesem unberührt. Die Erlaubnis der Verarbeitung personenbezogener Daten aus datenschutzrechtlicher Sicht führt daher nicht zu einer Entbindung des Arztes von seiner Schweigepflicht. Dieses als „**Zwei-Schranken-Prinzip**"[182] bezeichnete Nebeneinander der beiden Rechtsgebiete bedeutet, dass neben der datenschutzrechtlichen Erlaubnis der Verarbeitung personenbezogener Daten auch eine Entbindung von der Schweigepflicht erforderlich ist. Etwas anderes gilt immer dann, wenn die Landeskrankenhausgesetze spezielle Erlaubnistatbestände enthalten.[183] Die bereichsspezifischen Vorschriften normieren Verarbeitungsvorgänge mit personenbezogenen Daten, die typischerweise von der ärztlichen Schweigepflicht umfasst sind. Die Regelungen sind gerade im Hinblick auf die besondere Vertraulichkeit der Daten im Arzt-Patienten-Verhältnis geschaffen worden und können daher tatbestandsausschließend oder als Rechtfertigungsgründe im Rahmen des § 203 Abs. 1 StGB herangezogen werden.[184]

---

176 Weidemann, in: von Heintschel-Heinegg, BeckOK StGB, 42. Ed., Stand 01.05.2019, § 203 StGB, Rn. 4.
177 Weidemann, in: von Heintschel-Heinegg, BeckOK StGB, 42. Ed., Stand 01.05.2019, § 203 StGB, Rn. 5 m.w.N.
178 Knauer/Brose, in: Spickhoff, Medizinrecht, 3. Aufl. 2018, § 203 StGB, Rn. 29.
179 Knauer/Brose, in: Spickhoff, Medizinrecht, 3. Aufl. 2018, § 203 StGB, Rn. 32.
180 Eisele, in: Schönke/Schröder, Strafgesetzbuch, 30. Aufl. 2019, § 203, Rn. 29.
181 Eisele, in: Schönke/Schröder, Strafgesetzbuch, 30. Aufl. 2019, § 203, Rn. 29 ff.
182 Kipker, in: Plagemann, Münchener Anwaltshandbuch Sozialrecht, 5. Aufl. 2018, § 48, Rn. 23.
183 Siehe hierzu oben unter Teil 3 A. I. 3. d).
184 Karaalp, Der Schutz von Patientendaten für die medizinische Forschung, 2016, S. 204.

## 8. Transfusionsgesetz

Das Transfusionsgesetz (TFG) dient gemäß § 1 TFG der sicheren Gewinnung von Blut und Blutbestandteilen und einer gesicherten und sicheren Versorgung der Bevölkerung mit Blutprodukten, was mit Hilfe der freiwilligen und unentgeltlichen Blutspende gefördert werden soll.

§ 21a Abs. 5 TFG enthält eine Erlaubnis für das deutsche Hämophilieregister anonymisierte Daten zu Forschungszwecken an die am Deutschen Hämophilieregister Beteiligten und an Dritte zu übermitteln.

## 9. Transplantationsgesetz

Das Transplantationsgesetz (TPG) bildet den gesetzlichen Rahmen für Organ- und Gewebespenden und soll die Bereitschaft zur Organspende in Deutschland fördern. Der Anwendungsbereich des Gesetzes bezieht sich auf menschliche Organe und Gewebe, soweit es um deren Spende und Entnahme zum Zweck der Übertragung, deren Übertragung sowie zugehörige Vorbereitungsmaßnahmen geht.

Nach dem Willen des Gesetzgebers ist die forschungsbedingte Nutzung menschlicher Organe und Gewebe, sofern diese nicht in klinischen Versuchen im oder am menschlichen Körper eingesetzt werden, nicht vom Anwendungsbereich erfasst.[185] Gleichwohl erlaubt § 14 Abs. 2a TPG die Verwendung von personenbezogenen Daten für Forschungszwecke und damit eine Abweichung von der strengen Zweckbindung des § 14 Abs. 2 S. 3 TPG. Die Erlaubnis der Verarbeitung gilt für eigene Forschungsvorhaben der Ärzte und des wissenschaftlichen Personals, welches am Organ- und Gewebespendeprozess beteiligt ist.[186] Insofern bedarf es keiner Einwilligung der betroffenen Person. An Dritte dürfen Daten hingegen nach § 14 Abs. 2a S. 2 TPG nur anonymisiert, mit Einwilligung der betroffenen Person oder bei einem überwiegenden öffentlichen Interesse an der Erforschung übermittelt werden.

## 10. Kirchenrecht

### a) Kirchendatenschutz nach der DS-GVO

Nach Art. 91 DS-GVO dürfen Kirchen oder religiöse Vereinigungen oder Gemeinschafen Regeln, die sie zum Schutz natürlicher Personen bei der Verarbeitung von Daten im Zeitpunkt des Inkrafttretens DSGVO anwenden, auch weiter anwenden, wenn sie mit der DSGVO in Einklang stehen oder gebracht werden. Nach Artikel 17 AEUV achtet die DS-GVO den Status, den Kirchen und religiöse Vereinigungen oder Gemeinschaften in den Mitgliedstaaten nach deren bestehenden verfassungsrechtlichen Vorschriften genießen. Sowohl die katholische Kirche als auch die in der Evangelischen Kirche Deutschland (EKD) zusammengeschlossenen evangelischen

[185] BT-Drs. 16/3146, 23.
[186] Scholz/Middel, in: Medizinrecht, 3. Aufl. 2018, § 14 TPG, Rn. 6.

Landeskirchen haben **eigene Datenschutzgesetze** erlassen und üben so ihr verfassungsrechtlich verbürgtes Selbstbestimmungsrecht der Religionsgesellschaften aus Art. 140 GG i.V.m. Art. 137 Abs. 3 WRV aus.[187]

Ferner müssen auch Kirchen und religiöse Vereinigungen oder Gemeinschaften, die umfassende Datenschutzregeln anwenden, der **Aufsicht durch eine unabhängige Aufsichtsbehörde** unterliegen, die die in Kapitel VI DSGVO niedergelegten Bedingungen erfüllt. Diese Aufsicht ist von Bedeutung für die Eigenständigkeit der Kirchen gegenüber dem Staat. Die Ausübung der Befugnisse einer Aufsichtsbehörde aus Art. 58 Abs. 1e und f, z.B. der erzwungene Zugang zu personenbezogenen Daten und zu Geschäftsräumen und Datenverarbeitungsanlagen, wäre ein erheblicher staatlicher Eingriff in die internen Angelegenheiten einer Religionsgesellschaft. Daher und zur Erfüllung der Anforderungen des Art. 17 Abs. 1 AEUV normiert Art. 91 Abs. 2 eine Sonderregelung für die datenschutzrechtliche Aufsicht über Religionsgesellschaften. Auch im kirchlichen Bereich soll eine Datenschutzaufsicht „im Kern“ unabhängig sein.[188]

### b) Datenschutz der katholischen Kirche

Für die katholische Kirche haben die einzelnen Diözesen Anordnungen über den kirchlichen Datenschutz erlassen, die im Wesentlichen inhaltsgleich mit der als Mustergesetz von der Vollversammlung des Verbandes der Diözesen Deutschlands beschlossenen „Anordnung über den kirchlichen Datenschutz (KDO)“ waren.[189] Die KDO wurde im Mai 2018 von dem Gesetz über den kirchlichen Datenschutz (KDG) abgelöst, mit dem die katholische Kirche, „den Einklang mit der EU-DSGVO [herstellen]“ will.[190] Diese neue Musterregelung muss nunmehr seitens jedes einzelnen Diözesanbischofs für seinen Jurisdiktionsbereich in Kraft gesetzt werden.[191] Die Neuordnung des katholischen Datenschutzrechts führte dazu, dass auch eine kirchliche Datenschutzgerichtsordnung beschlossen wurde. Es gibt daher nunmehr eine kircheneigenen Datenschutzgerichtsbarkeit sowie einen kircheneigenen Instanzenzug.[192] Erstinstanzlich wurde ein interdiözesanes Datenschutzgericht eingerichtet und als zweite Instanz ein Datenschutzgericht der Deutschen Bischofskonferenz. Die kircheneigene Datenschutzgerichtsbarkeit wird allerdings eine Inanspruchnahme staatlichen Rechtsschutzes nicht ausschließen können.[193]

---

[187] Seifert, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 1. Aufl. 2019, Art. 91 DS-GVO, Rn. 6; siehe hierzu auch: Kipker, in: Plagemann, Münchener Anwaltshandbuch Sozialrecht, 5. Auflage 2018, § 48, Rn. 24; Kühling, MedR 2019, 611, 619.

[188] Hoeren, NVwZ 2018, 373, 374; zu den Anforderungen an eine kircheneigene Aufsichtsorganisation: Hense, in: Sydow, Europäische Datenschutzgrundverordnung, 2. Auflage 2018, DSGVO, Art. 91, Rn. 28 f.

[189] Seifert, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 1. Aufl. 2019, Art. 91 DS-GVO, Rn. 6.

[190] Seifert, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 1. Aufl. 2019, Art. 91 DS-GVO, Rn. 6.

[191] Hense, in: Sydow, Europäische Datenschutzgrundverordnung, 2. Aufl. 2018, Art. 91 DSGVO, Rn. 32.

[192] Dekret der Apostolischen Signatur vom 3. Mai 2018 – Prot. N. 53224/17 VAR, abgedruckt in: Amtsblatt des Erzbistums Köln, Stück 10, 158. Jahrgang, 1. September 2018, 143; vgl. Hense, in: Sydow, Datenschutzgrundverordnung, 2. Auflage 2018, DSGVO, Art. 91, Rn. 33.

[193] Hense, in: Sydow, Datenschutzgrundverordnung, 2. Auflage 2018, DSGVO, Art. 91, Rn. 33.

### c) Datenschutz der evangelischen Kirche

Der Datenschutz der Evangelischen Kirche in Deutschland ist einheitlich im Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD) für sämtliche Stellen der evangelischen Kirche – also die EKD, die Landeskirchen sowie die ihnen zugeordneten kirchlichen und diakonischen Werke und Einrichtungen geregelt.[194]

### d) Gemeinsamkeiten und Unterschiede

Die Datenschutzgesetze der beiden großen Kirchen in Deutschland orientieren sich sehr stark an dem Regelungsmodell der DSGVO und weisen viele Übereinstimmungen auf.[195] Die Struktur der DS-GVO und die Kapitelüberschriften wurden weitgehend übernommen. Gleiches gilt für die Grundsätze der Verarbeitung von Daten und die Bestimmungen zu personenbezogenen Daten. Auch die Betroffenenrechte entsprechen denen der DS-GVO. Unterschiede ergeben sich in der Höhe der Geldbuße, diese sind im Kirchenrecht deutlich niedriger, konkret auf 500.000 € begrenzt. Nach § 51 Abs. 6 KDG sind kirchliche Stellen sogar von der **Verhängung von Geldbußen ausgenommen**:

> *„Gegen kirchliche Stellen im Sinne des § 3 Absatz 1, soweit sie im weltlichen Rechtskreis öffentlich-rechtlich verfasst sind, werden keine Geldbußen verhängt; dies gilt nicht, soweit sie als Unternehmen am Wettbewerb teilnehmen."*

Dadurch ist der Bereich amtskirchlichen Handels vollständig von einer datenschutzrechtrechtlichen und strafrechtlichen Kontrolle ausgenommen. Interessanterweise findet sich auch hier die bereits aus den Landesdatenschutzgesetzen bekannte Ausnahmestellung für die Situation der Wettbewerbsteilnahme. Die Bestellung des Datenschutzbeauftragten erfolgt in der katholischen Kirche durch den Diözesanbischof nach § 42 KDG. Der **Diözesandatenschutzbeauftragte** wird dem kirchlichen Recht unterworfen, s. § 43 KDG, und ist nicht nur für die Diözese, die Kirchengemeinden, den Deutschen Caritasverband, die Diözesan-Caritasverbände, ihre Untergliederungen und ihre Fachverbände ohne Rücksicht auf deren Rechtsform sondern auch für Stiftungen, Anstalten, Einrichtungen und sonstige kirchliche Rechtsträger ohne Rücksicht auf ihre Rechtsform zuständig (vgl. § 3 KDG). An der Legitimation dieser Bestellung wird gezweifelt.[196]

### e) Bereichsspezifische Regelungen des Kirchendatenschutzrechts

Krankenhäuser in kirchlicher Trägerschaft haben einen relevanten Anteil an der stationären Versorgung in Deutschland. Etwa ein Drittel der Krankenhäuser steht in „frei-gemeinnütziger Trägerschaft",[197] etwa ein Viertel

---

[194] Seifert, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 1. Aufl. 2019, Art. 91 DS-GVO, Rn. 6.

[195] Gola, in: Gola, Datenschutz-Grundverordnung, 2. Auflage, 2018, DS-GVO, Art. 91, Rn. 12; Hoeren, NVwZ 2018, 373, 374; Seifert, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 1. Aufl. 2019, Art. 91 DS-GVO, Rn. 6.

[196] Hoeren, NVwZ 2018, 373

[197] https://de.statista.com/statistik/daten/studie/180058/umfrage/anteile-der-krankenhaeuser-in-deutschland-nach-traegerschaft/

in Trägerschaft der christlichen Kirchen.[198] Beide Kirchen haben bereichsspezifische Datenschutzvorschriften erlassen, so etwa für die **Verarbeitung von Patientendaten in den kirchlichen Krankenhäusern**.[199] Die Bremische Evangelische Kirche beispielsweise hat eine Verordnung zum Schutz von Patientendaten in kirchlichen Krankenhäusern erlassen.[200] Die Verordnung enthält in § 7 eine Forschungsklausel, die die Verarbeitung von Patientendaten zu Forschungszwecken erlaubt, soweit

- schutzwürdige Belange insbesondere wegen der Art der Daten, wegen ihrer Offenkundigkeit oder wegen der Art der Verarbeitung nicht beeinträchtigt werden
- oder wenn das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Belange des Patienten erheblich überwiegt
- und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann
- und bestimmte Nachweispflichten erbracht werden.

Die Vorgaben gleichen denen des Bremischen Krankenhausdatenschutzgesetzes. Diese Situation stellt sich in vielen Kirchenrechten ähnlich dar. Die Ordnung zum Schutz von Patientendaten in katholischen Krankenhäusern in der Diözese Osnabrück[201] etwa normiert in § 7, dass die Verarbeitung und Nutzung von Patientendaten für Eigenforschung zulässig ist.

Die ohnehin unübersichtliche Regelungsvielfalt für Krankenhäuser, die gleichzeitig die DS-GVO, das Landesdatenschutzgesetz und das gegebenenfalls bestehende Landeskrankenhausgesetz zu berücksichtigen haben, wird also für den Fall der Krankenhäuser in kirchlicher Trägerschaft noch um entsprechende kirchengesetzliche Regelungen erweitert.

### f) Anwendungsbereich des Kirchendatenschutzrechts

Der Geltungsbereich von Art. 17 Abs. 1 AEUV und das Selbstbestimmungsrecht der Religionsgesellschaften wird verfassungsrechtlich in Art. 140 GG iVm Art. 137 Abs. 3 WRV gewährleistet. Dieses gilt für die als Körperschaft des öffentlichen Rechts nach Art. 137 Abs. 5 WRV anerkannten Religionsgesellschaften und die privatrechtlich organisierten Religionsgesellschaften (z.B. als eingetragene Vereine).[202] Diesen Schutz können die als Körperschaften des öffentlichen Rechts organisierten evangelischen Landeskirchen, die EKD, die Diözesen der katholischen Kirche, die Neuapostolische Kirche, die verschiedenen jüdischen Gemeinden und der Zentralrat der Juden in Deutschland sowie die muslimische Ahmadiyya-Gemeinde in Anspruch nehmen. Auch die in den

198 https://christliche-krankenhaeuser.de/#/wer-wir-sind
199 Seifert, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 1. Aufl. 2019, Art. 91 DS-GVO, Rn. 6.
200 Verordnung zum Schutz von Patientendaten in kirchlichen Krankenhäusern v. 21.02.2018 (GVM 2008 Nr. 1 S. 63).
201 Kirchliches Amtsblatt für die Diözese Osnabrück, Band 48, Nr. 7, S. 41 ff.
202 Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, DSGVO Art. 91 Rn. 9

Einrichtungen des Diakonischen Werkes der EKD zusammengeschlossenen Vereinigungen und Einrichtungen des Deutschen Caritasverbandes und der Diözesancaritasverbände sind entsprechend geschützt.

Der **Anwendungsbereich** kirchlichen Datenschutzrechts ist allerdings seit Jahren in der Diskussion. Weitgehende Einigkeit besteht darin, dass die Kirchen ihre datenschutzrechtlichen Rahmen selbst gestalten können, sofern er ihre **eigenen innerkirchlichen Angelegenheiten** betrifft. Wenn die Kirchen von dieser verfassungsrechtlich verbürgten Option Gebrauch machen, verbleibt kein Raum für die Anwendung des staatlichen Datenschutzrechts. Falls aber keine umfassenden Regelungen dazu erlassen werden, gilt das staatliche Datenschutzrecht, z.B. in Form des Bundesdatenschutzgesetzes, auch für den innerkirchlichen Bereich. In diesem Fall fungiert das BDSG als eine Reserveregelung zur Sicherstellung eines umfassenden Datenschutzes.[203]

Es besteht weitgehend Konsens darüber, dass die Regelwerke für den Datenschutz der beiden großen deutschen Kirchen im Sinne des Art. 91 DS-GVO als „umfassend" anzusehen sind und weitgehend mit der DS-GVO in Einklang gebracht wurden. „Umfassend" bedeutet, dass der Unionsgesetzgeber nicht lediglich isoliert bestehende kirchenrechtliche Vorschriften zum Datenschutz, sondern ausschließlich ganze datenschutzrechtliche Regelungskomplexe, die eine eigenständige Kohärenz und Regelungssystematik aufweisen, privilegieren möchte.[204] Diese können daher nach Geltungsbeginn der DS-GVO gem. deren Art. 91 Abs. 1 auch angewandt werden. Dennoch bleibt jedoch die seit vielen Jahren diskutierte Frage des Anwendungsbereichs weiterbestehen. Hierzu finden sich unterschiedliche Ansichten, die z.B. nach der **Organisationsform** (öffentlich-rechtlich oder privatrechtlich), der **Art der Tätigkeit** (betrifft es den religiösen Kernbereich oder nicht) und den **betroffenen Personen** (geht es um Mitglieder der Religionsgemeinschaft oder nicht-Zugehörige) differenzieren.[205] Keine Zuordnung zu einer Religionsgesellschaft und auch kein besonderer verfassungsrechtlicher Schutz gilt daher z.B. bei Wirtschaftsbetrieben der Kirchen wie z.B. bischöflichen Weingütern.[206]

### g) Speziell Krankenhäuser in kirchlicher Trägerschaft

Krankenhäuser der Kirchen sind i.d.R. privatrechtlich organisiert[207] und auch Wirtschaftsbetriebe. Zwischen diesen beiden Kriterien muss unterscheiden werden.

---

[203] BeckOK DatenschutzRecht Mundil, DS-GVO Art. 91 Rn. 9
[204] Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, DSGVO Art. 91 Rn. 12
[205] Sydow, Europäische Datenschutzgrundverordnung, DSGVO Art. 91, Rn. 4
[206] Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, DSGVO Art. 91 Rn. 10
[207] Hoeren, NVwZ 2018, 373.

### aa) Anwendung in Bezug auf die Rechtsform

Zum einen ist zu klären, ob **juristischen Personen des Privatrechts** in den Anwendungsbereich des staatlichen Datenschutzes fallen oder ob wegen der Tatsache, dass die Gesellschaftsanteile von einer Kirche gehalten werden, die Anwendung des kirchlichen Datenschutzrechts geboten ist. Zu dieser Frage verhalten sich Rechtsprechung und Literatur uneinheitlich. Privatrechtlich organisierte kirchliche Einrichtungen werden in Art. 91 DS-GVO nicht explizit erwähnt.[208] Die Frage des Verhältnisses zwischen staatlichen und kirchlichen Datenschutzrechts ist auch durch Art. 91 DS-GVO nicht abschließend geklärt.[209] Nach Ansicht der Kirchen sowie einem Teil der Literatur greift das kirchliche Selbstbestimmungsrecht unabhängig von der Rechtsform, durch die die Kirche ihre Tätigkeiten und ihr Wirken ausübt.[210] Eine zufällige Stichprobe aus acht Krankenhäusern in Trägerschaft der evangelischen Kirche und acht Krankenhäusern in Trägerschaft der katholischen Kirche ergab jedenfalls, dass diese sich in ihrer Datenschutzerklärung auf der Webseite ganz überwiegend auf die die DS-GVO und das jeweilige Kirchendatenschutzrecht beziehen.

In der Diskussion über die Anwendbarkeit des kirchlichen Datenschutzrechts auf privatrechtlich organisierte Einrichtungen der Kirchen[211] ist in den Blick zu nehmen, dass die Kirchen naturgemäß mit einer besonderen Kategorie personenbezogener Daten zu tun haben: Der religiösen Überzeugung im Sinne des Artikels 9 Abs. 1 DS-GVO. Dies unterscheidet sie in der Tat von anderen Einrichtungen, bei denen keine Notwendigkeit besteht, die Frage der **Religionszugehörigkeit in der Datenverarbeitung** zu erfassen. Nur am Rande sei angemerkt, dass die notwendige Verarbeitung von besonderen Kategorien personenbezogener Daten allein noch kein eigenes Datenschutzrecht zu begründen vermag. Wäre dies allein tragend, müssten auch Parteien und Gewerkschaften ein eigenes Datenschutzrecht haben.

Die Anwendung kirchlichen Datenschutzrechts auf ein Krankenhaus allein mit der Begründung, dass die Anteile der Krankenhaus-GmbH von einer Kirche oder Religionsgemeinschaft gehalten werden, erscheint nicht ausreichend begründet.

### bb) Anwendung in Bezug auf die Tätigkeit

Für den Betrieb des Krankenhauses, die Versorgung der Patienten und die Kooperation mit anderen medizinischen Einrichtungen ist die Erhebung oder Verarbeitung personenbezogener Daten, aus denen die religiöse Überzeugung hervorgeht, nicht erforderlich. Aus der Trägerschaft der juristischen Person allein lässt

---

208 Hierauf hinweisend auch: Hoeren, NVwZ 2018, 373, 374.

209 Herbst, in: Kühling/Buchner, DS-GVO BDSG, 2. Auflage 2018, DS-GVO, Art. 91, FN 26.

210 Gola, in: Gola, Datenschutz-Grundverordnung, 2. Auflage, 2018, DS-GVO, Art. 91, Rn. 12; Hoeren, , NVwZ 2018, 373, 373.

211 Pauly, in: Paal/Pauly, DS-GVO BDSG, 2. Auflage 2018, DS-GVO, Art. 91, Rn. 10; Zum anstoßgebenden Charakter des Art. 91 DS-GVO siehe auch: Hense, in: Sydow, Datenschutzgrundverordnung, 2. Auflage 2018, DSGVO, Art. 91, Rn. 34. Hense in HK-EuDSchVO Art. 91 Rn. 4 ff.; Mundil in BeckOK DatenschutzR Art. 91 Rn. 7 ff.; Dammann in Simitis BDSG § 2 Rn. 84 ff., 136 ff.; Preuß ZD 2015, 217 (218 ff.); TBP DatenschutzR 148 ff.

sich eine solche datenschutzrechtliche Privilegierung, die zudem auf eine Befreiung von der Kontrolle durch die staatlichen Datenschutzaufsichtsbehörden mit sich bringt, also nicht herleiten. Das Privileg, außerhalb der staatlichen Regelungen eigenen Datenschutz zu definieren und über eine eigene Datenschutzaufsicht zu kontrollieren, kann und sollte daher sinnvollerweise auch auf den Bereich beschränkt werden, für den dieses Recht geschaffen wurde.

Auf europäischer Ebene ist Art. 91 DS-GVO vor dem Hintergrund von Art. 17 AEUV zu interpretieren.[212] Dieser bezieht sich „in erster Linie auf den Status und nicht auf Tätigkeiten von Religionsgesellschaften".[213] Die oben dargestellten Argumente sprechen dafür, dass im Hinblick auf die Verarbeitung von Patientendaten durch privatwirtschaftlich organisierte Krankenhäuser, deren Träger die Kirche ist, das staatliche Datenschutzrecht Anwendung findet. Allerdings hat das Bundesverfassungsgericht 1980 – mithin vor bald 40 Jahren – entschieden[214], dass **unabhängig von der Rechtsform** die Gestaltungshoheit für den Rechtsrahmen von Krankenhäusern in kirchlicher Trägerschaft den Kirchen zusteht, denn

> *„die tätige Nächstenliebe ist eine wesentliche Aufgabe für den Christen und wird von den christlichen Kirchen als kirchliche Grundfunktion verstanden. Auch in der Staatspraxis nach dem zweiten Weltkrieg ist die karitative Tätigkeit in den Kirchenverträgen und Konkordaten als legitime Aufgabe der Kirchen ausdrücklich anerkannt und die Berechtigung dazu den Kirchen gewährleistet worden (…). Zu dieser karitativen Tätigkeit gehört die kirchlich getragene Krankenpflege. Ihr entspricht die Organisation des kirchlichen Krankenhauses und die auf sie gestützte, an christlichen Grundsätzen ausgerichtete umfassende Hilfeleistung für den Patienten."*

Diese Entscheidung des Bundesverfassungsgerichts vermag jedoch für die hier anstehende Frage der Anwendbarkeit des Datenschutzrechts auf länderübergreifende Forschungsvorhaben keine zwingende Vorgabe zu entfalten, denn von dieser *„Hilfeleistung für den Patienten"* ist der Forschungskontext zu unterscheiden. Wenn ein Krankenhaus in kirchlicher Trägerschaft an einem Forschungsvorhaben mit anderen Krankenhäusern teilnimmt, lässt sich, zumindest mit der in der Entscheidung vom Bundesverfassungsgericht dargelegten Argumentation, nicht zwingend die Geltung des kirchlichen Datenschutzrechts für dieses Forschungsvorhaben ableiten. Dies gilt insbesondere in Ansehung der Argumente für „die (…) Beschränkung auf Mitglieder und auf den religiösen Kernbereich".[215] Es spricht daher einiges dafür, dass auch für ein Krankenhaus in kirchlicher Trägerschaft eine **wettbewerbliche Situation bei Forschungsvorhaben** angenommen werden kann, die die

---

[212] Herbst, in: Kühling/Buchner, DS-GVO BDSG, 2. Auflage 2018, DS-GVO, Art. 91, Rn. 1.
[213] Pauly, in: Paal/Pauly, DS-GVO BDSG, 2. Auflage 2018, DS-GVO, Art. 91, Rn. 10.
[214] BVerfG, Beschluss vom 25. 3. 1980 - 2 BvR 208/76.
[215] Herbst, in: Kühling/Buchner, DS-GVO BDSG, 2. Auflage 2018, DS-GVO, Art. 91, Rn. 23.

Geltung des staatlichen Datenschutzrechts mit sich bringt. Diese Position wird durch das Sondervotum des Richters am Bundesverfassungsgericht Joachim Rottmann gestärkt, wonach es eine Staatsaufgabe ist,

> *„die Krankenhausversorgung der Bevölkerung zu sozial tragbaren Kosten sicherzustellen. Diese Aufgabe kann der Staat dadurch erfüllen, daß er unter Einbeziehung freier gemeinnütziger und kommunaler Träger ein bedarfsgerechtes Gesamtsystem leistungsfähiger Krankenhäuser unterhält und diese in der Weise finanziert, daß er die erforderlichen Investitionskosten übernimmt und die verbleibenden notwendigen Selbstkosten durch entsprechend festgesetzte Pflegesätze aufbringen läßt. Bei dem hier in Rede stehenden Betrieb konfessioneller Krankenhäuser im Rahmen dieses staatlich geplanten und finanzierten Systems handelt es sich materiell, der Natur der Sache und Zweckbeziehung nach um eine* ***gemeinsame Angelegenheit von Staat und konfessionellen Trägern, die in einem bestimmten Umfang auch staatlicher Regelung zugänglich*** *sein und bleiben muß (…).*
>
> *d) In derartigen Angelegenheiten, in denen sich staatliche Zuständigkeiten mit überkommenen Tätigkeitsbereichen der Religionsgesellschaften überschneiden, können weder die Religionsgesellschaften noch der Staat unbegrenzte Regelungsgewalt beanspruchen. Wie insbesondere die gemeinsame Erfüllung sozial- und gesundheitspolitischer Aufgaben zeigt, geht es dabei nicht nur um die Erhaltung der Unabhängigkeit der Religionsgesellschaften als selbständiger Partner dieser Zusammenarbeit, sondern auch vor allem um die Grundrechte und Grundbedürfnisse der Menschen, die auf die Erfüllung jener Aufgaben angewiesen sind.* ***Der Staat*** *ist nicht nur verfassungsrechtlich für die Sicherung der Grundrechte und die Befriedigung jener Grundbedürfnisse allein verantwortlich, sondern darüber hinaus* ***berechtigt und verpflichtet, alle anderen Aspekte des Gemeinwohls****, insbesondere die Wirtschaftlichkeit des letztlich von allen Staatsbürgern zu finanzierenden Systems der sozialen Gesundheitsfürsorge, zur Geltung zu bringen."*[216]

Es ist nichts ungewöhnliches, dass der rechtliche Rahmen in Deutschland im Übrigen auch für die Kirchen Anwendung findet, dies wird beispielsweise für das Bürgerliche Gesetzbuch niemand ernsthaft bestreiten. Trotz der Entscheidung des Bundesverfassungsgerichts aus dem Jahr 1980 beanspruchen die meisten Landeskrankenhausgesetze Geltung auch für die Krankenhäuser von Kirchen und anderen Religionsgemeinschaften sowie von Trägern, die diesen zugeordnet sind (kirchliche Krankenhäuser). Teilweise werden bestimmte Abschnitte oder einzelne Vorschriften hiervon ausgenommen, z.B. bezüglich der internen Struktur des Krankenhauses oder der finanziellen Beteiligung der ärztlichen Mitarbeiter (z.B. § 2 Abs. 3 LKHG BW; § 3 Abs. 2 RPLKG; § 2 Abs. 2 SächsKHG; § 2 Abs. 2 HessLKHG). Soweit ersichtlich, sind in den meisten Landeskrankenhausgesetzen die Vorgaben für die Forschung mit Patientendaten nicht von der Geltung für die kirchlichen Krankenhäuser ausgenommen. Viele Landesgesetzgeber haben also bisher von ihrer

[216] Sondervotum Richter Rottmann, BVerfG, Beschluss vom 25. 3. 1980 - 2 BvR 208/76

Gestaltungskompetenz für den Datenschutz in Forschungsvorhaben auch bezüglich der kirchlichen Krankenhäuser Gebrauch gemacht.

### h) Ergebnis

Aus alledem ergibt sich, dass für Forschungsvorhaben in (ggf. privatrechtlich organisierten) Krankenhäusern kirchlicher Trägerschaft die Anwendung des ggf. bestehenden Landeskrankenhausgesetzes oder des Bundesdatenschutzgesetzes als Konkretisierung der DS-GVO angenommen werden kann. Es ergibt sich des Weiteren, dass eine bundesrechtliche Vorgabe der Anwendung des BDSG auch für kirchliche Krankenhäuser in landesübergreifenden Forschungskontexten zulässig ist. Konkret gelten also für ein Krankenhaus in kirchlicher Trägerschaft zunächst die DS-GVO, ggf. das kirchliche Datenschutzrecht und das jeweilige Landeskrankenhausgesetz. Soweit der Bundesgesetzgeber eine Kompetenz zur Regelung von landesübergreifenden Forschungsvorhaben hat und hiervon Gebrauch macht, kann für dieses Krankenhaus bei einem gemeinsamen Forschungsvorhaben mit einem Krankenhaus in einem anderen Bundesland die entsprechende Bundesregelung angewandt werden.

## III. Analyse der Struktur der Aufsicht

Die föderalistische Struktur Deutschlands bringt nicht nur eine **unübersichtliche Rechtslage** mit sich, sondern auch die Zuständigkeit von 17 unterschiedlichen Landesdatenschutzbehörden.[217] Die Diskrepanz der Rechtslage wird daher verstärkt durch **unterschiedliche Auffassungen** der Landesdatenschutzbehörden, wodurch zusätzliche Rechtsunsicherheit entsteht. Besonders deutlich wird dies etwa beim Vergleich von Aussagen der Berliner Datenschutzbeauftragten mit solchen des Datenschutzbeauftragten Baden-Württemberg. Während der Landesbeauftragte für Datenschutz in Baden-Württemberg betont, dass die medizinische Forschung der Weiterentwicklung diagnostischen und therapeutischen Wissens dient und den Patienten durch Verbesserung der Behandlungsqualität nützt,[218] wird etwa aus dem Tätigkeitsbericht der Berliner Datenschutzbeauftragten aus dem Jahr 2011 deutlich, dass in erster Linie die Verwirklichungsbedingungen für die informationelle Selbstbestimmung der Patienten in den Fokus genommen werden. Der Nutzen der medizinischen Forschung wird nicht thematisiert. Die Berliner Datenschutzbeauftragte geht daher davon aus, dass Forschung „nur in engen Grenzen“ ohne Einwilligung der Patienten betrieben werden kann.[219] Diese Auffassung mündet auch in einer

---

[217] In Bayern gibt es, anders als in allen anderen Bundesländern, zwei Behörden.

[218] Der Landesbeauftragte für den Datenschutz Baden-Württemberg, 32. Tätigkeitsbericht 2014/2015, S. 118 abrufbar unter https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2016/02/32._TB.pdf, zuletzt abgerufen am 10.06.2019.

[219] Berliner Beauftragter für Datenschutz und Informationsfreiheit, Datenschutz und Informationsfreiheit – Bericht 2011, S. 48 abrufbar unter https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/jahresbericht/BlnBDI-Jahresbericht-2011-Web.pdf, zuletzt abgerufen am 10.06.2019

nach Wahrnehmung der Gutachter strengeren Kontrolle der Krankenhäuser des Landes Berlin, als das in Baden-Württemberg der Fall ist.

# B. Auswertung der Normanalyse

## I. Vorbemerkung

Die Analyse der Forschungsklauseln im Bundes- und Landesrecht hat offenbart, dass die Harmonisierung der Datenschutzvorschriften im Bereich der medizinischen Forschung nicht nur nicht geglückt ist, sondern das im Gegenteil von einer Zersplitterung des Rechts gesprochen werden muss. Insbesondere in den Landeskrankenhausgesetzen ist ein Vergleich schon deshalb kaum möglich, weil neben inhaltlich voneinander abweichenden Regelungen teilweise auch identische Regelungen unterschiedlich formuliert werden. Es wird gar davon gesprochen, dass bei bundesländer-übergreifenden Forschungsprojekten „die Einhaltung der Gesetze zum **Glücksspiel** [wird], selbst dann, wenn die Forschenden bemüht sind, die normativen Vorgaben des digitalen Grundrechtsschutzes zu beachten."[220]

Folgende **Nachteile** entstehen durch die Anwendbarkeit unterschiedlicher Datenschutzgesetze und unterschiedlicher Auffassungen der Aufsichtsbehörden der Länder in länderübergreifenden Forschungsvorhaben:

- Höherer Verwaltungsaufwand
- Effizienzverluste
- Wettbewerbsnachteile
- Standortnachteile
- Rechtsunsicherheit

**Im Ergebnis verkleinert sich die Schnittmenge der zulässigen Datenverarbeitung zu Forschungszwecken bei länderübergreifenden Forschungsvorhaben proportional mit der Anzahl der am Forschungsvorhaben beteiligten Länder.**

Die Datenschutzvorschriften in den Landeskrankenhausgesetzen weisen zahlreiche Unterschiede auf. Die unterschiedlichen Gesetzesstrukturen machen zunächst einen Vergleich der unterschiedlichen Begriffe schon schwierig, z.B. stehen „Erhebung, Verarbeitung, Nutzung, Offenbarung, Übermittlung" in unterschiedlichen

[220] Bernhardt/Ruhmann/Weichert, Die Forschungsklauseln im neuen Datenschutzrecht, Stand 18.10.2018, abrufbar unter https://www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_2018_forschungklauseln_181018.pdf, zuletzt abgerufen am 04.09.2019. S. 8 f.

Kontexten mit unterschiedlichen Voraussetzungen und Rechtsfolgen, so dass ich daraus unterschiedliche Interpretationen ergeben. Diese Unterschiede haben einen beachtlichen Einfluss auf die Verarbeitung von Patientendaten in den jeweiligen Bundesländern.

## II. Divergente Terminologie

Die Vorschriften enthalten einheitliche Begriffe, die aber unterschiedlich definiert werden. So erfassen z.B. Patientendaten in Baden-Württemberg auch die Angaben über Begleitpersonen, was in Berlin nicht der Fall ist, während Rheinland-Pfalz sogar sonstige Dritte einschließt, die dem Krankenhaus im Zusammenhang mit der Behandlung bekanntwerden (vgl. §§ 43 Abs. 4 Satz 1 BWLKG, 36 Abs. 1 Satz 4 RPLKG, 24 Abs. 2 Satz 1 BlnLKG).

## III. Unterschiedliche Normadressaten

Der Adressat der datenschutzrechtlichen Vorschriften in den Landeskrankenhausgesetzen ist der Krankenhausträger (z.B. § 24 LKHG Bln) oder das Krankenhaus (z.B. § 24 LKHG Bln, § 43 Abs. 1 S. 1 LKHG BW, § 2 Abs. 1 Nr. 1 GDSG NW, § 12 Abs. 1 HmbKHG). In einigen Bundesländern richten sich die Vorschriften aber auch an Krankenhausärzte (z.B. Art. 27 Abs. 4 BayKrG).

## IV. Vielfältige Forschungsklauseln

Die Möglichkeit der Begründung der Rechtmäßigkeit der Verarbeitung von Patientendaten für Forschungszwecke über die Einwilligung des Patienten unterliegt in den Landeskrankenhausgesetzen unterschiedlichen Voraussetzungen. Die Vorschriften weichen nicht nur im Wortlaut voneinander ab. In den Landeskrankenhausgesetzen einiger Bundesländer wird bei der Verarbeitung von Patientendaten für Forschungszwecke danach differenziert, ob die Daten intern oder extern verarbeitet werden (vgl. § 25 Abs. 1 S. 1 LKHG Bln). Diese Differenzierung findet sich in anderen Landeskrankenhausgesetzen nicht. Auch in diesem Kontext werden erneut unterschiedliche Begriffe verwandt (z.B. „krankenhausinterne Forschungsvorhaben“, § 25 Abs. 1 S. 1 LKHG Bln; „eigene wissenschaftliche Forschung“, § 12 Abs. 1 S. 1 HmbKHG; Verbleiben im „Gewahrsam des Krankenhauses“, Art. 27 Abs. 4 S. 2 a.E. BayKrG). In einigen Landeskrankenhausgesetzen finden sich weitere Beschränkungen, die die Veröffentlichung betreffen (§ 24 Abs. 4 LKHG Bln, § 6 Abs. 5 GDSG NW).

## V. Weitere regionale Besonderheiten

Schließlich sind Besonderheiten festzustellen, die sich auf ganz bestimmte Landeskrankenhausgesetze beziehen. So bedarf in Brandenburg die Offenlegung von Patientendaten an andere Stellen oder Personen für Forschungszwecke ohne Einwilligung der betroffenen Person der vorherigen Bestätigung der zuständigen Rechtsaufsichtsbehörde (§ 31 S. 1 Bbg.-KHEG).

Die Forschung in länderübergreifenden Konsortien ist daher zwar grundsätzlich möglich, unterliegt aber unter anderem insofern erschwerten Bedingungen als eine länderübergreifende Kooperation in der Regel zu einer **Verengung der Zulässigkeit** führt.

### VI. Die Gesetzeslage im Übrigen

Die detaillierten Betrachtungen des Arzneimittelrechts, des Gendiagnostikgesetzes, des Medizinproduktegesetzes, des Sozialrechts und des Strafrechts, des Strahlenschutzgesetzes und der Strahlenschutzverordnung, des Transfusion und des Transplantationsgesetzes ergaben demgegenüber keine Kollisionen und **keinen Anpassungsbedarf** im Hinblick auf länderübergreifende Forschungsvorhaben.

### VII. Kirchenrechtlicher Datenschutz

Mit der DS-GVO wurde zwar die Rechtsunsicherheit bezüglich der grundlegenden Kompetenz einer eigenen datenschutzrechtlichen Gestaltungsmöglichkeit für die Kirchen und Religionsgemeinschaften beseitigt. Dennoch besteht weiterhin Unsicherheit bezüglich der Anwendungsbereiche der kirchenrechtlichen Datenschutzvorschriften. Gleichzeitig bestehen erhebliche Abweichungen zur DS-GVO, z.B. bei den Strafvorschriften, und Unklarheiten zur Legitimation der aufsichtsrechtlichen Kompetenz. Insbesondere ist unklar, ob diese Vorschriften auf privatrechtliche Einrichtungen der Kirchen Anwendung finden können, wenn diese nicht im Kernbereich der Ausübung der Religion, nicht mit Angehörigen der Religionsgemeinschaft und im Wettbewerb mit anderen Privatrechtssubjekten, so bei der wissenschaftlichen Forschung, tätig sind.

## C. Lösungsvorschläge

### I. Bund-Länder-Staatsvertrag

*Krawczak* und *Weichert* schlagen eine bundesweit einheitliche Regelung für die medizinische Forschung in einem Bund-Länder-Staatsvertrag vor, die die verstreuten und teils widersprüchlichen Vorschriften des Bundes und der Länder zur medizinischen Forschung obsolet machen sollen, sodass diese ersatzlos gestrichen werden könnten.[221] In diesem Bund-Länder-Staatsvertrag könnten materiellrechtliche und prozessuale Voraussetzungen für die Zulässigkeit medizinischer Forschungsvorhaben, die Einbindung von Ethikkommissionen und die Zuständigkeit der Datenschutzaufsicht normiert werden sowie Transparenzverpflichtungen gegenüber der Öffentlichkeit normiert werden.

[221] Krawczak/Weichert, Vorschlag einer modernen Dateninfrastruktur für die medizinische Forschung in Deutschland (Version 1.9), 2017, S. 11.

Staatsverträge sind ein Instrument intraföderaler Kooperation.[222] Es handelt sich um Vereinbarungen öffentlich-rechtlichen Inhalts, die ein Land mit einem anderen Land oder mehreren anderen Ländern, mit dem Bund oder mit einem anderen Staat auf der Ebene der Gleichordnung trifft.[223] Der Staatsvertrag bedarf der Unterzeichnung durch die Ministerpräsidenten der Länder sowie der anschließenden Zustimmung der Landtage per Zustimmungsgesetz.[224]

Der Abschluss eines Bund-Länder-Staatsvertrags stellt aus unserer Sicht durchaus ein **probates Mittel** zur Harmonisierung des Datenschutzrechts im Bereich der medizinischen Forschung dar. Gleichwohl ist er nach unserem Dafürhalten **wenig praktikabel**. So ist zunächst eine Abstimmung auf Referentenebene erforderlich, die zu einem Konsens zwischen allen 16 Bundesländern sowie dem Bund führen muss. Sodann muss der Staatsvertrag in den Ländern sowie vom Bund ratifiziert werden, um Rechtsverbindlichkeit zu erlangen. Der Bund-Länder-Staatsvertrag ist daher mit einem erheblich Koordinations- und Abstimmungsaufwand verbunden. Allerdings kann er als langfristige Lösung in Betracht gezogen werden.

## II. Mustergesetzgebung

Eine andere Möglichkeit der Vereinheitlichung datenschutzrechtlicher Regelungen ist der Erlass eines Mustergesetzes.[225] Die Mustergesetzgebung ist keine vom Grundgesetz vorgesehene Gesetzgebungskompetenz, wird aber als Instrument der Harmonisierung der Ländergesetzgebung etwa im Bereich des Polizeirechts schon seit vielen Jahren genutzt.[226] Die Koordinierung von Mustergesetzen erfolgt in der Regel durch die zuständige Konferenz der Fachminister von Bund und Ländern. Um Rechtsverbindlichkeit zu erlangen, müssen Mustergesetze von den Ländern im Landesrecht umgesetzt werden, sie sind aber für die Länder nicht bindend.[227]

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (Bitkom) hat indes einen Vorschlag für einen Gesetzesentwurf zum Schutz personenbezogener Daten bei deren Verarbeitung im Krankenhaus erarbeitet, der sich zum Zeitpunkt der Abgabe dieses Gutachtens noch in der Abstimmung befand. Der Entwurf sieht eine „Rahmengesetzgebung“ für die Versorgung von Patienten in Krankenhäusern sowie Vorsorge- und Rehabilitationseinrichtungen vor. Da die Rahmengesetzgebung nach Art. 75 GG a.F. im Rahmen

---

222 Schladebach, VerwArch 2007, 238.
223 Schulz/Tallich, NVwZ 2010, 1338, 1339.
224 Martini, in: Gersdorf/Paal, BeckOK Informations- und Medienrecht, 24. Ed., Stand: 01.05.2019, § 1 RStV, Rn. 11.
225 Bernhardt/Ruhman/Weichert, Die Forschungsklauseln im neuen Datenschutzrecht, Stand: 18.10.2018, S. 9, abrufbar unter: https://www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_2018_forschungklauseln_181018.pdf (zuletzt abgerufen am 05.09.2019).
226 Das Gefahrenabwehrrecht der Länder beruht im Wesentlichen auf dem Musterentwurf eines einheitlichen Polizeigesetzes des Bundes und der Länder aus dem Jahr 1977, Götz, NVwZ 1984, 211.
227 Aden/Fährmann, Polizeirecht vereinheitlichen? – Kriterien für Muster-Polizeigesetze aus rechtsstaatlicher und bürgerrechtlicher Perspektive, E-Paper der Heinrich-Böll-Stiftung, 2018, S. 11, abrufbar unter https://www.boell.de/sites/default/files/endf_e-paper_polizeirecht_vereinheitlichen.pdf?dimension1=division_demo (zuletzt abgerufen: 15.09.2019).

der Föderalismusreform im Jahr 2006 aus dem Grundgesetz gestrichen wurde, ist davon auszugehen, dass es sich insofern um einen Vorschlag für ein **Mustergesetz** handeln dürfte.

Der Gesetzentwurf hat zum Ziel, das Recht auf informationelle Selbstbestimmung im Bereich der Patientenversorgung zu gewährleisten und enthält auch Vorschriften zur Verarbeitung von Patientendaten zu Forschungszwecken.

## III. Regelung auf Bundesebene

Die Normierung einer Rechtsgrundlage für die Verarbeitung personenbezogener Daten zu Forschungszwecken im Zusammenhang mit länderübergreifenden Forschungsvorhaben sowie die Neuordnung der aufsichtsbehördlichen Zuständigkeit in diesen Fällen sollte nach unserem Dafürhalten auf Bundesebene geschehen. Das Bundesdatenschutzgesetz hält mit § 27 BDSG eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten zu Forschungszwecken bereit.[228] Der Auffassung, dass § 27 Abs. 1 BDSG das Vorliegen einer gesonderten Rechtsgrundlage aus Art. 6 DS-GVO voraussetzt,[229] kann aus verschiedenen Gründen nicht gefolgt werden. Zum einen enthält § 27 Abs. 1 BDSG alle Merkmale einer datenschutzrechtlichen Ermächtigungsgrundlage.[230] Zum anderen ist nicht ersichtlich, in welchem Fall die Voraussetzungen von § 27 Abs. 1 BDSG vorliegen, die des Art. 6 Abs. 1 lit. f) DS-GVO – auf den der nationale Gesetzgeber explizit verweist – aber nicht.[231] Die Hinzuziehung von Art. 6 Abs. 1 DS-GVO ist aber auch schon deshalb abwegig, da dieser nicht die Verarbeitung von Gesundheitsdaten legitimieren kann.

Im Ergebnis erachten wir eine Anknüpfung an § 27 BDSG für zielführend. Dieser Regelungsort bietet sich ebenso für die Datenspende zu wissenschaftlichen Forschungszwecken an.

### 1. Gesetzgebungskompetenz des Bundes

#### a) Ausschließliche Bundeszuständigkeit

Eine Gestaltungskompetenz des Bundes zur Festlegung von Regelungen für die Verarbeitung von Patientendaten zu Forschungszwecken lässt sich aus den Gegenständen der ausschließlichen Gesetzgebung gemäß Art. 73 GG nicht herleiten. Die Untersuchung fokussiert sich daher auf mögliche Gegenstände der konkurrierenden Gesetzgebung in Art. 74 GG.

---

228 Buchner/Tinnefeld, in: Kühling/Buchner, DS-GVO BDSG, 2. Aufl. 2018, § 27 BDSG, Rn. 8; Johannes/Richter, DuD 2017, 300, 302.
229 BT-Drs. 18/11325, 99.
230 Johannes/Richter, DuD 2017, 300, 302.
231 Johannes/Richter, DuD 2017, 300, 302.

## b) Konkurrierende Bundeszuständigkeit

### aa) Recht der Wirtschaft (Art. 74 Abs. 1 Nr. 11 GG)

Aus Art. 74 Abs. 1 Nr. 11 GG lässt sich eine Gesetzgebungskompetenz des Bundes hinsichtlich der länderübergreifenden Verarbeitung von Patientendaten zu Forschungszwecken ableiten. Die konkurrierende Bundeszuständigkeit für das Recht der Wirtschaft gilt als die wichtigste und gleichzeitig auch besonders schwierig abzugrenzende Kompetenznorm des Bundes. Anerkannterweise ist der Beispielskatalog der Norm nicht abschließend, sodass noch weitere Wirtschaftszweige hinzutreten. Das Recht der Wirtschaft bezieht sich also auf alle Normen, die das wirtschaftliche Leben und die wirtschaftliche Betätigung regeln.[232] Als Regelungsmaterie gelten auch Fragen der Wirtschaftsorganisation, einzelner Wirtschaftszweige und bestimmter wirtschaftender Personen. Nur Wirtschaftszweige, die einen stärkeren Zusammenhang mit einer ausschließlichen Länderkompetenz aufweisen, sind ausgenommen.

So hat der Gesetzgeber in die Gesetzesbegründung zum Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 -wie folgt formuliert:

> *„Die Gesetzgebungskompetenz des Bundes folgt für Regelungen des Datenschutzes als Annex aus den jeweiligen Sachkompetenzen der Artikel 73 bis 74 des Grundgesetzes (GG). Im Bereich der öffentlichen Verwaltung bedarf es bundesrechtlicher Datenschutzbestimmungen, soweit dem Bund die Verwaltungskompetenz zusteht. Für nichtöffentliche Stellen folgt die Gesetzgebungskompetenz des Bundes im Bereich des Datenschutzes als Annex aus Artikel 74 Absatz 1 Nummer 11 GG (Recht der Wirtschaft). Nach Artikel 72 Absatz 2 GG steht dem Bund die Gesetzgebungskompetenz in diesen Fällen unter anderem dann zu, wenn und soweit eine bundesgesetzliche Regelung zur Wahrung der Rechtseinheit im gesamtstaatlichen Interesse erforderlich ist. Eine bundesgesetzliche Regelung des Datenschutzes ist zur Wahrung der Rechtseinheit im Bundesgebiet im gesamtstaatlichen Interesse erforderlich. Eine Regelung dieser Materie durch den Landesgesetzgeber würde zu erheblichen Nachteilen für die Gesamtwirtschaft führen, die sowohl im Interesse des Bundes als auch der Länder nicht hingenommen werden können. Insbesondere wäre* ***zu befürchten, dass unterschiedliche landesrechtliche Behandlungen gleicher Lebenssachverhalte erhebliche Wettbewerbsverzerrungen und störende Schranken für die länderübergreifende Wirtschaftstätigkeit zur Folge hätten****. Es bestünde die Gefahr, dass z.B. die Betroffenenrechte durch die verschiedenen Landesgesetzgeber unterschiedlich eingeschränkt würden, mit*

[232] Vgl. statt vieler: BVerfG, Beschluss vom 11. 7. 2006 - 1 BvL 4/00, NJW 2007, 51, 52

*der Folge, dass bundesweit agierende Unternehmen sich auf verschiedenste Vorgaben einrichten müssten."*[233]

In Literatur und Rechtsprechung viel diskutiert ist die Frage, ob und inwieweit der Bundesgesetzgeber für öffentlich-rechtliche Einrichtungen der Länder und Kommunen Gesetze im Rahmen dieser Bundeskompetenz erlassen darf. Die Frage wird z.B. für die öffentlich-rechtlichen Banken und Sparkassen, aber auch Energieversorgungsunternehmen relevant, die am allgemeinen wirtschaftlichen Wettbewerb teilnehmen.[234] Dementsprechend ist z.B. in den Landesdatenschutzgesetzen geregelt, dass soweit Unternehmen in öffentlich-rechtlicher Trägerschaft des Landes am Wettbewerb teilnehmen, für diese das Bundesdatenschutzgesetz anzuwenden ist. So heißt es beispielsweise in § 1 Abs. 3 S. 1 des bayerischen Landesdatenschutzgesetzes:

*„Soweit öffentliche Stellen als Unternehmen am Wettbewerb teilnehmen, gelten für sie selbst, ihre Zusammenschlüsse und Verbände die Vorschriften für nicht öffentliche Stellen."*

Hier wird die Geltung des BDSG für die öffentlichen Stellen im Wettbewerb klargestellt. Demgegenüber statuiert § 2 Abs. 6 des Berliner Landesdatenschutzgesetzes, dass öffentliche Stellen des Landes als nicht-öffentliche Stellen anzusehen sind, wenn sie „als Unternehmen" am Wettbewerb teilnehmen:

*„Abweichend von den Absätzen 1 und 2 gelten öffentliche Stellen, soweit diese als Unternehmen am Wettbewerb teilnehmen, als nicht-öffentliche Stellen."*

Und in § 2 Abs. 4 LDSG Baden-Württemberg ist von einer „entsprechenden Anwendung" die Rede:

*„Soweit öffentliche Stellen als Unternehmen mit eigener Rechtspersönlichkeit am Wettbewerb teilnehmen, sind die für nicht-öffentliche Stellen geltenden Vorschriften des Bundesdatenschutzgesetzes entsprechend anzuwenden."*

Die Vorschriften sind jeweils lediglich **Klarstellungen**, denn das BDSG gilt für diese Stellen als Bundesrecht kraft bundesrechtlicher Gesetzgebungskompetenz für das Recht der Wirtschaft. Eine aus der Landesgesetzgebung herrührende Konstituierung von Bundes- oder EU-Recht ist auch gar nicht möglich.

Der Kompetenznorm des Art. 74 Nr. 11 GG liegt der Gedanke zugrunde, dass Unternehmen in öffentlich-rechtlicher Trägerschaft, die nicht nur aus Gewinnerzielungsabsicht, sondern auch nach außen hin wie die

---

[233] BT-Drs. 18/11325, 71.
[234] Maunz/Dürig/Maunz, 86. EL Januar 2019, GG Art. 74 Rn. 135.

privaten Rechtsträger am wirtschaftlichen Leben teilnehmen, im gleichen rechtlichen Regelungsrahmen an der Wirtschaft teilnehmen sollten, wie Unternehmen in privater Trägerschaft.[235] In dieser Situation darf der Bundesgesetzgeber die Unternehmen in von ihm erlassene Gesetze zur Regelung des Wirtschaftskreises unabhängig von der Rechtsnatur des Normadressaten mit einbeziehen.

Vor diesem Hintergrund stellt sich die Frage, ob ein Krankenhaus in Trägerschaft einer öffentlichen Einrichtung eines Bundeslandes in der **wissenschaftlichen Forschung mit Patientendaten am Wettbewerb** mit anderen Unternehmen in privater Trägerschaft **teilnimmt**. Dies kann durchaus der Fall sein. So gibt es z.B. Tochtergesellschaften von Universitätsklinika, deren Geschäftsgegenstand die Durchführung klinischer Prüfungen ist, und die dabei im Wettbewerb mit privatwirtschaftlich aufgestellten Clinical Research Organisationen stehen. Soweit es sich dabei um Studien mit Arzneimitteln oder Medizinprodukten handelt, ist der Rechtsrahmen sowohl für die Unternehmen in öffentlich-rechtlicher wie auch in privater Trägerschaft durch das Arzneimittelgesetz bzw. das Medizinprodukterecht vorgegeben. Es gibt Studien oder Forschungsvorhaben, die sich außerhalb dieses bundesgesetzlich bereits präformierten Bereichs bewegen, wie etwa die Erhebung und Verarbeitung von annotierten Schnitt-Bildern zur Entwicklung Lernender Systeme in der diagnostischen Radiologie. Auch im Rahmen der Medizininformatik-Initiative gibt es Konsortien, die länderübergreifend aus Krankenhäusern gebildet werden, die Forschungsvorhaben mit Patientendaten durchführen. Die bei diesen Forschungsvorhaben entwickelten Produkte können durchaus solche sein, die im Wettbewerb mit Produkten aus solchen Forschungsvorhaben stehen, die von Krankenhäusern in privater Trägerschaft entwickelt werden. Hinzu kommen Forschungsvorhaben, die z.B. im Rahmen der Forschungsförderung des Bundes gebildet werden, und an denen sich Krankenhäuser in öffentlich-rechtlicher Trägerschaft der Länder gleichermaßen bewerben, wie Einrichtungen in privater Trägerschaft. Insoweit kann man bezüglich einer medizinischen Forschung mit Patientendaten (außerhalb der klinischen Prüfung von Arzneimitteln oder Medizinprodukten) durchaus von einer **wettbewerblichen Situation der Krankenhäuser in öffentlich-rechtlicher Trägerschaft** der Länder sprechen.

Im Ergebnis ist festzustellen, dass es für Krankenhäuser in öffentlich-rechtlicher Trägerschaft eines Bundeslandes Situationen gibt, in denen – über den ohnehin bundesrechtlich präformierten Bereich der Forschung mit Arzneimitteln und Medizinprodukten – eine wettbewerbliche Situation mit privaten Unternehmen bei Forschungsvorhaben mit Patientendaten entsteht. In diesen Fällen ist bereits jetzt das Landesdatenschutzrecht nicht einschlägig, sondern die Anwendung der Vorschriften für nicht öffentliche Stellen (damit der die DSGVO und des BDSG) geboten. Der damit vom Gesetzgeber intendierte Zweck, die Unternehmen der Landeskörperschaften vom Wettbewerbsnachteil des Landesrechts zu befreien, wird aber in der gegenwärtigen Situation dort konterkariert, wo ein bereichsspezifisches Recht, etwa das der **Landeskrankenhausgesetzgebung**, gleichwohl **zusätzliche administrative Hürden** errichtet und einen personellen Mehraufwand erfordert. Es wäre

[235] Maunz/Dürig/Maunz, 86. EL Januar 2019, GG Art. 74 Rn. 154

daher folgerichtig, das Recht für die nicht öffentlichen Stellen auch für diese Konkurrenzsituationen anzuwenden. Nach unserer Auffassung ergibt sich dies bereits aus dem Anwendungsbereich des Bundesdatenschutzgesetzes in Verbindung mit der DSGVO und bedürfte keiner weiteren Verankerung in den Landeskrankenhausgesetzen. Gleichwohl erscheint aus Gründen der Rechtssicherheit und Rechtsklarheit eine Klarstellung sowohl im Bundesdatenschutzgesetz wie auch in den jeweiligen Landeskrankenhausgesetzen geboten.

### bb) Förderung wissenschaftlicher Forschung (Art. 74 Abs. 1 Nr. 13 GG)

Es wurde bereits unter Teil 2 C II 1. dargestellt, dass der Bund im Rahmen der konkurrierenden Gesetzgebung Art. 74 Abs. 1 Nr. 13 GG, die Förderung der wissenschaftlichen Forschung, fruchtbar machen kann, um eine Gesetzgebungskompetenz für länderübergreifende Forschungsvorhaben abzuleiten. Hierfür müssten zusätzlich die Voraussetzungen des Art. 72 Abs. 2 2. Alt. GG gegeben sein, wonach die Bundeskompetenz davon abhängt, dass sie zur Wahrung der Rechts- oder Wirtschaftseinheit im gesamtstaatlichen Interesse erforderlich ist. Dieser Ansatz soll jetzt hier näher untersucht werden.

Bestandteil der konkurrierenden Gesetzgebungskompetenz des Bundes bildet gem. Art. 74 Abs. 1 Nr. 13 GG die Förderung wissenschaftlicher Forschung. Der Begriff der Förderung erfasst die Regelung finanzieller, organisatorischer und planerischer Maßnahmen einschließlich diesbezüglicher kontrollierender Maßnahmen.[236] Die Förderung kann personen-, projekt- oder auch einrichtungsbezogen durchgeführt werden.[237] Einschlägige Rechtsprechung zum Begriff der Forschungsförderung existiert nicht. Jedoch deckt sich der Begriff der Förderung wissenschaftlicher Forschung aus Art. 74 Abs. 1 Nr. 13 GG mit dem des Art. 91b GG. Unter Verweis auf die Gesetzesbegründung wird im Rahmen des Art. 91b GG ein weites Begriffsverständnis der wissenschaftlichen Forschung angenommen.[238] Hiervon ausgehend kann auch im Rahmen des Art. 74 Abs. 1 Nr. 13 GG der Begriff der Förderung weit ausgelegt werden. Jede Maßnahme, die geeignet ist, die wissenschaftliche Forschung zu ermöglichen, zu erleichtern, zu verbessern oder zu beschleunigen, kann daher als Förderung eingeordnet werden. Spiegelbildlich dazu ist auch der **Abbau forschungshemmender Umstände** als Förderung zu verstehen.

Der organisatorische Rahmen wissenschaftlicher Forschung wird durch die einschlägigen gesetzlichen Vorgaben geprägt und begrenzt. Die gegenwärtig in vielen Bereichen divergierende Datenschutzgesetzgebung der Länder erschwert Vorbereitung und Durchführung bundesweiter Forschungsvorhaben erheblich und macht diese teilweise sogar unmöglich. Eine **bundesweite Angleichung datenschutzrechtlicher Gesetze** im Bereich des Forschungswesens ist daher als Maßnahme zur Erleichterung der wissenschaftlichen Forschung und zum Abbau forschungshemmender Umstände, mithin als **Forschungsförderung**, zu verstehen.

---

[236] Maunz, in: Maunz/Dürig, Grundgesetz Kommentar, 86. Lieferung 2019, Art. 74 Rn. 179; Kunig, in: Münch/Kunig, Grundgesetz-Kommentar, 6. Auflage, Band 2, Art. 74, Rn. 59; Rengeling, in: Isensee/Kirchhof, Handbuch des Staatsrechts Band VI, § 135 Rn. 246.

[237] Oeter, in: Mangoldt/Klein/Starck, Grundgesetz-Kommentar, 7. Auflage, Band 2, Art. 74, Rn. 108.

[238] Suerbaum, in: BeckOK Grundgesetz, 51. Edition, 15.5.2019, Art. 91b, Rn. 11; BT-Drs. 16/813, S. 17.

### cc) Wirtschaftliche Sicherung der Krankenhäuser und Regelung der Krankenhauspflegesätze (Art. 74 Abs. 1 Nr. 19a GG)

Schon im Jahr 1969 wurde ein Teil des Krankenhauswesens in die Bundeszuständigkeit für die konkurrierende Gesetzgebung eingefügt.[239] Allerdings gab es schon immer vereinzelt Vorschriften, die den stationären Sektor berühren und die auf die konkurrierenden Kompetenzen in Art. 74 Abs. 1 Nr. 7, Nr. 10 und Nr. 12 gestützt wurden. Dies betrifft etwa krankenhausbezogene Vorschriften im Sozialversicherungsgesetzbuch, im Bundessozialhilfegesetz und im Bundesversorgungsgesetz. Auch für den Betrieb des Krankenhauses als Gewerbeunternehmen existiert Bundesgesetzgebung, z.B. in § 30 der Gewerbeordnung, der die Konzessionspflicht für private Krankenanstalten begründet. Generell gesehen unterfallen die Krankenhäuser im öffentlichen Bereich der Gesundheitsförderung, sodass die Zuständigkeiten zwischen Bund, Ländern und Gemeinden geteilt sind. Für die wirtschaftliche Sicherung der Krankenhäuser und die Pflegesätze begründet Nr. 19a eine Bundeskompetenz, von der auch intensiv Gebrauch gemacht wird.[240]

Die Kompetenz zur wirtschaftlichen Sicherung der Krankenhäuser ermöglicht Regelungen, die öffentlich-rechtlichen und privaten Krankenhäusern die für die notwendige Krankenhausversorgung der Bevölkerung erforderlichen finanziellen Mittel bereitstellen. Neben finanziellen Förderungsmaßnahmen gehören hierzu auch Regelungen über die Personalstruktur der Krankenhäuser, die Einkünfte der Ärzte, des nichtärztlichen Pflegepersonals und über die Klasseneinteilung des Krankenhauses, wenn diese Regelungen zur wirtschaftlichen Sicherung der Krankenhäuser erfolgen. Sogar Einschränkungen des Liquidationsrechts der Chefärzte (Ablieferungspflichten) sollen zulässig sein, wenn dabei die Grundsätze der Verhältnismäßigkeit und der Zumutbarkeit beachtet sind.[241]

Aus der hier vorliegenden Analyse ergibt sich der Befund, dass die unterschiedlichen Vorgaben des Bundes und der Länder für private und öffentlich-rechtliche Träger von Krankenanstalten einen administrativen und personellen Mehraufwand für die Durchführung von Forschungsvorhaben bedeuten. Sie können im Ergebnis auch dazu führen, dass Krankenhäuser in bestimmten Bundesländern an länderübergreifenden Forschungsvorhaben gar nicht erst beteiligt werden. Es ist

---

[239] 22. Gesetz zur Änderung des Grundgesetzes v. 12. 5. 69 (BGBl. I S. 363).

[240] z.B. Gesetz zur wirtschaftlichen Sicherung der Krankenhäuser und zur Regelung der Krankenhauspflegesätze (Krankenhausfinanzierungsgesetz) v. 29. 6. 1972 (BGBl. I S. 1009).

[241] Maunz/Dürig/Maunz, 86. EL Januar 2019, GG Art. 74 Rn. 220-223.

daher naheliegend und offensichtlich, dass allgemeine Regelungen zur Krankenhausplanung und -organisation in Bezug auf die Durchführung von länderübergreifenden Forschungsvorhaben einen Bezug zur wirtschaftlichen Sicherung der Krankenhäuser haben. Somit lässt sich eine bundeseinheitliche Vorgabe für länderübergreifende Forschungsvorhaben in Krankenhäusern auch auf diesen Kompetenzartikel des Grundgesetzes stützen.

#### dd) Erforderlichkeit einer bundesgesetzlichen Regelung aufgrund eines gesamtstaatlichen Interesses an einer Wahrung der Wirtschaftseinheit (Art. 72 Abs. 2 Alt. 2 GG)

##### aaa) Wahrung der Wirtschaftseinheit im gesamtstaatlichen Interesse

Ein Fall des Gesetzgebungsrechts des Bundes in Form der konkurrierenden Gesetzgebung liegt gem. Art. 72 Abs. 2 GG für den Bereich der Förderung wissenschaftlicher Forschung nach Art. 74 Nr. 13 GG vor, wenn die Wahrung der Rechts- oder Wirtschaftseinheit im gesamtstaatlichen Interesse eine bundesgesetzliche Regelung erforderlich macht. Es darf sich nicht um eine bloß sachlich nicht optimale Regelung, in welcher noch keine Beeinträchtigung der Funktionsfähigkeit gesehen werden, handeln.[242]

Die „Wahrung der Wirtschaftseinheit“ liegt im gesamtstaatlichen Interesse, wenn es um die Erhaltung der Funktionsfähigkeit des Wirtschaftsraums der Bundesrepublik durch bundeseinheitliche Rechtssetzung geht. Der Erlass von Bundesgesetzen zur Wahrung der Wirtschaftseinheit steht dann im gesamtstaatlichen, also im gemeinsamen Interesse von Bund und Ländern, wenn Landesregelungen oder das Untätigbleiben der Länder erhebliche Nachteile für die Gesamtwirtschaft mit sich bringen.[243] Sinn und Zweck des Art. 72 Abs. 2 Alt. 2 GG liegen darin, Schranken und Hindernisse für den wirtschaftlichen Verkehr im Bundesgebiet zu beseitigen.

Vorliegend dürfte die Wahrung der Wirtschaftseinheit im gesamtstaatlichen Interesse bundesgesetzliche Regelungen zur Förderung wissenschaftlicher Forschung erforderlich machen. Gegenstand der Wirtschaftseinheit ist auch die **Durchführung wissenschaftlicher Forschung**, denn der Begriff der „Wirtschaft“ in Art. 72 Abs. 2 GG ist in einem weiten Sinne zu verstehen und nicht nur auf den Begriff des „Rechts der Wirtschaft“ gem. Art. 74 Abs. 1 Nr. 11 Var. 1 GG bezogen.

Eine bundeseinheitliche Regelung datenschutzrechtlicher Vorgaben im Forschungsbereich würde zudem der „Wahrung der Wirtschaftseinheit“ dienen. Die wissenschaftliche Forschung der Krankenhäuser begegnet – betrachtet man den bundesweiten Wirtschaftsraum – durch die gegenwärtige landesgesetzliche Rahmengesetzgebung erheblichen Hürden. Länderübergreifende Forschungsvorhaben erfordern aufgrund der

---

[242] BVerfGE 111, 226, 254.
[243] BVerfG, Urteil vom 24.10.2002 - 2 BvF 1/01, in: NJW 2003, 41.

divergierenden datenschutzrechtlichen Regelungen einen personellen und finanziellen Mehraufwand. Die divergierenden Vorgaben benachteiligen Krankenhäuser aus Bundesländern mit höheren Anforderungen an die Datenverarbeitung, sei es, dass es sich um administrativ hohe Hürden handelt oder komplexe Voraussetzungen zu erfüllen sind. Auch der Wirtschaftsstandort als Ganzes kann benachteiligt werden, wenn ein ausländischer Sponsor einen anderen Forschungsstandort wegen einer homogeneren, weniger zersplitterten rechtlichen Situation bevorzugt. Die wissenschaftliche Forschung wird durch das sehr differenzierte Normengeflecht des Bundes und der Länder in ihrer Funktionsfähigkeit offensichtlich behindert. Insbesondere aufgrund des starken Aussagewertes multizentrischer Forschungsvorhaben, hat eine eingeschränkte Durchführbarkeit dieser Vorhaben enorme Auswirkungen auf die bundesweite Forschung von Krankenhäusern insgesamt.

Der „Wahrung" einer Wirtschaftseinheit steht auch nicht entgegen, dass mit einer Berufung auf die Bundeskompetenz zur Förderung der wissenschaftlichen Forschung erstmalig bundesweit einheitliche Datenschutzbestimmungen für die wissenschaftliche Forschung der Krankenhäuser geschaffen würden, denn bei der Wirtschaftseinheit der „Förderung wissenschaftlicher Forschung" handelt es sich um eine bereits etablierte Wirtschaftseinheit. Es geht bei den in Frage stehenden bundeseinheitlichen Datenschutzregelungen daher nicht um die erstmalige Herstellung der Wirtschaftseinheit, sondern um deren **Weiterentwicklung**. Die „Wahrung der Wirtschaftseinheit" beschränkt den Gesetzgeber jedoch gerade nicht auf die statische Verwaltung bereits bestehender Regelungen, sondern ermöglicht auch die **Schaffung neuer bundesgesetzlicher Regelungen**. Erforderlich ist dies beispielsweise in Fällen wirtschaftlicher Entwicklungen, die durch das geltende Recht keine hinreichende Berücksichtigung finden.[244] Entsprechendes muss daher gelten, wenn durch (datenschutz-)rechtliche Entwicklungen (auf Länderebene) der Wirtschaftseinheit Schranken setzen.

Eine Bundesgesetzgebung läge auch im **„gesamtstaatlichen Interesse".** Nicht die Interessen einzelner Länder erfordern eine Bundeszuständigkeit. Vielmehr sind die Gemeinwohlbelange der Gesamtheit betroffen, wenn, wie hier, eine dezentrale Regulierung sich bereits als erkennbar dysfunktional erwiesen hat.[245]

### bbb) Erforderlichkeit

Zur Wahrung der Wirtschaftseinheit im gesamtstaatlichen Interesse muss eine Bundeskompetenz auch „erforderlich" sein. Bei der Beurteilung der Erforderlichkeit verfügt der Bund über eine Einschätzungsprärogative, da die Wahrung des gesamtstaatlichen Interesses in seiner Zuständigkeit liegt. Der Bund muss seinen Eingriff in die Ländergesetzgebung jedoch nicht in gleichem Maße rechtfertigen wie im Falle eines Grundrechtseingriffs gegenüber dem Bürger. Eine Erforderlichkeit ist daher nur dann zu verneinen, wenn bereits eine Landesgesetzgebung durch im Wesentlichen gleichsinnige Landesgesetze das Vorhaben erreichen lässt.[246] Dies

[244] Uhle, in: Maunz/Dürig, Grundgesetz-Kommentar Werkstand: 86. EL Januar 2019, Art. 72, Rn. 157.
[245] Oeter, in: Mangoldt/Klein/Starck, Grundgesetz-Kommentar, 7. Auflage, Band 2, Art. 72, Rn. 112 f..
[246] Kunig, in: Münch/Kunig, Grundgesetz-Kommentar, 6. Auflage, Band 2, Art. 72, Rn. 27.

ist vorliegend nicht der Fall. Die Vereinfachung und Ermöglichung länderübergreifender Forschungsvorhaben **erfordert** nicht nur im Wesentlichen gleiche Voraussetzungen, sondern **bundesweit identische Regelungen**. Die Existenz nur marginal differenzierender rechtlicher Rahmenbedingungen führt zu einem erhöhten Verwaltungsaufwand und kann zu einem Scheitern eines Forschungsvorhabens führen.

### ccc) Rechtsprechung zu Art. 72 Abs. 2 GG

Die tatbestandlichen Voraussetzungen des Art. 72 Abs. 2 GG dürften insbesondere auch mit Blick auf die zu Art. 72 Abs. 2 GG ergangene Rechtsprechung des Bundesverfassungsgerichts vorliegen, wie ein Blick auf die hier kurz zusammengefassten Entscheidungen bezüglich dieses Topos zeigt:

- **„Filmförderung“:**[247]

  Das Bundesverfassungsgericht bestätigte die Bundeskompetenz gem. Art. 74 Abs. 1 Nr. 11, 72 Abs. 2 GG für eine Regelung des Filmförderungsgesetzes zur Erhebung einer Sonderabgabe („Filmabgabe“). Eine bundeseinheitliche Regelung sei zur Wahrung der Wirtschaftseinheit im gesamtstaatlichen Interesse erforderlich. Für Fortbestand und Weiterentwicklung der deutschen Filmwirtschaft sei eine von einer regionalen Standortbindung unabhängige Bundesförderung notwendig. Eine Bundesregelung zur Verwendung von Fördermitteln im gesamten deutschen Wirtschaftsraum sichere die Funktionsfähigkeit des Wirtschaftsraumes der Filmwirtschaft.

Eine vergleichbare Situation liegt hier insofern vor, als dass in im Filmförderungs-Urteil wie auch bei multizentrischen Forschungsvorhaben eine Verwendung von Fördermitteln über Ländergrenzen hinweg erfolgen soll. In beiden Konstellationen beeinträchtigt die Begrenzung der länderabhängige Mittelverwendung die Funktionsfähigkeit des Wirtschaftsraumes.

- **„Erbschaftssteuer“:**[248]

  Für die vorgelegten Normen gem. §§ 13a, 13b ErbStG (Befreiungen von der Erbschafts- und Schenkungssteuer beim unentgeltlichen Übergang betrieblichen Vermögens) stützte sich das Bundesverfassungsgericht auf eine Bundesgesetzgebungskompetenz nach Art. 105 Abs. 2, 72 Abs. 2 GG. Das Gericht hielt eine bundesgesetzliche Regelung zur Wahrung der Rechts- und Wirtschaftseinheit im gesamtstaatlichen Interesse für erforderlich. Bei einer Ländergesetzgebung drohe eine Rechtszersplitterung mit nicht unerheblichen Nachteilen für Erblasser, Erwerber und Finanzverwaltung. Je nach Wohnsitz des Erblassers und Betriebssitz oder Belegenheit der Sache käme es zu konkurrierenden Steueransprüchen

[247] BVerfG, Urteil vom 28. Januar 2014 – 2 BvR 1561/12, NVwZ 2014, 646.
[248] BVerfG, Urteil vom 17.12.2014 – 1 BvL 21/12, NJW 2015, 303.

mehrerer Länder. Um Mehrfachbelastungen zu vermeiden, wäre ein erheblicher Koordinierungs- und Administrierungsaufwand erforderlich. Bei Unternehmen mit mehreren Betriebsstätten würden sich zudem schwierige Abgrenzungsschwierigkeiten ergeben.

Das Bundesverfassungsgericht stützte sich hier auf einen erhöhten Koordinierungs- und Verwaltungsaufwand sowie auf Abgrenzungsschwierigkeiten bei Fragen der Rechtsanwendung, um die Beeinträchtigung von Rechts- und Wirtschaftseinheit zu begründen. Die hier vom Bundesverfassungsgericht herangezogenen Argumente entsprechen den Beobachtungen, die sich in dieser Analyse durch den Vergleich der unterschiedlichen, landesspezifischen Rechtsvorschriften ergeben. Störungen im Ablauf klinischer Prüfungen können auftreten, wenn während einer Studie durch den Eigentümerwechsel des Krankenhauses oder Prüfzentrums ein anderer Rechtsrahmen zu beachten ist, Beteiligte der klinischen Prüfung durch Wohnort- oder Arbeitgeberwechsel anderen Vorschriften unterfallen und bei multizentrischen Forschungsvorhaben Teilnehmer aus anderen Rechtskreisen hinzutreten.

- **„Altenpflege“:**[249]

  Im Altenpflegeurteil wurde eine Bundesgesetzgebungskompetenz gem. Art. 74 Abs. 1 Nr. 19, 72 Abs. 2 GG für die Regelungen des Altenpflegegesetzes zur Berufsausbildung der Altenpfleger bestätigt. Eine Bundesgesetzgebung diene in diesem Bereich dem Ziel der Wahrung der Wirtschaftseinheit: Zwischen den Ländern divergierende Ausbildungsregelungen und unklare Konturen des Altenpflegeberufes resultierten nach Ansicht des Bundesverfassungsgerichtes in einer mangelnden Attraktivität des Pflegeberufes und einer unzureichenden Zahl an Pflegekräften. Diese sich mittelbar aus unterschiedlichen Länderregelungen ergebende negative wirtschaftliche Auswirkungen sollten über eine bundeseinheitliche Regelung vermieden werden. Durch Bundesgesetz sollte dem Fachkräftemangel entgegengewirkt, die bundesweite Mobilität gestärkt und so eine gleichmäßige Verteilung des wirtschaftlichen Potentials im gesamten Bundesgebiet erreicht werden. Das Altenpflegegesetz wurde für erforderlich gehalten, da eine bundesweite Wirtschaftseinheit durch die bislang praktizierte Ländergesetzgebung nicht erreicht worden und als „milderes Mittel“ eine koordinierte Landesgesetzgebung nicht möglich sei.

Lediglich mittelbar aus unterschiedlichen Länderregelungen resultierende Beeinträchtigungen der Wirtschaftseinheit reichten im Altenpflegeurteil aus, um die Erforderlichkeit einer bundeseinheitlichen Regelung anzunehmen. Erst recht müssen dann aber unmittelbare Hemmnisse für die Funktionsfähigkeit der Wirtschaftseinheit eine Bundesregelung begründen können. Derartige unmittelbare Hemmnisse liegen vor,

[249] BVerfG, Urteil vom 24. 10. 2002 - 2 BvF 1/01, NJW 2003, 41.

wenn länderübergreifende wirtschaftliche Tätigkeiten mangels bundeseinheitlicher Regelungen gar nicht erst ausgeführt werden können – wie auch im Fall multizentrischer Forschungsvorhaben.

#### ee) Zwischenergebnis

Sowohl aus dem Kompetenztitel des Rechts der Wirtschaft, wie auch aus den Titeln zur Förderung der wissenschaftlichen Forschung und der wirtschaftlichen Sicherung der Krankenhäuser ergeben sich Argumente für eine Gesetzgebungskompetenz des Bundes, die sich auch mit der von der Verfassung aufgestellten Notwendigkeit einer gesamtstaatlichen Regelung unterfüttern lassen. In der Gesamtschau der Kompetenztitel erweist sich das Recht der Förderung der wissenschaftlichen Forschung als besonders plausibel: Die Länder haben von ihrer Gesetzgebungskompetenz für die Krankenhäuser in Trägerschaft der öffentlichen Stellen des Landes vielerorts Gebrauch gemacht und Vorgaben für die Datenverarbeitung in der wissenschaftlichen Forschung erstellt, die im Vergleich zur bundeseinheitlichen Anwendung von DS-GVO und BDSG ohne hinreichenden Grund überkomplex sind. Um diese Hindernisse zu beseitigen und die Forschung zu fördern ist der Kompetenztitel nach Paragraf Art. 73 Abs. 1 Nr. 13 GG als „passgenau“ anzusehen.

## 2. Materiellrechtlicher Regelungsbedarf

### a) Forschungsklausel

Für die Forschung mit personenbezogenen Gesundheitsdaten ist der rechtliche Regelungsrahmen im Bundesrecht gegenwärtig in § 27 BDSG verankert. Dieser gilt für Einrichtungen in privater Trägerschaft („nicht-öffentliche Stellen“), wie etwa Arztpraxen und medizinische Versorgungszentren (soweit sie nicht in Trägerschaft von Krankenhäusern des Landes stehen), sonstige privatrechtlich geführte Forschungseinrichtungen und Forschungseinrichtungen des Bundes. Für die Datenverarbeitung durch Krankenhäuser in Trägerschaft der öffentlichen Stellen der Länder besteht gegenwärtig keine Regelung auf der Ebene des Bundes, weder im BDSG noch andernorts, noch ließe sich eine solche aus der DS-GVO herleiten, da diese über die Öffnungsklauseln in Art. 9 die diesbezügliche Kompetenz den Mitgliedstaaten zuweist. Um die Anwendung einheitlichen Rechts bei länderübergreifenden Forschungsvorhaben auch einschließlich der Krankenhäuser in Trägerschaft einer öffentlichen Stelle eines Landes zu gewährleisten, ist es geboten, dieses im Gleichklang mit dem Recht der öffentlichen Stellen des Bundes und der nicht-öffentlichen Stellen umzusetzen. Eine entsprechende Regelung sollte daher im Bundesdatenschutzgesetz verortet werden, in dem sie sich sachgerecht, praktikabel und systemkonform implementieren ließe.

### b) Federführende Aufsichtsbehörde

Für ein Forschungsvorhaben, in das Krankenhäuser in öffentlich-rechtlicher Trägerschaft des Landes aus mehreren Bundesländern eingebunden sind, ergeben sich entsprechend der jeweiligen Gesetzgebung des

Bundeslandes die Zuständigkeit derjenigen Aufsichtsbehörde des jeweiligen Bundeslandes. So regelt etwa § 6 Abs. 1 des Thüringischen Landesdatenschutzgesetzes die Aufgaben des Landesbeauftragten für den Datenschutz (Artikel 57 und 31 der Verordnung (EU) 2016/679, Artikel 46 und 26 der Richtlinie (EU) 2016/680):

> *„Der Landesbeauftragte für den Datenschutz nimmt gegenüber den öffentlichen Stellen des Landes die Aufgaben nach Artikel 57 der Verordnung (EU) 2016/679 wahr. Dabei kontrolliert er die Einhaltung der Verordnung (EU) 2016/679, dieses Gesetzes sowie anderer datenschutzrechtlicher Bestimmungen."*

Für ein multizentrisches Forschungsvorhaben mit beispielsweise vier Krankenhäusern aus drei Bundesländern sind somit drei Aufsichtsbehörden gleichzeitig zuständig. Hieraus ergibt sich nicht nur eine unwirtschaftliche Befassung dreier Behörden mit einem Sachverhalt, sondern auch das Risiko unterschiedlicher Bewertungen mit nachfolgender Rechtsunsicherheit. Das Instrument der „federführenden Aufsichtsbehörde" ermöglicht in länderübergreifenden Forschungsprojekten die Vermeidung unwirtschaftlicher Behördentätigkeit und divergierender Auffassungen.

### aa) Regulatorischer Rahmen

Die Einführung einer federführenden Aufsichtsbehörde auf europäischer Ebene gemäß Art. 56 Abs. 1 DS-GVO bei grenzüberschreitenden Verarbeitungen hat dazu geführt, dass auch auf nationaler Ebene mit § 40 Abs. 2 BDSG Zuständigkeitsregelungen für die Aufsichtsbehörden bei Datenverarbeitungen eines Verantwortlichen mit mehreren Niederlassungen getroffen wurden.

Die §§ 18 und 19 BDSG regeln hingegen lediglich die Zusammenarbeit des Bundes und der Länder im Zusammenhang mit dem Kohärenzverfahren. Das ist dem Umstand geschuldet, dass die in Kapitel VII der DS-GVO geregelten Verfahren der Zusammenarbeit und Kohärenz zwar Zuständigkeitsverteilungen und Verfahrensregelungen zwischen den Aufsichtsbehörden verschiedener Mitgliedstaaten enthalten, aber keine Einzelheiten der innerstaatlichen Koordination und Willensbildung in Mitgliedstaaten mit mehr als einer Aufsichtsbehörde normieren. § 18 BDSG trifft daher eine konkrete Regelung zur Zusammenarbeit der Aufsichtsbehörden des Bundes und der Länder in Angelegenheiten der Europäischen Union. Er enthält allgemeine Grundsätze der Zusammenarbeit im europäischen Kontext und legt fest, wie Einvernehmen über einen gemeinsamen Standpunkt erzielt werden soll. § 18 Abs. 1 BDSG soll nach dem Willen des Gesetzgebers alle Fallgestaltungen erfassen, in denen aufgrund der Wirkung für und gegen die übrigen deutschen Datenschutzbehörden und deren Vollzugsentscheidungen eine inhaltliche Vorabstimmung erforderlich ist.[250] Der Begriff des „gemeinsamen Standpunkts" wird nicht legal definiert. Es handelt sich hierbei um den Inhalt der

[250] BT-Drs. 18/11325, 90.

gemeinsamen Positionierung, die die deutschen Datenschutzaufsichtsbehörden in das Verfahren der Zusammenarbeit und Kohärenz nach Kapitel VII DS-GVO und die Beratungen des EDSA einbringen.[251]

Auch § 19 BDSG bezieht sich allein auf die Zuständigkeiten und Verfahren der Zusammenarbeit und Kohärenz nach Kapitel VII DS-GVO.[252] Die Vorschrift trifft keine Regelung zur Bestimmung der zuständigen deutschen Datenschutzaufsichtsbehörde in Fällen der länderübergreifenden, aber rein nationalen Datenverarbeitung.[253]

Vorgaben zur Bestimmung der zuständigen Aufsichtsbehörde bei ausschließlich inländischen Sachverhalten macht hingegen § 40 Abs. 2 BDSG für die Datenverarbeitung durch nichtöffentliche Stellen. Für den Fall, dass ein Verantwortlicher oder Auftragsverarbeiter mehrere inländische Niederlassungen hat, findet demnach Art. 4 Nr. 16 DSG-VO, der die Hauptniederlassung legaldefiniert, entsprechend Anwendung.

Die Norm erfasst aber zum einen nur nicht-öffentliche Stellen und zum anderen nur die Situation, dass ein Verantwortlicher mehrere Niederlassungen hat. Im Zusammenhang mit länderübergreifenden Forschungsvorhaben sind aber in der Regel sowohl öffentliche Stellen als auch mehrere Verantwortliche beteiligt. Gleichwohl kann an diese Regelung angeknüpft werden. Es ist allerdings insofern erforderlich an den Sachzusammenhang anzuknüpfen und nicht an den Verantwortlichen.

Die Bündelung der Zuständigkeit datenschutzrechtlicher Aufsicht bei länderübergreifenden Forschungsvorhaben auf eine Aufsichtsbehörde würde zudem den erheblichen Vorteil einer Entlastung für die anderen Datenschutzbeauftragten mit sich bringen. Für ein Forschungsvorhaben im Rahmen der Medizininformatik-Initiative mit Beteiligten in neun Bundesländern wäre dann statt neun Aufsichtsbehörden lediglich eine Aufsichtsbehörde zuständig.

### bb) Verortung im nationalen Recht

Die Neuordnung der Zuständigkeit einer federführenden Aufsichtsbehörde bei länderübergreifenden Forschungsvorhaben mit mehreren Verantwortlichen sollte im Bundesdatenschutzgesetz verortet werden.

## c) Anwendung auf kirchliche Krankenhäuser

Die Ausdehnung der beiden vorgenannten Regelungen sollte auf kirchliche Krankenhäuser ebenfalls im Bundesdatenschutzgesetz erstreckt werden.

---

[251] Kisker, in: Wolff/Brink, BeckOK Datenschutzrecht, 28. Edition, Stand: 01.05.2019, § 18 BDSG, Rn. 5.
[252] BT-Drs. 18/11325, 92.
[253] Kisker, in: Wolff/Brink, BeckOK Datenschutzrecht, 28. Edition, Stand: 01.05.2019, § 19 BDSG.

### d) Datenspende

Die Ausgestaltung eines Regelungsrahmens für die Datenspende gestaltet sich als besonders anspruchsvoll, da hierzu im EU-rechtlichen Regelungskontext keine Öffnungsklauseln für die Zweckbindung und das Löschungsgebot nach Widerruf der Einwilligung existieren. Eine entsprechender Regelungsansatz erscheint dennoch gleichfalls im Rahmen für die Zwecke der wissenschaftlichen Forschung mit besonderen Kategorien personenbezogener Daten in § 27 BDSG sinnvoll.

## 3. Zwischenergebnis

Wir halten eine Regelung auf Bundesebene, die sowohl die Verarbeitung personenbezogener Daten in länderübergreifenden Forschungsvorhaben ermöglicht als auch die Zuständigkeiten der Aufsichtsbehörden insofern neu strukturiert, als in solchen Forschungsvorhaben jeweils nur eine Aufsichtsbehörde zuständig ist, für ein geeignetes Mittel der Harmonisierung des Datenschutzrechts bei länderübergreifenden Forschungsvorhaben. Ergänzend können in diesem Kontext die Einbindung der kirchlichen Krankenhäuser und die Datenspende geregelt werden.

## IV. Kollisionsnormen in Landeskrankenhausgesetzen

Eine weitere Möglichkeit der Harmonisierung des bereichsspezifischen Datenschutzrechts ist die Einfügung von Kollisionsnormen in die Landeskrankenhausgesetze, die im Fall von länderübergreifenden Forschungsvorhaben Bundesrecht für anwendbar erklären. Der Zweck der Norm stellte sich dabei gleichwertig dar: Eine Benachteiligung des Krankenhauses gegenüber Krankenhäusern in Bundesländern mit anderen Forschungsklauseln/-beschränkungen wird im Interesse der tragenden Körperschaft vermieden. Die legislative Vermutung eines ausreichenden Schutzes durch die bundesgesetzliche Regelung bzw. deren Verweis auf die DS-GVO/Ausfüllung der Öffnungsklausel ließe sich übertragen. In diesem Modell behalten die Länder die Hoheit über Datenverarbeitung in Krankenhäusern ihres Landes und geben nur anlassbezogen einem anderen Rechtsrahmen, dem des BDSG, Raum. Dies ist eine Vorgehensweise, die nicht nur über die Wettbewerbsklausel, sondern hinsichtlich der Durchführung der Rechtsaufsicht über die Verantwortlichen in privater Trägerschaft ohnehin bereits Rechtsrealität ist.

## V. Verfassungsänderung

Vor dem Hintergrund der Komplexität des Gesundheitsdatenschutzrechts und damit einhergehenden Doppelungen und Inkonsistenzen, die zu Rechtsunsicherheit und Wertungswidersprüchen führen, fordern Kühling und Kingreen die Einführung eines einheitlichen Gesundheitsdatenschutzgesetzes des Bundes.[254] Da dem Bund insofern die Gesetzgebungskompetenz fehlt, wird in diesem Zusammenhang die Schaffung einer spezifisch auf das Datenschutzrecht bezogenen Gesetzgebungskompetenz diskutiert.[255] Nur so könnten sektorspezifische

[254] Kingreen/Kühling, Gesundheitsdatenschutzrecht, 2015, S. 468.
[255] Kingreen/Kühling, Gesundheitsdatenschutzrecht, 2015, S. 469.

Vorgaben – nicht nur im Gesundheitswesen, sondern auch in anderen Bereichen –abgebaut und in das allgemeine Datenschutzrecht reintegriert werden. Besondere Gründe für eine föderalistische Ausgestaltung seien jedenfalls im Hinblick auf das Gesundheitsdatenschutzrecht nicht erkennbar.[256] Die auf Bundesebene erforderliche Gesetzgebungskompetenz solle als konkurrierende Kompetenz in den Katalog des Art. 74 GG aufgenommen und der Erforderlichkeitskontrolle des Art. 72 Abs. 2 unterworfen werden.[257]

Die Einführung eines Gesundheitsdatenschutzgesetzes ist aus unserer Sicht durchaus erstrebenswert, wird aber allenfalls ein langfristiges Ziel sein. Die Autoren räumen selbst ein, dass diese weitreichende Forderung jedenfalls kurzfristig nicht umsetzbar sein dürfte.[258] Es ist daher nach unserem Dafürhalten wichtig, dieses Konzept weiter zu entwickeln, gleichwohl sollten kurzfristig Maßnahmen getroffen werden, die – wie die Harmonisierung der Rechtsgrundlagen und die Zuständigkeit der Aufsicht im Zusammenhang mit länderübergreifender Forschung – keine Verfassungsänderung erfordern, aber gleichwohl einige der Herausforderungen adressieren. Die diesbezügliche Vereinheitlichung der bereichsspezifischen Vorschriften führt zu einer Aufwertung des Forschungsstandorts Deutschlands und beseitigt damit einen beachtlichen Standortnachteil.

## VI. Verhaltensregeln / Codes of Conduct

### 1. Allgemeines

Ein möglicher Ansatz zur Umsetzung rechtlicher Lösungen für die in diesem Gutachten aufgezeigten Herausforderungen des Datenschutzes in der medizinischen Forschung könnten die Verhaltensregeln nach Art. 40 DS-GVO sein. Art. 40 DS-GVO enthält Regelungen zum zulässigen Inhalt von Verhaltensregeln und zu den Vorlageberechtigten eines Entwurfs von Verhaltensregeln sowie zu Genehmigung, Kontrolle und Widerruf dieser Verhaltensregeln.

Diese Verhaltensregeln sind ein bereits seit längerem bekanntes Instrument der Selbstregulierung.[259] Schon nach dem alten Bundesdatenschutzgesetz konnten Berufsverbände und Vereinigungen Verhaltensregeln erstellen und sie einer zuständigen Aufsichtsbehörde zur Prüfung und Genehmigung vorlegen.[260] Die Rechtsgrundlage im europäischen Recht war Art. 27 der Richtlinie 95/46/EG. In der Praxis wurde von dieser Option allerdings wenig Gebrauch gemacht. In Deutschland haben **bisher nur zwei Verhaltensregeln** das Licht der Welt erblickt: Zum

[256] Kingreen/Kühling, Gesundheitsdatenschutzrecht, 2015, S. 469.
[257] Kingreen/Kühling, Gesundheitsdatenschutzrecht, 2015, S. 470 f.
[258] Kingreen/Kühling, Gesundheitsdatenschutzrecht, 2015, S. 471.
[259] Taeger/Gabel/Kinast, 3. Aufl. 2019, DS-GVO Art. 40 Rn. 5; ähnlich: Sydow, Europäische Datenschutzgrundverordnung, DSGVO Art. 40 Rn. 1.
[260] Vgl. § 38a BDSG a.F..

einen die Verhaltensregeln der Versicherungswirtschaft[261] und zum anderen der GeoBusiness Code of Conduct.[262]

Trotz der historischen Zurückhaltung mit diesem Instrument hat der europäische Gesetzgeber etwas Vergleichbares in Art. 40 der DS-GVO erneut vorgesehen. Die Vorschrift beschreibt nicht nur die Möglichkeit, solche Verhaltensregeln zu entwickeln und genehmigen zu lassen, sondern kleidet sie insgesamt in das Gewand eines **Förderauftrags an die Mitgliedstaaten**, die Aufsichtsbehörden, den Ausschuss und die Kommission. Diese fördern gem. Abs. 1 der Vorschrift

> *„die Ausarbeitung von Verhaltensregeln, die nach Maßgabe der Besonderheiten der einzelnen Verarbeitungsbereiche und der besonderen Bedürfnisse von Kleinstunternehmen sowie kleinen und mittleren Unternehmen zur ordnungsgemäßen Anwendung dieser Verordnung beitragen sollen".*

Die Funktion der Verhaltensregeln ist die einer **Präzisierung der Vorgaben der Datenschutz-Grundverordnung**, denn die Verordnung ist an vielen Stellen unbestimmt und die zahlreichen Öffnungsklauseln erweitern den Spielraum für den nationalen Gesetzgeber, der freilich auch nicht immer genutzt wird. Hinzu kommt, dass die Verordnung nicht sektorspezifisch ausgerichtet wurde, sodass ein Bedarf für eine **sektorspezifische Präzisierung** und Konkretisierung für die Besonderheiten des jeweiligen Sektors besteht.

Verhaltensregeln sollen nicht die Rechtsgrundlage für die Verarbeitung personenbezogener Daten aus der DS-GVO, aber deren wirksame Anwendung erleichtern. Auch Erwägungsgrund 98 betont, dass den Besonderheiten der in bestimmten Sektoren erfolgenden Verarbeitungen und den besonderen Bedürfnissen der Kleinstunternehmen, sowie der kleinen und mittleren Unternehmen Rechnung zu tragen ist. Art. 40 Abs. 1 DSGVO verknüpft den Förderungsauftrag daher mit einer spezifischen Zielsetzung: Die Förderung soll nicht nach dem „Gießkannenprinzip" entwickelt und umgesetzt werden, sondern sich vorrangig auf KMU beziehen. Dadurch soll gerade kleineren Entitäten der Umstieg auf die und die Anwendung der DSGVO erleichtert werden. Diese Hervorhebung von Kleinstunternehmen sowie kleinen und mittleren Unternehmen schließt aber nicht aus, dass im Rahmen von Verhaltensregeln auch Besonderheiten von Großunternehmen berücksichtigt und geregelt werden.[263]

Genehmigte Verhaltensregeln sind daher eine Hilfestellung zur Anwendung und Umsetzung des europäischen Datenschutzrechts mit einer sektorspezifischen Ausrichtung, und zwar sowohl für die

---

[261] https://www.gdv.de/resource/blob/23938/4aa2847df2940874559e51958a0bb350/download-code-of-conduct-data.pdf
[262] https://www.bmwi.de/Redaktion/DE/Publikationen/Geobusiness/publikation-code-of-conduct.pdf?__blob=publicationFile&v=4
[263] Sydow, Europäische Datenschutzgrundverordnung, DSGVO Art. 40 Rn. 18; Taeger/Gabel/Kinast, 3. Aufl. 2019, DS-GVO Art. 40 Rn. 13.

Verarbeitungsverantwortlichen (Controller) wie auch für die Auftragsverarbeiter (Processor) durch Präzisierung ihrer Pflichten. Zugleich beinhalten sie eine obligatorische Überwachung der Einhaltung. Nicht nur die Gestaltung und Regulierung erfolgt dabei auf freiwilliger Basis, sondern auch die Beteiligung der Verantwortlichen und Auftragsverarbeiter. Die Verhaltensregeln werden auf privatrechtlicher Grundlage erstellt und erst durch entsprechende Vereinbarung des Beitritts von Controller oder Prozessor wirksam, mit der sich dieser den Verhaltensregeln auch unterwirft.[264]

## 2. Zielsetzung von Verhaltensregeln

Verhaltensregeln sollen zur ordnungsgemäßen Anwendung der Datenschutz-Grundverordnung beitragen und Besonderheiten der einzelnen Verarbeitungsbereiche und der besonderen Bedürfnisse von Kleinstunternehmen sowie kleinen und mittleren Unternehmen einbeziehen. Insoweit ähneln sie Leitlinien und bilden eine gute Datenschutzpraxis ab, wie dies auch für technische Normen von Sachverständigen spezifischer Fachbereiche zutrifft. Daraus resultiert eine gewisse Standardisierung der Datenverarbeitung im Zusammenhang mit typischen Dienstleistungen und Produkten, die **branchenspezifisch auch die Interessen der Betroffenen** berücksichtigen kann.[265]

Verhaltensregeln sollen auch eine praxisnahe Interpretationshilfe für Unternehmen sein,[266] und dadurch eine gewisse Sicherheit bewirken, die Vorgaben der DS-GVO auch einhalten zu können.[267] Kurz gesagt, schließen sie Lücken der teilweise abstrakt gehaltenen DS-GVO vermittels einer besonderen Form der Selbstregulierung der Wirtschaft.[268] Zugleich ist aber ausgeschlossen, dass die Kontrolltätigkeit der Aufsichtsbehörden eingeschränkt oder das Datenschutzniveau abgesenkt wird. Die Verhaltensregeln haben daher das Potenzial, auf dem bestehenden Datenschutzniveau eine Konkretisierung und damit zugleich eine **Vereinheitlichung** zu bewirken, die insbesondere für die Schaffung **von Rechtssicherheit über Ländergrenzen** hinweg fruchtbar gemacht werden kann.[269] Dies gilt natürlich auch für vereinheitlichende Ansätze **innerhalb eines Mitgliedstaates**, wenn durch föderalistische Prinzipien eine innerstaatliche Differenzierung bei der Umsetzung der Öffnungsklauseln entstanden ist.

Die rechtliche Wirkung einer Verhaltensregel besteht auch darin, dass die Aufsichtsbehörde an die Verhaltensregel gebunden ist und die Konkretisierung der DSGVO durch diese **akzeptieren muss**. Im Ergebnis

---

[264] Ehmann/Selmayr/Schweinoch DS-GVO Art. 40 Rn. 1, 2.
[265] Sydow, Europäische Datenschutzgrundverordnung, DSGVO Art. 40 Rn. 3.
[266] Taeger/Gabel/Kinast, 3. Aufl. 2019, DS-GVO Art. 40 Rn. 5.
[267] Taeger/Gabel/Kinast, 3. Aufl. 2019, DS-GVO Art. 40 Rn. 5, m.V.a.: Laue/Nink/Kremer, Das neue Datenschutzrecht in der betrieblichen Praxis, § 8 Rn. 20.
[268] Taeger/Gabel/Kinast, 3. Aufl. 2019, DS-GVO Art. 40 Rn. 5.
[269] Kranig/Peintinger, ZD 2014, 3, 8.

kann daher ein Verhalten, das sich an einer genehmigten Verhaltensregel ausrichtet, nicht von einer Aufsichtsbehörde beanstandet werden.[270]

## 3. Regelungsgegenstände der Verhaltensregeln nach Art. 40 DS-GVO

Art. 40 Abs. 2 DS-GVO beschreibt mögliche Regelungsgegenstände von Verhaltensregeln i.S.v. Art. 40 DS-GVO sowie deren Grenzen.

### a) Präzisierung der Datenschutz-Grundverordnung sowie nationaler Datenschutzvorschriften

Nach Art. 40 Abs. 2 DS-GVO dienen Verhaltensregeln der Präzisierung der Anwendung der Datenschutz-Grundverordnung. Fraglich ist, ob neben der Anwendung der Datenschutz-Grundverordnung auch die Anwendung nationaler Datenschutzvorschriften durch Verhaltensregeln nach Art. 40 DS-GVO konkretisiert werden können. Für diese Möglichkeit spricht, dass das nationale Datenschutzrecht auf den Öffnungsklauseln der Datenschutz-Grundverordnung basiert und damit einen direkten Bezug zu ihr aufweist. Dafür spricht auch, dass mit Verhaltensregeln Besonderheiten der einzelnen Verarbeitungsbereiche besondere Berücksichtigung finden sollen (Art. 40 Abs. 1 DS-GVO). Dabei würde das Ausblenden nationaler Datenschutzvorschriften zu erheblichen Lücken führen.

### b) Katalog möglicher Regelungsgegenstände

Zur Förderung des Austauschs von Patientendaten bei grenzüberschreitenden Forschungsvorhaben kommt aus dem Katalog des Art. 40 Abs. 2 DS-GVO insbesondere eine Präzisierung der berechtigten Interessen des Verantwortlichen in bestimmten Zusammenhängen (Art. 40 Abs. 2 lit. b) DS-GVO), der Erhebung personenbezogener Daten (Art. 40 Abs. 2 lit. c) DS-GVO) sowie der Pseudonymisierung personenbezogener Daten (Art. 40 Abs. 2 lit. d) DS-GVO) in Betracht. Der Katalog möglicher Regelungsgegenstände in Art. 40 Abs. 2 DS-GVO ist nicht abschließend[271], so dass auch weitere Regelungsgegenstände in Betracht kommen.

Im Hinblick auf die unterschiedlichen datenschutzrechtlichen Vorgaben der Landesdatenschutzgesetze und Landeskrankenhausgesetze ist vorstellbar, durch Verhaltensregeln Kriterien aufzustellen, die für die **Abwägung zwischen dem Forschungsinteresse des Verantwortlichen und dem Interesse des Betroffenen** gelten. Bei Einhaltung dieser Kriterien wären dann auch die Aufsichtsbehörden der Bundesländer an diese gebunden und müssten eine entsprechende Umsetzung des Forschungsvorhabens akzeptieren oder eine gegebenenfalls notwendige Genehmigung erteilen. Ebenso vorstellbar ist dies für die Anforderungen an die **Pseudonymisierung**, die in einigen Landeskrankenhausgesetzen explizit angesprochen wird. Schließlich scheint auch das Thema der

[270] Taeger/Gabel/Kinast, 3. Aufl. 2019, DS-GVO Art. 40 Rn. 53
[271] Taeger/Gabel/Kinast, 3. Aufl. 2019, DS-GVO Art. 40 Rn. 27.

**Datenspende** hinsichtlich der Abwägung zur Vereinbarkeit des Forschungszwecks mit dem ursprünglich Zweck („Kompatibilitätsprüfung“) dafür geeignet.

### c) Grenzen

Verhaltensregeln dienen der Präzisierung[272]. Nach herrschender Auffassung dürfen durch Verhaltensregeln weder die Vorgaben der DS-GVO unterschritten werden[273] noch dürfen sie den Wortlaut der DS-GVO schlicht wiederholen, ohne einen „Mehrwert“[274] darzustellen. Art. 40 Abs. 1 DS-GVO lässt offen, „ob Verhaltensregeln inhaltlich über die Anforderungen der DSGVO hinausgehen dürfen.“[275] Von einem Teil der Literatur wird das „Aufstellen strengerer Regeln“ als unzulässig betrachtet.[276]

Durch Verhaltensregeln kann jedoch nicht die Gesetzeslage verändert werden, und zwar weder auf der Ebene der Europäischen Union, noch auf der legislativen Ebene der Mitgliedstaaten oder ihrer föderalen Untergliederungen, beispielsweise der Bundesländer. Es ist also **nicht möglich** durch Verhaltensregeln einschränkende Regelungen der Landesdatenschutzgesetze, der Landeskrankenhausgesetze oder des Gesundheitsdienstes-Datenschutzgesetzes NRW **aufzuheben oder anzugleichen**. Deren Bestand wird von Verhaltensregeln nicht tangiert. Hilfreich könnten Verhaltensregeln aber dort sein, wo durch Auslegungsspielräume Rechtsunsicherheiten entstehen.

Auch ist vorstellbar, Verhaltensregeln aufzustellen, deren Inhalt einen vollständigen und für alle Beteiligten akzeptablen Rahmen der Datenverarbeitung mit Forschungsdaten im ambulanten oder stationären Bereich oder anderen Bereichen wiedergibt, sodass im Wissen um die Existenz eines solchen Rechtsrahmens **vorhandene legislative Beschränkungen** durch den jeweiligen Gesetzgeber **aufgehoben** werden könnten. Es ist allerdings fraglich, ob Verhaltensregeln, die gegen nationales Recht verstoßen (es sei denn, dieses Recht stellt wiederum einen Verstoß gegen die DS-GVO dar), von einer Aufsichtsbehörde genehmigt werden dürfen. Auch wenn der Wortlaut der Norm nur auf die Vereinbarkeit mit der DS-GVO abstellt, muss u.E. analog zu den obigen Erwägungen (III.1.) auch die Vereinbarkeit mit nationalem Recht gewährleistet sein.

Ferner ist zu beachten, dass die Öffnungsklauseln, etwa für die Verarbeitung von personenbezogenen Gesundheitsdaten zu Forschungszwecken im Sinne des Artikels 9 Abs. 2 lit. j) DS-GVO durch das Sekundärrecht der Europäischen Union oder mitgliedstaatliche Gesetzgebung ausgefüllt werden müssen, um die

---

[272] Beispielsweise durch „Aufstellen von Regelbeispielen, Konkretisierung von branchentypischen Prozessen oder auch technischer Spezifikationen.“, Taeger/Gabel/Kinast, 3. Aufl. 2019, DS-GVO Art. 40 Rn. 31.

[273] Taeger/Gabel/Kinast, 3. Aufl. 2019, DS-GVO Art. 40 Rn. 29; m.V:a.: Raschauer, in: Sydow, EU-Datenschutzgrundverordnung, Art. 40 Rn. 5; Paal, in: Paal/Pauly, DS-GVO BDSG, Art. 40 Rn. 15.

[274] Taeger/Gabel/Kinast, 3. Aufl. 2019, DS-GVO Art. 40 Rn. 29.

[275] Taeger/Gabel/Kinast, 3. Aufl. 2019, DS-GVO Art. 40 Rn. 28.

[276] Taeger/Gabel/Kinast, 3. Aufl. 2019, DS-GVO Art. 40 Rn. 31.

Datenverarbeitung überhaupt erst zu ermöglichen. [277] Ein Ersatz dieser Ausgestaltung durch Verhaltensregeln ist nicht möglich, denn Verhaltensregeln werden nur anwendbar für diejenigen Rechtssubjekte, die durch einen aktiven Anerkennungsprozess den Verhaltensregeln beitreten.

## 4. Vorlageberechtigte

Art. 40 DS-GVO benennt die Vorlageberechtigten. Nach Art. 40 Abs. 2 DS-GVO können Verbände[278] und andere Vereinigungen, die Kategorien von Verantwortlichen oder Auftragsverarbeitern vertreten, Verhaltensregeln ausarbeiten oder ändern oder erweitern. Darunter können neben Verbänden und Vereinen alle anderen freiwilligen Zusammenschlüsse fallen.[279]

Folgende Voraussetzungen müssen erfüllt sein:

- Vertretung von Verantwortlichen oder Auftragsverarbeitern (nicht z.B. Vertretung von Betroffenen)[280]
- Vertretung einer Gruppe von Verantwortlichen oder Auftragsverarbeitern[281]
- Gewisses Maß an Homogenität hinsichtlich der vertretenen Gruppe[282]
- Gewisses Maß an Repräsentanz[283]

Folgende Voraussetzungen müssen hingegen nicht erfüllt sein:

- Die vertretene Gruppe muss weder vollständig noch in wesentlichen Teilen vertreten sein.[284]
- Eine wirtschaftliche Zielrichtung ist nicht erforderlich[285]

In Ansehung dieser Vorgaben sind beispielsweise AWMF, BVITG, BVMed, GVG, Deutsche Krankenhausgesellschaft, Spectaris, TMF vorlageberechtigt. Für ein Mitgliedstaats-übergreifendes Vorhaben sollten Verbände tätig werden, die auch in mehreren Mitgliedsstaaten tätig sind, z.B. EHTEL.

---

277 Art. 9 Abs. 2 j: „…auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht …“

278 Beispiele für Verbände: „Handels- oder Wirtschaftskammer oder ein Bankenverband“; Taeger/Gabel/Kinast, 3. Aufl. 2019, DS-GVO Art. 40 Rn. 18)

279 Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, DSGVO Art. 40 Rn. 33; m.V.a.: Kühling/Buchner/Bergt Art. 40 Rn. 13; Herfurth/Engel ZD 2017, 367 (367); für das BDSG aF s. Simitis/Petri § 38 a Rn. 12.

280 Taeger/Gabel/Kinast, 3. Aufl. 2019, DS-GVO Art. 40 Rn. 24; so sind z.B. Verbraucherschutzverbände ausgeschlossen, Taeger/Gabel/Kinast, 3. Aufl. 2019, DS-GVO Art. 40 Rn. 24; m.V.a.: Hötzendorfer, in: Gantschacher/Jelinek/Schmidl/Spanberger, DSGVO, S. 431; Bergt, CR 2016, 670, 674.)

281 Taeger/Gabel/Kinast, 3. Aufl. 2019, DS-GVO Art. 40 Rn. 15.

282 Taeger/Gabel/Kinast, 3. Aufl. 2019, DS-GVO Art. 40 Rn. 16.

283 Taeger/Gabel/Kinast, 3. Aufl. 2019, DS-GVO Art. 40 Rn. 17; m.V:a.: Schweinoch, in: Ehmann/Selmayr, DS-GVO, Art. 40 Rn. 24; Paal, in: Paal/Pauly, DS-GVO BDSG, Art. 40 Rn. 12; Bergt, CR 2016, 670, 674; Bergt, in: Kühling/Buchner, DS-GVO BDSG, Art. 40 Rn. 12.

284 Taeger/Gabel/Kinast, 3. Aufl. 2019, DS-GVO Art. 40 Rn. 17.

285 Taeger/Gabel/Kinast, 3. Aufl. 2019, DS-GVO Art. 40 Rn. 25.

## 5. Förderpflicht der Mitgliedstaaten

Den **Mitgliedstaaten**, den Aufsichtsbehörden, dem Ausschuss und der Kommission legt Art. 40 Abs. 1 DS-GVO eine Förderpflicht auf. Damit werden insbesondere auch die Bundesministerien aufgefordert, die Entwicklung und Umsetzung von Verhaltensregelungen aktiv voranzubringen. Art. 40 DS-GVO lässt offen, was „fördern" in dem Kontext des Ausarbeitens, Änderns oder Erweiterns von Verhaltensregeln bedeutet.[286]

Nach Ansicht der Literatur umfasse die Förderungspflicht ganz allgemein, „dass die genannten Stellen ein Umfeld schaffen müssen, in welchem selbstregulatorische Verhaltensregeln sich zu einem wirksamen Instrument datenschutzrechtlicher Selbstkontrolle entwickeln können."[287] Die Pflicht beschränke sich nicht auf „das Unterlassen von Behinderungen", sondern verlange vielmehr eine **„aktive" Förderung**, die von der Schaffung geeigneter Rahmenregelungen bis zu sonstigen Unterstützungsmaßnahmen reichen könne.[288] Die Mitgliedstaaten könnten beispielsweise „politische und publizistische Maßnahmen" ergreifen oder „durch Forschungs- und Entwicklungsprojekte Muster für geeignete Verhaltensregeln ausarbeiten lassen".[289] Der Begriff „fördern" umfasst, „geeignete Verbände und Vereinigungen zu ermutigen, Verhaltensregeln zu verfassen, bei der Erstellung beratend mitzuwirken, die Bekanntheit bestehender Verhaltensregeln zu verbessern und Verantwortliche zur Selbstverpflichtung auf Verhaltensregeln zu motivieren."[290] Letztlich unterliegt die Förderpflicht „einem großen Einschätzungsspielraum der Adressaten".[291]

Die Förderpflicht geht dabei auch in die Tiefe. § 40 Abs. 1 DS-GVO verpflichtet die Mitgliedstaaten sowie die anderen Adressaten, „die gängigen Anwendungsfälle von Datenverarbeitungen einer bestimmten Branche, die gängigen Arbeitsweisen, Produktionsabläufe etc zu definieren, die üblichen Fallkonstellationen in dieser Branche zu berücksichtigen, die heterogenen Interessen der Verantwortlichen und der Betroffenen bei der Ausarbeitung des Förderungskataloges gegeneinander abzuwägen und letztlich angemessene Fördermaßnahmen zu setzen."[292]

Letztlich sind auch die Bundesministerien durch Art. 40 DS-GVO aufgerufen, das europäische Datenschutzrecht über Verhaltensregelungen mitzuprägen. In Bezug auf die **grenzüberschreitende Verarbeitung von Patientendaten zu Forschungszwecken** könnte eine Initiative von den Bundesministerien ausgehen. Diese sollte an alle Interessenvertreter gerichtet sein und die Entwicklung von Verhaltensregeln anregen. Dabei dürfte das Bundesministerium konkrete Formulierungsvorschläge einbringen.

---

[286] So auch: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, DSGVO Art. 40 Rn. 27.
[287] Paal/Pauly/Paal, 2. Aufl. 2018, DS-GVO Art. 40 Rn. 5.
[288] Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, DSGVO Art. 40 Rn. 27; Hervorhebungen durch die Verfasser.
[289] Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, DSGVO Art. 40 Rn. 28.
[290] Gola DS-GVO/Lepperhoff, 2. Aufl. 2018, DS-GVO Art. 40 Rn. 7.
[291] Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, DSGVO Art. 40 Rn. 27.
[292] Sydow, Europäische Datenschutzgrundverordnung, DSGVO Art. 40 Rn. 19.

## 6. Verfahren für Verhaltensregeln für die Verarbeitung von personenbezogenen Daten in einem Mitgliedstaat

Art. 40 Abs. 5 und 6 DSGVO enthalten Regelungen zum Genehmigungsverfahren, wenn sich der Entwurf der Verhaltensregeln auf Verarbeitungstätigkeiten in nur einem Mitgliedstaat beziehen (vgl. Art. 40 Abs. 7 DS-GVO). Nachteil des Verfahrens nach Art. 40 Abs. 5 und Abs. 6 DSGVO ist, dass es dann lediglich auf nationaler Ebene gilt.[293]

## 7. Verfahren für Verhaltensregeln zu der Verarbeitung in mehreren Mitgliedstaaten

Art. 40 Abs. 7 DSGVO regelt die Genehmigung von Verhaltensregeln, wenn sich der Entwurf der Verhaltensregeln auf Verarbeitungstätigkeiten in mehreren Mitgliedstaaten bezieht. In diesem Fall legt die nach Art. 55 DS-GVO zuständige Aufsichtsbehörde – bevor sie den Entwurf der Verhaltensregeln bzw. den Entwurf zu deren Änderung oder Erweiterung genehmigt – dem Ausschuss vor (vgl. Art. 63 DS-GVO). Dieser nimmt zu der Frage Stellung, ob der Entwurf der Verhaltensregeln bzw. der Entwurf zu deren Änderung oder Erweiterung mit der Datenschutz-Grundverordnung vereinbar ist (vgl. Art. 40 Abs. 7 DS-GVO).

Wird durch die Stellungnahme nach Art. 40 Abs. 7 DS-GVO bestätigt, dass der Entwurf der Verhaltensregeln bzw. der Entwurf zu deren Änderung oder Erweiterung mit der Datenschutz-Grundverordnung vereinbar ist, so übermittelt der Ausschuss seine **Stellungnahme** der Kommission (Art. 40 Abs. 8 DS-GVO).

Die Kommission kann im Wege von **Durchführungsrechtsakten** beschließen, dass die ihr gemäß § 40 Abs. 8 DS-GVO übermittelten genehmigten Verhaltensregeln bzw. deren genehmigte Änderung oder Erweiterung allgemeine Gültigkeit in der Union besitzen (Art. 40 Abs. 9 S. 1, S. 2 i.V.m. Art. 93 Abs. 2 DS-GVO).

Art. 40 Abs. 10 u. 11 DS-GVO enthalten **Veröffentlichungspflichten**.

## 8. Überwachung

Art. 41 DS-GVO regelt die Überwachung der genehmigten Verhaltensregeln. Unbeschadet der Aufgaben und Befugnisse der zuständigen Aufsichtsbehörde kann die Überwachung der Einhaltung von Verhaltensregeln von einer Stelle durchgeführt werden, die über das geeignete Fachwissen hinsichtlich des Gegenstands der Verhaltensregeln verfügt und die von der zuständigen Aufsichtsbehörde zu diesem Zweck akkreditiert wurde (Art. 41 Abs. 1 DS-GVO).

[293] Taeger/Gabel/Kinast, 3. Aufl. 2019, DS-GVO Art. 40 Rn. 37.

## 9. Zwischenfazit

Art. 40 DS-GVO bildet für das Bundesministerium für Gesundheit Verpflichtung und Möglichkeit zugleich, Verbände und andere Vereinigungen bei der Ausarbeitung und Vorlage von Verhaltensregeln zu fördern. Die Verhaltensregeln können Unionsrecht und das Recht der Mitgliedstaaten und ihrer föderalen Untergliederungen auslegen und präzisieren. Verhaltensregeln sind für die Verantwortlichen und Auftragsverarbeiter verbindlich, wenn sie diese anerkennen. Auch die Aufsichtsbehörden müssen Verhaltensregeln berücksichtigen und entsprechendes Verhalten darf nicht beanstandet werden.

Bereichsspezifische Regelungen der Mitgliedstaaten oder ihrer Bundesländer werden von Verhaltensregeln in ihrem Regelungsinhalt freilich nicht beeinflusst. Daher ist eine Angleichung divergierender legislativer Vorgaben auf Ebene der Mitgliedstaaten oder ihrer Bundesländer durch Verhaltensregeln nicht möglich. Eine Präzisierung und einheitliche Auslegung ist aber beispielsweise möglich für die Abwägung des Forschungsinteresses eines Verantwortlichen mit dem Schutzinteresse des Betroffenen, die Vorgaben für eine nach Landesdatenschutzrecht notwendige Pseudonymisierung von Patientendaten oder für eine Datenspende.

# VII. Formulierung konkreter Handlungsempfehlungen

Unseres Erachtens ist die Einführung einer Rechtsgrundlage für die Verarbeitung personenbezogener Daten bei länderübergreifender Forschung und die Neuregelung der Zuständigkeit der Aufsichtsbehörden in diesen Fällen auf Bundesebene besonders zielführend und damit den anderen Vorschlägen gegenüber vorzugswürdig.

Die Einführung eines Gesundheitsdatenschutzgesetzes auf Bundesebene, der eine Verfassungsänderung vorausgehen müsste, stellt zwar – im Vergleich zu den anderen hier vorgestellten Lösungen – die umfänglichste Harmonisierung dar, ist aber gleichzeitig besonders komplex und damit sehr wahrscheinlich langwierig in der Umsetzung. Aber auch die Harmonisierung über ein Mustergesetz, über Kollisionsnormen in den Landeskrankenhausgesetzen und der Abschluss eines Bund-Länder-Staatsvertrags sind jedenfalls keine kurzfristig umsetzbaren Lösungen, als das Inkrafttreten der Regelungen von der Billigung von 16 Landesparlamenten und dem Bund abhängig ist. Damit wird sich die Vereinheitlichung der bereichsspezifischen Vorschriften sehr wahrscheinlich über viele Jahre ziehen, wenn sie denn überhaupt vollständig erreicht wird.

Um den Gesetzgebungsprozess zu initiieren, ist mit Blick auf die Normierung auf Bundesebene ein Referentenentwurf des Bundesministeriums für Gesundheit erforderlich, der dann in der Regierung mit den anderen Ministerien abgestimmt werden und sodann – nach der Zuleitung an den Bundesrat – ins Parlament eingebracht werden kann.

# Teil 5: Anhang – Formulierungsvorschläge

## A. Klausel des Bundes für länderübergreifende Forschungsvorhaben

### I. Wortlaut

Nach § 27 Abs. 4 BDSG ist folgender Absatz 5 einzufügen:

„Die Absätze 1 bis 4 gelten auch für die Verarbeitung besonderer Kategorien personenbezogener Daten zu Forschungszwecken, an denen nicht-öffentliche Stellen oder öffentliche Stellen des Bundes oder der Länder aus zwei oder mehr Bundesländern als Verantwortliche beteiligt sind (länderübergreifende Forschungsvorhaben).“

### II. Kursorische Begründung

In der medizinischen Forschung sind bundeslandübergreifende Forschungsvorhaben nicht mehr wegzudenken. Insbesondere bei Forschung mit Patientendaten außerhalb der Arzneimittel- und Medizinprodukteprüfung ergeben sich dabei Kollisionen der jeweils einschlägigen Landesdatenschutzgesetze, Landeskrankenhausgesetze und anderer landesspezifischer Normen. Auch die Krankenhäuser in Trägerschaft der öffentlichen Stellen eines Bundeslandes stehen aber bei dieser wissenschaftlichen Forschung im Wettbewerb mit Krankenhäusern in Trägerschaft der nicht-öffentlichen Stellen und der Krankenhäuser in Trägerschaft des Bundes. Es handelt sich insoweit um eine Wettbewerbssituation, wie sie auch in den Landesdatenschutzgesetzen erkannt wird und dort jeweils klarstellend formuliert ist, dass in einer solchen Wettbewerbssituation das Bundesdatenschutzrecht zur Anwendung kommt. Ein gleiches muss für die Forschung gelten und darf nicht durch die Landeskrankenhausgesetzgebung konterkariert werden. Der Bund hat aus den Kompetenztiteln für das Recht der Wirtschaft, der Förderung der Wissenschaft und der Finanzierung der Krankenhäuser die Gesetzgebungskompetenz für eine Zuweisung derartiger landesübergreifender Forschungsvorhaben in das Datenschutzrecht des Bundes. Die Ausübung dieser Kompetenz ist für die Einhaltung der gesamtwirtschaftlichen Lage innerhalb des Bundes geeignet und erforderlich. Der Entwurf bewegt sich innerhalb der Grenzen der Öffnungsklausel des Art. 9 Abs. 2 lit. j) DS-GVO.

# B. Federführende Aufsichtsbehörde

## I. Wortlaut

In § 27 Abs. 5 BDSG (neu) sind folgende Sätze 2 und 3 einzufügen:

„Bei länderübergreifenden Forschungsvorhaben benennen die Verantwortlichen einen Hauptverantwortlichen und melden diesen der für die Hauptniederlassung des Hauptverantwortlichen zuständigen Aufsichtsbehörde (federführende Aufsichtsbehörde). Artikel 56 und Artikel 60 der Verordnung (EU) 2016/679 sind entsprechend anzuwenden."

## II. Kursorische Begründung

Bei länderübergreifenden Forschungsvorhaben sind für die beteiligten verantwortlichen Stellen regelmäßig unterschiedliche Landesaufsichtsbehörden für den Datenschutz zuständig. Durch die im vorstehenden Entwurf gestaltete Anwendbarkeit des Bundesdatenschutzgesetzes für länderübergreifenden Forschungsvorhaben allein wird diese Häufung der Zuständigkeit noch nicht aufgelöst. Es bedarf daher einer Regelung für eine federführende Aufsichtsbehörde. Hierzu finden sich Vorbilder in der Datenschutz-Grundverordnung selbst (Artikel 56, 60 DS-GVO), wie auch in der für die klinische Prüfung von Arzneimitteln entwickelten Konzeption einer Leit-Ethikkommission für den Fall sogenannter Multicenter Studien, bei denen durch die Beteiligung mehrerer Krankenhäuser auch mehrere Ethikkommissionen zuständig sind (§ 8 Absatz 5 GCP-Verordnung). Entsprechend der Ausgestaltung auf der Ebene der EU wird den Verantwortlichen in der Neuregelung auferlegt, eine hauptverantwortliche Stelle zu benennen, die dann der für sie zuständigen Aufsichtsbehörde die Verantwortung für das länderübergreifende Forschungsvorhaben anzuzeigen hat. Maßgeblich ist der in Artikel 4 Nr. 16 DS-GVO definierte Begriff der „Hauptniederlassung", auf den § 40 Absatz 2 Satz BDSG Bezug nimmt und für einen inländischen Sachverhalt anwendbar macht. Der umfassende Bezug auf die Regelungen in Artikeln 56 und 60 der Verordnung (EU) 2016/679 ist zur Ausgestaltung des Verfahrens im Übrigen geeignet und erforderlich.

# C. Anwendung auf kirchliche Krankenhäuser

## I. Wortlaut

In § 27 Abs. 5 BDSG (neu) ist folgender Satz 4 einzufügen:

„Satz 1 bis 3 gelten auch für Krankenhäuser von Kirchen und anderen Religionsgemeinschaften sowie von Trägern, die diesen zugeordnet sind (kirchliche Krankenhäuser), soweit sie an länderübergreifenden Forschungsvorhaben teilnehmen."

### II. Kursorische Begründung

Die Harmonisierung des Datenschutzrechts für länderübergreifenden Forschungsvorhaben muss berücksichtigen, dass auch ein signifikanter Anteil (etwa ein Viertel) der Krankenhäuser in der Trägerschaft von Kirchen und anderen Religionsgemeinschaften sowie von Trägern, die diesen zugeordnet sind (kirchliche Krankenhäuser) steht. Insbesondere für die kirchlichen Krankenhäuser der beiden großen deutschen Kirchen kommt daher zumindest in Teilen die Anwendbarkeit des kirchlichen Datenschutzrechts in Betracht. Bei länderübergreifenden Forschungsvorhaben betätigen sich aber auch die kirchlichen Krankenhäuser außerhalb ihres innerkirchlichen Kerngebiets und außerhalb ihrer karitativen Zielsetzung. Die Anwendung des Bundesrechts bedeutet daher keine Einschränkung der verfassungsrechtlich gewährleisteten Freiheit der Kirchen, ihre eigenen Angelegenheiten zu regeln. Für die Forschung mit Patientendaten gilt auch für die kirchlichen Krankenhäuser in den meisten Bundesländern bereits jetzt das jeweilige Landeskrankenhausgesetz oder eine andere landesspezifische Regelung. Es entspricht daher dem Grundsatz der Gleichbehandlung für kirchliche Krankenhäuser in landesübergreifenden Forschungsvorhaben dieselbe Anwendbarkeit des Bundesrechts verbindlich auszugestalten wie für Krankenhäuser in Trägerschaft einer öffentlichen Stelle eines Bundeslandes.

## D. Datenspende

### I. Wortlaut

Nach § 27 Abs. 5 BDSG (neu) ist folgender Absatz 6 einzufügen:

„Abweichend von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 ist die Verarbeitung besonderer Kategorien personenbezogener Daten auch zulässig, wenn der Betroffene mit seiner Einwilligung gegenüber einem Verantwortlichem nach Satz 3 eine Zweckbindung zu wissenschaftlichen Forschungszwecken gemäß Artikel 5 Absatz 1b der Verordnung (EU) 2016/679 und einen Verzicht auf das Recht zum Widerruf gemäß Artikel 17 Absatz 1b der Verordnung (EU) 2016/679 erklärt hat (Datenspende). Eine Datenspende ist nur zulässig gegenüber einem Verantwortlichem, der entsprechend der Rechtsverordnung nach Satz 3 zugelassen ist (Treuhandstelle für Datenspenden zu wissenschaftlichen Forschungszwecken). Das Bundesministerium für Gesundheit wird ermächtigt, durch Rechtsverordnung ohne Zustimmung des Bundesrates das Nähere zu regeln zu

1. angemessenen und spezifischen Maßnahmen zur Wahrung der Interessen der betroffenen Person im Sinne des Artikels 89 der Verordnung (EU) 2016/679,
2. spezifischen Festlegungen für die Einwilligung zur Datenspende nach Satz 1,
3. dem Verfahren der Zulassung der Treuhandstelle.“

## II. Kursorische Begründung

In der gesellschaftspolitischen Diskussion der vergangenen Jahre wurde wiederholt der Ruf nach der Zulässigkeit einer Datenspende geäußert. Dem trägt der vorliegende Entwurf Rechnung, indem er diese als die Einwilligung zur Datenverarbeitung im Rahmen der medizinischen Forschung einer klaren, aber auch weiten Zweckbindung unterwirft (*broad consent*). Zugleich verzichtet der Betroffene im Rahmen des nach der DS-GVO Möglichen auf das Recht zum Widerruf der Einwilligung. Dieser Umstand ist von dem Verantwortlichen im Rahemn der Kompatibilitätsprüfung nach Artikel 6 Absatz 4 DS-GVO zu berücksichtigen. Um zugleich den größtmöglichen Schutz des Betroffenen zu gewährleisten, ist die Datenspende nur gegenüber einer Treuhandstelle zulässig, die die Voraussetzungen einer vom Bundesministerium für Gesundheit zu beschließenden Rechtsverordnung erfüllt und nach dieser zugelassen werden muss. Der Entwurf berücksichtigt den Rahmen der Öffnungsklausel des Artikel 9 Absatz 2 lit.j der Verordnung (EU) 2016/679 und der Bedingungen und Garantien gemäß Art. 89 Abs. 1 eben dieser Verordnung.