Praxishilfe zum Umgang mit Erlaubnistatbeständen bei der Verarbeitung von Gesundheitsdaten und genetischen Daten

Erarbeitet von Mitgliedern aus den nachfolgend genannten Verbänden:



Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V. (GMDS)

Arbeitsgruppe „Datenschutz und IT-Sicherheit im Gesundheitswesen“



Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e. V.

**Version 1**

Stand: 6. Juli 2024

**Autoren (alphabetisch)**

|  |  |
| --- | --- |
| Georg Karl Bittorf | Arbeiterwohlfahrt, Bezirksverband Westliches Westfalen e.V. |
| Stephan Kloep | Universität Bremen, Kompetenzzentrum für Klinische Studien |
| Sascha Lotzkat | Rechtsanwältin und Datenschutzbeauftragte |
| Johannes Mönter | CURACON GmbH Wirtschaftsprüfungsgesellschaft |
| Regina Mühlich | AdOrga Solutions GmbH |
| Mark Rüdlin | Rechtsanwalt + Datenschutzbeauftragter |
| Bernd Schütze | Deutsche Telekom Healthcare and Security GmbH |

Geschlechtergerechte Sprache

Hinweis bzgl. geschlechtsneutraler Formulierung im gesamten Text:

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

Haftungsausschluss

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

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

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

Copyright

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

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

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

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

Die Nutzung ist unter den folgenden Bedingungen möglich:

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

Im Weiteren gilt:

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

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

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

bzw. für den vollständigen Lizenztext

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

Inhaltsverzeichnis

[Zusammenfassung 1](#_Toc169934782)

[1 Einleitung 2](#_Toc169934783)

[2 Abgrenzung/Klarstellung 4](#_Toc169934784)

[3 Was sind besondere Datenkategorien entsprechend Art. 9 Abs. 1 DS-GVO? 5](#_Toc169934785)

[3.1 Welche Daten gehören zu diesen „besonderen Kategorien personenbezogenen Daten“? 5](#_Toc169934786)

[3.2 Sensibles Datum: Sich daraus ergebende Rahmenbedingungen 6](#_Toc169934787)

[4 Rechtfertigungsgründe in Art. 6 Abs. 1 DS-GVO 7](#_Toc169934788)

[4.1 Art. 6 Abs. 1 lit. a DS-GVO: Einwilligung 7](#_Toc169934789)

[4.2 Art. 6 Abs. 1 lit. b DS-GVO: Vertrag; eine Vertragspartei muss betroffene Person sein 7](#_Toc169934790)

[4.3 Art. 6 Abs. 1 lit. c DS-GVO: Zur Erfüllung einer rechtlichen Verpflichtung erforderlich 8](#_Toc169934791)

[4.4 Art. 6 Abs. 1 lit. d DS-GVO: Erforderlich, um lebenswichtige Interessen der betroffenen  
 Person oder einer anderen natürlichen Person zu schützen 9](#_Toc169934792)

[4.5 Art. 6 Abs. 1 lit. e DS-GVO: Erforderlich für Wahrnehmung einer Aufgabe, die im  
 öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt, die   
 Verantwortlichen übertragen wurde, erfolgt 10](#_Toc169934793)

[4.6 Art. 6 Abs. 1 lit. f DS-GVO: Interessenabwägung 12](#_Toc169934794)

[5 Zuordnung Bedingungen Art. 9 Abs. 2 DS-GVO zu Art. 6 Abs. 1 DS-GVO 16](#_Toc169934795)

[5.1 Art. 9 Abs. 2 lit. a DS-GVO 16](#_Toc169934796)

[5.2 Art. 9 Abs. 2 lit. b DS-GVO 16](#_Toc169934797)

[5.3 Art. 9 Abs. 2 lit. c DS-GVO 16](#_Toc169934798)

[5.4 Art. 9 Abs. 2 lit. d DS-GVO 16](#_Toc169934799)

[5.5 Art. 9 Abs. 2 lit. e DS-GVO 17](#_Toc169934800)

[5.6 Art. 9 Abs. 2 lit. f DS-GVO 17](#_Toc169934801)

[5.7 Art. 9 Abs. 2 lit. g DS-GVO 17](#_Toc169934802)

[5.8 Art. 9 Abs. 2 lit. h DS-GVO 18](#_Toc169934803)

[5.9 Art. 9 Abs. 2 lit. i DS-GVO 19](#_Toc169934804)

[5.10 Art. 9 Abs. 2 lit. j DS-GVO 20](#_Toc169934805)

[6 Nationale Erlaubnistatbestände: Rahmenbedingungen 21](#_Toc169934806)

[6.1 Nationale Gesetzgebung muss EU Grundrechtecharta beachten 21](#_Toc169934807)

[6.2 Rahmenbedingungen für nationale Gesetzgebung 21](#_Toc169934808)

[6.3 Reichweite der Öffnungsklausel in Art. 9 Abs. 4 DS-GVO für nationale Erlaubnisnormen 22](#_Toc169934809)

[6.4 Wie lange gilt ein Gesetz? 23](#_Toc169934810)

[6.5 Nationale Regelungen müssen Anforderungen aus Art. 6 Abs. 1 DS-GVO genügen 24](#_Toc169934811)

[6.6 Landes- vs. Bundesrecht 24](#_Toc169934812)

[6.6.1 Ärztliches Berufsrecht und ärztliche Schweigepflicht 26](#_Toc169934813)

[6.6.2 Sonderfall: Qualitätssicherung und Sozialversicherung 27](#_Toc169934814)

[6.6.3 Sonderfall: wissenschaftliche Forschung 28](#_Toc169934815)

[6.7 Deutsches Kirchenrecht 28](#_Toc169934816)

[7 Betrachtete nationale Gesetze 33](#_Toc169934817)

[7.1 Bundesrecht 33](#_Toc169934818)

[7.1.1 Bundesdatenschutzgesetz (BDSG) 33](#_Toc169934819)

[7.1.1.1 Patientenbehandlung 33](#_Toc169934820)

[7.1.1.2 Beschäftigungsverhältnis 33](#_Toc169934821)

[7.1.1.3 Forschung 34](#_Toc169934822)

[7.1.2 Gesetz zur Nutzung von Gesundheitsdaten zu gemeinwohlorientierten Forschungszwecken   
 und zur datenbasierten Weiterentwicklung des Gesundheitswesens  
 (Gesundheitsdatennutzungsgesetz, GDNG) 34](#_Toc169934823)

[7.1.2.1 Allgemein 34](#_Toc169934824)

[7.1.2.2 GDNG: Bundes- vs. Landesrecht 34](#_Toc169934825)

[7.1.2.3 Erlaubnistatbestände des GDNG 35](#_Toc169934826)

[7.1.3 Verarbeitung personenbezogener Daten durch Schwerbehindertenvertretung 35](#_Toc169934827)

[7.2 Kirchenrecht 37](#_Toc169934828)

[7.2.1 Landeskrankenhausrecht und Regelungen von Religionsgemeinschaften 37](#_Toc169934829)

[7.2.1.1 Geltungsbereich der Landeskrankenhausgesetze 37](#_Toc169934830)

[7.2.1.2 Ausnahmetatbestände in Landeskrankenhausgesetzen 39](#_Toc169934831)

[7.2.1.3 Ergebnis 40](#_Toc169934832)

[7.2.2 Erlaubnistatbestände der ev. Kirche in Bezug auf Patientenversorgung 40](#_Toc169934833)

[7.2.2.1 Bremische evangelische Kirche 40](#_Toc169934834)

[7.2.3 Erlaubnistatbestände der kath. Kirche in Bezug auf Patientenversorgung 42](#_Toc169934835)

[7.2.3.1 Seelsorge im Krankenhaus 42](#_Toc169934836)

[7.3 Landesrecht 43](#_Toc169934837)

[7.3.1 Landeskrankenhausgesetze 43](#_Toc169934838)

[7.3.1.1 Patientenbehandlung 43](#_Toc169934839)

[7.3.1.2 Forschung 44](#_Toc169934840)

[7.3.1.3 Soziale Betreuung 45](#_Toc169934841)

[7.3.1.4 Rechnungsprüfung und -stellung 45](#_Toc169934842)

[7.3.1.5 Zwecke der Qualitätssicherung 46](#_Toc169934843)

[7.3.1.6 Auswertung zu statistischen Zwecken 47](#_Toc169934844)

[7.3.1.7 Aus-, Fort- und Weiterbildung von Ärzten und von Angehörigen anderer Berufe des   
 Gesundheitswesens 48](#_Toc169934845)

[7.3.1.8 Für Zwecke des Patienten- und Beschäftigtenschutzes, Hygiene 49](#_Toc169934846)

[7.3.1.9 Unterrichtung von Angehörigen oder anderen Bezugspersonen, 49](#_Toc169934847)

[7.3.2 Landesrettungsdienstgesetze 50](#_Toc169934848)

[8 Interessenabwägung 52](#_Toc169934849)

[8.1 Vorgaben der DS-GVO 52](#_Toc169934850)

[8.1.1 Keine Legitimierung der Verarbeitung personenbezogener Daten durch Behörden 52](#_Toc169934851)

[8.1.2 Mindestens zu berücksichtigende Faktoren 53](#_Toc169934852)

[8.1.3 Nachweispflicht 54](#_Toc169934853)

[8.1.4 Interessenabwägung bei Kindern 55](#_Toc169934854)

[8.1.5 Informationspflichten 55](#_Toc169934855)

[8.1.6 Widerspruchsrecht beachten 55](#_Toc169934856)

[8.2 Rechtsprechung des EuGH 56](#_Toc169934857)

[8.2.1 Konkrete Umstände und Sensibilität der Daten berücksichtigen 56](#_Toc169934858)

[8.2.2 Einzelfallbetrachtung erforderlich 57](#_Toc169934859)

[8.2.3 Zusammenführen/Verketten personenbezogener Daten 57](#_Toc169934860)

[8.2.4 Interesse muss aktuell vorliegen 57](#_Toc169934861)

[8.2.5 Informationspflichten beachten 57](#_Toc169934862)

[9 Beispiele 58](#_Toc169934863)

[9.1 Radiologische Forschung: Daten aus dem niedergelassenen Bereich 58](#_Toc169934864)

[9.1.1 Beschreibung des Vorhabens 58](#_Toc169934865)

[9.1.2 Berechtigtes Interesse 58](#_Toc169934866)

[9.1.3 Erforderlichkeit 60](#_Toc169934867)

[9.1.4 Interessenabwägung 60](#_Toc169934868)

[9.1.4.1 Interessiert das Vorhaben die Allgemeinheit und nützt das Forschungsergebnis der   
 Allgemeinheit? 60](#_Toc169934869)

[9.1.4.2 Schutz der betroffenen Personen 61](#_Toc169934870)

[9.1.4.3 Individualinteresse der betroffenen Personen 62](#_Toc169934871)

[9.1.4.4 Ergebnis der Interessenabwägung 62](#_Toc169934872)

[9.1.4.5 Bewertung 62](#_Toc169934873)

[9.2 Retrospektives Forschungsvorhaben eines Krankenhauses in Schleswig-Holstein 63](#_Toc169934874)

[10 Abkürzungen 65](#_Toc169934875)

[11 Literatur 67](#_Toc169934876)

[11.1 Internet 67](#_Toc169934877)

[Anhang 1. Abdingbarkeit der Sicherheit der Verarbeitung 68](#_Toc169934878)

[Anhang 1.1 Die gesetzlichen Vorgaben 68](#_Toc169934879)

[Anhang 1.1.1 Europäisches Recht 68](#_Toc169934880)

[Anhang 1.1.2 Deutsches Recht 70](#_Toc169934881)

[Anhang 1.1.3 Zu beachtende gesetzliche Vorgaben die Einwilligung betreffend 72](#_Toc169934882)

[Anhang 1.2 Urteile zum Thema 73](#_Toc169934883)

[Anhang 1.2.1 Deutsche Gerichte 73](#_Toc169934884)

[Anhang 1.2.2 EuGH 74](#_Toc169934885)

[Anhang 1.3 Die Sicht von Datenschutz-Aufsichtsbehörden 75](#_Toc169934886)

[Anhang 1.3.1 Deutsche Aufsichtsbehörden 75](#_Toc169934887)

[Anhang 1.3.2 Österreichische Aufsichtsbehörde 77](#_Toc169934888)

[Anhang 1.4 Diskussion 77](#_Toc169934889)

[Anhang 1.5 Fazit 78](#_Toc169934890)

[Anhang 2. Gesetze im Internet 80](#_Toc169934891)

[Anhang 2.1 Bundesrecht 80](#_Toc169934892)

[Anhang 2.1.1 Bundesdatenschutzgesetz 80](#_Toc169934893)

[Anhang 2.1.2 Gesetz zur Nutzung von Gesundheitsdaten zu gemeinwohlorientierten Forschungszwecken und zur datenbasierten Weiterentwicklung des Gesundheitswesens (Gesundheitsdatennutzungsgesetz, GDNG) 80](#_Toc169934894)

[Anhang 2.2 Landeskrankenhausgesetze nach Bundesländern 80](#_Toc169934895)

[Anhang 2.2.1 Baden-Württemberg 80](#_Toc169934896)

[Anhang 2.2.2 Bayern 80](#_Toc169934897)

[Anhang 2.2.3 Berlin 80](#_Toc169934898)

[Anhang 2.2.4 Brandenburg 81](#_Toc169934899)

[Anhang 2.2.5 Bremen 81](#_Toc169934900)

[Anhang 2.2.6 Hamburg 81](#_Toc169934901)

[Anhang 2.2.7 Hessen 81](#_Toc169934902)

[Anhang 2.2.8 Mecklenburg-Vorpommern 82](#_Toc169934903)

[Anhang 2.2.9 Niedersachsen 82](#_Toc169934904)

[Anhang 2.2.10 Nordrhein-Westfalen 82](#_Toc169934905)

[Anhang 2.2.11 Rheinland-Pfalz 82](#_Toc169934906)

[Anhang 2.2.12 Saarland 82](#_Toc169934907)

[Anhang 2.2.13 Sachsen 83](#_Toc169934908)

[Anhang 2.2.14 Sachsen-Anhalt 83](#_Toc169934909)

[Anhang 2.2.15 Schleswig-Holstein 83](#_Toc169934910)

[Anhang 2.2.16 Thüringen 83](#_Toc169934911)

[Anhang 2.3 Landesrettungsdienstgesetze nach Bundesländern 83](#_Toc169934912)

[Anhang 2.3.1 Baden-Württemberg 83](#_Toc169934913)

[Anhang 2.3.2 Bayern 83](#_Toc169934914)

[Anhang 2.3.3 Berlin 84](#_Toc169934915)

[Anhang 2.3.4 Brandenburg 84](#_Toc169934916)

[Anhang 2.3.5 Bremen 84](#_Toc169934917)

[Anhang 2.3.6 Hamburg 84](#_Toc169934918)

[Anhang 2.3.7 Hessen 84](#_Toc169934919)

[Anhang 2.3.8 Mecklenburg-Vorpommern 84](#_Toc169934920)

[Anhang 2.3.9 Niedersachsen 85](#_Toc169934921)

[Anhang 2.3.10 Nordrhein-Westfalen 85](#_Toc169934922)

[Anhang 2.3.11 Rheinland-Pfalz 85](#_Toc169934923)

[Anhang 2.3.12 Saarland 85](#_Toc169934924)

[Anhang 2.3.13 Sachsen 85](#_Toc169934925)

[Anhang 2.3.14 Sachsen-Anhalt 85](#_Toc169934926)

[Anhang 2.3.15 Schleswig-Holstein 86](#_Toc169934927)

[Anhang 2.3.16 Thüringen 86](#_Toc169934928)

# Zusammenfassung

Jede Verarbeitung personenbezogener Daten muss sich grundsätzlich am Grundsatz der Verhältnismäßigkeit messen lassen, d. h. an der Verfolgung eines legitimen Zwecks, der Eignung der Verarbeitung zur Erreichung dieses Zwecks und der Verhältnismäßigkeit der Verarbeitung in Bezug auf die Beeinträchtigung der Grundrechte der von der Verarbeitung betroffenen Menschen. Dies gilt selbstverständlich auch für die Pseudonymisierung bzw. Anonymisierung, denn beides stellt eine Verarbeitung im Sinne von Art. 4 Ziff. 2 DS-GVO dar.

Nach dem Urteil des Gerichtshofs der Europäischen Union (EuGH) vom 21. Dezember 2023 ist für die Verarbeitung von Daten, welche unter die in Art. 9 Abs. 1 DS-GVO genannten Kategorien fallen, ein Erlaubnistatbestand gem. Art. 9 Abs. 2 DS-GVO erforderlich, zusätzlich muss aber mindestens eine der in Art. 6 Abs. 1 DS-GVO genannten Bedingungen für die Rechtmäßigkeit der Verarbeitung (mit den Worten des EuGH: eine der Rechtmäßigkeitsvoraussetzungen) erfüllt sein.

Dies ergibt sich schon aus dem Wortlaut der DS-GVO: Art. 5 Abs. 1 lit. a DS-GVO gibt unter anderem vor, dass personenbezogene Daten auf rechtmäßige Weise verarbeitet werden müssen. Nach Art. 6 Abs. 1 DS-GVO kann eine Verarbeitung personenbezogener Daten nur dann rechtmäßig erfolgen, wenn mindestens einer der in Art. 6 Abs. 1 lit. a-f DS-GVO genannten Tatbestände erfüllt wird.

Insbesondere auch bei der Verarbeitung von genetischen Daten und Gesundheitsdaten muss daher beachtet werden, dass neben den in Art. 9 Abs. 2 DS-GVO bzw. im nationalen Recht genannten Erlaubnistatbeständen mindestens einer der in Art. 6 Abs. 1 DS-GVO genannten Rechtfertigungsgründe erfüllt ist.

Entsprechend der Rechtsprechung des EuGH ist die Zuordnung eines Datums als „sensibles Datum“ im Sinne des Art. 9 Abs. 1 DS-GVO weit zu verstehen. Auch wenn ein Datum für sich genommen kein sensibles Datum darstellt, ist nach der Rechtsprechung des EuGH zu prüfen, ob „mittels gedanklicher Kombination oder Ableitung“ auf die in Art. 9 Abs. 1 DS-GVO genannte Datenkategorien geschlossen werden kann. Ist dies der Fall, sind entsprechende Daten auch als sensible Daten im Sinne des Art. 9 Abs. 1 DS-GVO anzusehen. Weiterhin entschied der EuGH, dass ein Datensatz, der sowohl sensible als auch nicht sensible Daten enthält, insgesamt als sensibles Datum im Sinne des Art. 9 Abs. 1 DS-GVO anzusehen ist.

Im Zusammenhang mit der Behandlung von Patienten ist Art. 9 Abs. 2 lit. h DS-GVO i. V. m. Art. 6 Abs. 1 lit. b DS-GVO anwendbar: Die Verarbeitung ist erforderlich zur Vertragserfüllung, genauer des Behandlungsvertrages.

Außerhalb der Patientenbehandlung wird es schwieriger: Liegt keine Einwilligung vor, so muss häufig ein überwiegendes öffentliches Interesse an der Verarbeitung der Patientendaten nachgewiesen werden. Ist dies nicht möglich, ist in der Regel eine Interessenabwägung nach Art. 6 Abs. 1 lit. f DS-GVO erforderlich – einschließlich des Nachweises, dass das Interesse der Patienten an der Nicht-Verarbeitung ihrer sensiblen Daten das berechtigte Interesse des Verantwortlichen an der jeweiligen Verarbeitung nicht überwiegt.

Dies gilt auch für Forschungsprojekte. Der bisherige alleinige Verweis auf nationale Regelungen, wie sie beispielsweise in den Landeskrankenhausgesetzen zu finden sind, reicht nicht mehr aus. Die DS-GVO verlangt für jede Verarbeitung, somit auch für die Verarbeitung in Forschungsprojekten, das Erfüllen von mindestens einen der in Art. 6 Abs. 1 DS-GVO aufgeführten Rechtfertigungsgründe.

# Einleitung

Die Frage nach der erforderlichen Rechtsgrundlage für die Verarbeitung personenbezogener Daten ergibt sich schon aus grundrechtlicher und damit verfassungsrechtlicher Sicht.[[1]](#footnote-1) Jede Verarbeitung personenbezogener Daten muss sich grundsätzlich am Grundsatz der Verhältnismäßigkeit messen lassen, d. h. an der Verfolgung eines legitimen Zwecks, der Eignung der Verarbeitung zur Erreichung dieses Zwecks und der Verhältnismäßigkeit der Verarbeitung.

Entsprechend dem Urteil des Gerichtshofs der Europäischen Union (EuGH) vom 21. Dezember 2023[[2]](#footnote-2) ist für die Verarbeitung von Daten, welche zu den in Art. 9 Abs. 1 DS-GVO genannten Kategorien zählen, sowohl ein Erlaubnistatbestand gem. Art. 9 Abs. 2 DS-GVO erforderlich, ergänzend muss jedoch mindestens einer der in Art. 6 Abs. 1 DS-GVO genannten Rechtmäßigkeitsvoraussetzungen erfüllt sein. Dies ergibt sich bereits aus dem Wortlaut der DS-GVO: Art. 5 Abs. 1 lit. a DS-GVO verlangt u. a., dass personenbezogene Daten auf rechtmäßige Weise verarbeitet werden müssen. Nach Art. 6 Abs. 1 DS-GVO kann eine Verarbeitung personenbezogener Daten nur dann rechtmäßig erfolgen, wenn mindestens eine der in Art. 6 Abs. 1 lit. a-f DS-GVO genannten Voraussetzungen erfüllt ist.

Der EuGH konnte letztlich nicht anders entscheiden. Dennoch wurde diese Vorgabe der DS-GVO auch in Deutschland vielfach ignoriert und hinsichtlich der Zulässigkeit der Verarbeitung genetischer und Gesundheitsdaten nur auf nationale Erlaubnistatbestände abgestellt – bestenfalls wurden noch die Vorgaben des Art. 9 DS-GVO berücksichtigt. Jetzt ist klar, dass dieses Vorgehen nicht ausreicht und seit dem Wirkeintritt der DS-GVO auch nie ausreichend war.

Bei der Verarbeitung von in Art. 9 Abs. 1 DS-GVO genannten Kategorien von Daten, zu denen auch genetische und Gesundheitsdaten gehören, muss beachtet werden, dass zusätzlich zu den in Art. 9 Abs. 2 DS-GVO bzw. im nationalen Recht, welches auf Art. 9 Abs. 4 DS-GVO i. V. m. Art. 6 Abs. 2, 3 DS-GVO und den sich daraus ergebenden Vorgaben beruhen muss, genannten Tatbestände mindestens einer der in Art. 6 Abs. 1 DS-GVO genannten Anforderungen erfüllt wird.

Das Urteil des EuGH vom 21. Dezember 2023 in der Rechtssache C‑667/21 bedeutet insbesondere auch in organisatorischer Hinsicht Anpassungsbedarf bei der Verarbeitung der in Art. 9 Abs. 1 DS-GVO genannten besonderen Datenkategorien. Beispielsweise müssen Verantwortliche:

* Die Rechtsgrundlagen sind zu überprüfen und zu überarbeiten.
* Informations- und Auskunftspflichten sind anzupassen. Betroffene Personen müssen ggf. über geänderte Rahmenbedingungen informiert werden, z. B., weil ihnen nun gemäß Art. 13 Abs. 1 lit. d bzw. Art. 14 Abs. 2 lit. b DS-GVO die berechtigten Interessen des Verantwortlichen mitgeteilt werden müssen.
* Dokumentationen wie beispielsweise das Verzeichnis der Verarbeitungstätigkeiten müssen angepasst werden.
* Ggf. müssen auch Prozesse überarbeitet werden, wenn beispielsweise beim Risikomanagement auch die Bewertung einer Interessenabwägung berücksichtigt werden muss.

Im Folgenden wird betrachtet, welche der in Art. 9 und Art. 6 DS-GVO genannten Rechtfertigungsgründe für die Verarbeitung personenbezogener Daten miteinander in Beziehung gesetzt werden könnten, gleichermaßen werden ausgewählte Regelungen aus Deutschland betrachtet. Hierzu ist zunächst zu untersuchen, wann ein sensibles Datum im Sinne des Art. 9 Abs. 1 DS-GVO vorliegt.

# Abgrenzung/Klarstellung

Diese Praxishilfe beschäftigt sich nur mit gesetzlichen Regelungen, welche die Verarbeitung der in Art. 9 Abs. 1 DS-GVO genannten Kategorien von personenbezogenen Daten zum Inhalt haben. Erlaubnistatbestände, die in einzelnen Kollektivvereinbarungen zwischen Partnern vereinbart werden, sind nicht Bestandteil, dennoch wird kurz auf die Rahmenbedingungen von Betriebsvereinbarungen eingegangen.

Gesetzliche Normen, welche eine Verarbeitung vorschreiben, wie beispielsweise Dokumentationspflichten bei der Behandlung, sind ebenfalls nicht Gegenstand dieser Praxishilfe. Entsprechende Regelungen stellen keine Erlaubnisnormen dar, sondern sind Folgen aus der Tatsache, dass personenbezogene Daten verarbeitet wurden und sich aus dieser Verarbeitung Pflichten ergeben, wie z. B. Dokumentationspflichten oder die Pflicht zur Gewährleistung der IT-Sicherheit.

Diese Praxishilfe adressiert die Gesundheitsversorgung. Daher liegt der Schwerpunkt auf diejenigen Erlaubnistatbestände, welche die Verarbeitung von Gesundheitsdaten (im Rahmen dieser Praxishilfe überwiegend Patientendaten) regeln. Andere Regelungen wie beispielsweise die Verarbeitung von biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, wie beispielsweise ein Fingerabdruck oder ein Gesichtsscan, werden nicht berücksichtigt, jedoch kann natürlich bei entsprechenden nationalen Regelungen die Zuordnung zu den Vorgaben aus Art. 9 und 6 DS-GVO entsprechend den Darstellungen dieser Praxishilfe erfolgen, sodass auch in diesen Fällen eine Arbeitserleichterung zu erwarten ist.

# Was sind besondere Datenkategorien entsprechend Art. 9 Abs. 1 DS-GVO?

## Welche Daten gehören zu diesen „besonderen Kategorien personenbezogenen Daten“?

Art. 9 Abs. 1 DS-GVO benennt besondere Kategorien personenbezogener Daten, die häufig als besonders sensible personenbezogene Daten bezeichnet werden. Unter diese Kategorien fallen:

* Rassische und ethnische Herkunft,
* Politische Meinungen,
* Meinungen, aus denen religiöse oder weltanschauliche Überzeugungen hervorgehen,
* Meinungen, aus denen die Gewerkschaftszugehörigkeit hervorgeht,
* Genetischen Daten,
* Biometrischen Daten,
* Gesundheitsdaten,
* Daten zum Sexualleben einer natürlichen Person,
* Daten der sexuellen Orientierung einer natürlichen Person.

In Art. 4 DS-GVO finden sich die Legaldefinitionen zu einigen der genannten Begrifflichkeiten:

* Art. 4 Nr. 1 DS-GVO: personenbezogene Daten
* Art. 4 Nr. 13 DS-GVO: genetische Daten
* Art. 4 Nr. 14 DS-GVO: biometrische Daten
* Art. 4 Nr. 15 DS-GVO: Gesundheitsdaten.

Auf eine Besprechung der einzelnen Datenkategorien wird an dieser Stelle verzichtet und auf die vorhandene Literatur und Rechtsprechung verwiesen.

Art. 9 Abs. 1 DS-GVO verbietet kategorisch alle Verarbeitungen dieser besonderen Kategorien personenbezogener Daten. Damit fällt auch jegliche Verarbeitung von Patientendaten unter dieses „Verbot mit Erlaubnisvorbehalt“. Art. 9 Abs. 2 DS-GVO schränkt dieses Verbot ein: Liegt ein gesetzlich normierter Erlaubnistatbestand zur Verarbeitung vor, ist die Verarbeitung nur für diesen erlaubten Zweck statthaft.

Entsprechend der Rechtsprechung des EuGH ist die Zuordnung eines Datums als „sensibles Datum“ i. S. d. Art. 9 Abs, 1 DS-GVO weit zu verstehen[[3]](#footnote-3). Auch wenn ein Datum aufgrund der eigenen Bedeutung nach an sich kein sensibles Datum darstellt, ist entsprechend dem Urteil des EuGH zu prüfen, ob „mittels gedanklicher Kombination oder Ableitung“ auf diese in Art. 9 Abs. 1 DS-GVO genannten Datenkategorien geschlossen werden kann. Trifft dies zu, sind entsprechende Daten auch als sensible Daten i. S. d. Art. 9 Abs. 1 DS-GVO anzusehen. Ist somit ein Datum als „personenbezogen oder personenbeziehbar“ klassifiziert, so muss bei der Prüfung, ob es sich um ein sensibles Datum i. S. d. Art. 9 Abs. 1 DS-GVO handelt, entsprechend vorgegangen werden. D. h., dass auch indirekt mögliche Aussagen geprüft werden müssen.

Beispiel: Eine Person besucht eine Arztpraxis. Die Standortdaten, also Straße, Postleitzahl und Ort, der Arztpraxis stellen eigentlich keine sensiblen Daten i. S. v. Art. 9 Abs. 1 DS-GVO dar. Da aber bekannt ist, dass eine Arztpraxis aufgesucht wird und dies i. d. R. für eine medizinische Betreuung erfolgt, ist diese Information damit als sensibles Datum aufzufassen.

Weiterhin urteilte der EuGH, dass ein Datensatz, der sowohl sensible als auch nicht sensible Daten enthält, insgesamt als sensibles Datum i. S. v. Art. 9 Abs. 1 DS-GVO anzusehen ist.[[4]](#footnote-4)

## Sensibles Datum: Sich daraus ergebende Rahmenbedingungen

ErwGr. 51 DS-GVO hebt hervor, dass die in Art. 9 Abs. 1 DS-GVO genannten Datenkategorien im Hinblick auf die Grundrechte und Grundfreiheiten besonders sensibel sind und daher einen besonderen Schutz verdienen. Die Verarbeitung dieser Daten ist grundsätzlich mit erheblichen Risiken für die Grundrechte und Grundfreiheiten der betroffenen Personen verbunden.

Daher ist die Verarbeitung dieser personenbezogenen Datenkategorien entsprechend Art. 9 Abs. 1 DS-GVO grundsätzlich verboten, d. h. für die Verarbeitung solcher Daten muss immer ein Erlaubnistatbestand vorliegen, der gemäß ErwGr. 52 DS-GVO angemessene Garantien für den Schutz personenbezogener Daten und anderer Grundrechte enthalten muss. Dies gilt auch für eine Einwilligung: Gemäß den Anforderungen von ErwGr. 51 DS-GVO sollten stets angemessene Schutzmaßnahmen für die Verarbeitung dieser sensiblen Daten vorliegen. Neben der DS-GVO bestimmen diverse europäische und deutsche Rechtsakte Mindestanforderungen hinsichtlich der Gewährleistung einer IT-Sicherheit (ausführlichere Diskussion zu dieser Thematik siehe Anhang 1). Dementsprechend kann die Sicherheit der Verarbeitung nicht ohne Weiteres durch eine Einwilligung reduziert werden.

ErwGr. 53 DS-GVO betont, dass besondere Kategorien personenbezogener Daten, die einen höheren Schutz erfordern, nur dann für gesundheitsbezogene Zwecke verarbeitet werden dürfen, wenn die Verarbeitung für das Erreichen dieser Zwecke im Interesse einzelner natürlicher Personen oder der Gesellschaft als Ganzes erforderlich ist. Dies gilt nach ErwGr. 53 DS-GVO insbesondere

* im Zusammenhang mit der Verwaltung der Dienste und Systeme des Gesundheits- oder Sozialbereichs,
* einschließlich der Verarbeitung dieser Daten durch die Verwaltung und die zentralen nationalen Gesundheitsbehörden zwecks Qualitätskontrolle, Verwaltungsinformationen,
* sowie der allgemeinen nationalen und lokalen Überwachung des Gesundheitssystems oder des Sozialsystems
* und zwecks Gewährleistung der Kontinuität der Gesundheits- und Sozialfürsorge
* und der grenzüberschreitenden Gesundheitsversorgung
* oder Sicherstellung und Überwachung der Gesundheit und Gesundheitswarnungen
* oder für im öffentlichen Interesse liegende Archivzwecke, zu wissenschaftlichen oder historischen Forschungszwecken oder statistischen Zwecken, die auf Rechtsvorschriften der Union oder der Mitgliedstaaten beruhen, die einem im öffentlichen Interesse liegenden Ziel dienen müssen,
* sowie für Studien, die im öffentlichen Interesse im Bereich der öffentlichen Gesundheit durchgeführt werden.

D. h., nach den Vorgaben von Art. 53 DS-GVO muss bei der Verarbeitung von Gesundheits- und genetischen Daten zu den oben genannten Zwecken nachgewiesen werden, dass

1. die jeweilige Verarbeitung im Interesse einzelner natürlicher Personen erforderlich ist, oder
2. die jeweilige Verarbeitung im Interesse der Gesellschaft insgesamt erforderlich ist.

# Rechtfertigungsgründe in Art. 6 Abs. 1 DS-GVO

## Art. 6 Abs. 1 lit. a DS-GVO: Einwilligung

Zum Thema „Einwilligung“ wird auf vorhandene und frei verfügbare Literatur verwiesen.[[5]](#footnote-5)

Der EuGH urteilte,[[6]](#footnote-6) dass der Verantwortliche insbesondere nachweisen muss, dass die betroffenen Personen ihre jeweilige Einwilligung durch aktives Verhalten gaben und zuvor über alle Umstände im Zusammenhang mit der Verarbeitung informiert wurden, sodass die betroffenen Personen ihre Einwilligung in voller Kenntnis der Konsequenzen abgaben, die Einwilligung also in voller Kenntnis der Sachlage erteilt wurde. Kann der für die Verarbeitung Verantwortliche dies nicht nachweisen, liegt keine rechtsgültige Einwilligung vor, d. h. die Verarbeitung wird nicht durch eine Einwilligung legitimiert.[[7]](#footnote-7)

Damit eine Einwilligung als „freiwillig“ erteilt gilt, darf die Einwilligung entsprechend dem Urteil des EuGH[[8]](#footnote-8) keine zwingende Voraussetzung für Datenverarbeitungsvorgänge, die für die Erfüllung des Vertrags nicht erforderlich sind, sein. Erfolgt eine medizinische Versorgung bei Privatpatienten, so ist die Abrechnung der Leistungen durch eine private Abrechnungsgesellschaft (inclusive Forderungsübertragung[[9]](#footnote-9)) grundsätzlich nicht erforderlich, da der Leistungserbringer auch selbst abrechnen kann. Eine Verweigerung der Behandlung aufgrund der Tatsache, dass eine entsprechende Einwilligung verweigert wird, ist somit grundsätzlich nicht zulässig.

## Art. 6 Abs. 1 lit. b DS-GVO: Vertrag; eine Vertragspartei muss betroffene Person sein

Entsprechend Art. 6 Abs. 1 lit. b DS-GVO kann eine Verarbeitung rechtmäßig erfolgen, wenn

1. diese Verarbeitung zur Erfüllung eines Vertrages (z. B. Behandlungsvertrag), dessen Vertragspartei die betroffene Person ist oder
2. zur Durchführung vorvertraglicher Maßnahmen, welche auf Anfrage der betroffenen Person erfolgen,

erforderlich ist. Dabei erfasst „Vertrag“ grundsätzlich rechtsgeschäftliche oder rechtsgeschäftsähnliche Schuldverhältnisse, somit insbesondere auch allgemeine Geschäftsbedingungen (AGB). Zu beachten ist jedoch, dass datenschutzrechtlich nur zur Erfüllung eines Vertrages **erforderliche** Verarbeitungen erfasst werden, somit ggf. andere in einem Vertrag erfasste Verarbeitungen von Art. 6 Abs. 1 lit. b DS-GVO nicht legitimiert werden können. Es muss ein unmittelbarer Zusammenhang zwischen der Verarbeitung und dem konkreten Zweck des Vertragsverhältnisses bestehen.[[10]](#footnote-10)

Verarbeitungen im Rahmen von Mitgliedschaftsverhältnissen, wie sie bei Vereinen und anderen entsprechenden Organisationen vorkommen, können – eine autonome Entscheidung der jeweiligen betroffenen Person vorausgesetzt – durch Art. 6 Abs. 1 lit. b DS-GVO legitimiert werden. Hierbei ist die Ausgestaltung des Vereinszweckes von Bedeutung, da ggf. durch darin enthaltene Vorgaben die Erforderlichkeit der Verarbeitung zu begründen ist.

Im Zusammenhang mit Beschäftigten ist zu unterscheiden, in welchem Umfang eine Verarbeitung für die Durchführung der aus dem Arbeitsvertrag resultierenden Pflichten bzw. Aufgaben erforderlich ist und welche Verarbeitungen von Beschäftigtendaten nicht den eigentlichen Vertragszweck betreffen. Eine Videoüberwachung des Arbeitsplatzes beispielsweise wird i. d. R. für die Durchführung des Arbeitsverhältnisses nicht erforderlich sein und kann somit nur dann rechtmäßig erfolgen, wenn diese Verarbeitung auf eine andere Rechtsgrundlage gestützt werden kann.

Im Rahmen einer medizinischen Behandlung besteht in den meisten Fällen auch ein Vertragsverhältnis zwischen behandelnden Personen und den Patienten. Hierbei ist zu beachten, dass Art. 6 Abs. 1 lit. b DS-GVO allein die Verarbeitung von Gesundheitsdaten nicht legitimieren kann, sondern Vertragsverhältnisse in diesem Zusammenhang den Anforderungen von Art. 9 Abs. 2 lit. h und Abs. 3 DS-GVO genügen müssen (siehe Kapitel 5.8).

Vorvertragliche Maßnahmen wie beispielsweise Vertragsverhandlungen können nur dann durch Art. 6 Abs. 1 lit. b DS-GVO legitimiert werden, wenn die Anfrage von der betroffenen Person ausgeht. Patienten, welche sich zur Behandlung in ein Krankenhaus begeben, dürfen grundsätzlich nicht unter Berufung auf Art. 6 Abs. 1 lit. b DS-GVO zur Bereitschaft zur Teilnahme an Forschungsprojekten angesprochen werden. Hier wird regelmäßig nur eine Interessenabwägung nach Art. 6 Abs. 1 lit. f DS-GVO die Ansprache der Patienten legitimieren können.

## Art. 6 Abs. 1 lit. c DS-GVO: Zur Erfüllung einer rechtlichen Verpflichtung erforderlich

Art. 6 Abs. 1 lit. c DS-GVO selbst kann keine Verarbeitung legitimieren, sondern entsprechend Art. 6 Abs. 3 DS-GVO muss immer eine den Anforderungen des Art. 6 Abs. 3 DS-GVO genügende konkrete Grundlage im Unionsrecht oder im Recht des jeweiligen Mitgliedstaats bestehen.

Die in einer nationalen oder europarechtlichen Vorschrift des objektiven Rechts enthaltene rechtliche Verpflichtung muss sich gemäß Art. 6 Abs. 3 S. 1 DS-GVO unmittelbar auf die Datenverarbeitung beziehen. Art. 6 Abs. 1 lit. c DS-GVO adressiert somit ausschließlich Verpflichtungen kraft objektiven Rechts, jedoch keine gesetzlich geregelten Möglichkeiten, um personenbezogene Daten zu verarbeiten. Allein der Umstand, dass ein Verantwortlicher eine rechtliche Verpflichtung erfüllen soll, kann die Verarbeitung personenbezogene Daten dabei auch nicht legitimieren, denn Art. 6 Abs. 3 S. 2 und 4 DS-GVO verlangt „spezifische Bestimmungen“. Wenn die Verarbeitung seitens Gesetzes nicht konkret genug vorgeschrieben ist, wird zudem die Erforderlichkeit der Verarbeitung rechtlich nur schwer darstellbar sein.

Im deutschen Recht finden sich beispielsweise diverse Verpflichtungen zur Speicherung und Übermittlung von Daten, z. B. im Steuer- oder Telekommunikationsrecht. Diese fallen unter diese Regelung, da sie den Verantwortlichen zu einer bestimmten Verarbeitung verpflichten.

Gesetzliche Erlaubnistatbestände, Daten zu verarbeiten, wenn der Verantwortliche dies möchte, fallen hingegen nicht darunter; ohne eine Pflicht zur Verarbeitung für den Verantwortlichen ist die Bedingung der Erforderlichkeit nicht erfüllt.[[11]](#footnote-11) Somit finden gesetzliche Regelungen, welche die Verarbeitung z. B. für wissenschaftliche oder historische Forschungszwecke sowie statistische Zwecke erlauben, keine Entsprechung in Art. 6 Abs. 1 lit. c DS-GVO. D. h., in diesen Fällen muss ein anderer Rechtfertigungstatbestand aus Art. 6 Abs. 1 DS-GVO gefunden werden.

## Art. 6 Abs. 1 lit. d DS-GVO: Erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen

Entsprechend ErwGr. 112 S. 2 DS-GVO wird unter lebenswichtigen Interessen die körperliche Unversehrtheit oder eine Gefährdung des Lebens selbst verstanden, sei es die betroffene Person selbst oder einer anderen Person betreffend.

ErwGr. 46 S. 2 DS-GVO beinhaltet die Vorgabe, dass personenbezogene Daten „grundsätzlich nur dann aufgrund eines lebenswichtigen Interesses einer anderen natürlichen Person verarbeitet werden [sollten], wenn die Verarbeitung offensichtlich nicht auf eine andere Rechtsgrundlage gestützt werden kann“. Insbesondere bei der Argumentation hinsichtlich der Erforderlichkeit der Verarbeitung bzgl. lebenswichtiger Interessen Dritter ist daher diese vorgegebene Nachrangigkeit dieses Rechtsgrunds zu beachten.

In Anbetracht der Vorgabe des EuGH, dass die Tatbestände von Art. 6 und 9 DS-GVO eng auszulegen sind,[[12]](#footnote-12) wird man bei diesem Tatbestand immer eine natürliche Person, welche bezüglich ihrer körperlichen Integrität und Gesundheit entsprechend gefährdet ist, benennen müssen. Eine abstrakte Gefährdung wird hier keine Verarbeitung legitimieren können.

## Art. 6 Abs. 1 lit. e DS-GVO: Erforderlich für Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt, die Verantwortlichen übertragen wurde, erfolgt

Entsprechend ErwGr. 45 S. 1 DS-GVO wird durch diese Regelung einerseits eine erforderliche Verarbeitung zur Wahrnehmung einer Aufgabe im öffentlichen Interesse adressiert, andererseits eine erforderliche Verarbeitung im Kontext der Ausübung öffentlicher Gewalt. Dies kann grundsätzlich auch durch eine natürliche oder juristische Person des Privatrechts, der diese Aufgabe übertragen worden ist, erfolgen.[[13]](#footnote-13)

Normadressat der Regelung sind jedoch ausschließlich diejenigen Verantwortlichen, denen eine solche Aufgabe auch tatsächlich übertragen wurde, Dritte werden nicht adressiert. Insbesondere kann somit eine Weitergabe an Dritte, wie sie möglicherweise durch Nutzung von IT-Systemen im Rahmen von Wartungsmaßnahmen oder Zugriff durch Behörden aus Drittländern erfolgen könnte, grundsätzlich nicht durch diese Regelung legitimiert werden.

Zu beachten ist hierbei, dass Art. 6 Abs. 1 lit. e DS-GVO allein eine Verarbeitung nicht legitimieren kann, sondern entsprechend Art. 6 Abs. 3 DS-GVO stets eine den Anforderungen des Art. 6 Abs. 3 DS-GVO genügende konkrete Grundlage im Unionsrecht oder im Recht des jeweiligen Mitgliedstaats vorliegen muss. Die konkrete Befugnis zur Verarbeitung muss dem jeweiligen Verantwortlichen im Rahmen der sachlichen Verantwortung somit gesetzlich zugewiesen sein.

ErwGr. 45 S. 2 DS-GVO betont, dass die DS-GVO „nicht für jede einzelne Verarbeitung ein spezifisches Gesetz verlangt“, sondern ein Gesetz als Grundlage für mehrere Verarbeitungsvorgänge ausreichend sein kann, wenn die jeweilige Verarbeitung aufgrund einer dem Verantwortlichen obliegenden rechtlichen Verpflichtung erfolgt. Eine konkrete gesetzliche Grundlage muss zur Nutzung dieses Rechtfertigungstatbestandes jedoch immer vorhanden sein. Als im öffentlichen Interesse liegende Verarbeitungen führt ErwGr. 45 S. 6 beispielhaft gesundheitliche Zwecke wie die öffentliche Gesundheit, die soziale Sicherheit oder die Verwaltung von Leistungen der Gesundheitsfürsorge auf.

D. h., behauptet ein Verantwortlicher, er handele im „öffentlichen Interesse“, muss der Verantwortliche insbesondere

1. das konkrete Interesse benennen,
2. nachweisen, dass es sich um ein öffentliches Interesse handelt,
3. die gesetzliche Regelung (Unionsrecht/Recht des Mitgliedstaates) benennen, welches eine Verarbeitung für genau dieses öffentliche Interesse erlaubt und
4. darstellen, wie seine Verarbeitung dieses öffentliche Interesse bedient.

Aufgrund des öffentlichen Interesses darf die geplante Verarbeitung dann entsprechend den Vorgaben der gesetzlichen Regelung (Art./§ 0815 in Gesetz „xy“) durchgeführt werden. Der Nachweis „öffentliches Interesse“ allein kann keine Verarbeitung legitimieren, immer muss eine für den Verantwortlichen geltende gesetzliche Regelung die Verarbeitung bei Vorliegen des in der gesetzlichen Regelung konkret benannten öffentlichen Interesses auch erlauben.

Hierzu ein Beispiel:

Art. 9 Abs. 2 lit. i DS-GVO benennt beispielsweise verschiedene Aspekte bzgl. öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wobei ergänzend zu Art. 9 Abs. 2 lit. i DS-GVO wiederum Unionsrecht oder nationales Recht erforderlich ist. In Deutschland besteht ein öffentliches Interesse an der Qualitätssicherung der medizinischen Versorgung, dies wird im 9. Abschnitt des 4 Kapitels SGB V (§§ 135 ff. SGB V) gesetzlich geregelt. Warum dürfen Krankenhäuser Patientendaten an ein externes statistisches Institut liefern?

1. Es besteht ein öffentliches Interesse an einer hohen Qualität der Gesundheitsversorgung sowie der Feststellung, in welchen Einrichtungen Mindestvorgaben zur Qualität der Versorgung nicht eingehalten werden.
2. Rechtsgrundlage sind §§ 135 ff. SGB V i. V. m. Art. 9 Abs. 2 lit. i DS-GVO,
3. Rechtfertigungstatbestand ist Art. 6 Abs. 1 lit. e DS-GVO.

Aufgabenwahrnehmung im öffentlichen Interesse kann beispielsweise auch Handlungen einer Ärztekammer in Bezug auf Mitglieder legitimieren, ebenso die Verarbeitung personenbezogener Daten innerhalb einer öffentlichen Schule. In beiden Fällen wurden die Aufgaben vom Gesetzgeber an die entsprechenden Akteure durch entsprechende nationale gesetzliche Regelungen übertragen.

Die Ausübung öffentlicher Gewalt hingegen betrifft die Wahrnehmung hoheitlicher Aufgaben auf der Grundlage rechtlich festgelegter Aufgaben und Befugnisse. D. h. privatwirtschaftliche Tätigkeiten, welche nicht auf hoheitlichem Sonderrecht beruhen, werden von dieser Vorschrift nicht abgebildet. Der Betrieb eines Gefängnisses, bei welchem entsprechende hoheitliche Aufgaben delegiert wurden, könnte hierunter fallen oder die Entsorgung von Abfall oder Abwasser.

Aus verfassungsrechtlicher Sicht unterliegt der Gesetzgeber bezüglich der Übertragung von Aufgaben keiner Beschränkung, weswegen grundsätzlich alle öffentlichen Aufgaben übertragungsfähig sind, auch solche der hoheitlichen Verwaltung.[[14]](#footnote-14) Allerdings kann der Einsatz privater Dienstleister und die Übertragung des staatlichen Gewaltmonopols sich rechtlich schwierig gestalten, wenn diese privaten Dienstleister bzw. Personen nicht in einem Dienst- und Treueverhältnis zum Staat stehen.[[15]](#footnote-15)

Nimmt eine privatwirtschaftliche Stelle aufgrund einer Übertragung hoheitliche Aufgaben wahr, dann trifft diese Stelle selbst keine Pflicht zum Ersatz schuldhaft verursachter Schäden gegenüber Bürgern, sondern die Haftung wird gemäß § 839 BGB im Wege der befreienden Schuldübernahme (Art. 34 S. 1 GG) auf die Anstellungskörperschaft, d. h. die beauftragende öffentliche Stelle) übergeleitet. Die Patientenbehandlung erfolgt i. d. R. nicht in Ausübung eines öffentlichen Amtes i. S. d. Art. 34 GG, selbst wenn die behandelnde Stelle öffentlich-rechtlich organisiert ist und auf der Behandlungsseite beamtete Ärzte tätig werden.[[16]](#footnote-16)

Es gibt jedoch Fallkonstellationen, in denen eine ärztliche Behandlung hoheitlicher Natur sein kann, wie beispielsweise im Rahmen der Tätigkeit in Erfüllung öffentlicher Aufgaben (ein Sanitätsoffizier bei der Truppenbehandlung oder Polizeiärzte) oder im Rahmen des öffentlichen Gesundheitsdienstes durch einen Amtsarzt.[[17]](#footnote-17) Grundsätzlich können hoheitliche Aufgaben bei entsprechender Übertragung auch von Ärzten im Krankenhaus ausgeübt werden:[[18]](#footnote-18) Im Krankenhaus kann der Leiter eines rechtsmedizinischen Instituts bei der Leichenöffnung und den nachfolgenden Untersuchungen nach §§ 87 Abs. 2, 91 StPO in Ausübung eines öffentlichen Amtes handeln. Auch die Tätigkeit des Rettungsdienstes kann hoheitlicher Natur sein, wenn das Rettungswesen öffentlich-rechtlich organisiert ist.[[19]](#footnote-19) Die Wahrnehmung hoheitlicher Aufgaben setzt grundsätzlich voraus, dass die Übertragung der Wahrnehmung einer öffentlichen Aufgabe durch ein Gesetz oder eine Beauftragung durch die vom Gesetz beauftragte öffentliche Stelle erfolgt.

Eine betroffene Person hat gemäß Art. 21 Abs. 1 DS-GVO das Recht, jederzeit gegen eine Verarbeitung, welche entweder im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, Widerspruch einzulegen. Dieses Recht kann die betroffene Person natürlich nur ausüben, wenn sie zuvor über diese Verarbeitung informiert wurde: Entsprechend Art. 21 Abs. 4 DS-GVO muss eine betroffene Person auf das Recht zum Widerspruch einer Verarbeitung, welche unter Verweis auf Art. 6 Abs. 1 lit. e DS-GVO legitimiert wird, informiert werden. Erfolgt ein Widerspruch, so dürfen die vom Widerspruch erfassten Daten nicht mehr verarbeitet werden. Eine Weiterverarbeitung ist gemäß Art. 21 Abs. 1 DS-GVO nur möglich, wenn

1. der Verantwortliche entweder zwingende schutzwürdige Gründe, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, für die Verarbeitung nachweisen kann,
2. oder die Verarbeitung der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen dient.

Entsprechend Art. 21 Abs. 6 DS-GVO besitzt eine betroffene Person ebenfalls ein Widerspruchsrecht, wenn sie betreffende personenbezogene Daten zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken verarbeitet werden. Diesem Widerspruch muss zwingend Folge geleistet werden, d. h. die Daten dürfen nicht weiter verarbeitet werden, es sei denn, die Verarbeitung ist zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe erforderlich.

## Art. 6 Abs. 1 lit. f DS-GVO: Interessenabwägung

Art. 6 Abs. 1 lit. f DS-GVO gilt ausdrücklich nicht für Behörden und kann daher die Verarbeitung personenbezogener Daten durch Behörden oder eine Verarbeitung im Auftrag von Behörden nicht legitimieren. In ErwGr. 47 S. 5 DS-GVO heißt es entsprechend:

„Da es dem Gesetzgeber obliegt, per Rechtsvorschrift die Rechtsgrundlage für die Verarbeitung personenbezogener Daten durch die Behörden zu schaffen, sollte diese Rechtsgrundlage nicht für Verarbeitungen durch Behörden gelten, die diese in Erfüllung ihrer Aufgaben vornehmen.“

Gemäß Art. 6 Abs. 1 lit. f DS-GVO kann eine Verarbeitung u. U. dann rechtmäßig erfolgen, wenn drei kumulative Bedingungen erfüllt sind:

1. Es sich um ein berechtigtes Interesse des Verantwortlichen oder eines Dritten handelt.
2. Die Verarbeitung ist zur Wahrung dieser Interessen erforderlich.
3. Die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, gegenüber den Interessen des Verantwortlichen oder eines Dritten nicht überwiegen.

Grundsätzlich können neben den Interessen des Verantwortlichen auch die Interessen Dritter berücksichtigt werden. Wenn in nachfolgenden Teilen dieses Kapitel daher vom „Verantwortlichen“ gesprochen wird, gilt dies für Interessen Dritter daher analog.

Der Kreis dieser Dritten ist grundsätzlich weit gefasst, endet aber einerseits an der Definition des „Dritten“ in Art. 4 Ziff. 10 DS-GVO, andererseits an den Schranken von Art. 6 Abs. 1 lit. f DS-GVO:

* Dritter muss eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen sein, d. h. „Allgemeininteresse“, „öffentliches Interesse“ usw., wo kein Bezug zu einer einzelnen Person existiert, wird von der Regelung nicht erfasst.
* Interessen von Behörden können in diesem Zusammenhang grundsätzlich nicht berücksichtigt werden, da diese vom Anwendungsbereich der Interessenabwägung ausgenommen sind.

Ausgeschlossen ist ferner, dass nicht-öffentliche Stellen eine Verarbeitung mit der Wahrnehmung von Allgemeininteressen wie Terrorismusabwehr oder Volksgesundheit rechtfertigen.[[20]](#footnote-20)

Zunächst ist das Interesse des Verantwortlichen zu bestimmen. Dies muss grundsätzlich anhand der Zweckbestimmung der Verarbeitung erfolgen. Gemäß Art. 5 Abs. 1 lit. b DS-GVO kann eine Verarbeitung nur rechtmäßig erfolgen, wenn die Verarbeitung nur „für festgelegte, eindeutige und legitime Zwecke“ stattfindet. Ein berechtigtes Interesse an einer Verarbeitung muss somit an einer „für festgelegte, eindeutige und legitime Zwecke“ Verarbeitung bestehen. Nach dem Wortlaut der Regelung bestehen, abgesehen von dem Erfordernis der Rechtmäßigkeit des Interesses, jedoch keine weiteren Anforderungen: Grundsätzlich kann jedes rechtliche, wirtschaftliche oder auch ideelle Interesse in Betracht gezogen werden. Dieses weite Verständnis von „berechtigtem Interesse“ kann u. a. aus den in ErwGr. 47 DS-GVO genannten Beispielen abgeleitet werden:

* Satz 2: Ein berechtigtes Interesse könnte beispielsweise vorliegen, wenn eine maßgebliche und angemessene Beziehung zwischen der betroffenen Person und dem Verantwortlichen besteht, z. B. wenn die betroffene Person ein Kunde des Verantwortlichen ist oder in seinen Diensten steht.
* Satz 6: Die Verarbeitung personenbezogener Daten im für die Verhinderung von Betrug unbedingt erforderlichen Umfang stellt ebenfalls ein berechtigtes Interesse des jeweiligen Verantwortlichen dar.
* Satz 7: Die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung kann als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden.

ErwGr. 48 DS-GVO stellt klar, dass auch innerhalb einer Unternehmensgruppe oder einer Gruppe von Einrichtungen Verantwortliche ein berechtigtes Interesse haben können, personenbezogene Daten innerhalb der Unternehmens- oder Einrichtungsgruppe für interne Verwaltungszwecke, einschließlich der Verarbeitung personenbezogener Daten von Kunden und Beschäftigten, zu übermitteln. ErwGr. 48 S. 2 DS-GVO enthält ergänzend noch die Klarstellung, dass die Grundprinzipien für die Übermittlung personenbezogener Daten innerhalb von Unternehmensgruppen an ein Unternehmen in einem Drittland davon unberührt bleiben, eine Rechtsgrundlage für die Übermittlung in ein Drittland also vorhanden sein muss.

Ist das Interesse bestimmt, muss geprüft werden, ob dieses Interesse gegen die gesetzlichen Vorgaben der Union oder des betreffenden Mitgliedstaates verstößt; ein berechtigtes Interesse kann nur vorliegen, wenn dieses Interesse nicht gegen Rechtsvorschriften verstößt.

Sind die Interessen rechtmäßig, ist zu prüfen, ob die geplante Verarbeitung insbesondere den Anforderungen aus Art. 5 Abs. 1 DS-GVO genügt. Das berechtigte Interesse und die geplante Verarbeitung dürfen insbesondere auch nicht gegen Treu und Glauben (Art. 5 Abs. 1 lit. a DS-GVO) und den Grundsatz der Erforderlichkeit verstoßen. Diese in Art. 6 Abs. 1 lit. f DS-GVO vorgegebene Prüfung der Erforderlichkeit beinhaltet regelmäßig auch die Prüfung (und den Nachweis), dass dem Verantwortlichen zur Erreichung des Zweckes, aus dem sich das berechtigte Interesse ableitet, kein weniger intensiv in die Grundrechte und Grundfreiheiten der betroffenen Person der betroffenen Personen eingreifendes Mittel zur Verfügung steht (mildeste Mittel).

Besteht ein berechtigtes Interesse, so müssen die Interessen der betroffenen Personen identifiziert und gegen die Interessen des Verantwortlichen „auf die Waagschale“ gelegt werden. Überwiegen die Interessen der betroffenen Person an der Nicht-Verarbeitung der personenbezogenen Daten, darf die Verarbeitung nicht erfolgen. Entsprechend dem Wortlaut von Art. 6 Abs. 1 lit. f DS-GVO erlaubt bereits ein gleichwertiges Ergebnis die Verarbeitung der personenbezogenen Daten, ein geringeres Interesse der betroffenen Personen dementsprechend natürlich erst recht.

Zu beachten ist hierbei, dass Art. 6 Abs. 1 lit. f DS-GVO ausdrücklich nur vom Verantwortlichen „berechtigte Interessen“ verlangt, auf Seiten der betroffenen Person jedoch nur „Interessen“ fordert. Somit kann eine betroffene Person auch unberechtigte oder sogar „illegitime“ Interessen in die Abwägung einbringen.[[21]](#footnote-21) Wird beispielsweise in Arztbewertungsportalen auf die nachweislich (z. B. gerichtlich festgestellte) unzulässige Behandlungen einer Arztpraxis hingewiesen, so stellt die Nicht-Nennung der Arztpraxis ein Interesse der Arztpraxis dar, welche im Rahmen einer Interessenabwägung berücksichtigt werden muss.

Zu beachten ist weiterhin, dass eine Bewertung der berechtigten Interessen des für die Verarbeitung Verantwortlichen und der betroffenen Person von den konkreten Umständen des betroffenen Einzelfalls abhängt und daher eine Einzelfallprüfung erforderlich sein kann.[[22]](#footnote-22) Sollen Patientendaten z. B. für eine Forschung verwendet werden, muss ggf. geprüft werden, ob sich unter den für die Forschung vorgesehenen Patienten evtl. Personen befinden, die aufgrund individueller Ereignisse ein besonderes Bedürfnis haben, dass ihre Daten nicht verwendet werden. Personen, die beispielsweise aufgrund von Datenpannen diskriminiert oder stigmatisiert wurden, weisen ein entsprechend hohes Schutzbedürfnis auf, welches in einer Interessenabwägung berücksichtigt werden muss.

Eine Dokumentation der Argumente der Interessenabwägung sowie auch des Ergebnisses ist entsprechend Art. 5 Abs. 2 DS-GVO durch den zur Rechenschaft verpflichteten Verantwortlichen zwingend erforderlich.

Ausführliche Betrachtungen dieser Regelung, insbesondere auch Vorgaben, die sich aus der Rechtsprechung des EuGH ergeben, finden sich in Kapitel 8.

# Zuordnung Bedingungen Art. 9 Abs. 2 DS-GVO zu Art. 6 Abs. 1 DS-GVO

## Art. 9 Abs. 2 lit. a DS-GVO

Art. 9 Abs. 2 lit. a DS-GVO beinhaltet die ausdrückliche Einwilligung, hier wird direkt Art. 6 Abs. 1 lit. a ebenfalls erfüllt.

Zu beachten: Es können auch mehrere Tatbestände aus Art. 6 Abs. 1 DS-GVO zutreffen. Wenn beispielsweise ein App-Hersteller sensible personenbezogene Daten - wie z. B. Gesundheitsdaten (Puls, Schrittzahl usw.) durch Fitness-Apps – verarbeitet, so kann nur eine Einwilligung nach Art. 9 Abs. 2 lit. a DS-GVO diese Verarbeitung legitimieren (siehe auch Kapitel 5.8 die Hinweise zu einem Vertrag mit einem Angehörigen eines Gesundheitsberufs). Als Rechtfertigungsgrund aus Art. 6 Abs. 1 DS-GVO können in diesen Fällen sowohl Art. 6 Abs. 1 lit. a DS-GVO (Einwilligung) aber ggf. auch Art. 6 Abs. 1 lit. b DS-GVO (Vertragserfüllung) zutreffen. Im Kontext „Einwilligung und Vertragserfüllung“ muss allerdings die in Art. 7 Abs. 4 DS-GVO als „Koppelungsverbot“ enthaltene Vorgabe beachtet werden (siehe auch Hinweis EuGH-Urteil zu Freiwilligkeit im Kapitel 4.1).

Wie es im Urteil des EuGH2 in Leitsatz 3 ausgeführt, muss „mindestens eine der in Art. 6 Abs. 1 genannten Rechtmäßigkeitsvoraussetzungen erfüllt sein; es können aber auch mehrere erfüllt sein.

## Art. 9 Abs. 2 lit. b DS-GVO

Art. 9 Abs. 2 lit. b DS-GVO erlaubt die Verarbeitung, sofern diese erforderlich ist, damit der „Verantwortliche oder die betroffene Person die ihm bzw. ihr aus dem Arbeitsrecht und dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte ausüben und seinen bzw. ihren diesbezüglichen Pflichten nachkommen“ können. Pflichten aus dem Arbeitsrecht können einerseits aus nationalen Gesetzen resultieren, aber auch aus einem Arbeitsvertrag, korrespondierende Tatbestände wären dementsprechend Art. 6 Abs. 1 lit. b DS-GVO (Erfüllung vertraglicher Pflichten) oder Art. 6 Abs. 1 lit. c DS-GVO (Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt).

Bzgl. des zweiten Teils von Art. 9 Abs. 2 lit. b DS-GVO (Recht der sozialen Sicherheit und des Sozialschutzes) finden sich die gesetzlichen Regelungen in den deutschen Sozialgesetzbüchern, somit wird hier ebenfalls Art. 6 Abs. 1 lit. c DS-GVO (Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt) entsprochen.

## Art. 9 Abs. 2 lit. c DS-GVO

Art. 9 Abs. 2 lit. c DS-GVO gestattet die Verarbeitung im erforderlichen Umfang zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person, sofern die betroffene Person aus körperlichen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben. Diese Regelung findet ihre Entsprechung in Art. 6 Abs. lit. d DS-GVO, sodass mit Art. 9 Abs. 2 lit. c DS-GVO zugleich auch Art. 6 Abs. 1 lit. d DS-GVO eingehalten wird.

## Art. 9 Abs. 2 lit. d DS-GVO

Art. 9 Abs. 2 lit. d DS-GVO erlaubt eine Verarbeitung auf der Grundlage geeigneter Garantien durch eine politisch, weltanschaulich, religiös oder gewerkschaftlich ausgerichtete Stiftung, Vereinigung oder sonstige Organisation ohne Gewinnerzielungsabsicht im Rahmen ihrer rechtmäßigen Tätigkeiten, jedoch nur, wenn sich die Verarbeitung

1. ausschließlich auf die Mitglieder oder
2. ehemalige Mitglieder der Organisation oder
3. auf Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßige Kontakte mit ihr unterhalten,

bezieht und die personenbezogenen Daten nicht ohne Einwilligung der betroffenen Personen nach außen offengelegt werden.

Hierzu findet sich keine direkte Entsprechung in Art. 6 Abs. 1 DS-GVO. Bzgl. Mitgliedern oder ehemaligen Mitgliedern kann – sofern ein Vertrag bzgl. Mitgliedschaft in der jeweiligen Organisation oder auch eine Satzung entsprechendes berücksichtigt – Art. 6 Abs. 1 lit. b DS-GVO (Erfüllung vertraglicher Pflichten) herangezogen werden. Dies gilt jedoch nicht für Personen, die lediglich Kontakte mit der jeweiligen Organisation unterhalten bzw. unterhielten. Hier muss i. d. R. Art. 6 Abs. 1 lit. f DS-GVO als Rechtfertigungstatbestand herangezogen und im Rahmen einer Interessenabwägung geprüft werden, ob eine Verarbeitung statthaft ist. Bei einer Verarbeitung von durch Art. 9 Abs. 2 lit. d DS-GVO adressierten Daten handelt es sich naturgemäß um Daten der besonders schützenswerten Kategorien, entsprechend hoch sind die Interessen betroffener Personen zu bewerten und zu berücksichtigen.

## Art. 9 Abs. 2 lit. e DS-GVO

Der Tatbestand in Art. 9 Abs. 2 lit. e DS-GVO betrifft Verarbeitung von personenbezogenen Daten, welche die betroffene Person offensichtlich öffentlich gemacht hat. Auch hier findet sich keine entsprechende Regelung in Art. 6 Abs. 1 DS-GVO, sodass auch in diesen Fällen i. d. R. eine Interessenabwägung gemäß Art. 6 Abs. 1 lit. f DS-GVO erforderlich sein wird.

## Art. 9 Abs. 2 lit. f DS-GVO

Art. 9 Abs. 2 lit. f DS-GVO gestattet die Verarbeitung im erforderlichen Umfang zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen sowie die Verarbeitung bei Handlungen der Gerichte, sofern diese im Rahmen ihrer justiziellen Tätigkeit erforderlich ist. In den meisten Fällen, in denen diese Regelung angewandt wird, wird auch Art. 6 Abs. 1 lit. c DS-GVO (Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt) zutreffen.

Erfolgt die Verarbeitung hingegen eher vorsorglich, z. B., um Daten für ein mögliches Gerichtsverfahren in unbestimmter Zukunft zu speichern, so wird sich keine gesetzliche Regelung finden lassen, die dies vom Verantwortlichen verlangt, sodass ein rechtliches Erfordernis nicht gegeben ist. Auch in diesen Fällen wird eine Interessenabwägung nach Art. 6 Abs. 1 lit. f DS-GVO erforderlich sein und eine Verarbeitung nur dann möglich sein, wenn die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person nicht überwiegen.

## Art. 9 Abs. 2 lit. g DS-GVO

Art. 9 Abs. 2 lit. g DS-GVO erlaubt eine Verarbeitung, wenn diese

1. aus Gründen eines erheblichen öffentlichen Interesses erforderlich ist und
2. Unionsrecht oder deutsches Recht dies erlaubt, wobei diese gesetzliche Regelung
   1. in angemessenem Verhältnis zu dem verfolgten Ziel stehen,
   2. den Wesensgehalt des Rechts auf Datenschutz wahren und
   3. angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsehen muss.

Der Verantwortliche muss also diese Vorgaben prüfen, bevor Art. 9 Abs. 2 lit. g DS-GVO überhaupt angewendet werden kann. Art. 6 Abs. 1 lit. e DS-GVO (Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe) wird durch Art. 9 Abs. 2 lit. g DS-GVO i. d R ebenfalls entsprochen.

## Art. 9 Abs. 2 lit. h DS-GVO

Art. 9 Abs. 2 lit. h DS-GVO beinhaltet diverse Zwecke und erlaubt eine Verarbeitung im erforderlichen Umfang für Zwecke

1. der Gesundheitsvorsorge,
2. der Arbeitsmedizin,
3. der Beurteilung der Arbeitsfähigkeit des Beschäftigten,
4. der medizinischen Diagnostik,
5. der Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder
6. der Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich,

wobei entweder Unionsrecht oder deutsches Recht oder ein Vertrag mit einem Angehörigen eines Gesundheitsberufs dies erlaubt.

Im deutschen Recht finden sich hier diverse Regelungen, welche dies adressieren: im Bundesrecht z. B. die Sozialgesetzbücher, im Landesrecht, beispielsweise die Rettungsdienstgesetze der Länder oder die Landeskrankenhausgesetze.

Hinsichtlich vertraglicher Regelung ist in Deutschland insbesondere auf den in §§ 630a ff BGB geregelten Behandlungsvertrag hinzuweisen.

Hinsichtlich der in Art. 9 Abs. 2 lit. h DS-GVO enthaltenen vertraglichen Rechtsgrundlage ist das Erfordernis zu beachten, dass der Vertrag mit „Angehörigen eines Gesundheitsberufs“ abgeschlossen werden muss. Der Begriff „Angehörige eines Gesundheitsberufs“ ist europarechtlich in Art. 3 lit. f Richtlinie 2011/24/EU[[23]](#footnote-23) geregelt:

„Einen Arzt, eine Krankenschwester oder einen Krankenpfleger für allgemeine Pflege, einen Zahnarzt, eine Hebamme oder einen Apotheker im Sinne der Richtlinie 2005/36/EG oder eine andere Fachkraft, die im Gesundheitsbereich Tätigkeiten ausübt, die einem reglementierten Beruf im Sinne von Artikel 3 Absatz 1 Buchstabe a der Richtlinie 2005/36/EG[[24]](#footnote-24) vorbehalten sind, oder eine Person, die nach den Rechtsvorschriften des Behandlungsmitgliedstaats als Angehöriger der Gesundheitsberufe gilt.“

In Deutschland dürften „Angehörige eines Gesundheitsberufs“ weitestgehend mit jenen Berufen übereinstimmen, welche von § 203 Abs. 1 Ziff. 1 StGB adressiert werden: „Arzt, Zahnarzt, Tierarzt, Apotheker oder Angehörigen eines anderen Heilberufs, der für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung erfordert“.[[25]](#footnote-25)

Somit werden Verträge mit Ärzten, Krankenpflegepersonal usw. wohl mit der Regelung in Art. 9 Abs. 2 lit. h DS-GVO adressiert, Verträge mit anderen Dienstleistern (z. B. zur Terminvermittlung zwischen einem Patienten und einem niedergelassenen Arzt, was entsprechend der weiten Auslegung3, 4 des Art. 9 Abs. 1 DS-GVO ebenfalls eine Verarbeitung sensibler Daten darstellt) werden hierdurch wohl eher nicht legalisiert werden können; ein Vertrag zwischen Verantwortlichen, der kein Angehöriger eines Gesundheitsberufes ist, und betroffenen Personen kann Art. 6 Abs. 1 lit. b DS-GVO genügen, jedoch nicht die Verarbeitung von Daten legitimieren, welche zu den in Art. 9 Abs. 1 DS-GVO genannten Kategorien zählen. I. d. R. wird hier nur eine Einwilligung nach Art. 9 Abs. 2 lit. a DS-GVO die Verarbeitung legalisieren können.[[26]](#footnote-26) Richtigerweise wird daher auch für digitale Pflegeanwendungen nach § 40a SGB XI (DiPA) und digitale Gesundheitsanwendungen gemäß § 33a SGB V (DiGA) in den jeweiligen Verordnungen nur eine Einwilligung als Rechtsgrundlage akzeptiert.[[27]](#footnote-27)

Je nach Anwendung des Art. 9 Abs. 2 lit. h DS-GVO finden sich verschiedene Regelungen in Art. 6 Abs. 1 DS-GVO. Basiert die Verarbeitung auf der Grundlage eines Vertrages mit einem Angehörigen eines Gesundheitsberufs, so wird Art. 6 Abs. 1 lit. b DS-GVO (Erfüllung vertraglicher Pflichten) ebenfalls erfüllt sein.

Erfolgt die Verarbeitung hingegen aufgrund einer der diversen gesetzlichen Regelungen in Deutschland, so wird wohl eher Art. 6 Abs. 1 lit. c DS-GVO (Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt) zutreffen.

## Art. 9 Abs. 2 lit. i DS-GVO

Art. 9 Abs. 2 lit. i DS-GVO erlaubt die Verarbeitung, wenn diese aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit erforderlich ist. Beispielhaft wird angegeben:

* Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren oder
* Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten.

Weiterhin muss entweder das Unionsrecht oder das deutsche Recht die Verarbeitung erlauben. Dieses Recht muss angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person, insbesondere des Berufsgeheimnisses, vorsehen, ansonsten genügt das Recht nicht den Anforderungen von Art. 9 Abs. 2 lit. i DS-GVO.

In diesen Fällen wird bei Vorliegen eines Erlaubnistatbestandes nach Art. 9 Abs. 2 lit. i DS-GVO häufig auch den Anforderungen von Art. 6 Abs. 1 lit. e DS-GVO (Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe) genügt werden.

Hierbei ist jedoch zu beachten, dass Art. 6 Abs. 3 DS-GVO neben der Grundlage einer nationalen oder unionsrechtlichen Rechtsgrundlage (siehe auch Kap. 6 sowie die dortigen Unterkapitel) verlangt, dass die Verarbeitung der personenbezogenen Daten erforderlich zur Erfüllung ist. D. h., ohne diese Verarbeitung kann die im öffentlichen Interesse liegende oder in Ausübung öffentlicher Gewalt erfolgende Aufgabe nicht erfüllt werden.

## Art. 9 Abs. 2 lit. j DS-GVO

Art. 9 Abs. 2 lit. j DS-GVO erlaubt die Verarbeitung personenbezogener Daten für

* im öffentlichen Interesse liegende Archivzwecke,
* für wissenschaftliche oder historische Forschungszwecke oder
* für statistische Zwecke gemäß Art. 89 Abs. 1 DS-GVO.

Damit dieser Erlaubnistatbestand angewendet werden kann, muss entweder das Unionsrecht oder das deutsche Recht die jeweilige Verarbeitung erlauben, wobei dieses Recht

1. in angemessenem Verhältnis zu dem verfolgten Ziel stehen,
2. den Wesensgehalt des Rechts auf Datenschutz wahren und
3. angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person

vorsehen muss.

Die Verarbeitung für im öffentlichen Interesse liegende Archivzwecke findet in Art. 6 Abs. 1 lit. e DS-GVO (Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe) einen entsprechenden Erlaubnistatbestand; siehe hierzu auch die Hinweise im Kapitel 5.9.

Dies kann, muss aber nicht, auch für wissenschaftliche oder historische Forschungszwecke sowie statistische Zwecke gelten, je nachdem, ob die Forschung/Statistik im öffentlichen Interesse liegt oder nicht; der Verantwortliche muss nachweisen (können), dass ein öffentliches Interesse an der Forschung/Statistik besteht. Was regelhaft nicht allein durch das Vorhandensein von öffentlichen (Förder-)Gelder erreicht werden kann; diese können wohl einen Hinweis auf öffentliches Interesse geben, aber nicht allein als Nachweis dienen.

Liegen die wissenschaftlichen oder historischen Forschungszwecke bzw. die statistischen Zwecke nicht im (nachweisbaren) öffentlichen Interesse, wird in diesen Fällen i. d. R. eine Interessenabwägung entsprechend Art. 6 Abs. 1 lit. f DS-GVO erforderlich sein.

# Nationale Erlaubnistatbestände: Rahmenbedingungen

## Nationale Gesetzgebung muss EU Grundrechtecharta beachten

Weiterhin ist zu beachten, dass Art. 7 und 8 der Charta der Grundrechte der Europäischen Union nur eingeschränkt werden können, wenn entsprechende Einschränkungen gemäß Art. 52 Abs. 1 der Charta gesetzlich vorgesehen sind und den Wesensgehalt der Grundrechte sowie den Grundsatz der Verhältnismäßigkeit wahren.[[28]](#footnote-28) Nach Rechtsprechung des EuGH28 dürfen Einschränkungen nur vorgenommen werden, wenn

1. sie erforderlich sind und
2. den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen.

Basierend auf diesen Vorgaben erlassene Einschränkungen müssen sich auf das absolut Notwendige beschränken. Die den Eingriff enthaltende Regelung muss klare und präzise Bestimmungen für die Tragweite und die Anwendung der betreffenden Maßnahme vorsehen und zudem über ausreichende Garantien verfügen, die einen wirksamen Schutz der personenbezogenen Daten vor Missbrauchsrisiken ermöglichen.[[29]](#footnote-29)

## Rahmenbedingungen für nationale Gesetzgebung

Nationale Regelungen müssen entsprechend Art. 6 Abs. 2 DS-GVO „spezifische Anforderungen für die Verarbeitung sowie sonstige Maßnahmen präziser bestimmen, um eine rechtmäßig und nach Treu und Glauben erfolgende Verarbeitung zu gewährleisten“ - eine reine Wiederholung von Texten der DS-GVO entspricht nicht diesen Anforderungen.[[30]](#footnote-30) Spezifischere Regelungen „müssen auf den Schutz der Rechte und Freiheiten […] hinsichtlich der Verarbeitung ihrer personenbezogenen Daten […] abzielen und geeignete und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person umfassen“30.

Um dem Erfordernis der Verhältnismäßigkeit zu genügen, muss die der Verarbeitung zugrunde liegende nationale Regelung klare und präzise Regeln für die Tragweite und die Anwendung der betreffenden Maßnahme vorsehen sowie Mindesterfordernisse beinhalten, sodass die Personen, deren personenbezogene Daten betroffen sind, über ausreichende Garantien verfügen, die einen wirksamen Schutz ihrer Daten vor Missbrauchsrisiken ermöglichen.[[31]](#footnote-31)

Eine nationale Regelung muss nach nationalem Recht zudem bindend sein und insbesondere Angaben dazu enthalten, unter welchen Umständen und unter welchen Voraussetzungen eine Maßnahme, die die Verarbeitung personenbezogener Daten vorsieht, getroffen werden darf, damit gewährleistet ist, dass sich der Eingriff auf das absolut Notwendige beschränkt.31

Eine nationale Regelung, die eine Offenbarungsbefugnis gegenüber Behörden beinhaltet, muss sich bei der Festlegung der Umstände und Voraussetzungen, unter denen ein Verantwortlicher verpflichtet ist, personenbezogene Daten über seine Kunden/Nutzer/Patienten zu übermitteln, auf objektive Kriterien stützen.31

## Reichweite der Öffnungsklausel in Art. 9 Abs. 4 DS-GVO für nationale Erlaubnisnormen

Art. 9 Abs. 4 DS-GVO gestattet Mitgliedstaaten zusätzliche Bedingungen, einschließlich Beschränkungen, einzuführen oder aufrechtzuerhalten, soweit die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten betroffen ist. D. h., Mitgliedstaaten können nicht beliebig Regelungen für alle in Art. 9 Abs. 1 DS-GVO genannten Daten erlassen, sondern sind beschränkt auf die in Art. 9 Abs. 4 DS-GVO genannten Datenkategorien.

Aufgrund der offenen Formulierung des Tatbestandsmerkmals sind nach herrschender Meinung nationale Regelungen zulässig, welche die Rechtmäßigkeitsanforderungen verschärfen, also die Verarbeitung entsprechender Datenkategorien an zusätzliche Voraussetzungen knüpfen.

Ob Art. 9 Abs. 4 DS-GVO jedoch auch nationale Bestimmungen gestattet, welche die Verarbeitungsmöglichkeiten erweitern oder deren Anforderungen absenken, wird in der juristischen Literatur überwiegend abgelehnt.[[32]](#footnote-32)

Gegen eine Öffnungsklausel, welche zusätzliche Erlaubnistatbestände oder die Absenkung der Anforderungen erlaubt, spricht der Wortlaut der Regelung, in der gerade nicht von weiteren „Ausnahmen“ die Rede ist, sondern nur von weiteren „Bedingungen“ für die in Art. 9 Abs. 2 DS-GVO genannten Ausnahmen gesprochen wird. Insbesondere unter Berücksichtigung von ErwGr. 53 S. 4 und 5 DS-GVO wird dies offensichtlich. Auch spricht die Sichtweise des EuGH gegen eine weite Auslegung der Regelungen in Art. 9 DS-GVO: Der EuGH urteilte, dass die Regelungen in Art. 6 und 9 DS-GVO eng auszulegen sind.[[33]](#footnote-33)

Bei der Gestaltung zusätzlicher Bedingungen ist der nationale Gesetzgeber allerdings nicht völlig frei, er muss sich an die Vorgaben der DS-GVO halten und darf das Schutzniveau nicht beliebig herabsenken.

Zu beachten ist, dass die Öffnungsklausel ausschließlich für die Mitgliedstaaten selbst gelten, eine Übertragbarkeit dieses Rechts des nationalen Gesetzgebers auf andere ist nicht vorgesehen und entsprechend EU-Recht auch nicht möglich. Für die in Art. 9 Abs. 2 lit. b DS-GVO genannten Kollektivvereinbarungen existieren diese Möglichkeiten daher nicht, sodass Kollektivvereinbarungen beispielsweise keine zusätzlichen Bedingungen in Bezug auf eine Einwilligung aufstellen dürfen.

## Wie lange gilt ein Gesetz?

Es kann zu Recht bezweifelt werden, dass diverse vom deutschen Gesetzgeber erlassene Regelungen diesen Vorgaben entsprechen, insbesondere auch Regelungen aus jüngerer Zeit wie beispielsweise das „Gesetz zur verbesserten Nutzung von Gesundheitsdaten“ (Gesundheitsdatennutzungsgesetz, GDNG). Im letztgenannten Gesetz fehlen beispielsweise „klare und präzise Regeln für die Tragweite und die Anwendung“, welche betroffenen Personen einerseits aufklären, wer wann zu welchen genauen Zwecken (medizinische „Forschung“ ist keine präzise Angabe und auch nicht jede Forschung liegt im oder dient dem öffentlichen Interesse) ihre Daten verarbeiten darf, andererseits verfügen betroffene Personen über keine ausreichenden Garantien hinsichtlich Missbrauchsschutz, ja erfahren i. d. R. nicht einmal, welche (natürliche oder juristische) Person die persönlichen Daten zu welchen Zwecken verarbeitet. Entsprechende Kritik wurde von Fachleuten bereits geäußert.[[34]](#footnote-34)

Ein Gesetz ist allerdings so lange rechtskräftig anwendbar, bis entweder der Gesetzgeber das jeweilige Gesetz änderte oder ein Gericht dieses Gesetz für rechtswidrig und nicht anwendbar erklärte. Bei aller vorhandenen Kritik sind die Gesetze bis zum Widerruf durch den Gesetzgeber selbst oder bis zu einem entsprechenden Gerichtsurteil also anwendbar. Im Falle der Erlaubnistatbestände zur Verarbeitung personenbezogener Daten entsteht für Verantwortliche ggf. jedoch ein Risiko: Erkennt ein Gericht die Unrechtmäßigkeit eines Gesetzes an, so konnte das Gesetz die Verarbeitung der Daten niemals legitimieren. Entsprechend Treu und Glauben kann der Verantwortliche für die unrechtmäßige Verarbeitung in der Vergangenheit zwar nicht belangt werden, aber aufgrund der Unrechtmäßigkeit müssen alle Daten gelöscht werden, ggf. sogar Verarbeitungsergebnisse, die ja nie hätten angefertigt werden dürfen. Im Bereich von Medizinprodukten kann dies beispielsweise dazu führen, dass diese aufgrund fehlender Datengrundlage und damit fehlendem Wirknachweis wieder vom Markt genommen werden müssen. Somit muss ein Verantwortlicher jeweils selbst abschätzen, ob für die eigene Verarbeitung die ggf. rechtswidrige gesetzliche Grundlage genutzt werden soll oder ob aus Sicherheitsgründen ein anderer, rechtssicherer Erlaubnistatbestand vielleicht besser geeignet ist.

## Nationale Regelungen müssen Anforderungen aus Art. 6 Abs. 1 DS-GVO genügen

Alle nationalen Erlaubnistatbestände zur Verarbeitung von personenbezogenen Daten sind nur in Verbindung mit den Vorgaben aus Art. 6 Abs. 2 DS-GVO sowie bei Verarbeitung von personenbezogenen Daten der besonderen Kategorie ergänzend denen aus Art 9 Abs. 4 DS-GVO anwendbar.

Nationale Gesetze, Rechtsverordnungen usw. können/müssen für die Zeitdauer ihrer Gültigkeit angewendet werden. Aufgrund des in Art. 9 Abs. 1 DS-GVO enthaltenen Verbots der Verarbeitung von besonderen Kategorien personenbezogener Daten muss jedoch immer auch ein Erlaubnistatbestand aus Art. 9 DS-GVO diese Verarbeitung (mit) erlauben. Weiterhin muss aufgrund des EuGH-Urteils auch bei nationalen Erlaubnistatbeständen zur Verarbeitung von besonderen Kategorien personenbezogener Daten immer auch mindestens einer der in Art. 6 Abs. 1 DS-GVO angeführten Rechtfertigungsgründe erfüllt sein.

D. h., für alle nationalen Gesetze, Rechtsverordnungen usw., die von einem Verantwortlichen angewendet werden, ist neben der nationalen Regelung und dem Bezug der nationalen Regelung zu Art. 9 DS-GVO immer auch mindestens ein erfüllter Rechtfertigungsgrund aus Art. 6 Abs. 1 DS-GVO zu finden und anzugeben, wenn die Verarbeitung von in Art. 9 Abs. 1 DS-GVO genannten besonderen Kategorien personenbezogener Daten legalisiert werden soll.

Im deutschen Recht existiert eine Vielzahl von entsprechenden Erlaubnistatbeständen, z. B. finden sich diverse Erlaubnistatbestände in §§ 64a ff. SGB X. Findet sich keine Entsprechung in den in Art. 6 Abs. 1 lit. a bis e DS-GVO genannten Rechtfertigungsgründen, ist in diesen Fällen eine Interessenabwägung nach Art. 6 Abs. 1 lit. f DS-GVO erforderlich. Eine Verarbeitung darf bei Erfordernis einer Interessenabwägung trotz des Vorliegens eines nationalen Erlaubnistatbestandes in diesen Fällen nur durchgeführt werden, wenn die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person gegenüber den berechtigten Interessen des Verantwortlichen (oder eines Dritten) nicht überwiegen.

## Landes- vs. Bundesrecht

Die Gesetzgebungskompetenzen im Bereich des Krankenhausrechts wurde 2019 vom Wissenschaftlichen Dienst des Deutschen Bundestages betrachtet[[35]](#footnote-35), 2022 wurde vom Dienst der verfassungsrechtliche Rahmen für die Regelung der stationären medizinischen Versorgung im Rahmen einer Kurzinformation dargestellt.[[36]](#footnote-36) Krankenhausorganisation und die Krankenhausplanung fallen in die Gesetzgebungskompetenz der Länder, daher ist bei rechtlichen Widersprüchen in diesen Fällen das Landesrecht vorrangig gegenüber dem Bundesrecht anzuwenden.

2019 antwortete der wissenschaftliche Dienst auch auf die Frage der Gesetzgebungskompetenz des Bundes für den Öffentlichen Gesundheitsdienst, was auch die Gesetzgebungskompetenz für Berufsrecht beinhaltete.[[37]](#footnote-37) Die Regelung der ärztlichen Weiterbildung nach Erteilung der Approbation und damit die gesamte Regelung des Facharztwesens gehört entsprechend dem Gutachten des Wissenschaftlichen Dienstes des Deutschen Bundestages in die Gesetzgebungszuständigkeit der Länder, somit auch der Umgang mit Telemedizin oder eHealth.

Prof. Wollenschläger (Universität Augsburg) fertigte im Zuge der Krankenhausreformpläne von Prof. Lauterbach ein Rechtsgutachten für die Länder Bayern, Nordrhein-Westfalen und Schleswig-Holstein an und kommt zum Ergebnis, dass dem Bund in etlichen Bereichen entsprechend Grundgesetz (GG) nicht das Recht zur Regelung zusteht bzw. der Bundesgesetzgeber im Bereich der konkurrierenden Gesetzgebung (= Sozialversicherung, wirtschaftliche Sicherung der Krankenhäuser) die Grenzen beachten muss.[[38]](#footnote-38)

Entsprechend Art. 74 Abs. 1 Nr. 19a GG existiert eine konkurrierende Zuständigkeit von Bund- und Landesgesetzgeber, wobei Art. 74 Abs. 1 Nr. 19a GG der gesetzgeberischen Zuständigkeit des Bundes für das Gebiet der Krankenhäuser prinzipiell klare Grenzen setzt.[[39]](#footnote-39) Aus Art. 74 Abs. 1 Nr. 19a GG in Verbindung mit Art. 70 Abs. 1 GG ergibt sich das Primat der Länder für Fragen der Krankenhausplanung und -organisation.[[40]](#footnote-40), [[41]](#footnote-41) Weiter ergibt sich aus Art. 2 Abs. 2 S. 1 GG i. V. m. dem Sozialstaatsprinzip u. a., dass es Aufgabe des jeweiligen Bundeslandes ist, die stationäre Versorgung zu gewährleisten.[[42]](#footnote-42) Die Länder erließen in Wahrnehmung ihrer Kompetenz jeweils eigene Krankenhausgesetze.

Entsprechend Art. 74 Abs. 1 Nr. 19a GG stehen dem Bund lediglich die Regelungen der wirtschaftlichen Sicherung der Krankenhäuser und der Krankenhauspflegesätze zu.[[43]](#footnote-43) Gemäß Art. 72 Abs. 2 GG muss für eine Gesetzgebung des Bundes im Kontext des Art. 74 Abs. 1 Nr. 19a GG die Herstellung gleichwertiger Lebensverhältnisse im Bundesgebiet oder die Wahrung der Rechts- oder Wirtschaftseinheit im gesamtstaatlichen Interesse eine bundesgesetzliche Regelung erforderlich sein. Dementsprechend darf der Bund Fragen, welche die Krankenhausplanung betreffen, nur dann regeln, wenn der Bezug zur wirtschaftlichen Sicherung der Krankenhäuser offensichtlich ist und den Ländern eigenständige und erhebliche Ausgestaltungsspielräume bleiben.[[44]](#footnote-44) Weist der Bund das Erfordernis nicht nach und die jeweiligen Bundesländer machten von ihrer Gesetzgebungskompetenz Gebrauch (= keine Regelungslücke beim jeweiligen Landesgesetzgeber), so ist das jeweilige Landesrecht vorrangig gegenüber dem Bundesrecht anzuwenden.

Umstrukturierungen im Gesundheitswesen können sich deshalb nur sehr eingeschränkt auf den Kompetenztitel der Nr. 19a stützen.39 „Regelungen betreffend die Krankenhaus- und Personalstruktur, die Bezüge des Personals bzw. das Liquidationsrecht der Ärzte sind damit grundsätzlich ebenso wenig gedeckt wie Regelungen zur Verfolgung gesundheitspolitischer Ziele, die über einen allgemeinen Standard der Krankenhausversorgung hinausgehen.“[[45]](#footnote-45)

### Ärztliches Berufsrecht und ärztliche Schweigepflicht

Entsprechend Art. 74 Abs. 1 Nr. 19 GG besteht u. a. bzgl. der Zulassung zu ärztlichen und anderen Heilberufen eine konkurrierende Gesetzkompetenz. Das Bundesverfassungsgericht urteilte, dass der Bund im Bereich des Gesundheitswesens seine nur begrenzten Zugriffsmöglichkeiten nicht unter Berufung auf die öffentliche Fürsorge ausweiten darf: „Die Entscheidung der Verfassung (Art. 74 Nr. 19 und 19a GG), dem Bund für das Gesundheitswesen nur in eingeschränktem Maße Gesetzgebungskompetenzen zuzuweisen, darf nicht durch eine erweiternde Auslegung der Gesetzgebungskompetenz für die öffentliche Fürsorge unterlaufen werden“.[[46]](#footnote-46)

Unter den Begriff der ärztlichen Heilberufe fallen die Berufe des Arztes, des Zahnarztes, des Tierarztes sowie solche, welche die Heilkunde unmittelbar zum Gegenstand haben wie beispielsweise Hebammen, Krankenpfleger, Altenpfleger, Krankengymnasten, Notfallsanitäter, Diätassistenten oder auch Heilpraktiker.

Die Zulassung i. S. d. Art. 74 Abs. 1 Nr. 19 GG umfasst im Hinblick auf ärztliche Heilberufe Vorschriften, die sich auf Erteilung, Zurücknahme und Verlust der Approbation oder auf die Befugnis zur Ausübung des ärztlichen Berufs beziehen. Entsprechend seiner Gesetzgebungskompetenz erließ der Bundesgesetzgeber mit der Bundesärzteordnung (BÄO) ein Bundesgesetz, welches die Berufszulassung zum Arztberuf regelt.

Die Regelung der ärztlichen Weiterbildung nach Erteilung der Approbation und damit die gesamte Regelung des Facharztwesens gehört dagegen in die Gesetzgebungszuständigkeit der Länder, da dies der Berufsausübung zugeordnet wird.[[47]](#footnote-47) Hierzu gehört die Berufsordnung für Ärztinnen und Ärzte des jeweiligen Bundeslandes, in welcher auch die ärztliche Schweigepflicht enthalten ist. Eingriffe in die entsprechende Länderkompetenz sind nach Urteil des BVerfG46 restriktiv zu handhaben, entsprechend kann der Bundesgesetzgeber nur sehr begrenzt Regelungen zur ärztlichen Schweigepflicht treffen. Das in § 203 StGB geregelte Verbot der unbefugten Offenbarung unterliegt jedoch der Gesetzgebungskompetenz des Bundes.

Obwohl § 9 MBO-Ä und § 203 StGB unterschiedliche Formulierungen nutzen, bestehen zwischen den Normen hinsichtlich des Schutzcharakters keine großen Unterschiede. Der in § 203 StGB verwendete Geheimnisbegriff wird insbesondere im medizinischen Kontext so weit ausgelegt, dass § 203 StGB ebenso umfassend schützt wie § 9 MBO-Ä: Auch nach § 203 StGB ist der Umstand, „dass ein Patient einen Arzt, einen Psychologen oder einen Psychotherapeuten aufsucht, bereits ein Geheimnis“,[[48]](#footnote-48) was auch für eine Aufnahme in ein Krankenhaus oder für eine ambulante Behandlung in einer Praxis gilt.

Erlegen gesetzliche Vorschriften einem Arzt eine Melde- oder Auskunftspflicht auf, so ist der Arzt zur Offenbarung des Patientengeheimnisses befugt,[[49]](#footnote-49) Dabei ist es unerheblich, ob die Erlaubnis sich aus Unions-, Bundes- oder Landesrecht ableitet: Mit einem gesetzlichen Erlaubnistatbestand zur Offenbarung kann keine unbefugte Offenbarung vorliegen. Zu beachten ist jedoch, dass

1. in untergesetzlichen Rechtsnormen, wie sie beispielsweise auch die jeweilige Landesberufsordnung für Ärzte darstellt, geregelte Auskunftspflichten nicht für eine Offenbarungsbefugnis ausreichen;83 das BVerfG beschrieb im sog. Volkszählungsurteil[[50]](#footnote-50) die Voraussetzung einer verfassungsgemäßen gesetzlichen Grundlage, die dem rechtsstaatlichen Gebot der Normenklarheit entsprechen muss;
2. weiterhin muss darauf geachtet werden, dass die entsprechende Regelung zur Schweigepflicht in der jeweiligen Landesberufsordnung i. d. R. die Pflicht enthält, über eine Einschränkung der ärztlichen Schweigepflicht die jeweiligen Patienten zu unterrichten.

### Sonderfall: Qualitätssicherung und Sozialversicherung

Aus der sich aus Art. 74 Abs. 1 Nr. 12 GG resultierenden Kompetenz zur Regelung der Sozialversicherung, auf deren Grundlage das SGB V beruht, können insbesondere Vorgaben zur Qualitätssicherung der medizinischen Versorgung seitens des Bundesgesetzgebers abgeleitet werden, allerdings darf auch unter Bezugnahme auf diese Regelungskompetenz die planungsrechtliche Kompetenz der Länder im Krankenhauswesen durch den Bundesgesetzgeber nicht angetastet werden; den Ländern muss die inhaltliche Ausgestaltung der bundesgesetzlichen Vorgaben ermöglicht werden.

### Sonderfall: wissenschaftliche Forschung

Entsprechend Art. 74 Abs. 1 Nr. 13 GG existiert auch bzgl. der Förderung der wissenschaftlichen Forschung eine konkurrierende Zuständigkeit von Bund- und Landesgesetzgeber, wobei „Forschung“ i. S. d. Art. 5 Abs. 3 GG zu verstehen ist. Entsprechend dem „Hochschul-Urteil“ des BVerfG[[51]](#footnote-51) wird unter wissenschaftliche Tätigkeit „alles, was nach Inhalt und Form als ernsthafter planmäßiger Versuch zur Ermittlung der Wahrheit anzusehen ist“, verstanden. Art. 5 Abs. 3 GG ist bzgl. Forschung entsprechend der Rechtsprechung des BVerfG als "die geistige Tätigkeit mit dem Ziele, in methodischer, systematischer und nachprüfbarer Weise neue Erkenntnisse zu gewinnen" auszulegen.

Die Gesetzgebungskompetenz des Bundes zur Förderung der wissenschaftlichen Forschung ist durch die Vorgaben des GG begrenzt. Im Bereich der universitären Forschung beschränkt sich die Kompetenz des Bundes nach Art. 74 Abs. 1 Nr. 33 GG eingeräumte Kompetenz auf Regelungen der Hochschulzulassung und der Hochschulabschlüsse, von denen die Länder gem. Art. 72 Abs. 3 GG abweichen können.[[52]](#footnote-52) Die Regelungen der universitären Forschung selbst ist Sache der Länder, nicht des Bundes.

Gleichermaßen liegt die Kompetenz zur Regelung der Nutzung von zur Patientenversorgung erhobenen personenbezogenen Daten (sog. „Sekundärnutzung“) bei den jeweiligen Ländern, die von dieser Regelungskompetenz in den jeweiligen Landeskrankenhausgesetzen Gebrauch gemacht haben.

Eine Regelungskompetenz des Bundes kann sich nur aus Art. 74 Abs. 2 GG ergeben. Zu den Voraussetzungen, unter denen der Bund Art. 74 Abs. 2 GG anwenden kann, siehe oben im Abschnitt 6.6.

Allerdings können Bund und Länder entsprechend Art. 91b GG aufgrund von Vereinbarungen in Fällen überregionaler Bedeutung bei der Förderung von Wissenschaft, Forschung und Lehre zusammenwirken, d. h. Bund und Länder können bei der Planung und Finanzierung von überregional bedeutsamen Förderungsvorhaben auf den Gebieten von Wissenschaft, Forschung und Lehre gemeinsam tätig werden. Allerdings stellen entsprechende Vereinbarungen keine Erlaubnisnorm zur Forschung i. S. d. Art. 74 Abs. 1 Nr. 13 GG dar.

## Deutsches Kirchenrecht

Nach Art. 140 GG sind die Bestimmungen der Artikel 136, 137, 138, 139 und 141 der deutschen Verfassung vom 11. August 1919 („Weimarer Verfassung“) Bestandteil des GG. In Art. 137 der Weimarer Verfassung findet sich eine Regelung zur Kirche:

1. Es besteht keine Staatskirche.
2. Die Freiheit der Vereinigung zu Religionsgesellschaften wird gewährleistet. Der Zusammenschluss von Religionsgesellschaften innerhalb des Reichsgebiets unterliegt keinen Beschränkungen.
3. Jede Religionsgesellschaft ordnet und verwaltet ihre Angelegenheiten selbständig innerhalb der Schranken des für alle geltenden Gesetzes. Sie verleiht ihre Ämter ohne Mitwirkung des Staates oder der bürgerlichen Gemeinde.
4. Religionsgesellschaften erwerben die Rechtsfähigkeit nach den allgemeinen Vorschriften des bürgerlichen Rechtes.
5. Die Religionsgesellschaften bleiben Körperschaften des öffentlichen Rechtes, soweit sie solche bisher waren. Anderen Religionsgesellschaften sind auf ihren Antrag gleiche Rechte zu gewähren, wenn sie durch ihre Verfassung und die Zahl ihrer Mitglieder die Gewähr der Dauer bieten. Schließen sich mehrere derartige öffentlich-rechtliche Religionsgesellschaften zu einem Verband zusammen, so ist auch dieser Verband eine öffentlich-rechtliche Körperschaft.
6. Die Religionsgesellschaften, welche Körperschaften des öffentlichen Rechtes sind, sind berechtigt, auf Grund der bürgerlichen Steuerlisten nach Maßgabe der landesrechtlichen Bestimmungen Steuern zu erheben.
7. Den Religionsgesellschaften werden die Vereinigungen gleichgestellt, die sich die gemeinschaftliche Pflege einer Weltanschauung zur Aufgabe machen.
8. Soweit die Durchführung dieser Bestimmungen eine weitere Regelung erfordert, liegt diese der Landesgesetzgebung ob.

Art. 140 GG i. V. m.  Art. 137 Abs. 3 S. 1 Weimarer Verfassung gewährt den Kirchen und anderen Religionsgemeinschaften somit ein Selbstverwaltungsrecht in eigenen Angelegenheiten, wobei die Regelung in den Grenzen von Art. 4 GG betrachtet werden muss;[[53]](#footnote-53) Art. 4 GG enthält im Gegensatz zu Art. 137 Abs. 3 Weimarer Verfassung ein Grundrecht. Für die Abgrenzung der eigenen Angelegenheiten ist das Selbstverständnisses der jeweiligen Religionsgemeinschaft zu berücksichtigen. können Zu den eigenen Angelegenheiten können nach der Rechtsprechung des BVerfG u. a. gehören

* Arbeits- und dienstrechtliche Gestaltung[[54]](#footnote-54),
* Berufsbildung im kirchlichen Dienst[[55]](#footnote-55),
* Mitbestimmung und Personalvertretung[[56]](#footnote-56),
* Fragen der Mitgliedschaft[[57]](#footnote-57).

Eine Grenze besteht bei Beziehungen zu Personen, die nicht der Religionsgemeinschaft angehören bzw. zu ihr in keiner Sonderbeziehung stehen: Hier handelt es sich grundsätzlich um keine eigene Angelegenheit einer Kirche.[[58]](#footnote-58) Eine weitere Grenze findet sich im Wortlaut von Art. 137 Abs. 3 S. 1 Weimarer Verfassung, wonach kirchliche Regelungen „innerhalb der Schranken des für alle geltenden Gesetzes“ erfolgen müssen. Darunter fallen entsprechend der Rechtsprechung des BVerfG[[59]](#footnote-59) alle Gesetze, die für die Religions- und Weltanschauungsgemeinschaften „dieselbe Bedeutung haben wie für jedermann“. Das BVerfG urteilte 1980, dass ggf. im Wege der Abwägung ein angemessenes Verhältnis zwischen der aus Art. 137 Abs. 3 S. 1 Weimarer Verfassung, resultierenden Kirchenfreiheit und mit dieser kollidierenden „für alle geltende“ Gesetze hergestellt werden sollen.[[60]](#footnote-60)

Nach Art. 17 Abs. 1 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV)[[61]](#footnote-61) muss die Europäische Union den Status, den Kirchen und religiöse Vereinigungen oder Gemeinschaften in den Mitgliedstaaten nach deren Rechtsvorschriften genießen, achten und darf ihn nicht beeinträchtigen. Im AEUV ist verpflichtend vereinbart, dass das europäische Recht vorrangiges Recht ist, was auch für Kirchenrecht gilt, welches nicht unmittelbar kirchliche Angelegenheiten betrifft.

Im Arbeitsrecht urteilte beispielsweise 2018 der EuGH[[62]](#footnote-62), dass die Richtlinie 2000/78 zwar auf den Schutz des Grundrechts der Arbeitnehmer abzielt, nicht wegen ihrer Religion oder Weltanschauung diskriminiert zu werden. Entsprechend Art. 4 Abs. 2 Richtlinie 2000/78 ist es Kirchen und anderen entsprechenden öffentlichen oder privaten Organisationen gemäß dem in Art. 17 Abs. 1 AEUV verankertem Recht gestattet, ihrem jeweiligen Ethos auf religiösen Grundsätzen oder Weltanschauungen Rechnung zu tragen. Die Regelung dient dem Ausgleich zwischen dem Recht auf Autonomie der Kirchen und der anderen Organisationen, deren Ethos auf religiösen Grundsätzen oder Weltanschauungen beruht, und dem Recht der Arbeitnehmer, insbesondere bei der Einstellung nicht wegen ihrer Religion oder Weltanschauung diskriminiert zu werden. Kommt es zum Rechtsstreit, muss eine solche Abwägung aber gegebenenfalls von einer unabhängigen Stelle, also nicht von der Kirche oder Organisation selbst, und letztlich von einem innerstaatlichen Gericht überprüft werden können. Kirchen müssen dem EuGH zufolge gerichtlich überprüfbar bei einer Handlung oder Entscheidung wie der Ablehnung einer Bewerbung auf eine bei ihr zu besetzende Stelle begründen, nach der Art der betreffenden Tätigkeiten oder den vorgesehenen Umständen ihrer Ausübung eine wesentliche, rechtmäßige und gerechtfertigte berufliche Anforderung aus dem Ethos der Kirche oder Organisation besteht. Aus Art. 17 Abs. 1 AEUV abgeleitetes Recht kann niemals folgen, dass die Einhaltung europäischen Rechts einer wirksamen gerichtlichen Kontrolle entzogen wird, was insbesondere auch für datenschutzrechtliche Regelungen von Kirchen und entsprechenden Organisationen gelten muss.

Der EuGH stellte im Urteil weiterhin fest62: Ob die Religion oder Weltanschauung überhaupt eine solche berufliche Anforderung darstellen kann, hängt nur von der „Art“ der fraglichen Tätigkeiten oder den „Umständen“ ihrer Ausübung ab. Die Rechtmäßigkeit einer Ungleichbehandlung wegen der Religion oder der Weltanschauung nach Maßgabe dieser Vorschrift hängt also vom objektiv überprüfbaren Vorliegen eines direkten Zusammenhangs zwischen der vom Arbeitgeber aufgestellten beruflichen Anforderung und der fraglichen Tätigkeit ab.

Auch im Datenschutzrecht wird der Vorgabe von Art. 17 Abs. 1 AEUV hinsichtlich des Rechts der Kirchen und entsprechender Organisation zur Selbstverwaltung ihrem jeweiligen Ethos auf religiösen Grundsätzen oder Weltanschauungen Rechnung getragen. In Art. 91 DS-GVO heißt es:

Art. 91 Bestehende Datenschutzvorschriften von Kirchen   
und religiösen Vereinigungen oder Gemeinschaften

1. Wendet eine Kirche oder eine religiöse Vereinigung oder Gemeinschaft in einem Mitgliedstaat zum Zeitpunkt des Inkrafttretens dieser Verordnung umfassende Regeln zum Schutz natürlicher Personen bei der Verarbeitung an, so dürfen diese Regeln weiter angewandt werden, sofern sie mit dieser Verordnung in Einklang gebracht werden.
2. Kirchen und religiöse Vereinigungen oder Gemeinschaften, die gemäß Absatz 1 umfassende Datenschutzregeln anwenden, unterliegen der Aufsicht durch eine unabhängige Aufsichtsbehörde, die spezifischer Art sein kann, sofern sie die in Kapitel VI niedergelegten Bedingungen erfüllt.

Die Vorgabe aus Art. 91 DS-GVO ist also u. a.

1. Die kirchliche Regelung muss zum Zeitpunkt des Inkrafttretens der DS-GVO gelten. Die DS-GVO ist am 24. Mai 2016 in Kraft getreten.
2. Es müssen umfassende Regelung gewesen sein.
3. Die Regelungen müssen „in Einklang“ mit der DS-GVO gebracht werden, d. h. die kirchlichen Regelungen müssen den Vorgaben der DS-GVO entsprechen. Insbesondere dürfen die kirchlichen Regelungen somit nicht den Vorgaben der DS-GVO widersprechen[[63]](#footnote-63).

Entsprechend Art. 91 DS-GVO sind Religionsgesellschaften somit grundsätzlich an das staatliche Datenschutzrecht gebunden und von diesem im Sinne eines allgemein geltenden Gesetzes beschränkt.

Im Datenschutzrecht urteilte der EuGH bisher noch nicht über das Zusammenspiel zwischen Kirchenrecht und europäischem Recht. Aber aus dem Urteil zum Arbeitsrecht kann man festhalten:

1. Kirchliche Entscheidungen über Angelegenheiten, die nicht originäre kirchliche Fragen wie beispielsweise Glaubensfragen betreffen, müssen gegebenenfalls von einer unabhängigen Stelle, also nicht von der Kirche selbst, überprüft werden können. Insbesondere bei Entscheidungen mit Auswirkungen auf das Leben muss die Entscheidung von einem innerstaatlichen, nicht-kirchlichem Gericht überprüfbar sein. Insbesondere wenn die Entscheidung auch Personen betrifft, die selbst nicht der Kirche oder Organisation angehören, die aber dem kirchlichen Recht ausgeliefert sind.
2. Kirchenrechtliche Vorgaben müssen darauf beruhen, dass nach Art und vorgesehenen Umständen eine wesentliche, rechtmäßige und gerechtfertigte Anforderung aus dem Ethos der Kirche oder Organisation für die jeweilige Angelegenheit, z. B. für die Berufsausübung oder die medizinische Versorgung, besteht und hieraus die Rechtmäßigkeit einer Ungleichbehandlung wegen der Religion oder der Weltanschauung abgeleitet werden kann.
3. Ist es einem mit einem Rechtsstreit befassten nationales Gericht nicht möglich, das einschlägige nationale Recht im Einklang mit dem europäischen Recht zu bringen, ist das nationale Gericht verpflichtet, „im Rahmen seiner Befugnisse den dem Einzelnen aus den Art. 21 und 47 der Charta der Grundrechte der Europäischen Union erwachsenden Rechtsschutz zu gewährleisten und für die volle Wirksamkeit dieser Bestimmungen zu sorgen, indem es erforderlichenfalls jede entgegenstehende nationale Vorschrift unangewendet lässt“.[[64]](#footnote-64)

Die Ausführungen in dieser Praxishilfe zu den Rechtfertigungsgründen (Kap. 4) und der Zuordnung von Erlaubnistatbeständen zur Verarbeitung von Daten der besonderen Kategorien zu den Rechtfertigungsgründe (Kap. 5.) können als Grundlage für die Beurteilung der kirchlichen Regelungen dienen.

# Betrachtete nationale Gesetze

Die deutschen Gesetze müssen vor Anwendung daraufhin geprüft werden, welcher in Art. 6 Abs. 1 DS-GVO genannte Rechtfertigungstatbestände zu welcher deutschen Regelung passt, die Verarbeitung somit legitimieren kann.

Dabei adressieren verschiedene nationale Gesetze dieselben Inhalte, beispielsweise findet sich in den einzelnen Landeskrankenhausgesetzen regelhaft die Erlaubnisnorm, Patientendaten zu deren Behandlung wie auch zu medizinischer Forschung zu nutzen. Mehrere Regelungen, auch aus unterschiedlichen Bundesländern, können daher thematisch gemeinsam betrachtet werden.

Aufgrund der Vielzahl an deutschen Regelungen kann an dieser Stelle nicht auf alle gesetzlichen Regelungen eingegangen werden. Basierend auf den in dieser Praxishilfe durchgeführten Diskussionen sollte jedoch auch für diese nicht besprochenen gesetzlichen Regelungen ein Rechtfertigungstatbestand aus Art. 6 Abs. 1 DS-GVO durch analoge Anwendung der Ausführungen gefunden werden.

## Bundesrecht

### Bundesdatenschutzgesetz (BDSG)

#### Patientenbehandlung

§ 22 Abs. 1 BDSG wiederholt in Abs. 1 und 2 lediglich die Regelungen aus Art. 9 Abs. 2 DS-GVO; laut Gesetzesbegründung aus Gründen der nationalen Umsetzung, da verschiedene Regelungen in Art. 9 Abs. 2 DS-GVO auf das „Recht der Mitgliedstaaten“ verweisen. Bei diesen Regelungen findet man einen Rechtfertigungsgrund, indem die Ausführungen in Kapitel 5 angewendet werden.

#### Beschäftigungsverhältnis

§ 26 Abs. 2 BDSG regelt die Verarbeitung personenbezogener Daten von Beschäftigten auf der Grundlage einer Einwilligung und adressiert somit Art. 9 Abs. 2 lit. a DS-GVO, korrespondierend dazu Art. 6 Abs. 1 lit. a DS-GVO. § 26 Abs. 2 BDSG enthält zusätzliche Bedingungen für die Einwilligung (Freiwilligkeit, Schriftform) und nutzt dabei die Öffnungsklausel in Art. 9 Abs. 4 DS-GVO. Da Art. 9 Abs. 4 DS-GVO dem nationalen Gesetzgeber nur erlaubt, zusätzliche Bedingungen für die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten zu gestalten, können diese zusätzlichen Bedingungen daher auch nur auf diese drei Kategorien angewendet werden, nicht jedoch auf alle in Art. 9 Abs. 1 DS-GVO genannten Kategorien,

§ 26 Abs. 3 und 4[[65]](#footnote-65) BDSG regelt die Verarbeitung der in Art. 9 Abs. 1 DS-GVO genannten besonderen Kategorien personenbezogener Daten für Zwecke des Beschäftigungsverhältnisses. § 26 Abs. 3 und 4 BDSG ist hier als Ergänzung zu Art. 9 Abs. 2 lit. b DS-GVO zu sehen.

Somit können weder auf § 26 Abs. 3 BDSG noch auf § 26 Abs. 4 BDSG beruhende Kollektivvereinbarungen über die Erlaubnisgrenzen von Art. 9 Abs. 2 lit. b DS-GVO hinausreichen, die Möglichkeiten zur Erlaubnis der Verarbeitung besonderer Kategorien von Beschäftigtendaten findet hier also ihre Grenzen.

Nach Art. 9 Abs. 2 lit. b DS-GVO ist nur nationales Recht zulässig, welches geeignete Garantien für die Grundrechte und die Interessen der betroffenen Person vorsieht. Dies gilt selbstverständlich auch für Kollektivvereinbarungen, welche ebenfalls nur gültig sein können, wenn entsprechende Garantien in den Kollektivvereinbarungen enthalten sind; auf die entsprechende Rechtsprechung wird hingewiesen.[[66]](#footnote-66)

Im Rahmen des Beschäftigungsverhältnisses findet man einen Rechtfertigungstatbestand in Art. 6 Abs. 1 lit. b DS-GVO, der auch vorvertragliche Maßnahmen umfasst.

#### Forschung

§ 27 Abs. 1 BDSG erlaubt als nationale Umsetzung von Art. 9 Abs. 2 lit. j DS-GVO die Nutzung von genetischen und Gesundheitsdaten für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke, wenn die Daten für diese Zwecke erforderlich sind und eine Interessenabwägung ergibt, dass die „Interessen des Verantwortlichen an der Verarbeitung die Interessen der betroffenen Person an einem Ausschluss der Verarbeitung erheblich überwiegen“. Somit ist Art. 6 Abs. 1 lit. f DS-GVO hier der Rechtfertigungstatbestand. Hingewiesen muss an dieser Stelle jedoch auf den Umstand, dass entsprechend § 27 Abs. 1 BDSG ein „erhebliches“ Überwiegen nachgewiesen werden muss, ein einfaches überwiegendes Interesse eines Verantwortlichen reicht nicht.

### Gesetz zur Nutzung von Gesundheitsdaten zu gemeinwohlorientierten Forschungszwecken und zur datenbasierten Weiterentwicklung des Gesundheitswesens (Gesundheitsdatennutzungsgesetz, GDNG)

#### Allgemein

Das GDNG enthält leider diverse Rechtsunsicherheiten. Beispielsweise soll entsprechend § 1 Abs. 3 GDNG Regelungen des GDNG gegenüber Regelungen des fünften und elften SGB vorrangig gelten. Jedoch ist die Verarbeitung von Sozialdaten in den Sozialgesetzbüchern abschließend geregelt (§ 35 Abs. 2 SGB I). Ohne Änderung des § 35 Abs. 2 SGB I dürfte das GDNG keine hiervon abweichende Regelung erlassen. Für den Rechtsanwender ist somit unklar, welche Regelungen anzuwenden sind.

Letztlich muss ein Rechtsanwender selbst entscheiden, ob er im GDNG enthaltene Regelungen zur Erlaubnis der Verarbeitung personenbezogener Daten nutzen will, oder aufgrund der rechtlichen Unsicherheiten darauf verzichtet.

#### GDNG: Bundes- vs. Landesrecht

Das GDNG unterliegt als Bundesgesetz den Beschränkungen, denen der Bundesgesetzgeber unterliegt (siehe Kapitel 6.6), insbesondere gilt für Krankenhäuser vorrangig das Landesrecht. Beispielsweise verlangt § 38 Abs. 1 LKHG Schleswig-Holstein für die Nutzung von Patientendaten zu Forschungszwecken grundsätzlich eine Einwilligung; diese Regelung ist gegenüber Regelungen des GDNG vorrangig anzuwenden, d. h., das GDNG kann keine Verarbeitung erlauben, wenn der Landesgesetzgeber andersartige Regelungen erlassen hat. Nur wenn der Landesgesetzgeber keine Regelungen für Krankenhäuser erlassen hat, kann die Regelungslücke durch das GDNG genutzt werden und Verarbeitungen erlauben.

#### Erlaubnistatbestände des GDNG

§ 6 Abs. 1 GDNG erlaubt datenverarbeitenden Gesundheitseinrichtungen, die bei Ihnen rechtmäßig gespeicherten Daten zu Zwecken

1. der Qualitätssicherung und zur Förderung der Patientensicherheit,
2. der medizinischen, zur rehabilitativen und zur pflegerischen Forschung sowie
3. zu statistischen Zwecken, einschließlich der Gesundheitsberichterstattung

zu verarbeiten, soweit dies zur Erreichung des jeweiligen Zweckes erforderlich ist.

§ 6 Abs. 1 lit. a GDNG adressiert Art. 9 Abs. 2 lit. i DS-GVO, soweit diese Regelung der Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung dient. Eine hohe Qualität in der Patientenversorgung liegt im öffentlichen Interesse, Rechtfertigungstatbestand ist somit Art. 6 Abs. 1 lit. e DS-GVO. Die von Art. 6 Abs. 3 DS-GVO verlangte nationale Rechtsgrundlage für diese Aufgabe im öffentlichen Interesse stellt die Regelung im GDNG dar. Ob § 6 Abs. 1 S. 2 GDNG den Erfordernissen aus Art. 9 Abs. 2 lit. i DS-GVO genügt, also

* angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person vorsieht,
* insbesondere eine Verarbeitung auf das erforderliche Maß begrenzt
* und das Berufsgeheimnisses wahrt,

muss insbesondere auf die Wahrung des Berufsgeheimnisses bezweifelt werden; § 6 GDNG verlangt nicht, dass die Daten von Verantwortlichen verarbeitet werden, welche dem Berufsgeheimnis unterliegen.

§ 6 Abs. 1 lit. b und c GDNG sind Regelungen, welche ihre Entsprechung in Art. 9 Abs. 2 lit. j DS-GVO. Hier wird i. d. R. eine Interessenabwägung nach Art. 6 Abs. 1 lit. f DS-GVO erforderlich sein (siehe Kapitel 5.10).

### Verarbeitung personenbezogener Daten durch Schwerbehindertenvertretung

Eine Schwerbehindertenvertretung (SBV) ist nach § 177 Abs. 1 SBG IX immer dann einzurichten, wenn in einer Organisation mindestens fünf schwerbehinderte Menschen nicht nur vorübergehend beschäftigt sind. Abweichend von den Regelungen des BetrVG sind dabei auch leitende Angestellte in den berücksichtigenden Personenkreis einzubeziehen. Die Tätigkeit der SBV ist eng mit dem Beschäftigungsverhältnis verknüpft. Die Regelungen des § 26 BDSG bei nicht-öffentlichen Arbeitgebenden bzw. aus den Landesdatenschutzgesetzen (z. B. § 15 LDSG BW) gelten entsprechend.

Die Verarbeitung personenbezogener Daten durch die SBV kann insbesondere zulässig sein, wenn

* es dafür eine klare gesetzliche Grundlage gibt (z. B. § 167 Abs. 2 SGB IX zum Betrieblichen Eingliederungsmanagement (BEM), wo nach Zustimmung der betroffenen Person[[67]](#footnote-67) die SBV wie auch eine Mitarbeitervertretung in den Prozess einbezogen werden darf),
* der Beschäftigte eingewilligt hat oder
* eine entsprechende kollektivrechtliche Vereinbarung (Betriebsvereinbarung o.ä.) besteht.

Bzgl. Betriebsvereinbarung siehe auch den Hinweis zum laufenden EuGH-Verfahren in Kapitel 7.1.1.2.

Die Aufgaben der SBV sind u.a. in § 178 SGB IX geregelt.

* Nach § 178 Abs. 1 SGV IX unterstützt die SBV beschäftigte Personen bei Anträgen auf Feststellung einer Behinderung, ihres Grades und einer Schwerbehinderung bei den nach § 152 Abs 1 SGB IX zuständigen Behörden sowie bei Anträgen auf Gleichstellung bei der Agentur für Arbeit. Die Unterstützung erfolgt auf der Grundlage einer vorausgehenden Einwilligung des Beschäftigten.
* Gemäß § 178 Abs. 2 S. 4 SGB IX hat die SBV bei Bewerbungen ein Recht auf Einsicht in die entscheidungsrelevanten[[68]](#footnote-68) Teile der Bewerbungsunterlagen, und zwar nicht nur der schwerbehinderten Menschen, sondern sämtlicher Bewerber. Entsprechend hat die SBV ein Teilnahmerecht an den Vorstellungsgesprächen der schwerbehinderten und der nicht behinderten Bewerbern; dies allerdings nur, wenn sich ein schwerbehinderter oder gleichgestellter behinderter Mensch beworben hat.[[69]](#footnote-69)
* Ein Einsichtsrecht der SBV in die Personalakte besteht dagegen nur, wenn der schwerbehinderte Mensch zuvor ausdrücklich hierin nach Maßgabe der DS-GVO eingewilligt hat (§ 178 Abs. 3 SGB IX).

Auch in diesen Fällen ist für die Verarbeitung von personenbezogenen Daten durch eine SBV immer eine Einwilligung der jeweiligen von der Verarbeitung betroffenen Person erforderlich. Dies gilt ebenfalls für ein Einsichtsrecht der SBV in die Personalakte. Der schwerbehinderte Mensch hat zuvor ausdrücklich hierin nach Maßgabe der DS-GVO einzuwilligen (§ 178 Abs. 3 SGB IX).

Möchte der Arbeitgeber Darlehen oder Zuschüsse für die Schaffung von Arbeits- und Ausbildungsplätze für schwerbehinderte Menschen gemäß § 15 SchwAV oder Leistungen zur behindertengerechten Einrichtung von Arbeits- und Ausbildungsplätzen für schwerbehinderte Menschen gemäß § 26 SchwAV stellen, so kann die Antragstellung beim Inklusionsamt und folglich die Weitergabe von personenbezogenen Daten (z.B. Arbeitsvertrag, Gehalts- und Lohnabrechnung, Kopie des Schwerbehindertenausweises, etc.) nur auf Basis einer Einwilligung durch den Beschäftigten erfolgen.

Das Führen einer Schwerbehindertendatei gehört nicht zu den gesetzlichen Aufgaben der SBV. Ohne besonderen Anlass ist diese in der Regel unzulässig. Sie kann somit regelmäßig nur angelegt und verwendet werden, wenn die betroffenen Personen hierzu vorab, freiwillig und (bei Gesundheitsdaten) ausdrücklich ihre Einwilligung erteilt haben.

## Kirchenrecht

### Landeskrankenhausrecht und Regelungen von Religionsgemeinschaften

Die Frage, ob für Krankenhäuser, welche von Religionsgemeinschaften wie beispielsweise der evangelischen oder katholischen Kirche betrieben werden, die Landesgesetze für Krankenhäuser ebenfalls gelten oder nicht, wird in der Praxis immer wieder gestellt.

Unabhängig von den Erläuterungen in Kap. 6.7 sind bei der Beantwortung dieser Fragestellung zwei Aspekte zu berücksichtigen:

1. Fallen die jeweiligen Krankenhäuser in den Geltungsbereich der entsprechenden Landesgesetze?
2. Enthalten die jeweiligen Landesgesetze Ausnahmetatbestände für Religionsgemeinschaften?

#### Geltungsbereich der Landeskrankenhausgesetze

Der Geltungsbereiche der Landeskrankenhausgesetze sind in Deutschland sehr unterschiedlich geregelt. Einige Gesetze gelten beispielsweise für Krankenhäuser, welche nach dem Krankenhausfinanzierungsgesetz (KHG) gefördert werden, einige beziehen sich auf die Definition von Krankenhäusern im KHG, wieder andere beanspruchen, für alle Krankenhäuser des Bundeslandes zu gelten, wieder andere orientieren sich an im SGB V zu findenden Begriffsbestimmungen. Eine Übersicht gibt nachfolgende Tabelle:

| **Bundesland** | **Regelung** | **Alle Krkh.** | **KHG** | **SGB V** |
| --- | --- | --- | --- | --- |
| Baden-Württemberg | § 2 LKHG |  | förderfähig |  |
| Bayern | Art. 2 BayKrG |  | förderfähig |  |
| Berlin | § 2 LKG | X |  |  |
| Brandenburg | § 1 BbgKHEG | X |  |  |
| Bremen | § 1 BremKrhG | X |  |  |
| Hamburg | § 2 HmbKHG | X |  |  |
| Hessen | § 2 HKHG 2011 | X |  |  |
| Mecklenburg-Vorpommern | § 3 LKHG M-V | X |  |  |
| Niedersachsen | § 1 Abs. 2 NKHG |  | § 2 Nr. 1 | 107 Abs. 2 |
| Nordrhein-Westfalen | § 2 GDSG NW |  |  | § 107 Abs. 1 u. 2, § 108, § 111 |
| Rheinland-Pfalz | § 3 LKG |  | § 2 Nr. 1 |  |
| Saarland | § 2 SKHG | X |  |  |
| Sachsen | § 2 SächsKHG |  | § 8 Abs. 1 S. 1 |  |
| Sachsen-Anhalt | § 1 KHG LSA |  | § 1 Abs. 1 |  |
| Schleswig-Holstein | § 2 LKHG |  | Förderfähig |  |
| Thüringen | § 3 ThürKHG |  | § 2 Nr. 1 |  |

Die Definitionen im KHG und im SGB V sind leider nicht übereinstimmend:

* § 2 Nr. 1 KHG: Krankenhäuser = Einrichtungen, in denen durch ärztliche und pflegerische Hilfeleistung Krankheiten, Leiden oder Körperschäden festgestellt, geheilt oder gelindert werden sollen oder Geburtshilfe geleistet wird und in denen die zu versorgenden Personen untergebracht und verpflegt werden können.
* § 107 SGB V
  + Abs. 1 definiert Krankenhäuser, Abs. 2 Vorsorge- oder Rehabilitationseinrichtungen
  + Krankenhäuser sind Einrichtungen, die
    1. der Krankenhausbehandlung oder Geburtshilfe dienen,
    2. fachlich-medizinisch unter ständiger ärztlicher Leitung stehen, über ausreichende, ihrem Versorgungsauftrag entsprechende diagnostische und therapeutische Möglichkeiten verfügen und nach wissenschaftlich anerkannten Methoden arbeiten,
    3. mit Hilfe von jederzeit verfügbarem ärztlichem, Pflege-, Funktions- und medizinisch-technischem Personal darauf eingerichtet sind, vorwiegend durch ärztliche und pflegerische Hilfeleistung Krankheiten der Patienten zu erkennen, zu heilen, ihre Verschlimmerung zu verhüten, Krankheitsbeschwerden zu lindern oder Geburtshilfe zu leisten,

und in denen

* + 1. die Patienten untergebracht und verpflegt werden können.
  + Vorsorge- oder Rehabilitationseinrichtungen sind Einrichtungen, die

1. der stationären Behandlung der Patienten dienen, um
   1. eine Schwächung der Gesundheit, die in absehbarer Zeit voraussichtlich zu einer Krankheit führen würde, zu beseitigen oder einer Gefährdung der gesundheitlichen Entwicklung eines Kindes entgegenzuwirken (Vorsorge) oder
   2. eine Krankheit zu heilen, ihre Verschlimmerung zu verhüten oder Krankheitsbeschwerden zu lindern oder im Anschluss an Krankenhausbehandlung den dabei erzielten Behandlungserfolg zu sichern oder zu festigen, auch mit dem Ziel, eine drohende Behinderung oder Pflegebedürftigkeit abzuwenden, zu beseitigen, zu mindern, auszugleichen, ihre Verschlimmerung zu verhüten oder ihre Folgen zu mildern (Rehabilitation), wobei Leistungen der aktivierenden Pflege nicht von den Krankenkassen übernommen werden dürfen.
2. fachlich-medizinisch unter ständiger ärztlicher Verantwortung und unter Mitwirkung von besonders geschultem Personal darauf eingerichtet sind, den Gesundheitszustand der Patienten nach einem ärztlichen Behandlungsplan vorwiegend durch Anwendung von Heilmitteln einschließlich Krankengymnastik, Bewegungstherapie, Sprachtherapie oder Arbeits- und Beschäftigungstherapie, ferner durch andere geeignete Hilfen, auch durch geistige und seelische Einwirkungen, zu verbessern und den Patienten bei der Entwicklung eigener Abwehr- und Heilungskräfte zu helfen,

und in denen

1. die Patienten untergebracht und verpflegt werden können.

§ 8 Abs. 1 S. 1 KHG beschreibt, welche Krankenhäuser förderfähig sind, zielt also ebenfalls auf die Förderfähigkeit ab. § 108 SGB V beinhaltet die Vorgaben, welche Krankenhausbehandlung von gesetzlichen Krankenkassen bezahlt werden dürfen und § 111 SGB V adressiert Versorgungsverträge zwischen Krankenkassen und Vorsorge- oder Rehabilitationseinrichtungen.

Alle von Religionseinrichtungen betriebenen Krankenhäuser werden entsprechend KHG gefördert und entsprechen den Begriffsbestimmungen bzgl. Krankenhäuser sowohl im KHG als auch im SGB V, sodass die jeweiligen Landesgesetze auch für von Religionseinrichtungen betriebenen Krankenhäuser gelten.

#### Ausnahmetatbestände in Landeskrankenhausgesetzen

Diverse Landeskrankenhausgesetze enthalten Ausnahmetatbestände für Religionsgemeinschaften. Diese betreffen in folgenden Bundesländern jedoch nicht die für Krankenhäuser geltenden datenschutzrechtlichen Regelungen:

* Baden-Württemberg,
* Brandenburg,
* Hessen,
* Mecklenburg-Vorpommern,
* Rheinland-Pfalz,
* Sachsen,
* Thüringen.

Keine Ausnahmen beinhalten die Regelungen der folgenden Bundesländer:

* Bayern,
* Berlin,
* Niedersachsen,
* Sachsen-Anhalt.

Einige Landeskrankenhausgesetze enthalten Regelungen, welche Religionsgemeinschaften erlauben, eigene Datenschutzregelungen für die Verarbeitung von Patientendaten zu erlassen. Ist dies erfolgt, sind diese anwendbar. Entsprechende Öffnungstatbestände weisen folgende Landesgesetz auf:

* Bremen: § 36 BremKrhG,
* Hamburg: § 7 Abs. 4 HmbKHG,
* Nordrhein-Westfalen: § 2 Abs. 3 GDSG NW,
* Saarland: § 2 Abs. 2 Saarländisches Krankenhausgesetz,
* Schleswig-Holstein: § 2 Abs. 4 LKHG.

Die Landeskrankenhausgesetze erlauben i. d. R. jedoch nur „gleichwertige“ Regelungen von Religionsgemeinschaften, d. h. Regelungen, welche den Umgang mit Patientendaten im Krankenhaus adressieren.

#### Ergebnis

Wenn man im jeweiligen Bundesland nach Erwägung aller Umstände zum Ergebnis kommt, dass die datenschutzrechtlichen Landesregelungen für Krankenhäuser auch für von Religionsgemeinschaften betriebenen Krankenhäuser gelten, so gelten neben allen anderen Vorgaben selbstverständlich auch die Erlaubnistatbestände zur Verarbeitung von personenbezogenen Daten (siehe Kap. 7.2.2) für diese Einrichtungen.

### Erlaubnistatbestände der ev. Kirche in Bezug auf Patientenversorgung

Die evangelische Kirche unterteilt sich in Deutschland in verschiedene Regionen, ähnlich wie Deutschland selbst sich auch in die Bundesländer aufteilt. Einige erließen spezielle Regelungen zur Patientenversorgung, andere wiederum nicht.

#### Bremische evangelische Kirche

Die bremische evangelische Kirche erließ 2021 eine Patientendatenverordnung (PatientendatenVO)[[70]](#footnote-70). Diese gilt gemäß § 1 Abs. 1 PatientendatenVO für die Verarbeitung von Patientendaten durch Krankenhäuser in Trägerschaft einer kirchlichen Stelle der Bremischen Evangelischen Kirche, wobei Krankenhäuser entsprechend § 1 Abs. 2 PatientendatenVO gemäß § 2 Nr. 1 Krankenhausfinanzierungsgesetz definiert werden.

§ 36 Abs. 3 BremKrhG enthält die Öffnungsklausel, dass bei Krankenhäusern, die von kirchlichen oder religiösen Vereinigungen oder Gemeinschaften oder diesen zuzuordnenden Einrichtungen betrieben werden, die Vorschriften des achten Abschnitts des BremKrhG („Datenschutz“) nur gelten, wenn die kirchlichen oder religiösen Vereinigungen oder Gemeinschaften keine Regeln entsprechenden erließen, welche den Anforderungen des Art. 91 DS-GVO genügen. Bzgl. Anforderungen aus dem Europarecht an Regelungen der Religionsgemeinschaften wird auf Kap. 6.7 verwiesen.

Mit der PatientendatenVO existiert für das Bundesland Bremen eine eigene Regelung, sodass die Datenschutzvorgaben des BremKrhG für die Verarbeitung von Patientendaten nicht anwendbar sind, sondern die der PatientendatenVO.

§ 3 PatientendatenVO benennt Erlaubnistatbestände zur Verarbeitung von Patientendaten ohne Einwilligung:

* § 3 Abs. 1 Nr. 1 PatientendatenVO: Hier wird die Verarbeitung von Patientendaten in dem Umfang erlaubt, welcher zur Erfüllung der Pflichten des Behandlungsvertrages erforderlich ist. Damit korrespondiert diese Vorschrift mit Art. 9 Abs. 2 lit. h DS-GVO, d. h. u. a. müssen die Vorgaben von Art. 9 Abs. 3 DS-GVO erfüllt werden. Durch den Verweis auf den Behandlungsvertrag wird hier Art. 6 Abs. 1 lit. b DS-GVO als der entsprechende Rechtfertigungstatbestand anwendbar sein.
* § 3 Abs. 1 Nr. 2 PatientendatenVO: Diese Regelung adressiert § 115 SGB V, d. h. dreiseitige Verträge und Rahmenempfehlungen zwischen Krankenkassen, Krankenhäusern und Vertragsärzten. Existieren in Bremen entsprechende Verträge zwischen Leistungsträgern, Kassenärztlicher Vereinigung und Landeskrankenhausgesellschaft, so wird mit dieser Regelung die Verarbeitung der Patientendaten erlaubt.

Diese Regelung dient zwar der Versorgung von Patienten, adressiert jedoch nicht den Behandlungsvertrag. Entsprechend § 115 Abs. 2 SGB V soll die Versorgungsstruktur verbessert werden. § 115 SGB V adressiert nicht die Versorgung des jeweiligen Patienten, sondern – ähnlich wie ein Krankenhausbedarfsplan – strukturelle Formen der Versorgung.

Daher kann Art. 9 Abs. 2 lit. h DS-GVO hier nicht herangezogen werden. Art. 9 Abs. 2 lit. i DS-GVO erlaubt die Verarbeitung personenbezogener Daten zur „Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung“, was durch § 115 SGB V erreicht werden soll.

Somit beruht § 3 Abs. 1 Nr. 2 PatientendatenVO auf Art. 9 Abs. 2 lit. i DS-GVO, korrespondierender Rechtfertigungstatbestand ist Art. 6 Abs. 1 lit. e DS-GVO.

Art. 6 Abs. 1 lit. e DS-GVO bedingt, dass die Vorgaben von Art. 6 Abs. 3 DS-GVO erfüllt sind. Diese sind:

* 1. Zweck der Verarbeitung muss in der Rechtsgrundlage festgehalten sein. Die Rechtsgrundlage ist § 115 SGB V, worin die Zwecke allerdings offenbleiben; § 115 Abs. 2 SGB V ist nur eine beispielhafte, aber keine abschließende Aufzählung. Da die Zwecke in der Rechtsgrundlage angegeben werden müssen, ist eine Festlegung im jeweiligen auf § 115 SGB V beruhenden Vertrag unzureichend.
  2. Erforderlichkeit der Verarbeitung der Patientendaten kann aufgrund der fehlenden Zweckangabe in der Rechtsgrundlage ebenfalls nicht bewertet werden. Jedoch sollten Rechtsanwender zumindest prüfen, ob im auf den Vorgaben von § 115 SGB V beruhenden Vertrag nur erforderliche Verarbeitungen und erforderliche Patientendaten gefordert werden.
* § 3 Abs. 1 Nr. 3 PatientendatenVO: Patientendaten dürfen entsprechend dieser Regelung zur Erkennung, Verhütung und Bekämpfung von Krankenhausinfektionen genutzt werden. Auch diese Regelung korrespondiert mit Art. 9 Abs. 2 lit. i DS-GVO, Art. 6 Abs. 1 lit. e DS-GVO ist der entsprechende Rechtfertigungstatbestand. Daher muss hier ebenfalls beachtet werden, ob die Vorgaben von Art. 6 Abs. 3 DS-GVO erfüllt sind (s. Hinweise zu § 3 Abs. 1 Nr. 2 PatientendatenVO).
* § 3 Abs. 1 Nr. 4 PatientendatenVO: Gemäß dieser Regelung dürfen Patientendaten zur Aus-, Fort- oder Weiterbildung eines Heilberufs oder eines Gesundheitsfachberufs im Krankenhaus verarbeitet werden.

Diese Regelung findet keine Entsprechung in Art. 9 Abs. 2 DS-GVO.

* § 3 Abs. 1 Nr. 5 PatientendatenVO: Patientendaten können entsprechend dieser Regelung zu Zwecken der Qualitätssicherung der Behandlung im Krankenhaus und zur Durchführung qualitätssichernder Maßnahmen verarbeitet werden. Diese Regelung beruht auf Art. 9 Abs. 2 lit. i DS-GVO, folglich ist auch hier Art. 6 Abs. 1 lit. e DS-GVO der entsprechende Rechtfertigungstatbestand. Auch hier muss daher beachtet werden, ob die Vorgaben von Art. 6 Abs. 3 DS-GVO erfüllt sind (s. Hinweise zu § 3 Abs. 1 Nr. 2 PatientendatenVO).
* § 3 Abs. 1 Nr. 6 PatientendatenVO: Diese Regelung erlaubt die Verarbeitung von Patientendaten „zur verwaltungsmäßigen Abwicklung des Behandlungsverhältnisses, insbesondere zur Abrechnung der erbrachten Leistungen, einschließlich belegärztlicher und wahlärztlicher Leistungen“. Diese Regelung findet ihre Entsprechung in Art. 9 Abs. 2 lit. f DS-GVO, denn die Berechnung erbrachter Gesundheitsleistungen wie auch die Überprüfung dieser Abrechnungen ist Bestandteil der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen. Bzgl. Rechtfertigungstatbestand aus Art. 6 DS-GVO wird auf Kap. 5.6 verwiesen.

### Erlaubnistatbestände der kath. Kirche in Bezug auf Patientenversorgung

#### Seelsorge im Krankenhaus

Das „Gesetz zum Schutz von Patientendaten bei der Seelsorge in katholischen Einrichtungen des Gesundheitswesens in der (Erz-)Diözese[[71]](#footnote-71)“ (SeelsorgePatDSG) gilt gemäß § 1 Abs. 1 SeelsorgePatDSG für die Verarbeitung von Patientendaten bei der Seelsorge in katholischen Einrichtungen des Gesundheitswesens. Das Krankenhaus selbst wird in der Regelung nicht definiert, wohl aber Patientendaten (§ 2 Abs. 1 lit. b SeelsorgePatDSG).

Der Begriff der Patientendaten wird im SeelsorgePatDSG weit gefasst: Gemäß § 2 Abs. 1 lit. b Seelsorge-PatDSG sind Patientendaten alle personenbezogenen Daten von Patienten der katholischen Einrichtung des Gesundheitswesens sowie zudem personenbezogene Daten von Angehörigen, Begleitpersonen oder anderen Bezugspersonen des Patienten sowie sonstiger Dritter, soweit sie der katholischen Einrichtung des Gesundheitswesens im Zusammenhang mit der Behandlung des Patienten bekannt werden. Dies gilt ungeachtet ihrer Eigenschaft als „Dritte“ im Sinne des § 4 Nr. 12 KDG (analog Art. 4 Nr. 10 DS-GVO). Patientendaten sind „Gesundheitsdaten“ im Sinne des § 4 Nr. 17 KDG (analog Art. 4 Nr. 15 DS-GVO) und fallen unter die besonderen Kategorien personenbezogener Daten.

Inwieweit diese Regelung in Krankenhäusern Anwendung finden muss, regelt sich nach den Vorgaben im jeweiligen Landeskrankenhausgesetz. Die in diesem Gesetz enthaltenen Regelungen stellen keine Alternative zu den Datenschutzregelungen in den Landeskrankenhausgesetzen dar, sodass es vielleicht eher als Ergänzung der jeweiligen Landesregelung angesehen werden kann.

§ 3 Abs. 1 SeelsorgePatDSG gestattet die Verarbeitung von Patientendaten durch einen Krankenhausseelsorger im Rahmen des § 11 Abs. 2 KDG (analog Art. 9 Abs. 2 DS-GVO), „wenn im Rahmen des Behandlungsvertrages auf die konzeptionelle Implementierung von Krankenhausseelsorge und die damit einhergehende Einbindung eines Krankenhausseelsorgers in das Behandlungsteam in angemessener Form hingewiesen wird“.

Gemäß § 4 Seelsorge-PatDSG darf ein Patient beim Abschluss des Behandlungsvertrages unter Hinweis auf die Freiwilligkeit und die Folgen seiner Angabe zum Zwecke der Seelsorge nach seiner Religion/Konfession befragt werden. Ist die Seelsorge vom Verantwortlichen nicht im System der katholischen Einrichtung des Gesundheitswesens konzeptionell implementiert, dürfen einer mit Seelsorgeauftrag der zuständigen kirchlichen Stelle ausgestatteten Person auch bei fehlender ausdrücklicher Einwilligung zum Zwecke der Seelsorge ausschließlich Vor- und Nachname des Patienten, seine Religion/Konfession, sein Aufenthaltsort in der katholischen Einrichtung des Gesundheitswesens sowie das Aufnahmedatum offengelegt werden, soweit der Patient eine Religion/Konfession angegeben hat. Dies gilt allerdings nicht, wenn ein Patient deutlich gemacht hat, dass keine Seelsorge gewünscht wird.

Dieses Kirchengesetz regelt die Erlaubnis in katholischen Einrichtungen, Patientendaten für die Seelsorge, als unmittelbarer Ausdruck des Auftrags der Kirche zum Dienst am Menschen, zu nutzen. Seelsorge versteht sich in diesem Kontext ohne Ansehung der Religions- bzw. Konfessionszugehörigkeit des Patienten in Ergänzung zur medizinischen, pflegerischen und sozialen Behandlung als spiritueller und ethischer Beitrag zu einer ganzheitlichen Behandlung („spiritual care“). Damit wird die Verarbeitung von Patientendaten ohne Einwilligung erlaubt, daher kann die Regelung nur aus Art. 9 Abs. 2 lit. d DS-GVO abgeleitet werden.

Art. 9 Abs. 2 lit. d DS-GVO verlangt, dass entsprechende Regelungen sich ausschließlich auf die Mitglieder oder ehemalige Mitglieder beziehen. D. h. diese Regelungen darf aufgrund europarechtlicher Vorgaben nur auf Mitglieder der katholischen Kirche angewendet werden. Da ggf. auch Nicht-Mitglieder der katholischen Kirche religiösen Beistand wünschen, z. B. Mitglieder der evangelischen Kirche, könnte ein Krankenhaus – falls von diesem gewünscht – hier eine entsprechende Möglichkeit auf Grundlage einer Einwilligung der betroffenen Person schaffen.

§ 3 Abs. 1 SeelsorgePatDSG beruht auf Art. 9 Abs. 2 lit. d DS-GVO, dazu findet sich keine direkte Entsprechung in Art. 6 Abs. 1 DS-GVO. Gleichwohl darf die Verarbeitung nicht ohne entsprechenden Rechtfertigungstatbestand erfolgen. Die seelische Betreuung ist eine Kernaufgabe der katholischen Kirche, die allen Mitgliedern der katholischen Kirche gewährt werden muss. Entsprechend wird man für Mitglieder der katholischen Kirche Art. 6 Abs. 1 lit. b DS-GVO (Erfüllung vertraglicher Pflichten) als Rechtfertigungstatbestand heranziehen können. Jedoch ist zu beachten, dass das Europarecht nur „erforderliche“ Verarbeitungen erlaubt; die Begrenzung auf die Erforderlichkeit fehlt in der kirchlichen Regelung.

## Landesrecht

### Landeskrankenhausgesetze

#### Patientenbehandlung

Diverse Landeskrankenhausgesetze enthalten die Erlaubnis, Patientendaten zur Behandlung zu nutzen:

* § 45 Abs. 1 Ziff. 1 LKHG Baden-Württemberg
* Art. 27 Abs. 4 S. 1 BayKrG
* § 24 Abs. 4 Ziff. 2 LKG Berlin
* § 28 Abs. 1 Ziff. 1 BbgKHEG
* § 38 Abs. 1 Ziff. 1 BremKrhG
* § 10 Abs. 1 Ziff. 1, 2 HmbKHG
* § 33 Abs. 1 LKHG M-V
* § 10 Abs. 1 Buchst. a GDSG NW
* § 36 Abs. 2 Ziff. 1 LKG RP
* § 13 Abs. 2 SKHG
* § 28 Abs. 3 Ziff. 1 SächsKHG
* § 16 Abs. 3 Ziff. 2 KHG LSA
* § 36 Abs. 1 Ziff. 1 und 2 LKHG Schleswig-Holstein
* § 27 Abs. 3 Ziff. 1 ThürKHG

Diese Regelungen stellen das jeweilige in Art. 9 Abs. 2 lit. h DS-GVO aufgeführte „Recht eines Mitgliedstaats“ dar. Zu beachten ist hier, dass dieses nationale Recht nur unter den Voraussetzungen von Art. 9 Abs. 3 DS-GVO Anwendung finden darf, d. h.

* diese Daten müssen von Fachpersonal oder unter dessen Verantwortung verarbeitet werden und
* dieses Fachpersonal muss nach dem Unionsrecht oder dem Recht eines Mitgliedstaats oder den Vorschriften nationaler zuständiger Stellen dem Berufsgeheimnis unterliegen, oder wenn die Verarbeitung durch eine andere Person erfolgt, die ebenfalls nach dem Unionsrecht oder dem Recht eines Mitgliedstaats oder den Vorschriften nationaler zuständiger Stellen einer Geheimhaltungspflicht unterliegt.

In Deutschland wird dies erfüllt, wenn die Vorgaben von § 203 StGB erfüllt sind, bei ärztlichem Personal gelten ergänzend die Vorgaben zur Schweigepflicht in der jeweiligen Landesberufsordnung für Ärztinnen und Ärzte.

In all diesen Fällen liegt entsprechend deutschem Recht immer auch ein Behandlungsvertrag vor, sodass der in Art. 6 Abs. 1 lit. b DS-GVO enthaltene Rechtfertigungstatbestand anwendbar ist.

#### Forschung

Diverse Landeskrankenhausgesetze enthalten die Erlaubnis, Patientendaten zur Forschung zu nutzen:

* Art. 27 Abs. 4 S. 1 BayKrG
* § 25 Abs. 1 LKG Berlin
* § 31 BbgKHEG
* § 39 Abs. 1 Ziff. 1 und Abs. 2 BremKrhG
* § 12 Abs. 1 HmbKHG
* § 37 Abs. 1, 2 LKHG M-V
* § 34 Abs. 1 Ziff. 1 LKHG M-V i. V. m. § 37 LKHG M-V
* § 6 Abs. 1, 2 GDSG NW
* § 37 Abs. 1, 2, 3 LKG RP
* § 14 Abs. 1, 2, 3 SKHG
* § 29 Abs. 1, 2, 3 SächsKHG
* § 17 Abs. 1, 2, 3 KHG LSA
* § 38 Abs. 1 LKHG Schleswig-Holstein
* § 27 Abs. 4 S. 1 ThürKHG  
  § 27a Abs. 1, 2 ThürKHG

Sofern die Regelung im jeweiligen Landesgesetz auf eine erforderliche Verarbeitung begrenzt ist, findet diese Regelung ihre Entsprechung in Art. 9 Abs. 2 lit. j DS-GVO („für wissenschaftliche oder historische Forschungszwecke“). Zu beachten ist hierbei:

1. Art. 9 Abs. 2 lit. j DS-GVO verlangt, dass das nationale Recht
   1. in angemessenem Verhältnis zu dem verfolgten Ziel steht,
   2. den Wesensgehalt des Rechts auf Datenschutz wahrt und
   3. angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht;

dies ist im jeweiligen Landesrecht zu prüfen.

1. Ergänzend muss Art. 89 Abs. 1 DS-GVO beachtet werden. Dies bedeutet, dass das nationale Recht
   1. geeigneten Garantien für die Rechte und Freiheiten der betroffenen Person gemäß der DS-GVO vorsieht und
   2. diese Garantien sicherstellen, dass technische und organisatorische Maßnahmen bestehen, mit denen insbesondere die Achtung des Grundsatzes der Datenminimierung gewährleistet wird.

Auch dies ist im jeweiligen Landesrecht zu prüfen.

#### Soziale Betreuung

Diverse Landeskrankenhausgesetze enthalten die Erlaubnis, Patientendaten zur sozialen Betreuung und Beratung der Patientin oder des Patienten zu nutzen:

* § 28 Abs. 1 Ziff. 3 BbgKHEG
* § 10 Abs. 1 Ziff. 3 HmbKHG
* § 13 Abs. 3 SKHG
* § 28 Abs. 4 Ziff. 9 SächsKHG
* § 16 Abs. 3 Ziff. 4 KHG LSA
* § 36 Abs. 1 Ziff. 3 LKHG Schleswig-Holstein

Ist diese soziale Betreuung im Kontext der Versorgung oder Behandlung im Gesundheits- oder Sozialbereich, ggf. auch post-stationär, erforderlich, stellen diese Regelungen das jeweilige in Art. 9 Abs. 2 lit. h DS-GVO aufgeführte „Recht eines Mitgliedstaats“ dar. Zu beachten ist hier, dass dieses nationale Recht nur unter den Voraussetzungen von Art. 9 Abs. 3 DS-GVO Anwendung finden darf (siehe 7.3.1.1).

Entsprechend deutschem Recht liegt in diesen Fällen im Krankenhaus immer auch ein Behandlungsvertrag mit den jeweiligen Patienten vor, sodass der in Art. 6 Abs. 1 lit. b DS-GVO enthaltene Rechtfertigungstatbestand anwendbar ist.

#### Rechnungsprüfung und -stellung

Einige Landeskrankenhausgesetze enthalten die Erlaubnis, Patientendaten für Zwecke der verwaltungsmäßigen Abwicklung des Behandlungsverhältnisses, insbesondere zur Abrechnung der erbrachten Leistungen des Patienten sowie zur Rechnungsprüfung zu nutzen:

* § 45 Abs. 1 Ziff. 2 LKHG Baden-Württemberg,  
  Rechnungsprüfung § 45 Abs. 3 Ziff. 3 LKHG Baden-Württemberg
* Art. 27 Abs. 4 S. 4 BayKrG
* § 24 Abs. 4 Ziff. 3 LKG Berlin
* § 28 Abs. 1 Ziff. 2 BbgKHEG
* § 38 Abs. 1 Ziff. 6 BremKrhG
* § 10 Abs. 1 Ziff. 4 HmbKHG  
  § 11 Abs. 1 Ziff. 8 HmbKHG Übermittlung zu Zwecken der Rechnungs-, Krankenhausentgelt- und Pflegesatzprüfung  
  § 11 Abs. 1 Ziff. 5 HmbKHG Übermittlung zur Abwehr von Ansprüchen oder Verfolgung von Straftaten oder Ordnungswidrigkeiten, die gegen das Krankenhaus oder seine Mitarbeiterinnen und Mitarbeiter gerichtet sind
* § 34 Abs. 1 Ziff. 1, 6 LKHG M-V
* § 10 Abs. 1 Buchst. a GDSG NW  
  § 11 Abs. 1 Buchst. d, e GDSG NW bzgl. Übermittlung
* § 13 Abs. 2 SKHG  
  § 13 Abs. 4 Ziff. 8 SKHG Übermittlung zur Rechnungsprüfung
* § 28 Abs. 4 Ziff. 7 SächsKHG bzgl. Übermittlung zu Abrechnungszwecken
* § 16 Abs. 3 Ziff. 1, 3, 10 KHG LSA
* § 36 Abs. 1 Ziff. 7 LKHG Schleswig-Holstein
* § 27 Abs. 5 ThürKHG

Sofern dies auf die erforderliche Verarbeitung begrenzt ist, findet diese Regelungen ihre Entsprechung in Art. 9 Abs. 2 lit. f DS-GVO, denn die Abrechnung erbrachter Gesundheitsleistungen wie auch die Überprüfung dieser Abrechnungen ist Bestandteil der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen. Bzgl. Rechtfertigungstatbestand aus Art. 6 DS-GVO wird auf Kap. 5.6 verwiesen.

#### Zwecke der Qualitätssicherung

Die meisten Landeskrankenhausgesetze enthalten für die Krankenhausbetreiber die Befugnis die Patientendaten zu Zwecken der Qualitätssicherung zu nutzen:

* § 45 Abs. 3 Ziff. 1 LKHG Baden-Württemberg  
  § 46 Abs. 1 Ziff. 2 LKHG Baden-Württemberg bzgl. Übermittlung an externe Stellen
* § 24 Abs. 4 Ziff. 4 LKG Berlin
* § 28 Abs. 2 Ziff. 1 BbgKHEG  
  § 29 Ziff. 2 BbgKHEG für Übermittlung an externe Stellen
* § 38 Abs. 1 Ziff. 5 BremKrhG  
  § 40 Abs. 1 Ziff. 8 BremKrhG bzgl. Übermittlung an externe Stellen
* § 10 Abs. 1 Ziff. 7 HmbKHG
* § 12 Abs. 2 Ziff. 7 HKHG 2011, Übermittlung an externe Stellen
* § 34 Abs. 1 Ziff. 1 LKHG M-V
* § 11 Abs. 2 GDSG NW
* § 36 Abs. 2 Ziff. 2 LKG RP  
  § 36 Abs. 3 Ziff. 4 LKG RP bzgl. Übermittlung
* § 13 Abs. 4 Ziff. 10 SKHG Übermittlung zur Qualitätssicherung in der stationären Versorgung,
* § 28 Abs. 4 Ziff. 5 SächsKHG bzgl. Übermittlung
* § 16 Abs. 3 Ziff. 6 KHG LSA
* § 36 Abs. 1 Ziff. 10 LKHG Schleswig-Holstein
* § 27 Abs. 5 ThürKHG bzgl. Übermittlung zur Durchführung qualitätssichernder Maßnahmen in der Krankenversorgung

Sofern diese Regelung auf eine erforderliche Verarbeitung begrenzt ist und insbesondere die „Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten“ adressiert, findet diese Regelung ihre Entsprechung in Art. 9 Abs. 2 lit. i DS-GVO. Zu beachten ist hierbei, dass Art. 9 Abs. 2 lit. i DS-GVO von entsprechendem nationalem Gesetz fordert

1. nur erforderliche Verarbeitungen zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung sind erlaubt,
2. nur erforderliche Daten werden verarbeitet,
3. die nationale Regelung sieht „angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person“ vor und
4. das Berufsgeheimnis bleibt gewahrt.

Dies ist im jeweiligen Landesrecht zu prüfen.

Entsprechend deutschem Recht liegt in diesen Fällen zwar immer auch ein Behandlungsvertrag mit den jeweiligen Patienten vor, jedoch erfolgt die Qualitätssicherung patientenübergreifend, da Ereignisse oder auch Behandlungsergebnisse regelhaft von mehreren Patienten verglichen werden. Daher kann der Behandlungsvertrag für diese Verarbeitungen keinen Rechtfertigungstatbestand nach Art. 6 DS-GVO darstellen; insbesondere ist eine patientenübergreifende Qualitätssicherung nicht für die Versorgung des jeweiligen Patienten erforderlich.

Allerdings liegt eine hohe Qualität in der Patientenversorgung im öffentlichen Interesse, weswegen die Qualitätssicherung der medizinischen Versorgung auch in den Sozialgesetzbüchern verankert ist. Rechtfertigungstatbestand ist somit Art. 6 Abs. 1 lit. e DS-GVO. Die von Art. 6 Abs. 3 verlangte nationale Rechtsgrundlage für diese Aufgabe im öffentlichen Interesse stellt die jeweilige Regelung im entsprechenden Landeskrankenhausgesetz dar.

#### Auswertung zu statistischen Zwecken

Einige Landeskrankenhausgesetze enthalten die Erlaubnis, Patientendaten für statistische Zwecke zu nutzen:

* § 10 Abs. 1 Ziff. 5 HmbKHG
* § 36 Abs. 1 Ziff. 8 LKHG Schleswig-Holstein

Sofern diese Regelung auf eine erforderliche Verarbeitung begrenzt ist, findet dies die Entsprechung in Art. 9 Abs. 2 lit. j DS-GVO („statistische Zwecke“). Zu beachten ist hierbei:

1. Art. 9 Abs. 2 lit. j DS-GVO verlangt, dass das nationale Recht
   1. in angemessenem Verhältnis zu dem verfolgten Ziel steht,
   2. den Wesensgehalt des Rechts auf Datenschutz wahrt und
   3. angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht;

dies ist im jeweiligen Landesrecht zu prüfen.

1. Ergänzend muss Art. 89 Abs. 1 DS-GVO beachtet werden. Dies bedeutet, dass das nationale Recht
   1. geeigneten Garantien für die Rechte und Freiheiten der betroffenen Person gemäß der DS-GVO vorsieht und
   2. diese Garantien sicherstellen, dass technische und organisatorische Maßnahmen bestehen, mit denen insbesondere die Achtung des Grundsatzes der Datenminimierung gewährleistet wird.

Auch dies ist im jeweiligen Landesrecht zu prüfen.

#### Aus-, Fort- und Weiterbildung von Ärzten und von Angehörigen anderer Berufe des Gesundheitswesens

Verschiedene Landeskrankenhausgesetze enthalten die Erlaubnis, Patientendaten zu Zwecken der Ausbildung, Fortbildung und Weiterbildung von Ärzten und von Angehörigen anderer Berufe des Gesundheitswesens zu nutzen:

* § 45 Abs. 3 Ziff. 4 LKHG Baden-Württemberg
* Art. 27 Abs. 4 S. 1 BayKrG
* § 24 Abs. 4 Ziff. 1 LKG Berlin
* § 28 Abs. 2 Ziff. 3 BbgKHEG
* § 38 Abs. 1 Ziff. 4 BremKrhG
* § 10 Abs. 1 Ziff. 8 HmbKHG
* § 34 Abs. 1 Ziff. 5 LKHG M-V
* § 11 Abs. 2 GDSG NW
* § 36 Abs. 2 Ziff. 2 LKG RP
* § 13 Abs. 3 SKHG
* § 28 Abs. 3 Ziff. 1 SächsKHG
* § 16 Abs. 3 Ziff. 5 KHG LSA
* § 36 Abs. 1 Ziff. 11 LKHG Schleswig-Holstein
* § 27 Abs. 3 Ziff. 2, Abs. 4 S. 1 ThürKHG

Diese Regelung findet im vorliegenden Umfang keine Entsprechung in Art. 9 Abs. 2 DS-GVO.

Die Fort- und Weiterbildung von „Angehörigen eines Gesundheitsberufs“ i. S. d. Art. 9 Abs, 2 lit. h DS-GVO kann ggf. als „zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung“ i. S. v. Art. 9 Abs. 2 lit. i DS-GVO angesehen werden. Die Ausbildung selbst kann hier jedoch nicht hinzugezählt werden, denn die Betreuung von Patienten im Behandlungskontext durch nicht ausgebildetes Personal birgt aufgrund des noch nicht vorhandenen Wissens und der nicht vorhandenen Erfahrungen Risiken, was eher als (notwendiges, denn ohne Ausbildung kann es keine ausgebildeten Kräfte geben) Absenkung der Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung angesehen werden muss.

Inwieweit Fort- und Weiterbildung auf Art. 9 Abs. 2 lit. i DS-GVO gestützt werden kann, richtet sich letztlich auch danach, ob die Fort- und Weiterbildung zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung erforderlich ist oder es sich doch eher um eine Fort- und Weiterbildung zu administrativen Zwecken handelt.

Kann die Fort- und Weiterbildung auf Art. 9 Abs. 2 lit. i DS-GVO gestützt werden, können verschiedene Tatbestände aus Art. 6 Abs. 1 DS-GVO zutreffen:

* In Deutschland herrscht bei der Behandlung von Patienten durch Ärzte der sog. „Facharztstandard“, d. h., jeder Arzt schuldet dem jeweiligen Patienten eine Behandlung, die dem Standard eines sorgfältig arbeitenden Facharztes in der Situation des behandelnden Arztes entsprechen muss. Die Gewährleistung dieses Standards verlangt entsprechend den jeweiligen Landesberufsordnungen der Ärzte eine regelmäßige Fort- und Weiterbildung. Somit muss zur Erfüllung des Behandlungsvertrages gewährleistet werden, dass behandelnden Ärzte über eine entsprechende Fort- und Weiterbildung absolvierten. In diesen Fällen kann Art. 6 Abs. 1 lit. b DS-GVO den Rechtfertigungstatbestand darstellen.
* Entsprechend § 630a Abs. 2 BGB muss die Behandlung „nach den zum Zeitpunkt der Behandlung bestehenden, allgemein anerkannten fachlichen Standards“ erfolgen, soweit nicht etwas anderes vereinbart ist. Dies kann beinhalten, dass auch nicht-ärztliches Personal entsprechende Fort- und Weiterbildungen absolvieren muss, bei denen Patientendaten verarbeitet werden. Ein Beispiel hierfür ist das auf Intensivstationen arbeitende Pflegepersonal, welches aufgrund der schnellen Entwicklung von Behandlungsformen eher regelmäßig Fort- und Weiterbildung benötigt. Auch in diesen Fällen kann Art. 6 Abs. 1 lit. b DS-GVO den Rechtfertigungstatbestand darstellen.
* In anderen Fällen muss u. U. eine Interessenabwägung nach Art. 6 Abs. 1 lit. f DS-GVO erfolgen und die Fort- und Weiterbildung mit Patientendaten darf nur erfolgen, wenn die Interessen oder Grundrechte und Grundfreiheiten der jeweiligen Patienten nicht überwiegen.

#### Für Zwecke des Patienten- und Beschäftigtenschutzes, Hygiene

Einige Landeskrankenhausgesetze enthalten die Erlaubnis, Patientendaten für Zwecke des Patienten- und Beschäftigtenschutzes und zur Hygiene zu nutzen:

* § 28 Abs. 2 Ziff. 4 BbgKHEG
* § 36 Abs. 1 Ziff. 5 LKHG Schleswig-Holstein

Sofern dies auf erforderliche Verarbeitung begrenzt ist, findet dies die Entsprechung in:

* Art. 9 Abs. 2 lit. b DS-GVO: Der Schutz der Beschäftigten resultiert aus dem Arbeitsrecht, der Schutz anderer Patienten als die betroffene Person selbst ist eine Ausprägung aus dem Recht der sozialen Sicherheit und des Sozialschutzes.
* Art. 9 Abs. 2 lit. i DS-GVO: Hygieneanforderungen resultieren unmittelbar aus der Anforderung, hohe Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung zu gewährleisten.

Entsprechend deutschem Recht liegt in diesen Fällen im Krankenhaus immer auch ein Behandlungsvertrag mit den jeweiligen Patienten vor, sodass der in Art. 6 Abs. 1 lit. b DS-GVO enthaltene Rechtfertigungstatbestand anwendbar ist.

#### Unterrichtung von Angehörigen oder anderen Bezugspersonen,

Einige Landeskrankenhausgesetze enthalten die Erlaubnis, Patientendaten zur Unterrichtung von Angehörigen oder anderen Bezugspersonen auch ohne Einwilligung des betroffenen Patienten zu nutzen:

* § 11 Abs. 1 Ziff. 11 HmbKHG
* § 12 Abs. 2 Ziff. 4 HKHG 2011
* § 36 Abs. 3 Ziff. 8 LKG RP
* § 13 Abs. 4 Ziff. 7 SKHG
* § 28 Abs. 4 Ziff. 8 SächsKHG
* § 36 Abs. 1 Ziff. 4 LKHG Schleswig-Holstein

Diese Regelung findet keine Entsprechung in Art. 9 Abs. 2 DS-GVO.

### Landesrettungsdienstgesetze

Analog zum Krankenhausrecht liegt die Gesetzgebungskompetenz für die Organisation des Rettungsdienstes beim jeweiligen Landesgesetzgeber, wobei der Bundesgesetzgeber Rahmenbedingungen hinsichtlich der Finanzierung und Ausbildung geben kann, der Landesgesetzgeber ergänzend Regelungen zur Fortbildung erlassen kann.[[72]](#footnote-72)

Dementsprechend existieren in jedem Bundesland Rettungsdienstgesetze, welche die Organisation des Rettungsdienstes regeln, insbesondere auch die Erlaubnis zur Verarbeitung personenbezogener Daten durch den jeweiligen Rettungsdienst. Die Verarbeitung ist hierbei stets auf den Grundsatz der Erforderlichkeit beschränkt; da die Anforderungen von Art. 5 DS-GVO vorrangiges Recht darstellen, ergibt sich dies auch schon direkt aus Art. 5 DS-GVO.

Hinsichtlich der Abbildung der landesrechtlichen Erlaubnistatbestände zur Verarbeitung personenbezogener Daten durch den Rettungsdienst kann wie bei der Abbildung der Landeskrankenhausgesetze vorgegangen werden. Die Landesrettungsdienstgesetze enthalten typischerweise insbesondere die folgenden Erlaubnistatbestände:

* für die Erbringung von rettungsdienstlichen Leistungen und die weitere medizinische Versorgung des Patienten:

hier liegt ein Behandlungsvertrag „mit einem Angehörigen eines Gesundheitsberufs“ vor, denn die Ausbildung zum Notfallsanitäter ist gesetzlich geregelt[[73]](#footnote-73), Rettungssanitäter wiederum in Landesgesetzen.[[74]](#footnote-74) Daher kann die Argumentation aus Kap. 7.3.1.1 angewendet werden, d. h. der in Art. 6 Abs. 1 lit. b DS-GVO enthaltene Rechtfertigungstatbestand auch hier anwendbar ist;

* zur Abrechnung der erbrachten Leistungen:

hier kann die Darstellung aus Kap. 7.3.1.4 genutzt werden;

* zum Nachweis ordnungsgemäßer Ausführung des Einsatzes, zur Klärung von Ansprüchen oder zur Verteidigung im Fall einer Verfolgung wegen Straftaten oder Ordnungswidrigkeiten:

diese Vorgabe korrespondiert mit Art. 9 Abs. 2 lit. f DS-GVO, bzgl. Rechtfertigungstatbestand siehe Argumentation in Kap.5.6;

* zur Qualitätssicherung im Rettungsdienst:

auch diese Regelung ist analog zu entsprechenden Regelungen in den Landeskrankenhausgesetzen zu betrachten, inklusive der zu beachtenden europarechtlichen Vorgaben, welche in Kap. 7.3.1.5kurz angesprochen wurden, d. h. die Argumentation in Kap. 7.3.1.5 kann auch hier angewendet werden;

* zur Ausbildung, Fortbildung und Weiterbildung des im Rettungsdienst eingesetzten Personals:

hier wird auf die Ausführungen in Kap. 7.3.1.7 verwiesen;

sowie

* zur Bestimmung des Bedarfs an Rettungsmitteln:

der Rettungsdienst ist ein Element der sozialen Sicherung, weswegen derzeit Überlegungen vorhanden sind, Regelungen hierzu im SGB V zu verankern[[75]](#footnote-75). Daher ist Art. 9 Abs. 2 lit. b anwendbar, bzgl. Abbildung auf einen in Art. 6 DS-GVO genannten Rechtfertigungstatbestand siehe die Argumentation in Kap.5.2.

Einzelne Landesgesetze enthalten auch noch Regelungen

* für Zwecke der wissenschaftlichen notfallmedizinischen Forschung oder
* für die Unterrichtung von Angehörigen oder
* zur Personenauskunft bei Großschadensereignissen und Katastrophen an die zuständigen Gefahrenabwehr- und Polizeibehörden.

Auch in diesen Fällen kann analog zu den Regelungen in den Landeskrankenhausgesetzen argumentiert werden und so mindestens einer der in Art. 6 DS-GVO enthaltenen Rechtfertigungstatbestände den nationalen gesetzlichen Regelungen zugewiesen werden.

# Interessenabwägung

Der EuGH stellte fest, dass die Tatbestände von Art. 6 und 9 DS-GVO eng auszulegen sind.[[76]](#footnote-76) Entsprechend gilt dies auch für die in Art. 6 Abs. 1 lit. f DS-GVO enthaltene Interessenabwägung. Die Verarbeitung von in Art. 9 Abs. 1 DS-GVO genannten Datenkategorien kann grundsätzlich nicht allein durch eine Interessenabwägung legitimiert werden, hierzu ist immer ein in Art. 9 Abs. 2 DS-GVO enthaltener Erlaubnistatbestand erforderlich. Art. 9 Abs. 4 DS-GVO erlaubt Mitgliedsstaaten zwar die Einführung oder Aufrechterhaltung zusätzlicher Bedingungen für die in Art. 9 Abs. 2 DS-GVO genannten Erlaubnistatbestände, nicht jedoch die Schaffung neuer Ausnahmen von dem in Art. 9 Abs. 1 DS-GVO enthaltenen grundsätzlichen Verbot der Verarbeitung der dort genannten besonderen Kategorien personenbezogener Daten.

Jedoch kann Art. 6 Abs. 1 lit. f DS-GVO den ergänzend erforderlichen Rechtfertigungstatbestand darstellen. Die Vorgabe der engen Auslegung durch den EuGH bedingt allerdings, dass Verantwortliche im Zweifelsfall immer von einem überwiegenden Interesse der betroffenen Personen ausgehen müssen. Nur bei einem eindeutig erkennbaren gleichwertigen oder sogar überwiegenden Interesse des Verantwortlichen kann Art. 6 Abs. 1 lit. f DS-GVO einen Rechtfertigungstatbestand darstellen.

Aufgrund der in Art. 5 Abs. 2 DS-GVO enthaltenen Nachweispflicht muss der Verantwortliche den Nachweis bringen, dass die Interessen der betroffenen Person die eigenen nicht überwiegen.

Mindestens nachfolgende Faktoren sind bei einer Interessenabwägung zu berücksichtigen:

* Handelt es sich bei der betroffenen Person um ein Kind?
* Die Art der Daten sowie deren Sensibilität. Unterliegen die Daten beispielsweise einem Berufsgeheimnis?
* Der Umfang der Daten, die über eine Person verarbeitet werden.
* Wie wurden die Daten erhoben?
* Wurde der betroffenen Person bei der Erhebung der Umstand der Interessenabwägung sowie die Möglichkeit eines Widerspruchs gegen die darauf basierende Verarbeitung mitgeteilt?
* Der Aussagegehalt der Daten, insbesondere auch aus Sicht der betroffenen Person.
* Die Möglichkeit, Daten mit Daten aus anderen Verarbeitungsverhältnissen zu kombinieren und daraus weitergehenden Aussagen zu erhalten.
* Sollen Profile der betroffenen Person erstellt werden?
* Soll das Verhalten der betroffenen Person erkannt oder vorhergesagt werden?
* Wie hoch ist das Risiko für die Rechte und Freiheiten der betroffenen Person?
* Welche Eingreifmöglichkeiten in die Verarbeitung hat die Person?

## Vorgaben der DS-GVO

### Keine Legitimierung der Verarbeitung personenbezogener Daten durch Behörden

Entsprechend Art. 6 Abs. 1 lit. f. S. 2 DS-GVO gilt die Regelung nicht für von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitungen. Auch Verarbeitungen im Zusammenhang mit Öffentlichkeitsarbeit durch Behörden (wie beispielsweise Teilnehmerlisten oder Fotoaufnahmen) können nicht durch eine Interessenabwägung legitimiert werden.

### Mindestens zu berücksichtigende Faktoren

ErwGr. 47 S. 3 DS-GVO verlangt bei einer Interessenabwägung eine besonders sorgfältige Abwägung vom Verantwortlichen. Entsprechend ErwGr. 47 DS-GVO stellt ein Faktor, der bei jeder Interessenabwägung berücksichtigt werden muss, die „vernünftigen Erwartungen“ der betroffenen Person dar, die auf der Beziehung der Person zu dem Verantwortlichen beruhen.

Ein weiterer zu beachtender Punkt liegt nach ErwGr. 47 DS-GVO in dem Umstand, ob eine betroffene Person zum Zeitpunkt der Erhebung der personenbezogenen Daten und angesichts der Umstände, unter denen sie erfolgt, vernünftigerweise absehen kann, dass möglicherweise eine Verarbeitung für diesen Zweck erfolgen wird. Laut ErwGr 47 DS-GVO können die Interessen der betroffenen Person insbesondere dann überwiegen, wenn personenbezogene Daten in Situationen verarbeitet werden, in denen eine betroffene Person vernünftigerweise nicht mit einer weiteren Verarbeitung rechnen muss.

Grundsätzlich kommen als schutzwürdige Interessen der Betroffenen alle menschlichen Ziele in Betracht, wie beispielsweise das Streben nach Geld oder Anerkennung wie auch der Wunsch nach Privatheit. Dabei gilt, dass die Interessen der Betroffenen als umso schutzwürdiger anzusehen sind,

* je sensitiver die Daten sind und
* je größer die Zahl der die Daten verarbeitenden Personen bzw., bei Übermittlungen, der Abrufberechtigten ist.

Gesundheits- und genetische Daten gehören zu den besonders sensiblen Daten mit dem höchsten Schutzbedarf, die i. d. R. auch besonders missbrauchsanfällig sind. Bei diesen Daten muss regelhaft davon ausgegangen werden, dass betroffene Personen eine von ihnen nicht bewilligte Verarbeitung ihrer Daten nicht wünschen.

Sollen personenbezogen Daten zur Erstellung von Bewegungs-, Nutzungs-, Persönlichkeitsprofilen usw. genutzt werden, ist grundsätzlich von einem überwiegenden Interesse der betroffenen Personen auszugehen.[[77]](#footnote-77) Dies gilt insbesondere natürlich dann, wenn diese Daten zu den in Art. 9 Abs. 1 DS-GVO genannten besonders sensiblen Datenkategorien gehören.

Sollen Daten mit anderen Daten zusammengeführt werden, so gehen mit einer entsprechenden Zusammenführung immer auch deutlich höhere Gefährdungen für die Rechte und Freiheiten betroffener Personen einher. Eine „Anreicherung“ von Daten durch Hinzufügung oder Verkettung mit anderen Datensätzen begründet immer einen hohen Schutzbedarf und somit eine entsprechende Gewichtung bei einer Interessenabwägung. In der Literatur wird z. T. auch vertreten, dass eine Interessenabwägung bei der Verkettung von Datensätzen immer zugunsten der betroffenen Personen ausfällt, insbesondere, wenn personenbezogene Daten von mehreren Akteuren gemeinsam verarbeitet werden sollen.77

Bei jeder Interessenabwägung müssen selbstverständlich immer auch die Auswirkungen berücksichtigt werden, die die Verarbeitung der personenbezogenen Daten für die betroffene Person haben kann. Dabei sind die Folgen einer Verarbeitung umfassend zu berücksichtigen, d. h. es müssen auch Folgen berücksichtigt werden, deren Eintreten nicht sicher, jedoch möglich sind und somit als Risiko zu bewerten sind.[[78]](#footnote-78) Bei entsprechend hohen Risiken kann eine Datenschutz-Folgenabschätzung erforderlich sein,[[79]](#footnote-79) um die der Verarbeitung innewohnenden Risiken auf ein aus Sicht der betroffenen Person akzeptables Maß zu senken. Entsprechend ErwGr. 75 DS-GVO stellen beispielsweise Diskriminierung oder ein Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten, wozu es bei der Verarbeitung von genetischen oder Gesundheitsdaten kommen könnte, große Risiken dar. Gleiches gilt für die unbefugte Aufhebung einer Pseudonymisierung. Im Kontext einer Interessenabwägung ist all dies abzuwägen und zu bewerten.

Bei unrichtigen Daten erfolgt die Interessenabwägung immer zugunsten der betroffenen Personen, d. h. eine Interessenabwägung kann eine Verarbeitung von (wahrscheinlich) unrichtigen Daten nicht legitimieren; Art. 5 Abs. 1 lit. d DS-GVO verlangt, dass ausschließlich sachlich richtige und erforderlichenfalls auf dem neuesten Stand befindliche personenbezogene Daten verarbeitet werden dürfen.

Bei der Darstellung der Betroffeneninteressen kann die schon 1973 vom BVerfG entwickelte Sphärentheorie[[80]](#footnote-80) helfen:

* Ein Eingriff in die Intimsphäre muss vermieden werden, da hier der Kern der Menschenwürde betroffen ist. Dieser Kernbereich hat „seine Grundlage in dem durch Art. 2 Abs. 1 GG verbürgten Recht auf freie Entfaltung der Persönlichkeit. Bei der Bestimmung von Inhalt und Reichweite des Grundrechts aus Art. 2 Abs. 1 GG muss berücksichtigt werden, dass nach der Grundnorm des Art. 1 Abs. 1 GG die Würde des Menschen unantastbar ist und gegenüber aller staatlichen Gewalt Achtung und Schutz beansprucht. Überdies darf nach Art. 19 Abs. 2 GG auch das Grundrecht aus Art. 2 Abs. 1 GG nicht in seinem Wesensgehalt angetastet werden. Selbst überwiegende Interessen der Allgemeinheit können einen Eingriff in den absolut geschützten Kernbereich privater Lebensgestaltung nicht rechtfertigen; eine Abwägung nach Maßgabe des Verhältnismäßigkeitsgrundsatzes findet nicht statt.“80
* Soweit staatliche Maßnahmen nicht den unantastbaren Bereich privater Lebensgestaltung beeinträchtigen, muss „jedermann staatliche Maßnahmen hinnehmen, die im überwiegenden Interesse der Allgemeinheit unter strikter Wahrung des Verhältnismäßigkeitsgebots getroffen werden“.80 Bei einem Eingriff in die Privat- oder Sozialsphäre gilt: Je stärker der Eingriff, desto gewichtiger muss das verfolgte Gemeinwohlinteresse (= Verarbeitungszweck) sein.

### Nachweispflicht

Der Wortlaut von Art. 6 Abs. 1 lit. f DS-GVO beinhaltet indirekt, dass betroffene Personen nachweisen müssen, dass ihre Interessen überwiegen. Diese Betrachtungsweise greift jedoch zu kurz, da einerseits Verantwortliche die Rechtmäßigkeit der Verarbeitung nachweisen müssen, was ein Überwiegen ihrer Interessen beinhaltet. Andererseits resultiert für Verantwortliche aus Art. 5 Abs. 2 DS-GVO zusätzlich eine Nachweispflicht, was ebenfalls den Nachweis verlangt, dass die Interessen betroffener Personen nicht überwiegen. Erfolgt ein auf Art. 21 Abs. 1 DS-GVO beruhender Widerspruch der betroffenen Person, so muss ein Verantwortlicher ein Überwiegen seiner Interessen ebenfalls nachweisen. In Summe wird man daher davon ausgehen müssen, dass ein Verantwortlicher zum Nachweis der Rechtmäßigkeit der Verarbeitung bei Nutzung des in Art. 6 Abs. 1 lit. f DS-GVO enthaltenen Rechtfertigungsgrundes verpflichtet ist.

### Interessenabwägung bei Kindern

Werden personenbezogene Daten von Kindern wie beispielsweise in der pädiatrischen Forschung verarbeitet, ist entsprechend Wortlaut von Art. 6 Abs. 1 lit. f DS-GVO von einem Überwiegen der Betroffeneninteressen auszugehen. „Kind“ wird seitens DS-GVO nicht definiert, in der Literatur findet sich der Hinweis, im Wege eines Umkehrschlusses[[81]](#footnote-81) das Alter des Kindes aus Art. 8 Abs. 1 DS-GVO abzuleiten, sodass jedenfalls bis zum vollendeten sechzehnten Lebensjahr von einer besonderen Schutzbedürftigkeit ausgegangen werden kann, im Fall des dreizehnten Jahres i. d. R. auch von einer überwiegenden Schutzbedürftigkeit.

### Informationspflichten

Verantwortliche müssen betroffene Personen entsprechend Art. 13 Abs. 1 lit. d bzw. Art. 14 Abs. 2 lit. b DS-GVO aktiv über die (überwiegenden) Interessen des Verantwortlichen informieren.

### Widerspruchsrecht beachten

Entsprechend Art. 21 Abs. 1 DS-GVO hat eine betroffene Person das Recht, jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten, die aufgrund von Art. 6 Abs. 1 lit. f erfolgt, Widerspruch einzulegen. Dieses Recht kann die betroffene Person natürlich nur ausüben, wenn sie zuvor über diese Verarbeitung informiert wurde; die Informationspflicht des für die Verarbeitung Verantwortlichen ist hier die Grundlage dafür, dass eine Person ihr Widerspruchsrecht ausüben kann. Erfolgt ein Widerspruch, so dürfen die vom Widerspruch erfassten Daten nicht mehr verarbeitet werden. Eine Weiterverarbeitung ist nur möglich, wenn

1. der Verantwortliche entweder zwingende schutzwürdige Gründe, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, für die Verarbeitung nachweisen kann,
2. oder die Verarbeitung der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen dient.

Entsprechend Art. 21 Abs. 6 DS-GVO besitzt eine betroffene Person ebenfalls ein Widerspruchsrecht, wenn sie betreffende personenbezogene Daten zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken verarbeitet werden. Dem Widerspruch muss Folge geleistet werden, d. h. die Daten dürfen nicht weiter verarbeitet werden, ausgenommen, die Verarbeitung ist zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe erforderlich.

## Rechtsprechung des EuGH

Entsprechend Rechtsprechung des EuGH sind bei einer Interessenabwägung immer drei Voraussetzungen zu erfüllen:[[82]](#footnote-82)

1. Es muss von dem für die Verarbeitung Verantwortlichen oder von einem Dritten ein berechtigtes Interesse wahrgenommen werden. Dies setzt zwingend voraus, dass die mit der Verarbeitung verfolgten Ziele rechtmäßig sind und im Einklang mit der Rechtsordnung des jeweiligen Mitgliedstaats und dem Unionsrecht stehen.
2. Die Verarbeitung der personenbezogenen Daten muss zur Verwirklichung des berechtigten Interesses erforderlich sein. Hierbei ist stets zu prüfen, „ob das berechtigte Interesse an der Verarbeitung der Daten nicht in zumutbarer Weise ebenso wirksam mit anderen Mitteln erreicht werden kann, die weniger stark in die Grundrechte und Grundfreiheiten der betroffenen Personen, insbesondere die durch die Art. 7 und 8 der Charta garantierten Rechte auf Achtung des Privatlebens und auf Schutz personenbezogener Daten, eingreifen“.
3. Die Interessen oder Grundrechte und Grundfreiheiten der Person, deren Daten geschützt werden sollen, dürfen nicht überwiegen.

### Konkrete Umstände und Sensibilität der Daten berücksichtigen

Die im Rahmen einer Interessenabwägung einander gegenüberstehenden Rechte und Interessen von Verantwortlichem und betroffenen Personen müssen grundsätzlich anhand der konkreten Umstände des betroffenen Einzelfalls ermittelt und bewertet werden.[[83]](#footnote-83)

Dabei gilt laut Urteil des EuGH[[84]](#footnote-84): Je sensibler die zu verarbeitenden Daten, desto schwerer ist der Eingriff in die in Art. 7 und 8 der Charta verankerten Grundrechte der betroffenen Person, sodass auch die Sensibilität der Daten im Rahmen einer Interessenabwägung zu berücksichtigen ist. Bei den in Art. 9 Abs. 1 DS-GVO benannten besonderen Kategorien von personenbezogenen Daten handelt es sich naturgemäß um Daten der besonders schützenswerten Kategorien, entsprechend hoch sind die Interessen betroffener Personen zu bewerten und zu berücksichtigen.

Im Unterschied zur Verarbeitung von Daten, die aus öffentlich zugänglichen Quellen stammen, impliziert die Verarbeitung von Daten aus nicht öffentlich zugänglichen Quellen, dass der für die Verarbeitung Verantwortliche und gegebenenfalls der bzw. die Dritten, denen die Daten übermittelt werden, von Informationen über die Privatsphäre der betroffenen Person Kenntnis erlangen. Dies stellt eine schwerere Beeinträchtigung der in den Art. 7 und 8 der Charta verbürgten Rechte der betroffenen Person dar und ist bei einer Interessenabwägung entsprechend zu berücksichtigen und gegen das berechtigte Interesse abzuwägen, das von dem für die Verarbeitung Verantwortlichen oder von dem bzw. den Dritten wahrgenommen wird, denen die Daten übermittelt werden.[[85]](#footnote-85)

### Einzelfallbetrachtung erforderlich

Bei der Bewertung, ob die Interessen oder Grundfreiheiten und Grundrechte der Person, deren Daten geschützt werden sollen, gegenüber dem berechtigten Interesse des Verantwortlichen oder eines Dritten überwiegen oder nicht, ist immer eine Abwägung der jeweiligen einander gegenüberstehenden Rechte und Interessen erforderlich, die grundsätzlich von den konkreten Umständen des Einzelfalls abhängt.[[86]](#footnote-86)

Außerdem können die Interessen und Grundrechte der betroffenen Person das Interesse des Verantwortlichen insbesondere dann überwiegen, wenn personenbezogene Daten in Situationen verarbeitet werden, in denen eine betroffene Person vernünftigerweise nicht mit einer solchen Verarbeitung rechnet.86

### Zusammenführen/Verketten personenbezogener Daten

Das Vorhandensein derselben personenbezogenen Daten in mehreren Quellen verstärkt den Eingriff in das Recht der betroffenen Person auf Achtung des eigenen Privatlebens.86 Daher ist in allen Fällen, in denen personenbezogene Daten zusammengeführt werden, eine entsprechend höhere Gewichtung bei den Interessen der betroffenen Personen zu beachten, die Rechte und Freiheiten betroffener Personen entsprechend höher zu gewichten.

### Interesse muss aktuell vorliegen

Ein berechtigtes Interesse muss zum Zeitpunkt der Verarbeitung, inklusive der Erhebung der Daten, tatsächlich vorhanden sein[[87]](#footnote-87). Zu diesem Zeitpunkt darf das Interesse nicht hypothetischer Natur sein.

Eine Vorratsdatenspeicherung kann also niemals durch eine Interessenabwägung legitimiert werden. Ebenso wenig können beispielsweise Daten länger gespeichert werden, weil möglicherweise ein Gerichtsprozess kommen könnte, wo man diese Daten noch brauchen könnte. Ohne konkreten Anhaltspunkt für das Stattfinden eines Ereignisses sind die Interessen immer nur hypothetischer Natur, können entsprechend der Rechtsprechung des EuGH kein berechtigtes Interesse im Sinne von Art. 6 Abs. 1 lit. f DS-GVO darstellen.

### Informationspflichten beachten

Zu beachten ist weiterhin, dass Art. 13 Abs. 1 lit. d sowie Art. 14 Abs. 2 lit. b DS-GVO verlangen, dass betroffene Personen über die berechtigten Interessen informiert werden müssen. Der EuGH urteilte sogar, dass eine solche Verarbeitung nur dann als zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich angesehen werden kann, wenn ein Verantwortlicher betroffenen Personen ein mit der Datenverarbeitung verfolgtes berechtigtes Interesse mitteilte.[[88]](#footnote-88) Zu beachten: Entsprechend Art. 21 Abs. 4 DS-GVO muss eine betroffene Person auf das Recht zum Widerspruch einer Verarbeitung auf Grundlage einer Interessenabwägung hingewiesen werden.

# Beispiele

## Radiologische Forschung: Daten aus dem niedergelassenen Bereich

### Beschreibung des Vorhabens

Zielsetzung und somit Zweck der Forschung: Reduzierung der initialen Fehldiagnosen beim Mammographie-Screening

Hintergrund des Forschungsvorhabens:

Die Befunde von 250 bis 400 pro 1000 Frauen (je nach Studie Untersuchungszeitraum 20 Jahre) werden fehlerhaft als gutartig eingestuft. Daraus resultieren auch Nachuntersuchungen mit zusätzlicher Strahlenbelastung.

Das Forschungsvorhaben soll eine Verringerung der falsch negativen, als auch die falsch positiven Befunde erzielt werden. Hierzu sollen automatisierte Qualitätssicherungsmaßnahmen entwickelt werden, welche einem Screeningarzt bei seiner Arbeit zusätzlich unterstützen. Dies soll durch eine KI erfolgen: Automatisierte Qualitätssicherungsmaßnahmen sollen aus dem Training eines neuronalen Netzwerkes („KI“) resultieren, welches eine automatische Detektion relevanter Befunde ermöglicht.

Zum Training dieser KI werden die Bilddaten und endgültigen Befunde vorhandener Untersuchungen benötigt.

### Berechtigtes Interesse

Die Reduzierung der Strahlenbelastung für Patientinnen stellt ein legitimes Interesse dar. Das Vorhaben findet eine Erlaubnisnorm in § 27 Abs. 1 BDSG:

„[…] 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.“

Für den niedergelassenen Bereich findet das BDSG Anwendung, Landeskrankenhausgesetze sind für diesen Bereich nicht anwendbar. Jedoch sind Vorgaben der Berufsordnung für Ärztinnen/Ärzte zu beachten.

§ 27 Abs. 1 BDSG stellt die nationale Umsetzung der rechtlichen Vorgaben von Art. 9 Abs. 2 lit. j DS-GVO dar. Art. 9 Abs. 2 lit. j DS-GVO verlangt von der Rechtsnorm, dass diese

1. in angemessenem Verhältnis zu dem verfolgten Ziel steht,
2. den Wesensgehalt des Rechts auf Datenschutz wahrt und
3. angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht.

§ 27 Abs. 1 BDSG entspricht vom Wortlaut Art. 9 Abs. 2 lit. j DS-GVO, entspricht also seitens der Angemessenheit derjenigen der DS-GVO und wahrt ebenso das Recht auf Datenschutz der betroffenen Person. Hinsichtlich der „angemessenen und spezifischen Maßnahmen“ verweist § 27 Abs. 1 S. 2 BDSG auf § 22 Abs. 2 S. 2 BDSG.

Die Vorgaben in § 22 Abs. 2 S. 2 BDSG enthalten teilweise dieselben Anforderungen wie Art. 32 DS-GVO, stellen also lediglich Wiederholungen dar. Dies gilt für:

* § 22 Abs. 2 S. 2 Ziff. 1 BDSG: Wiederholung von Art. 24 Abs. 1 DS-GVO
* § 22 Abs. 2 S. 2 Ziff. 2 BDSG: Wiederholung von Art. 32 Abs. 1 lit. b DS-GVO
* § 22 Abs. 2 S. 4 Ziff. 5 BDSG: Da alle erforderlichen Zugriffe erfolgen müssen, folgt diese Anforderung unmittelbar aus Art. 5 Abs. 1 DS-GVO
* § 22 Abs. 2 S. 2 Ziff. 6 BDSG: Wiederholung von Art. 32 Abs. 1 Buchst. a DS-GVO
* § 22 Abs. 2 S. 2 Ziff. 7 BDSG: Wiederholung von Art. 32 Abs. 1 Buchst. a DS-GVO
* § 22 Abs. 2 S. 2 Ziff. 8 BDSG: Wiederholung von Art. 32 Abs. 1 Buchst. b, c DS-GVO
* § 22 Abs. 2 S. 2 Ziff. 9 BDSG: Wiederholung von Art. 32 Abs. 1 Buchst. d DS-GVO
* § 22 Abs. 2 S. 2 Ziff. 10 BDSG: Stellt lediglich die Aufforderung dar, sich an bestehendes Recht zu halten.

Entsprechend der Rechtsprechung des EuGH stellen Wiederholungen der DS-GVO im nationalen Recht jedoch keine „spezifischen“ Maßnahmen dar.

§ 22 Abs. 2 S. 3 Ziff. 3 und 4 BDSG stellen keine Wiederholungen dar, können als die DS-GVO ergänzende spezifischere Maßnahme gelten. Daraus folgt, dass § 27 Abs. 1 BDSG aus Sicht der DS-GVO eine Konkretisierung Art. 9 Abs. 2 lit. j DS-GVO darstellt und somit eine Verarbeitung als nationales Recht legitimieren kann. Forschende, die sich auf diese Erlaubnisnorm berufen, müssen bei Forschungsprojekten

* einen Datenschutzbeauftragten benannt haben (§ 22 Abs. 2 S. 2 Ziff. 4 BDSG) und ebenso
* an den Verarbeitungsvorgängen beteiligte Personen sensibilisieren (§ 22 Abs. 2 S. 2 Ziff. 3 BDSG),

damit eine Verarbeitung als rechtskonform angesehen werden kann.

Die „(Muster-)Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte“ (MBO-Ä) selbst stellt lediglich eine Musterformulierung ohne Rechtswirkung dar, ist rechtlich also nicht bindend. Dies sind nur die Berufsordnungen der jeweiligen deutschen Bundesländer. Die Regelung zur Forschung aus der Muster-Berufsordnung wird jedoch in jeder der Landesberufsordnungen übernommen, sodass die Bewertung der Muster-Berufsordnung zugleich eine Bewertung jeder einzelnen Landesberufsordnung entspricht.

Die aktuelle Fassung der Muster-Berufsordnung ist die Fassung des Beschlusses des 124. Deutschen Ärztetages vom 5. Mai 2021. Die Regelung zu Forschung findet sich in § 15 MBO-Ä. Darin finden sich folgende Vorgaben:

* § 15 Abs. 1 MBO-Ä: Werden in einem Forschungsprojekt Daten verwendet, die sich einem bestimmten Menschen zuordnen lassen, muss sichergestellt werden, dass vor der Durchführung des Forschungsvorhabens eine Beratung erfolgt, die auf die mit ihm verbundenen berufsethischen und berufsrechtlichen Fragen zielt und die von einer bei der zuständigen Ärztekammer gebildeten Ethik-Kommission oder von einer anderen, nach Landesrecht gebildeten unabhängigen und interdisziplinär besetzten Ethik-Kommission durchgeführt wird.
* § 15 Abs. 3 MBO-Ä: Ärztinnen und Ärzte beachten bei der Forschung am Menschen nach § 15 Absatz 1 die in der Deklaration von Helsinki des Weltärztebundes in der Fassung der 64. Generalversammlung 2013 in Fortaleza niedergelegten ethischen Grundsätze für die medizinische Forschung am Menschen.

Bzgl. Forschung enthält die MBO-Ä keine Erlaubnisnorm, wohl aber zu beachtende Vorgaben für von Ärztinnen und Ärzten durchgeführte Forschungsprojekte.

Für das Forschungsvorhaben besteht ein berechtigtes Interesse im Sinne § 27 Abs. 1 BDSG i. V. m. Art. 9 Abs. 2 lit. j DS-GVO, Art. 6 Abs. 1 lit. f DS-GVO bildet den dazu gehörenden Rechtfertigungstatbestand. Die Forschung ist daher legitim, das Interesse somit als „berechtigtes Interesse“ i. S. d. DS-GVO zu werten.

### Erforderlichkeit

Die Daten müssen zur Erreichung des Zweckes verarbeitet werden, anders kann der Zweck nicht erreicht werden.

Zum Training der KI sowie zur Evaluation des KI-Modells werden die Bilddaten selbst sowie die Befunde benötigt. Jedoch werden Namen von Patienten und Untersuchern, die sich in den DICOM-Daten befinden nicht benötigt, müssen also entfernt werden. Die Daten werden als „pseudonyme Daten“ klassifiziert, da ein binärer Abgleich der Forschungsdaten mit den Originaldaten in den jeweiligen niedergelassenen Arztpraxen eine Re-Identifizierung ermöglichen würde.

### Interessenabwägung

§ 27 Abs. 1 BDSG verlangt ein „erhebliches“ überwiegendes Interesse des Verantwortlichen. Von einem überwiegenden Forschungsinteresse kann insbesondere ausgegangen werden, wenn

1. an der Durchführung des Forschungsvorhabens ein öffentliches Interesse besteht und
2. der Eingriff in die Rechte der betroffenen Person so gering wie nur möglich gehalten wird und
3. der Grundrechtseingriff gegenüber der betroffenen Person nicht außer Verhältnis zu dem angestrebten Zweck steht.

Der Nachweis, dass das öffentliche Interesse an den Ergebnissen der Forschung vorhanden ist, stellt auch ein entsprechendes überwiegendes Interesse dar. Um „öffentliches Interesse“ darstellen zu können, kann man Abschnitt 86 Richtlinien für das Strafverfahren und das Bußgeldverfahren (RiStBV) analog anwenden. Dementsprechend liegt ein öffentliches Interesse vor, wenn

* das Vorhaben ein gegenwärtiges Anliegen der Allgemeinheit beinhaltet oder
* das Vorhaben ein gegenwärtiges Anliegen der Allgemeinheit ist.

Zum Nachweis eines „öffentlichen Interesses“ müssen daher zwei Fragen beantwortet werden:

1. Interessiert das Vorhaben die Allgemeinheit?
2. Nützt das Ergebnis des Vorhabens der Allgemeinheit?

#### Interessiert das Vorhaben die Allgemeinheit und nützt das Forschungsergebnis der Allgemeinheit?

Brustkrebs ist weltweit die häufigste krebsbedingte Todesursache: In der Gruppe der 50 bis 51-jährigen Frauen gibt es 690.500 Frauen[[89]](#footnote-89), die aufgrund ihres Alters berechtigt am Screeningprogramm teilnehmen dürfen, 2014 nahmen 624.800 Frauen[[90]](#footnote-90) am Screening teil.

Daraus resultiert statistisch, dass 156.200 Frauen in 20 Jahren Screening einen in der Abklärung negativen Befund erhalten, dies entspricht 7810 Frauen pro Jahr. Aber statistisch entsprechen bei 8.510 Frauen pro Jahr die endgültigen Ergebnisse nicht dem initialen Screeningbefund.

Daraus resultieren zum einen Kosten für die Allgemeinheit:

* Innerhalb von 20 Jahren Screening werden zusätzlich ca. 22.400 Frauen biopsiert, bei denen kein Karzinom nachweisbar ist. Entsprechend der EBM-Ziffer 08320 (Mammastanzbiopsie) resultieren daraus rund 1.000.000 Euro nur für die Stanzbiopsie.
* Weitere Kosten, die aufgrund der Diagnosestellung resultierenden:
  + Falsche Diagnosen bei den Frauen führen direkt zu Ausfällen bei der Arbeit mit entsprechenden wirtschaftlichen Verlusten.
  + Ehe- oder Lebenspartner muss Aufgaben übernehmen, welche die Frau aufgrund ihrer Krankheitsbewältigung nicht länger selbst wahrnehmen kann. Fällt die Frau für die Versorgung der Familie aus, so hat dies Auswirkungen bis hin zum Arbeitgeber des Lebenspartners, da dieser dann mehr privat gefordert wird und ggf. im Berufsleben weniger verfügbar ist.
  + Lebenspartner fällt im Arbeitsleben aus, was – betrachtet man die Summe aller Erkrankten – wiederum Auswirkungen auf die gesamtwirtschaftliche Leistung in Deutschland hat.

In Summe werden die Kosten sich – sehr konservativ geschätzt – allein für die krankheitsbezogenen medizinischen Maßnahmen sicherlich in einem zweistelligen Millionenbetrag belaufen. Hinzu kommen noch die Begleitkosten.

Es besteht daher ein öffentliches Interesse daran, Fehldiagnosen bei Screening reduzieren, um so die Krankheitskosten zu senken und die Anzahl der Fehlbehandlungen generell und insbesondere die aufgrund einer fehlerhaften Diagnostik erfolgten Fehlbehandlungen weiter zu reduzieren – was sich auf die Stabilität der Beitragszahlungen für die Krankenkasse auswirken kann. Der Wirtschaftsstandort Deutschland profitiert von der Verringerung von Arbeitsausfällen, woraus sich ebenfalls ein entsprechendes Interesse ableiten lässt.

Es muss von einem hohen öffentlichen Interesse an einer Verringerung der Fehldiagnosen ausgegangen werden.

#### Schutz der betroffenen Personen

Die betroffenen Personen sind für die Forschung nicht identifizierbar. Die Überarbeitung der Bildmetadaten gewährleistet, dass die Identifizierung des Bilderzeugers nicht möglich ist, ebenso ist die Quelle der Bilddaten nicht mehr identifizierbar. Für das Training wie auch der Validierung der KI werden die Daten beim Export so aufbereitet, dass in den Bilddaten alle personenidentifizierbaren Merkmale entfernt werden.

Die Aufbereitung der Bilddaten erfolgt direkt in der Arztpraxis selbst, die Originaldaten stehen den Forschern zu keinem Zeitpunkt zur Verfügung. Mittels Ende-zu-Ende-Verschlüsselung werden die für das Training des KI-Modells sowie der Validierung des KI-Modells benötigten überarbeiteten Daten aus der jeweiligen Arztpraxis an das KI-Trainingszentrum gesendet. Eine elektronische Signatur gewährleistet, dass Veränderungen der Daten für die Forscher unmittelbar ersichtlich sind.

Alle Personen sind zusätzlich auf Verschwiegenheit und Einhaltung datenschutzrechtlicher Vorschriften verpflichtet.

Das Ergebnis des trainierten Netzwerks ist vollständig anonymisiert.

Es verbleibt ein minimales Restrisiko, dass jemand außerhalb der jeweiligen Screeningeinheit eine Frau anhand eines solch aufbereiteten Mammographiebildes re-identifizieren kann. Diese Re-Identifikation kann nur durch Personen bzw. IT-Systemen erfolgen, denen bereits mindestens eine andere Mammographie-Untersuchung der entsprechenden Person inklusive der personenidentifizierenden Merkmale als Referenzwert vorliegt. Bei einem Mammographie-Screening werden gesunde Frauen untersucht, bei denen eine Voruntersuchung i. d. R. nicht vorliegt. Die Wahrscheinlichkeit für eine Re-Identifikation kann man nur schätzen und sie wird deutlich geringer als 1:1:500.000 sein.

#### Individualinteresse der betroffenen Personen

Für die operierten Frauen resultiert aus einer Brustoperation häufig eine unglaublich starke emotionale Belastung, die sich auch zu einer sehr ernsten psychischen Erkrankung wandeln kann, wenn die Brust teilweise oder komplett entfernt wird.

Je nach Verwandtschaftsgrad besteht ein deutlich erhöhtes Risiko, ebenfalls ein Mammakarzinom auszubilden. Die Diagnose wie auch die Fehldiagnose bei einer Mutter belastet mit auch deren Töchter, was wiederum eine zusätzliche Belastung für die jeweilige Patientin darstellt.

Es ist daher im Interesse jeder Frau, wenn die Anzahl der Fehltherapien generell und vor allem die aufgrund einer fehlerhaften Diagnostik erfolgten Fehltherapien verringert werden.

Aufgrund der technisch-organisatorischen Maßnahmen ist das Risiko eines Datenmissbrauchs für betroffene Personen denkbar gering. Zugleich können Frauen bei einer weiteren Untersuchung ggfs. von den Ergebnissen der Forschung selbst profitieren, ebenso ihre Töchter.

Es muss daher davon ausgegangen werden, dass die Forschung sogar im Interesse der jeweiligen betroffenen Person erfolgt.

#### Ergebnis der Interessenabwägung

Es besteht ein sehr großes Interesse der Öffentlichkeit an einer Verringerung von Fehldiagnosen beim Mammographie-Screening.

Das Risiko für betroffene Personen, dass ihre Daten Unbefugten offenbart werden, ist praktisch nicht vorhanden.

Dafür besteht seitens der betroffenen Personen wahrscheinlich selbst ein sehr starkes Interesse an Reduzierung von Fehldiagnosen, da

* sie bei Wiederholungsuntersuchungen im Screening selbst von den Ergebnissen profitieren könnten,
* ebenso bei kurativen Mammographie-Untersuchungen in der Nachsorge und
* die eigenen Nachkommen (bei ca. 4 bis 9 % aller Neuerkrankungen besteht eine erbliche Vorbelastung[[91]](#footnote-91)) ebenso von den Forschungsergebnissen profitieren könnten.

Die Forschung erfolgt wahrscheinlich sogar im Eigeninteresse der betroffenen Person.

#### Bewertung

Das öffentliche Interesse an der Forschung überwiegt das Interesse der jeweils betroffenen Person an der Nicht-Nutzung ihrer personenbezogenen Daten erheblich. Damit besteht insbesondere auch ein erhebliches überwiegendes Interesse des Verantwortlichen an der Verarbeitung gegenüber den Interessen der betroffenen Person an einem Ausschluss der Verarbeitung. Die nationale rechtliche Norm, welche die Forschung bei erheblich überwiegendem Interesse gestattet, ist § 27 Abs. 1 BDSG i.V.m. Art. 9 Abs. 2 lit. j DS-GVO (siehe auch Kapitel 7.1.1.3), Rechtfertigungstatbestand ist Art. 6 Abs. 1 lit. f DS-GVO.

## Retrospektives Forschungsvorhaben eines Krankenhauses in Schleswig-Holstein

Ein Krankenhaus in Schleswig-Holstein möchte die Daten aus der Patientenversorgung retrospektiv für ein medizinisches Forschungsprojekt nutzen. Eine Einwilligung der Patienten i. S. d. DS-GVO – für den bestimmten Fall, in informierter Weise und ausdrücklich für den konkreten Zweck abgeben – liegt nicht vor.

§ 6 Abs. 1 S. 1 Gesundheitsdatennutzungsgesetz (GDNG) erlaubt datenverarbeitenden Gesundheitseinrichtungen, zu denen auch das die Forschung beabsichtigende Krankenhaus gehört, rechtmäßig gespeicherte Daten für Zwecke der medizinischen, zur rehabilitativen und zur pflegerischen Forschung weiterverarbeiten, soweit dies erforderlich ist. § 6 Abs. 1 DS-GVO ist somit ein von Art. 9 Abs. 2 lit. j DS-GVO adressiertes Recht eines Mitgliedstaats, welches Forschung erlaubt, wenn dieses Recht des Mitgliedstaats

1. in angemessenem Verhältnis zu dem verfolgten Ziel steht,
2. den Wesensgehalt des Rechts auf Datenschutz wahrt und
3. angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht.

§ 6 GDNG enthalten folgende Anforderungen

* § 6 Abs. 1 S. 2 GDNG: Die personenbezogenen Daten sind zu pseudonymisieren; sie sind zu anonymisieren, sobald dies im Rahmen der Weiterverarbeitung für den jeweiligen Zweck nach Satz 1 möglich ist.
* § 6 Abs. 1 S. 3 GDNG: Sind mehrere natürliche Personen in der datenverarbeitenden Gesundheitseinrichtung tätig, hat ein Rechte- und Rollenkonzept zu gewährleisten, dass nur befugte Personen die Daten nach weiterverarbeiten können sowie unbefugte Weiterverarbeitungen protokolliert und geahndet werden können.
* § 6 Abs. 1 S. 4 GDNG: Daten, die im Rahmen einer Weiterverarbeitung nach Satz 1 gespeichert werden, sind spätestens nach zehn Jahren, nachdem die Rechtsgrundlage für die ursprüngliche Datenerhebung weggefallen ist, zu löschen, sofern nicht andere gesetzliche Regelungen der Löschung entgegenstehen.
* § 6 Abs. 3 GDNG: Die Weitergabe der personenbezogenen Daten an Dritte ist im Rahmen der Weiterverarbeitung nach Absatz 1 untersagt. Abweichend von Satz 1 ist die Weitergabe von personenbezogenen Daten im Rahmen der Weiterverarbeitung nach Absatz 1 zulässig, soweit die betroffene Person eingewilligt hat oder eine andere gesetzliche Vorschrift dies vorsieht. Die datenverarbeitenden Gesundheitseinrichtungen dürfen die für die in Artikel 9 Absatz 2 Buchstabe h der Verordnung (EU) 2016/679 rechtmäßig gespeicherten Gesundheitsdaten anonymisieren, um die anonymisierten Daten zu den in Absatz 1 Satz 1 genannten Zwecken an Dritte zu übermitteln.

Bewertung: Pseudonymisierung wird bereits von Art. 32 Abs. 1 lit. a DS-GVO gefordert. Dass der Zugriff nur für befugte Personen im erforderlichen Umfang statthaft ist, ist eine direkte Auswirkung von Art. 5 DS-GVO, Art. 32 Abs. 1 lit. b DS-GVO verlangt entsprechende technische und organisatorische Maßnahmen. Die Löschvorgaben der DS-GVO bedingen eine Löschung nach Erreichung des Zweckes, die in § 6 Abs. 2 S. 4 GDNG deutlich länger angegebene Speicherdauer steht in keinem angemessenen Verhältnis zum Zweck/Ziel und wahrt auch nicht den Wesensgehalt auf Datenschutz. Die in § 6 Abs. 2 S. 2 bis 4 GDNG angegebenen Maßnahmen erfüllen somit nicht die Anforderungen von Art. 9 Abs. 2 lit. j DS-GVO. § 6 Abs. 3 GDNG erlaubt die Weitergabe der Patientendaten an Dritte ohne Einwilligung, was eher eine Einschränkung der Grundrechte und Interessen der betroffenen Person entspricht, somit ebenfalls nicht die in Art. 9 Abs. 2 lit. j DS-GVO genannten Anforderungen erfüllt.

2022 wurde vom wissenschaftlichen Dienst des Bundestages der verfassungsrechtliche Rahmen für die Regelung der stationären medizinischen Versorgung im Rahmen einer Kurzinformation dargestellt[[92]](#footnote-92) und dabei festgestellt, dass Krankenhausorganisation und die Krankenhausplanung in die Gesetzgebungskompetenz der Länder fallen; daher ist bei rechtlichen Widersprüchen in diesen Fällen das Landesrecht vorrangig gegenüber dem Bundesrecht anzuwenden.

Grundsätzlich ist daher zu prüfen, ob der jeweilige Gesetzgeber des betreffenden Bundeslandes seine Gesetzgebungskompetenz nutzte. Ist dies nicht der Fall, kann Bundesrecht angewendet werden, ansonsten ist vorrangig das Landesrecht anzuwenden.

§ 38 LKHG Schleswig-Holstein enthält spezielle Vorgaben für die Verarbeitung von Patientendaten im Rahmen von Forschungsvorhaben, ist also vorrangig anzuwenden. Entsprechend § 38 Abs. 1 LKHG Schleswig-Holstein ist grundsätzlich eine Einwilligung erforderlich, Forschung ohne Einwilligung ist seitens des Landesgesetzgebers nicht vorgesehen.

Da der Landesgesetzgeber seine Gesetzgebungskompetenz nutzte, kann dem Landesrecht widersprechendes Bundesrecht nicht angewendet werden. Somit ist auch eine retrospektive Nutzung von Patientendaten im betrachteten Fall nur mit Einwilligung möglich.

D. h., alle in Frage kommenden Patienten müssen um eine den Vorgaben der DS-GVO entsprechende Einwilligung unter Beachtung der Vorgaben von § 36 Abs. 2 LKHG Schleswig-Holstein ersucht werden. Es dürfen nur Daten von Patienten genutzt werden, die für das konkrete Forschungsprojekt ihre Einwilligung erteilten.

Mit erteilter Einwilligung ist die Rechtsgrundlage § 38 Abs. 1 LKHG Schleswig-Holstein i. V. m. Art. 9 Abs. 2 lit. a DS-GVO, Rechtfertigungstatbestand ist Art. 6 Abs. 1 lit. a DS-GVO.

# Abkürzungen

|  |  |
| --- | --- |
| Abs. | Absatz |
| AEUV | Vertrag über die Arbeitsweise der Europäischen Union |
| a. F. | Alte Fassung |
| AGB | Allgemeine Geschäftsbedingungen |
| Art. | Artikel |
| BÄO | Bundesärzteordnung |
| BDSG | Bundesdatenschutzgesetz |
| BEM | Betrieblichen Eingliederungsmanagement |
| BGG | Gesetz zur Gleichstellung von Menschen mit Behinderungen (Behindertengleichstellungsgesetz) |
| BSIG | Gesetz über das Bundesamt für Sicherheit in der Informationstechnik |
| BSI-KritisV | Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung) |
| BvD | Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e. V. |
| BVerfG | Bundesverfassungsgericht |
| bvitg | Bundesverband Gesundheits-IT – bvitg e. V. |
| DigiG | Gesetz zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz) |
| DSG | Datenschutzgesetz |
| DS-GVO | Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) |
| DSK | Datenschutzkonferenz |
| EDPB | European Data Protection Board |
| EDSA | Europäischer Datenschutzausschuss |
| EDV | Elektronische Datenverarbeitung |
| EN | Europäische Norm |
| ErwGr. | Erwägungsgrund/Erwägungsgründe |
| EU | Europäische Union |
| EuGH | Europäischer Gerichtshof |
| EWR | Europäischer Wirtschaftsraum |
| GDD | Gesellschaft für Datenschutz und Datensicherheit (GDD) e. V. |
| GDNG | Gesetzes zur verbesserten Nutzung von Gesundheitsdaten (Gesundheitsdatennutzungsgesetz) |
| GG | Grundgesetz |
| GMDS | Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V. |
| Hs. | Halbsatz |
| i. d. R. | in der Regel |
| i. S. | im Sinne |
| i. S. d. | Im Sinne des/der |
| i. S. d. | im Sinne der/des |
| i. V. m. | in Verbindung mit |
| i. S. v. | im Sinne von |
| ISO | International Organization for Standardization |
| IT | Informationstechnik, informationstechnisches… |
| Kap. | Kapitel |
| KDG | Gesetz über den Kirchlichen Datenschutz |
| KHG | Krankenhausfinanzierungsgesetz |
| KHG | Krankenhausgesetz |
| LDSG | Landesdatenschutzgesetz |
| LKHG | Landeskrankenhausgesetz |
| LKG | Landeskrankenhausgesetz |
| lit. | littera (lat. „Buchstabe“) |
| MBO-Ä | (Muster-)Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte |
| Nr. | Nummer |
| OLG | Oberlandesgericht |
| PatientendatenVO | Verordnung zur Verarbeitung von Patientendaten in kirchlichen Krankenhäusern (Patientendatenverordnung) |
| RiStBV | Richtlinien für das Strafverfahren und das Bußgeldverfahren |
| RL | Richtlinie |
| Rn. | Randnummer |
| S. | Satz |
| SBV | Schwerbehindertenvertretung |
| SchwAV | Schwerbehinderten-Ausgleichsabgabeverordnung |
| SeelsorgePatDSG | Gesetz zum Schutz von Patientendaten bei der Seelsorge in katholischen Einrichtungen des Gesundheitswesens in der (Erz-)Diözese |
| SG | Sozialgericht |
| SGB | Sozialgesetzbuch |
| StGB | Strafgesetzbuch |
| Unterabs. | Unterabsatz |
| Urt. | Urteil |
| u. U. | unter Umständen |
| vgl. | vergleiche |
| vs. | versus (lat. „gegen“), wird häufig i. S. v. „Objekt/Begriff 1 gegenüber / im Vergleich zu Objekt/Begriff 2“ verwendet |
| VO | Verordnung |
| WRV | Verfassung des Deutschen Reiches vom 11. August 1919 (Weimarer Verfassung, oder auch Weimarer Reichsverfassung genannt) |
| Ziff. | Ziffer |

# Literatur

## Internet

* Wissenschaftliche Dienste Deutscher Bundestag. (2019) Gesetzgebungskompetenzen im Bereich des Krankenhausrechts. Online, zitiert am 2024-03-21; verfügbar unter <https://www.bundestag.de/resource/blob/648488/7920b181e85756ccdedff0334a18145b/WD-3-094-19-pdf-data.pdf>
* Wissenschaftliche Dienste Deutscher Bundestag. (2022) Verfassungsrechtlicher Rahmen für die Regelung der stationären medizinischen Versorgung. Online, zitiert am 2024-03-21; verfügbar unter <https://www.bundestag.de/resource/blob/899852/e48e78cfe536ee972862bab82b8618e9/WD-3-054-22-pdf-data.pdf>
* Wissenschaftliche Dienste Deutscher Bundestag. (2019) Zur Frage der Gesetzgebungskompetenz des Bundes für den Öffentlichen Gesundheitsdienst. Online, zitiert am 2024-03-21; verfügbar unter <https://www.bundestag.de/resource/blob/657236/c82ba2db1cd763e2f46439828d73c4e0/WD-9-043-19-pdf-data.pdf>
* Wollenschläger F. (2023) Verfassungskonformität der Reform der Krankenhausplanung auf der Basis der dritten Stellungnahme und Empfehlung der Regierungskommission für eine moderne und bedarfsgerechte Krankenhausversorgung „Grundlegende Reform der Krankenhausvergütung“. Online, zitiert am 2024-03-21; verfügbar unter <https://www.stmgp.bayern.de/wp-content/uploads/2023/04/gutachten_verfassungskonformitaet_krankenhausplanung.pdf>
* Wissenschaftlichen Dienste dt. Bundestag: WD 9 - 020/22 Gesetzgebungskompetenzen im Bereich des Rettungswesens (2022-03-07). Online, zitiert am 2024-06-18; verfügbar unter <https://www.bundestag.de/resource/blob/897344/b02aad2f6e6f696144af1a86966f5d94/WD-9-020-22-pdf.pdf>
* Wissenschaftlichen Dienste dt. Bundestag: WD 9 - 049/22 Ausbildung und Berufsausübung von Rettungssanitätern (2022-09-20). Online, zitiert am 2024-06-18; verfügbar unter <https://www.bundestag.de/resource/blob/912896/e896cc1c5c4599645ff6b1cbb4fd3deb/WD-9-049-22-pdf.pdf>

1. Abdingbarkeit der Sicherheit der Verarbeitung

Die Frage, ob das Niveau der IT-Sicherheit durch Einwilligung abgesenkt werden kann, wird gerade in Deutschland immer wieder angesprochen, wurde schon unter dem „alten“ Bundesdatenschutzgesetz[[93]](#footnote-93) diskutiert. Die herrschende Literatur ist der Ansicht, dass Art. 32 DS-GVO nicht disponibel bzw. abdingbar ist.[[94]](#footnote-94) Dies sagt aber zugleich aus, dass es auch davon abweichende Meinungen gibt. Neben der DS-GVO werden in diversen Rechtsakten der EU wie auch des deutschen Gesetzgebers Mindestanforderungen bestimmt, welche anzuwenden sind. IT-Sicherheit ist somit keine Anforderung, die nur und ausschließlich von der DS-GVO bestimmt wird, sondern es müssen darüber hinaus auch andere Rechtsakte beachtet werden.

Im Folgenden soll betrachtet werden, welche Rechtsakte u. a. hinsichtlich der Gewährleistung der IT-Sicherheit zu beachten sind und ob die gesetzlichen Vorgaben durch eine datenschutzrechtliche Einwilligung abgeschwächt werden dürfen. Diese Diskussion soll Verantwortliche informieren, damit diese ihre Entscheidung, wie sie mit dem Thema umgehen wollen, informierter treffen können.

Dazu werden zunächst die wichtigsten europäischen und deutschen gesetzlichen Rahmenbedingungen für die Gesundheitsversorgung kurz dargestellt, danach kurz auf die Rechtsprechung zu den datenschutzrechtlichen Aspekten (die meisten anderen Regelungen sind zu neu, als dass sich bereits Gerichte mit Fragen aus der Gesetzgebung befassten) eingegangen, gefolgt von der Sichtweise verschiedener Datenschutz-Aufsichtsbehörden, die sich aber naturgemäß nur mit der datenschutzrechtlichen Thematik befassen. Abschließend werden die Punkte diskutiert und in einem Fazit wesentliche Punkte festgehalten.

* 1. Die gesetzlichen Vorgaben
     1. Europäisches Recht

Art. 24, 25 und 32 DS-GVO verpflichtet Verantwortliche, geeignete technische und organisatorische Maßnahmen zu treffen, welche ein angemesseneres Schutzniveau gewährleisten.

Art. 24 Abs. 1 DS-GVO verlangt, dass der Verantwortliche „unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen“ umsetzt. Alle Maßnahmen müssen berücksichtigen, dass die Verarbeitung in Übereinstimmung mit den Vorgaben der DS-GVO durchgeführt wird. Art. 24 Abs. 2 DS-GVO hebt das Gebot für die Datenschutzvorkehrungen sogar ausdrücklich hervor, die Maßnahmen müssen „in einem angemessenen Verhältnis“ zu den Verarbeitungstätigkeiten und den mit diesen verbundenen Risiken stehen. Zugleich enthält Art. 24 Abs. 1 S. 1 DS-GVO eine Nachweispflicht.

Entsprechend Art. 25 DS-GVO muss der Verantwortliche für die gesamte Dauer der Verarbeitung -d. h. von der Planung der Verarbeitung bis zur Beendigung der Verarbeitung inkl. der Löschung aller Daten - geeignete Maßnahmen treffen, um zu gewährleisten, dass alle Rechte betroffener Personen geschützt sind und die DS-GVO vollständig eingehalten wird. Die zu berücksichtigenden Faktoren für die Bewertung der Geeignetheit von technischen und organisatorischen Maßnahmen werden in Art. 25 Abs. 1 DS-GVO abschließend genannt, die Einwilligung ist nicht dabei.

Art. 32 DS-GVO formt den in Art. 5 Abs. 1 lit. f DS-GVO befindlichen allgemeinen Grundsatz der Integrität und Vertraulichkeit näher aus und verlangt, dass ein angemessenes Schutzniveau für die Sicherheit personenbezogener Daten gewährleistet wird. Die Risiken, die durch Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung personenbezogener Daten entstehen können, müssen Verantwortliche – und auch deren Auftragsverarbeiter - als Faktoren bei der Wahl ihrer Schutzmaßnahmen in Rechnung stellen, denn eine einzige Schwachstelle kann den gesamten Schutz beeinträchtigen. Wird daher auch nur in einem einzigen Einzelfall das Schutzniveau gesenkt, müssen die Auswertungen betrachtet und in Form einer Risikobetrachtung dargestellt werden. Beispielsweise kann das Öffnen eines Mailanhangs diverse Schadsoftware den Weg in die eigentlich gesicherte IT-Umgebung ebnen.

Art. 24, 25 und 32 DS-GVO weisen Verantwortlichen Pflichten zu, ohne diese Pflichten von einer Zustimmung der betroffenen Personen abhängig zu machen, wie es der Gesetzgeber beispielsweise als Ausnahme in Art. 49 Abs. 1 lit. a DS-GVO bei der Drittlandübermittlung tat. Die rechtfertigende Wirkung, welche Art. 6 Abs. 1 lit. a DS-GVO der Einwilligung zugesteht, bezieht sich ausschließlich auf das „Ob“ der Verarbeitung, nicht aber auch auf das „Wie“.

Am 12. März 2024 wurde die Verordnung des Europäischen Parlaments und des Rates über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen („Cyber Resilience Act“) angenommen,[[95]](#footnote-95) bisher aber noch nicht im EU-Amtsblatt veröffentlicht und damit noch nicht rechtskräftig. Der Cyber Resilience Act gilt nicht für (Art. 2 Abs. 2-4) Verordnung (EU) 2017/745 (Medizinprodukte), Verordnung (EU) 2017/746 (In-vitro-Diagnostika), Verordnung (EU) 2019/2144 (Typgenehmigung von Kraftfahrzeugen und Kraftfahrzeuganhängern usw.), Verordnung (EU) 2018/1139 (Zivilluftfahrt), Richtlinie 2014/90/EU (Schiffsausrüstung). Dementsprechend gilt die Verordnung für alle medizinischen IT-Systeme, die keine Medizinprodukte darstellen.

Grundsätzlich betrifft die Verordnung in erster Linie Hersteller bzw. Händler/Akteure, welche entsprechende Produkte auf dem europäischen Markt bereitstellen. Gemäß Art. 6 Cyber Resilience Act müssen aber bei der Beschaffung oder Nutzung von Produkten mit digitalen Elementen (= Software- oder Hardwareprodukte) zwingend die in Anhang I und II vorgegebenen „grundlegenden Anforderungen“ umgesetzt werden (Art. 6). Zu den Vorgaben für Nutzer entsprechender Produkte gehört u. a. der Umgang mit Sicherheits-Schwachstellen, aber auch grundlegende Anforderungen an die IT-Sicherheit wie beispielsweise Authentifizierungs-, Identitäts- oder Zugangsverwaltungssysteme, welche die Software unterstützen muss. Indirekt entstehen mit diesen gesetzlich vorgegebenen Möglichkeiten, die Software bei der Nutzung bereitstellen muss, auch Anforderungen an die Nutzer bzgl. des Umgangs mit diesen Möglichkeiten.

Die NIS-2-Richtlinie[[96]](#footnote-96), welche bis zum 17. Oktober 2024 in deutsches Recht umgesetzt werden muss,[[97]](#footnote-97) erweitert den von der NIS-Richtlinie definierten Anwendungsbereich und umfasst neben kritischen Infrastrukturen auch „wesentliche und wichtige Einrichtungen“, d. h. es werden mehr Unternehmen von der Richtlinie erfasst. Entsprechend Art. 21 NIS-2-Richtlinie müssen Einrichtungen verhältnismäßige technische, operative und organisatorische Maßnahmen ergreifen, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die diese Einrichtungen für ihren Betrieb oder für die Erbringung ihrer Dienste nutzen, zu beherrschen und die Auswirkungen von Sicherheitsvorfällen auf die Empfänger ihrer Dienste und auf andere Dienste zu verhindern oder möglichst gering zu halten. Die Vorgaben müssen zwingend umgesetzt werden, eine Absenkung der IT-Sicherheit ist für von der europäischen Richtlinie betroffenen Einrichtungen nicht vorgesehen.

Die sog. CER-Richtlinie[[98]](#footnote-98), welche bis zum 17. Oktober 2024 in nationales Recht umgesetzt werden muss,[[99]](#footnote-99) legt Verpflichtungen für kritische Einrichtungen fest, die darauf abzielen, ihre Resilienz und ihre Fähigkeit zur Erbringung von Diensten zu gewährleisten. Mit Art. 13 CER-Richtlinie werden die durch Art. 6 Abs. 1 bestimmten kritischen Einrichtungen, wozu nach Anhang Ziff. 5 CER-Richtlinie insbesondere auch Gesundheitsdienstleister zählen können, dazu verpflichtet, geeignete und verhältnismäßige technische, sicherheitsbezogene und organisatorische Maßnahmen zur Gewährleistung ihrer Cyber-Resilienz zu ergreifen. Auch diese Vorgaben können nicht durch die Einwilligung betroffener Personen beschränkt werden.

* + 1. Deutsches Recht

Durch das DigiG wurde § 139 Abs. 10 SGB V dahingehend geändert, dass ein neuer Satz angefügt wurde:

„Sofern in den Festlegungen nach Satz 1 Anforderungen an ein geeignetes sicheres technisches Verfahren zur Authentifizierung des Versicherten vorgesehen werden, das einen hohen Sicherheitsstandard gewährleistet, ist in den Festlegungen auch zu regeln, dass der Versicherte nach umfassender Information durch den für die jeweilige Anwendung datenschutzrechtlich Verantwortlichen über die Besonderheiten des Verfahrens in die Nutzung eines Authentifizierungsverfahrens einwilligen kann, das einem niedrigeren Sicherheitsniveau entspricht.“

Hier wird gesetzlich normiert, dass eine betroffene Person bei der Nutzung von den in § 33a SGB V normierten digitalen Gesundheitsanwendungen („Apps auf Rezept“) in ein niedrigeres Schutzniveau einwilligen kann.

Grundsätzlich stellt sich hier die Frage, ob diese deutsche Regelung überhaupt mit den europäischen Vorgaben vereinbar ist. Die Regelung in Art. 32 DS-GVO beispielsweise ist abschließend und sieht keine Öffnung für nationale Gesetzgeber zu; der EuGH urteilte in ähnlich Fällen, dass das nationale Recht europarechtswidrig ist und nicht angewendet werden darf.

Aber auch unabhängig von dieser Sichtweise ist zu beachten, dass

1. die Senkung des Schutzniveaus aufgrund der Beschaffenheit der digitalen Gesundheitsanwendungen nur die betroffene Person selbst betrifft, die Entscheidung der betroffenen Person niemals Auswirkungen auf andere Patienten hat.
2. Weiterhin adressiert die Gesetzesnorm direkt den Patienten, nicht den Verantwortlichen, wie andere Normen, welche direkt Verantwortlichen eine Verpflichtung auferlegen.
3. Schließlich sieht die gesetzliche Regelung explizit die Einwilligung vor; in anderen Regelungen wurde dies vom deutschen Gesetzgeber nicht vorgesehen, was eher ein Anzeichen dafür ist, dass in allen Fällen, in denen keine ausdrückliche Erlaubnis zur Verringerung der Maßnahmen zur IT-Sicherheit durch Einholung einer rechtskonformen datenschutzrechtlichen Einwilligung eine entsprechende Abdingung dies auch nicht möglich ist.

Einige dieser gesetzlichen Vorgaben, in denen keine Absenkung der Maßnahmen zur Gewährleistung einer IT-Sicherheit geregelt wird, werden nachfolgend genannt.

§ 8a Abs. 1 BSIG verpflichtet Betreiber Kritischer Infrastrukturen dazu, „angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind.“ Im Bereich Gesundheit wird durch § 6 i. V. m. Anhang V BSI-KritisV festgelegt, welche Einrichtungen aus dem Gesundheitswesen als Kritische Infrastrukturen anzusehen sind. Fällt eine Einrichtung darunter, müssen die Maßnahmen umgesetzt werden, eine fehlende Umsetzung der Anforderungen durch eine Einwilligung betroffener Personen kann auch im Einzelfall den Rechtsbruch nicht legalisieren.

§ 390 SGB V enthält Anforderungen zur Gewährleistung der IT-Sicherheit in der vertragsärztlichen und vertragszahnärztlichen Versorgung. Entsprechend der Gesetzesbegründung sollen vor dem Hintergrund zunehmender Cyberattacken Sicherheitslücken auch bei kleinen und mittelständischen Praxen geschlossen werden, die keine kritische Infrastruktur i. S. d. BSI-Gesetzes darstellen und daher nicht unter die BSI-KritisV fallen.[[100]](#footnote-100) Die Kassenärztlichen Bundesvereinigungen müssen entsprechend § 390 Abs. 3 SGB V in einer Richtlinie Anforderungen festlegen, welche geeignet sein müssen, „abgestuft im Verhältnis zum Gefährdungspotenzial und dem Schutzbedarf der verarbeiteten Informationen, Störungen der informationstechnischen Systeme, Komponenten oder Prozesse der vertragsärztlichen Leistungserbringer in Bezug auf Verfügbarkeit, Integrität und Vertraulichkeit sowie der weiteren Sicherheitsziele zu vermeiden“. Dabei muss die Richtlinie entsprechend § 390 Abs. 4 SGB V dem Stand der Technik entsprechen.

An der vertragsärztlichen und vertragszahnärztlichen Versorgung teilnehmende Leistungserbringer müssen diese Richtlinie gemäß § 390 Abs. 6 SGB V verpflichtend umsetzen. Es ist nicht möglich, mittels einer Einwilligung einer betroffenen Person einzelne Anforderungen dieser Richtlinie als nicht-anwendbar zu erklären.

§ 391 Abs. 1 SGB V Abs. 1 S. 1 enthält eine allgemeine Pflicht, für Krankenhäuser angemessene organisatorische und technische Vorkehrungen zu implementieren, welche eine „Vermeidung von Störungen der Verfügbarkeit, Integrität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die für die Funktionsfähigkeit des jeweiligen Krankenhauses und den Schutzbedarf der verarbeiteten Patienteninformationen maßgeblich sind“ gewährleisten. Zur Bewertung der Angemessenheit enthält § 391 Abs. 3 SGB V die Vorgabe, dass Maßnahmen als angemessen anzusehen sind, „wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung des Krankenhauses oder dem Schutzbedarf der verarbeiteten Patienteninformationen steht“. Entsprechend § 391 Abs. 1 SGB V müssen die Maßnahmen dabei dem Stand der Technik entsprechen.

Alle Krankenhäuser, für welche diese Regelung anwendbar ist, müssen die Anforderungen erfüllen. Auch in diesen Fällen ist es nicht möglich, einzelne Anforderungen basierend auf der Einwilligung einer betroffenen Person für nicht anwendbar zu erklären.

§ 392 Abs. 1 SGB V verpflichtet gesetzliche Krankenkassen dazu, „nach dem Stand der Technik angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der jeweiligen Krankenkasse und die Sicherheit der verarbeiteten Versicherteninformationen maßgeblich sind.“ Auch hier gilt, dass eine Einwilligung von versicherten Personen die Pflicht nicht verändern kann.

§ 103a Abs. 1 SGB XI verpflichtet gesetzliche Krankenkassen dazu, „nach dem Stand der Technik angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der jeweiligen Pflegekasse und die Sicherheit der verarbeiteten Versicherteninformationen maßgeblich sind.“ Auch in diesen Fällen kann eine Einwilligung von versicherten Personen die Pflicht nicht verändern.

* + 1. Zu beachtende gesetzliche Vorgaben die Einwilligung betreffend

An dieser Stelle können die Vorgaben für eine datenschutzrechtliche Einwilligung nicht vollumfänglich besprochen werden; es wird hier auf die entsprechende Literatur verwiesen.[[101]](#footnote-101)

Gemäß Art. 4 Ziff. 11 DS-GVO ist eine Einwilligung eine Erklärung oder eine sonstige eindeutige bestätigende Handlung“, mit der die betroffene Person zu verstehen gibt, dass „sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist“. Eine Einwilligung ist eine Erklärung der betroffenen Person, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist, sagt aber nichts über das „wie“ der Verarbeitung aus. Allerdings muss die betreffende Person über das „wie“ der Verarbeitung aufgeklärt worden sein, sonst erfolgt eine Einwilligung nicht informiert, wie es Art. 4 Ziff. 11 DS-GVO verlangt. Eine Einwilligung legitimiert somit immer die Verarbeitung und nur indirekt auch das „wie“, dementsprechend muss eine Einwilligung immer der eigentlichen Verarbeitung gelten, nicht nur der Art und Weise wie Daten verarbeitet werden.

Eine Einwilligung kann sich nur auf die Beziehung zwischen dem Verantwortlichen und der betroffenen Person beziehen, aber niemals auf das Verhältnis zu Dritten erstrecken. Art. 25 und 32 DS-GVO beinhalten Anforderungen, welche der Verantwortliche für einen rechtskonformen Betrieb seiner IT-Systeme zwingend vorhalten muss. Er kann von diesen Anforderungen durch eine betroffene Person auf der Grundlage einer Einwilligung im Einzelfall – sofern man davon ausgeht, dass dies möglich ist, nur entbunden werden, wenn mit dieser auf einer Einwilligung beruhenden Absenkung des Schutzniveaus keine Beeinträchtigung Dritter einhergeht; der Schutz der Dritten (im Umfeld der Betrachtung dieser Praxishilfe i. d. R. anderer Patienten) muss vollumfänglich gewährleistet bleiben. Somit muss vorab immer eine entsprechende Risikoanalyse durchgeführt und das Ergebnis dieser Analyse genau auf die Auswirkungen für den Schutz der Daten Dritter analysiert werden.

Jedoch ist gerade im Gesundheitswesen das Abhängigkeitsverhältnis zwischen den behandelnden Personen, i. d. R. Ärzte, Arzt und dem jeweiligen Patienten zu beachten. Nach ErwGr. 43 DS-GVO soll in besonderen Fällen, „wenn zwischen der betroffenen Person und dem Verantwortlichen ein klares Ungleichgewicht besteht“ „und es in Anbetracht aller Umstände in dem speziellen Fall unwahrscheinlich ist, dass die Einwilligung freiwillig gegeben wurde“, eine solche Einwilligung nicht als gültige Rechtsgrundlage angesehen werden sollte. Daher muss immer auch die bestehende Abhängigkeit eines Patienten sowie die Umstände (z. B. Eingriffstiefe, Art des verarbeiteten Datums oder Umfang der Datenverarbeitung), unter denen die Einwilligung erteilt worden ist, bei der Beurteilung bzgl. des Vorliegens der Freiwilligkeit einer abgegebenen Einwilligung berücksichtigt werden. Weitere, zu berücksichtigende Aspekte können in einer konkreten Drucksituation, welcher der Patient ausgesetzt ist, liegen. Beispielsweise kann der Zeitpunkt der Einholung einer Einwilligung kurz vor oder nach Vertragsschluss (wie z. B. dem Behandlungsvertrag) ein Anhaltspunkt dafür sein, welcher die Freiwilligkeit infrage stellen kann.

Auf den Nachweis der Freiwilligkeit bei der Abgabe einer Einwilligung im Kontext des Arzt-Patienten-Verhältnisses (wie auch im Beschäftigungsverhältnis) ist daher besonders zu achten.

* 1. Urteile zum Thema
     1. Deutsche Gerichte

Das OLG Düsseldorf urteilte 2021,[[102]](#footnote-102) dass eine Einwilligung ein auf der privatautonomen Entscheidung des Betroffenen beruhender Rechtfertigungstatbestand ist und es der Privatautonomie widerspräche, wenn die Einwilligung nicht zu einem Verzicht auf Anonymisierungs-, Pseudonymisierungs- sowie Verschlüsselungstechniken führen könnte. Das OLG Düsseldorf sieht also eine Möglichkeit, dass die Einwilligung einer betroffenen Person die Herabsenkung eigentlich zur Gewährleistung eines angemessenen Schutzniveaus erforderlichen Maßnahmen legitimieren kann.

Das SG Hamburg urteilte 2023,[[103]](#footnote-103) dass „insbesondere beim Umgang mit sensiblen Sozialdaten konkrete Anforderungen an eine sichere Kommunikation, wie beispielsweise die Verschlüsselung, zu stellen sind“ und betroffene Personen grundsätzlich nicht wirksam in eine unverschlüsselte Kommunikation einwilligen können. Im Urteil wurde auch festgehalten, dass Art. 32 DS-GVO „keine Datensicherheit um jeden Preis“ verlangt, sondern es „muss eine Abwägung zwischen Schutzzweck und Aufwand vorgenommen werden“. [[104]](#footnote-104) Die klagende Person war blind. Im vom SG Hamburg beurteilten Fall musste eine Abwägung einerseits „die Verletzung des Grundrechts des Klägers auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG und zum anderen die Verletzung seines subjektiven Abwehrrechts aus dem Benachteiligungsverbot nach Art. 3 Abs. 3 Satz 2 GG“ beinhalten.104 Entsprechend dem Hamburgischen Behindertengleichstellungsgesetz i. V. m.  dem BGG hatte die Person das Recht auf zeitnahe Zustellung; ein Aufruf einer Homepage des beklagten Jobcenters für den Download der pdf-Datei war ihr aufgrund ihrer Erblindung nicht möglich, eine Entschlüsselung auch nicht. Es bestand ein Sonderfall, bei dem auf eine Diskriminierung und Schlechterstellung von erblindeten Personen Rücksicht genommen werden musste und eine unverschlüsselte Übersendung der Daten durch das Jobcenter als angemessen anzusehen war.

* + 1. EuGH

Ein Urteil seitens des EuGH, ob eine Einwilligung dazu dienen kann, durch Gesetz auferlegte Pflichten eines Verantwortlichen oder Auftragsverarbeiter zu ändern, liegt zum Zeitpunkt der Erstellung dieser Praxishilfe noch nicht vor. Jedoch urteilte der EuGH bereits, wie die Geeignetheit der technischen und organisatorischen Maßnahmen zu beurteilen ist, gleichermaßen äußerte er sich zu den Pflichten bzgl. Nachweis der Geeignetheit der Mittel.

Der EuGH urteilte,[[105]](#footnote-105) dass die Geeignetheit technischen und organisatorischen Maßnahmen in zwei Schritten zu beurteilen ist:

* Zum einen sind die von der betreffenden Verarbeitung ausgehenden Risiken einer Verletzung des Schutzes personenbezogener Daten und ihre möglichen Folgen für die Rechte und Freiheiten natürlicher Personen zu ermitteln. Diese Beurteilung muss konkret unter Berücksichtigung der Eintrittswahrscheinlichkeit und Schwere der ermittelten Risiken erfolgen.
* Zum anderen ist zu prüfen, ob die vom Verantwortlichen getroffenen Maßnahmen unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke dieser Verarbeitung diesen Risiken angemessen sind.

Bei der Kontrolle der Geeignetheit muss eine materielle Prüfung dieser Maßnahmen anhand aller genannten Kriterien sowie der Umstände des Einzelfalls und der dafür zur Verfügung stehenden Beweismittel vorgenommen werden.

Der für die betreffende Verarbeitung Verantwortliche trägt die Beweislast dafür, dass die von ihm getroffenen Sicherheitsmaßnahmen im Sinne von Art. 32 DS-GVO geeignet waren. Die Rechenschaftspflicht des Verantwortlichen verlangt, dass im Rahmen einer auf Art. 82 DS-GVO gestützten Schadenersatzklage der für die betreffende Verarbeitung Verantwortliche die Beweislast dafür trägt, dass die von ihm getroffenen Sicherheitsmaßnahmen im Sinne von Art. 32 DS-GVO geeignet waren.[[106]](#footnote-106)

Im Schadensfall obliegt es, entsprechend der Rechtsprechung des EuGH, dem Verantwortlichen zu beweisen, dass die getroffenen Maßnahmen geeignet i. S. d. DS-GVO waren. Bei der Bewertung der Geeignetheit spielt eine Einwilligung entsprechend EuGH-Urteil keine Rolle, wohl aber Folgen für die Rechte und Freiheiten natürlicher Personen.

Gerade im medizinischen Kontext gibt es Vorgänge, die zeitkritisch sind. Ein Beispiel:

Wird eine Frau mit Verdacht auf Gebärmutterhalskrebs operiert und intraoperativ genetisches Material zur Histologie geschickt wird, d. h. die Patientin in Narkose gehalten wird, bis das Ergebnis der Histologie eintrifft, dann spielen hier zeitkritische Faktoren eine Rolle: Z. B. beinhaltet jede Narkose ein Risiko, muss also so kurz wie möglich erfolgen, auch, um Nebenwirkungen zu vermeiden. Der Versand eines verschlossenen Briefumschlages mit dreitägiger Wartezeit ist hier keine Alternative zu einem Telefonat, welches immer das Risiko des Abhörens der Gesprächsinhalte beinhaltet.

Bei IP-Telefonie kann über das Netzwerk die Kommunikation mitgeschnitten und somit von Dritten auf die Inhalte zugegriffen werden. Bei Mobiltelefonen kann ein IMSI-Catcher eingesetzt werden, sodass sich Mobiltelefone mit diesem statt mit einer regulären Funkzelle verbinden, der Betreiber des IMSI-Catchers kann dann Gespräche mithören.

Trotz des potenziellen Risikos des Abhörens der Gesundheitsinformationen bei einem Telefongespräch wird in Anbetracht der voraussichtlichen negativen gesundheitlichen Folgen für die operierte Person sowie der äußerst geringen Eintrittswahrscheinlichkeit ein Telefongespräch das Mittel der Wahl darstellen, damit benötigte Informationen so schnell und auch so sicher, wie in Anbetracht der Umstände möglich und erforderlich, zwischen Histologen und Operateur ausgetauscht werden können.

* 1. Die Sicht von Datenschutz-Aufsichtsbehörden
     1. Deutsche Aufsichtsbehörden

Folgende deutsche Aufsichtsbehörden vertreten die Auffassung, dass unter bestimmten Bedingungen auf Grundlage einer Einwilligungserklärung in zu dokumentierenden individuellen Fällen auf angemessene technische und organisatorische Maßnahmen verzichtet werden kann:

* Das Bayrische Landesamt[[107]](#footnote-107) für Datenschutzaufsicht teilte diese Auffassung, allerdings noch unter Geltung des § 9 BDSG a. F., unter Geltung der DS-GVO vertrat die Behörde zumindest in Bezug auf E-Mail-Verschlüsselung[[108]](#footnote-108) eine der Hamburger Behörde ähnlichen Ansatz, d. h. geringeres Schutzniveau unter bestimmten Bedingungen möglich.
* Der Hamburger Datenschutzbeauftragte[[109]](#footnote-109) vertritt die Ansicht, dass Art. 32 DS-GVO durch Einwilligung unter bestimmten Bedingungen im konkreten Einzelfall abdingbar sei und somit zur Disposition des Betroffenen stehe.
* Auch der Sächsische Datenschutz- und Transparenzbeauftragte sieht zumindest in Bezug auf E-Mail-Kommunikation die Möglichkeit, dass betroffene Personen in ein niedrigeres Schutzniveau einwilligen können.[[110]](#footnote-110)
* Die Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche Deutschland bewertete 2022 in ihrem Beschluss, dass die § 26 KDG normierte Pflicht eines Verantwortlichen, geeignete technische und organisatorische Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus zu treffen, zwar grundsätzlicher Natur ist, im Einzelfall eine betroffene Person jedoch in das Nichtanwenden von einzelnen technischen und organisatorischen Schutzmaßnahmen gemäß § 6 Abs. 1 lit. b bzw. § 11 Abs. 2 lit. a KDG auf informierte Weise einwilligen kann.[[111]](#footnote-111)

Andere deutsche Aufsichtsbehörden vertreten die Meinung, dass eine Abdingung der gesetzlichen Vorgaben zur IT-Sicherheit durch eine Einwilligung nicht möglich ist.

* Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit stellte 2019 in seiner Stellungnahme zur steuerlichen Förderung der Elektromobilität fest, dass eine Einwilligung i. S. v.  Art. 4 Nr. 11 DS-GVO kein taugliches Instrument ist, um von dem zu beachtenden Grundsatz der Sicherheit der Verarbeitung abzuweichen; entsprechende Einwilligungen wären im Hinblick auf das zu wählende Schutzniveau ohne Wirkung.[[112]](#footnote-112)
* Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht des Landes Brandenburg vertrat 2020 in ihrem Tätigkeitsbericht die Auffassung, dass eine datenschutzrechtliche Einwilligung sich ausschließlich auf die Frage, ob die eigenen personenbezogenen Daten zu einem bestimmten Zweck verarbeitet werden dürfen, bezieht und eine Einwilligung somit „nicht Vorschriften zur Art und Weise ihrer Verarbeitung aushebeln“ kann.[[113]](#footnote-113)
* Das Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein verneint die Abdingbarkeit der vom Verantwortlichen zu ergreifenden Maßnahmen durch eine Einwilligung betroffener Personen.[[114]](#footnote-114)

Im November 2021 veröffentlichte die DSK einen Beschluss,[[115]](#footnote-115) wonach von Verantwortlichen vorzuhaltenden technischen und organisatorischen Maßnahmen auf objektiven Rechtspflichten, beruhen und daher nicht zur Disposition der Beteiligten stehen. Ein Verzicht auf die vom Verantwortlichen vorzuhaltenden technischen und organisatorischen Maßnahmen oder die Absenkung des gesetzlich vorgeschriebenen Standards auf der Basis einer Einwilligung ist daher nicht möglich.

Aber es kann, in zu dokumentierenden Einzelfällen, möglich sein, dass Verantwortliche auf ausdrücklichen, eigeninitiativen Wunsch der informierten betroffenen Person bestimmte vorzuhaltende technische und organisatorische Maßnahmen ihr gegenüber in vertretbarem Umfang nicht anwenden.

* + 1. Österreichische Aufsichtsbehörde

Die österreichische Datenschutzbehörde urteilte 2018, dass Datensicherheitsmaßnahmen nach Art. 32 DS-GVO allein von der Verantwortlichen zu beurteilen sind, die Einholung einer Einwilligung keine Abweichung von erforderlichen Maßnahmen erlauben kann.[[116]](#footnote-116)

* 1. Diskussion

Der Gesetzgeber hat das Recht – und nutzt dieses auch – den Willen von betroffenen Personen durch Gesetze außer Kraft zu setzen, sodass eine Verarbeitung auch durch eine Einwilligung nicht legitimiert werden kann. Ein Beispiel hierzu findet sich in der Sozialgesetzgebung.

Auch im Bereich der IT-Sicherheit gab der Gesetzgeber Regelungen vor, welche durch eine Einwilligung nicht geändert werden können. Neben den Regelungen der europäischen DS-GVO sind im Umfeld der Gesundheitsversorgung beispielsweise zu nennen:

* Die Gesetzgebung für kritische Infrastrukturen (BSIG i. V. m. BSI-KritisV),
* § 390 SGB V IT-Sicherheit in der vertragsärztlichen und vertragszahnärztlichen Versorgung,
* § 391 SGB V IT-Sicherheit in Krankenhäusern,
* § 392 SGB V IT-Sicherheit der gesetzlichen Krankenkassen sowie
* § 103a SGB XI IT-Sicherheit der Pflegekassen.

In diesen nationalen Regelungen werden den Normadressaten - wie beispielsweise Krankenhäusern oder niedergelassenen Arztpraxen - Pflichten auferlegt, welche durch eine Einwilligung nicht geändert werden können.

Art. 24, 25 und 32 DS-GVO erlegen Verantwortlichen Pflichten auf, sowohl in Art. 25 als auch in Art. 32 DS-GVO wird eine abschließende Reihe von Bedingungen genannt, welche bei der Feststellung des Schutzniveaus sowie der zu ergreifenden technischen und organisatorischen Maßnahmen zu berücksichtigen sind – die Einwilligung ist in beiden Fällen nicht darunter.

Für die Bewertung der Angemessenheit der Maßnahmen muss der Verantwortliche „Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen“ bewerten. Zu den Rechten und Freiheiten betroffener Personen gehört entsprechend Titel II („Freiheiten“) der Charta der Grundrechte der Europäischen Union neben dem Schutz personenbezogener Daten (Art. 8 Charta) auch das Recht auf Sicherheit (Art. 6 Charta). Das Recht auf Sicherheit ist nach Rechtsprechung des EuGH weit zu fassen.[[117]](#footnote-117) Dieses Recht umfasst nicht nur den Schutz vor Kriminalität und Gewalttaten, sondern auch die Sicherheit des eigenen Lebens sowie der Gesundheit. Dementsprechend muss ein Verantwortlicher bei der Bewertung der Angemessenheit des nach Art. 32 DS-GVO zu gewährleistenden Schutzniveaus auch immer die Auswirkungen der technisch-organisatorischen Maßnahmen auf Leben und Gesundheit einer betroffenen Person berücksichtigen.

Abseits der DS-GVO sehen europäische und deutsche Rechtsnormen eine Absenkung i. d. R. nicht vor, die Gedanken zur Einhaltung der EU-Grundrechtecharta gelten jedoch gleichermaßen. Auch in diesen Rechtsakten werden i. d. R. „geeignete und angemessene“ Maßnahmen gefordert, d. h. ein gewisser Spielraum zur Bewertung von angemessenen Maßnahmen verbleibt beim Rechtsanwender.

* 1. Fazit

Eine Einwilligung betroffener Personen wird die gesetzlichen Anforderungen bzgl. zu gewährleistender IT-Sicherheit nicht verändern können. Jedoch kann der Wille betroffener Personen – insbesondere, wenn es sich dabei um Patienten handelt und sich die Verarbeitung auf die Behandlung von gesundheitlichen Beeinträchtigungen handelt – einen wichtigen Faktor zur Bestimmung der Angemessenheit in einem konkreten Fall darstellen.

Eine Einwilligung gibt den Willen der betroffenen Person wieder, aber ob dem Willen in Anbetracht der individuellen Situation aus Gründen der Risikobetrachtung für die Rechte und Freiheiten der betroffenen Person gefolgt werden kann oder nicht, diese Entscheidung muss ein Verantwortlicher tragen.

Zumindest die DS-GVO bietet mit Art. 24, 25 und 32 DS-GVO einen großen Raum für „Ausnahmen“ und Einzelfallbetrachtungen hinsichtlich des individuellen Schutzumfangs, denn nach dem Wortlaut der Norm muss der Verantwortliche – ggf. entsprechend Art. 32 DS-GVO auch gemeinsam mit einem oder mehreren Auftragsverarbeitern – „geeignete“ Maßnahmen treffen, um ein „angemessenes“ Schutzniveau zu gewährleisten. Hierbei muss der Verantwortliche zwar auch den „Stand der Technik“ berücksichtigen, aber gleichermaßen die „Zwecke der Verarbeitung“ und die „Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen“, zu denen auch das Recht auf Leben sowie körperliche und geistige Gesundheit der betroffenen Person gehören, in die Bewertung einbeziehen. Die DS-GVO bietet also die Möglichkeit, über das Merkmal der Angemessenheit das konkrete Schutzniveau im Einzelfall festzustellen und den Interessen der betroffenen Personen Rechnung zu tragen, auch ohne Einwilligung.

Das deutsche Recht, welches die IT-Sicherheit in der stationären und ambulanten Versorgung sowie bei Kranken- und Pflegekassen regelt, verlangt hingegen den „Stand der Technik“, welcher i. d. R. durch die Verbandsvertretungen wie der Deutschen Krankenhausgesellschaft oder der Kassenärztlichen Bundesvereinigung herausgegebenen branchenspezifischen Sicherheitsstandards definiert wird, einzuhalten. Eine Einzelfallabwägung zugunsten von Patienten oder Versicherten sah der deutsche Gesetzgeber nicht vor.

Verantwortliche müssen entsprechend den europäischen und deutschen gesetzlichen Vorgaben die Sicherheit der Verarbeitung entsprechend dem Stand der Technik gewährleisten, wobei zumindest das europäische Recht einen Ermessensspielraum hinsichtlich der Vorgaben der Geeignetheit bzw. der Angemessenheit bietet. Ob im in einer bestimmten Situation für eine einzelne betroffene Person eine individuelle Entscheidung getroffen wird und darauf basierend eine Herabsenkung des Sicherheitsniveaus in einem individuellen Fall erfolgt, muss der jeweilige Verantwortliche selbst treffen; dieser muss die Entscheidung in letzter Konsequenz auch verantworten. Und im Zweifelsfall vor Gericht auch dafür haften.

1. Gesetze im Internet
   1. Bundesrecht
      1. Bundesdatenschutzgesetz

<https://www.gesetze-im-internet.de/bdsg_2018/>

* 1. § 22 Verarbeitung besonderer Kategorien personenbezogener Daten

<https://www.gesetze-im-internet.de/bdsg_2018/__22.html>

* 1. § 26 Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses

<https://www.gesetze-im-internet.de/bdsg_2018/__26.html>

* 1. § 27 Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken

<https://www.gesetze-im-internet.de/bdsg_2018/__27.html>

* + 1. Gesetz zur Nutzung von Gesundheitsdaten zu gemeinwohlorientierten Forschungszwecken und zur datenbasierten Weiterentwicklung des Gesundheitswesens (Gesundheitsdatennutzungsgesetz, GDNG)

<https://www.gesetze-im-internet.de/gdng/index.html>

* 1. § 6 Weiterverarbeitung von Versorgungsdaten zur Qualitätssicherung, zur Förderung der Patientensicherheit und zu Forschungszwecken  
     <https://www.gesetze-im-internet.de/gdng/__6.html>
  2. Landeskrankenhausgesetze nach Bundesländern
     1. Baden-Württemberg
* Landeskrankenhausgesetz Baden-Württemberg (LKHG)  
  <https://www.landesrecht-bw.de/perma?j=KHG_BW>
  + § 45 Zulässigkeit der Verarbeitung  
    <https://www.landesrecht-bw.de/bsbw/document/jlr-KHGBW2008V8P45>
  + § 46 Zulässigkeit der Übermittlung  
    <https://www.landesrecht-bw.de/bsbw/document/jlr-KHGBW2008V8P46>
    1. Bayern
* Bayerisches Krankenhausgesetz (BayKrG)  
  <https://www.gesetze-bayern.de/Content/Document/BayKrG>
  + Art. 27 Datenschutz  
    <https://www.gesetze-bayern.de/Content/Document/BayKrG-27>
    1. Berlin
* Landeskrankenhausgesetz (LKG)  
  <https://gesetze.berlin.de/perma?j=KHG_BE>
  + § 24 Verarbeitung von genetischen Daten und Gesundheitsdaten  
    <https://gesetze.berlin.de/bsbe/document/jlr-KHGBE2011V6P24>
  + § 25 Verarbeitung von genetischen Daten und Gesundheitsdaten zu wissenschaftlichen Forschungszwecken  
    <https://gesetze.berlin.de/bsbe/document/jlr-KHGBE2011V4P25>
    1. Brandenburg
* Gesetz zur Entwicklung der Krankenhäuser im Land Brandenburg (Brandenburgisches Krankenhausentwicklungsgesetz - BbgKHEG)  
  <https://bravors.brandenburg.de/gesetze/bbgkheg>
  + § 28 Verarbeitung von Patientendaten mit Ausnahme der Offenlegung  
    <https://bravors.brandenburg.de/gesetze/bbgkheg#28>
  + § 29 Offenlegung von Patientendaten  
    <https://bravors.brandenburg.de/gesetze/bbgkheg#29>
  + § 31 Datenschutz bei Forschungsvorhaben  
    https://bravors.brandenburg.de/gesetze/bbgkheg#31
    1. Bremen
* Bremisches Krankenhausgesetz (BremKrhG)  
  <https://www.transparenz.bremen.de/metainformationen/bremisches-krankenhausgesetz-bremkrhg-vom-24-november-2020-159875?template=20_gp_ifg_meta_detail_d>
  + § 38 Verarbeitung  
    <https://www.transparenz.bremen.de/metainformationen/bremisches-krankenhausgesetz-bremkrhg-vom-24-november-2020-159875?template=20_gp_ifg_meta_detail_d#jlr-KHGBR2020pP38>
  + § 39 Verarbeitung von Patientendaten zu Forschungszwecken  
    <https://www.transparenz.bremen.de/metainformationen/bremisches-krankenhausgesetz-bremkrhg-vom-24-november-2020-159875?template=20_gp_ifg_meta_detail_d#jlr-KHGBR2020pP39>
  + § 40 Übermitteln von Patientendaten an Stellen außerhalb des Krankenhauses  
    <https://www.transparenz.bremen.de/metainformationen/bremisches-krankenhausgesetz-bremkrhg-vom-24-november-2020-159875?template=20_gp_ifg_meta_detail_d#jlr-KHGBR2020pP38>
    1. Hamburg
* Hamburgisches Krankenhausgesetz (HmbKHG)  
  <https://www.landesrecht-hamburg.de/bsha/document/jlr-KHGHAV7IVZ/part/S>
  + § 8 Erhebung und Speicherung von Patientendaten  
    <https://www.landesrecht-hamburg.de/bsha/document/jlr-KHGHAV1P8/part/S>
  + § 10 Verwendung von Patientendaten innerhalb des Krankenhauses  
    <https://www.landesrecht-hamburg.de/bsha/document/jlr-KHGHAV6P10/part/S>
  + § 11 Offenlegung von Patientendaten  
    <https://www.landesrecht-hamburg.de/bsha/document/jlr-KHGHAV7P11/part/S>
  + § 12 Forschungsvorhaben und Sammlungen von Proben  
    <https://www.landesrecht-hamburg.de/bsha/document/jlr-KHGHAV7P12/part/S>
    1. Hessen
* Zweites Gesetz zur Weiterentwicklung des Krankenhauswesens in Hessen (Hessisches Krankenhausgesetz 2011 - HKHG 2011)  
  <https://www.rv.hessenrecht.hessen.de/perma?j=KHG_HE>
  + § 12 Datenschutz im Krankenhaus, Sicherung von Patientenunterlagen  
    <https://www.rv.hessenrecht.hessen.de/bshe/document/jlr-KHGHE2011rahmen/part/X>
    1. Mecklenburg-Vorpommern
* Krankenhausgesetz für das Land Mecklenburg-Vorpommern (Landeskrankenhausgesetz LKHG M-V)  
  <https://www.landesrecht-mv.de/bsmv/document/jlr-LKHGMV2011rahmen>
  + § 33 Rechtmäßigkeit der Datenverarbeitung  
    <https://www.landesrecht-mv.de/bsmv/document/jlr-LKHGMV2011rahmen/part/X>
  + § 34 Weitere Verarbeitung von Daten  
    <https://www.landesrecht-mv.de/bsmv/document/jlr-LKHGMV2011rahmen/part/X>
  + § 37 Datenverarbeitung für Forschungszwecke  
    <https://www.landesrecht-mv.de/bsmv/document/jlr-LKHGMV2011rahmen/part/X>
    1. Niedersachsen
* Krankenhausgesetz für das Land Mecklenburg-Vorpommern (Landeskrankenhausgesetz LKHG M-V)  
  <https://voris.wolterskluwer-online.de/browse/document/48094838-599b-3c15-be0f-0d6ac78f2244>
  + 1. Nordrhein-Westfalen
* Krankenhausgesetz des Landes Nordrhein-Westfalen - KHG NRW  
  <https://recht.nrw.de/lmi/owa/br_text_anzeigen?v_id=10000000000000000483>
* Gesetz zum Schutz personenbezogener Daten im Gesundheitswesen (Gesundheitsdatenschutzgesetz - GDSG NW)  
  <https://recht.nrw.de/lmi/owa/br_text_anzeigen?v_id=10000000000000000495>
  + § 6 Datenverarbeitung für wissenschaftliche Zwecke  
    <https://recht.nrw.de/lmi/owa/br_bes_detail?sg=0&menu=0&bes_id=4283&anw_nr=2&aufgehoben=N&det_id=357750>
  + § 10 Erhebung und Speicherung  
    <https://recht.nrw.de/lmi/owa/br_bes_detail?sg=0&menu=0&bes_id=4283&anw_nr=2&aufgehoben=N&det_id=357754>
  + § 11 Übermittlung und Nutzung von Daten  
    <https://recht.nrw.de/lmi/owa/br_bes_detail?sg=0&menu=0&bes_id=4283&anw_nr=2&aufgehoben=N&det_id=357755>
    1. Rheinland-Pfalz
* Landeskrankenhausgesetz (LKG) Rheinland-Pfalz  
  <https://www.landesrecht.rlp.de/bsrp/document/jlr-KHGRPrahmen/part/X>
  + § 36 Datenschutz  
    <https://www.landesrecht.rlp.de/bsrp/document/jlr-KHGRPV12P36>
  + § 37 Datenschutz bei Forschungsvorhaben  
    <https://www.landesrecht.rlp.de/bsrp/document/jlr-KHGRPV12P37>
    1. Saarland
* Saarländisches Krankenhausgesetz (SKHG)  
  <https://recht.saarland.de/bssl/document/jlr-KHGSL2015rahmen/part/R>
  + § 13 Patientendatenschutz  
    <https://recht.saarland.de/bssl/document/jlr-KHGSL2015V10P13>
  + § 14 Forschung und Patientendaten  
    <https://recht.saarland.de/bssl/document/jlr-KHGSL2015pP14>
    1. Sachsen
* Sächsisches Krankenhausgesetz (SächsKHG)  
  <https://www.revosax.sachsen.de/vorschrift/19826--SaechsKHG>
  + § 28 Datenschutz  
    <https://www.revosax.sachsen.de/vorschrift/19826--SaechsKHG#p28>
  + § 29 Datenschutz bei Forschungsvorhaben  
    <https://www.revosax.sachsen.de/vorschrift/19826--SaechsKHG#p29>
    1. Sachsen-Anhalt
* Krankenhausgesetz Sachsen-Anhalt (KHG LSA)  
  <https://landesrecht.sachsen-anhalt.de/bsst/document/jlr-KHGST2005V6P1>
  + § 16 Verarbeitung von Patientendaten  
    <https://landesrecht.sachsen-anhalt.de/bsst/document/jlr-KHGST2005V9P16>
  + § 17 Verarbeitung von Patientendaten zu Forschungszwecken  
    <https://landesrecht.sachsen-anhalt.de/bsst/document/jlr-KHGST2005V10P17>
    1. Schleswig-Holstein
* Krankenhausgesetz für das Land Schleswig-Holstein - Landeskrankenhausgesetz- (LKHG)  
  <https://www.gesetze-rechtsprechung.sh.juris.de/perma?j=KHG_SH>
  + § 36 Datenverarbeitung im Krankenhaus  
    <https://www.gesetze-rechtsprechung.sh.juris.de/bssh/document/jlr-KHGSHpP36>
  + § 38 Verarbeiten von Patientendaten im Rahmen von Forschungsvorhaben  
    <https://www.gesetze-rechtsprechung.sh.juris.de/bssh/document/jlr-KHGSHpP38>
    1. Thüringen
* Thüringer Krankenhausgesetz (ThürKHG)  
  <https://landesrecht.thueringen.de/perma?j=KHG_TH>
  + § 27 Schutz der Persönlichkeit und Datenschutz  
    <https://landesrecht.thueringen.de/bsth/document/jlr-KHGTH2003V3P27>
  + § 27a Datenverarbeitung für Forschungszwecke außerhalb des Krankenhauses  
    <https://landesrecht.thueringen.de/bsth/document/jlr-KHGTH2003V3P27a>
  1. Landesrettungsdienstgesetze nach Bundesländern
     1. Baden-Württemberg
* Gesetz über den Rettungsdienst (Rettungsdienstgesetz - RDG)   
  <https://www.landesrecht-bw.de/perma?j=RettDG_BW>
  + § 32 Verarbeitung personenbezogener Daten  
    <https://www.landesrecht-bw.de/bsbw/document/jlr-RettDGBW2010V3P32>
    1. Bayern
* Bayerisches Rettungsdienstgesetz  
  <https://www.gesetze-bayern.de/Content/Document/BayRDG>
  + Art. 47 Datenschutz  
    <https://www.gesetze-bayern.de/Content/Document/BayRDG-47>
    1. Berlin
* Gesetz über den Rettungsdienst für das Land Berlin (Rettungsdienstgesetz - RDG)  
  <https://gesetze.berlin.de/perma?j=RettDG_BE>
  + § 4 Datenschutz  
    <https://gesetze.berlin.de/bsbe/document/jlr-RettDGBEV7P4>
    1. Brandenburg
* Gesetz über den Rettungsdienst im Land Brandenburg (Brandenburgisches Rettungsdienstgesetz - BbgRettG)  
  <https://bravors.brandenburg.de/gesetze/bbgrettg>
  + § 19 Dokumentation, Datenschutz, Auskunftspflicht  
    <https://bravors.brandenburg.de/gesetze/bbgrettg#19>
    1. Bremen
* Bremisches Hilfeleistungsgesetz (BremHilfeG)  
  <https://www.transparenz.bremen.de/metainformationen/bremisches-krankenhausgesetz-bremkrhg-vom-24-november-2020-159875?template=20_gp_ifg_meta_detail_d>
  + § 61 Datenverarbeitung  
    <https://www.transparenz.bremen.de/metainformationen/bremisches-hilfeleistungsgesetz-bremhilfeg-vom-21-juni-2016-184267?asl=bremen203_tpgesetz.c.55340.de&template=20_gp_ifg_meta_detail_d#jlr-HilfeGBR2016V7P61>
  + § 62 Datenverarbeitung für das Qualitätsmanagement im Rettungsdienst  
    <https://www.transparenz.bremen.de/metainformationen/bremisches-hilfeleistungsgesetz-bremhilfeg-vom-21-juni-2016-184267?asl=bremen203_tpgesetz.c.55340.de&template=20_gp_ifg_meta_detail_d#jlr-HilfeGBR2016V7P62>
  + § 63 Datenerhebung und Zweckbindung  
    <https://www.transparenz.bremen.de/metainformationen/bremisches-hilfeleistungsgesetz-bremhilfeg-vom-21-juni-2016-184267?asl=bremen203_tpgesetz.c.55340.de&template=20_gp_ifg_meta_detail_d#jlr-HilfeGBR2016V7P63>
    1. Hamburg
* Hamburgisches Rettungsdienstgesetz (HmbRDG)  
  <https://www.landesrecht-hamburg.de/bsha/document/jlr-RettDGHA2019rahmen>
  + § 7 Datenschutz  
    <https://www.landesrecht-hamburg.de/bsha/document/jlr-RettDGHA2019pP7>
    1. Hessen
* Hessisches Rettungsdienstgesetz (HRDG)  
  <https://www.rv.hessenrecht.hessen.de/perma?j=RettDG_HE>
  + § 17 Datenschutz, Auskunftspflicht  
    <https://www.rv.hessenrecht.hessen.de/bshe/document/jlr-RettDGHE2010V3P17>
    1. Mecklenburg-Vorpommern
* Rettungsdienstgesetz Mecklenburg-Vorpommern (RDG M-V)  
  <https://www.landesrecht-mv.de/bsmv/document/jlr-RettDGMV2015rahmen>
  + § 15 Dokumentation, Datenschutz, Auskunftspflicht  
    <https://www.landesrecht-mv.de/bsmv/document/jlr-RettDGMV2015V1P15>
    1. Niedersachsen
* Niedersächsisches Rettungsdienstgesetz (NRettDG)  
  <https://voris.wolterskluwer-online.de/browse/document/7946845b-2902-345d-bc8d-2357a5a72e7c>
  + 1. Nordrhein-Westfalen
* Gesetz über den Rettungsdienst sowie die Notfallrettung und den Krankentransport durch Unternehmer (Rettungsgesetz NRW - RettG NRW)  
  <https://recht.nrw.de/lmi/owa/br_text_anzeigen?v_id=10000000000000000325>
  + § 7a Dokumentation, Datenschutz, Qualitätsmanagement  
    <https://recht.nrw.de/lmi/owa/br_bes_detail?sg=0&menu=0&bes_id=4300&anw_nr=2&aufgehoben=N&det_id=344712>
    1. Rheinland-Pfalz
* Landesgesetz über den Rettungsdienst sowie den Notfall- und Krankentransport (Rettungsdienstgesetz - RettDG )  
  <https://www.landesrecht.rlp.de/bsrp/document/jlr-RettDGRPrahmen>
  + §296 Dokumentationspflicht, Verarbeitung personenbezogener Daten, Informationsübermittlung  
    <https://www.landesrecht.rlp.de/bsrp/document/jlr-RettDGRPV8P29>  
    (Verweis auf § 39 LBKG)
  + § 39 LBKG: Verarbeitung personenbezogener Daten für Zwecke des Brand- und Katastrophenschutzes  
    <https://www.landesrecht.rlp.de/bsrp/document/jlr-Brand_KatSchGRPV14P39>
    1. Saarland
* Saarländisches Rettungsdienstgesetz  
  <https://recht.saarland.de/bssl/document/jlr-RettDGSL2020rahmen>
  + § 27 Datenschutz  
    <https://recht.saarland.de/bssl/document/jlr-RettDGSL2020pP27>
    1. Sachsen
* Sächsisches Gesetz über den Brandschutz, Rettungsdienst und Katastrophenschutz  
  <https://revosax.sachsen.de/vorschrift/4911-SaechsBRKG?follow_successor=no>
  + § 72 Datenschutz  
    <https://revosax.sachsen.de/vorschrift/4911-SaechsBRKG?follow_successor=no#p72>
    1. Sachsen-Anhalt
* Rettungsdienstgesetz des Landes Sachsen-Anhalt (RettDG LSA)  
  <https://www.landesrecht.sachsen-anhalt.de/perma?j=RettDG_ST>
  + § 47 Datenschutz  
    <https://www.landesrecht.sachsen-anhalt.de/bsst/document/jlr-RettDGST2013pP47>
    1. Schleswig-Holstein
* Schleswig-Holsteinisches Rettungsdienstgesetz (SHRDG)  
  <https://www.gesetze-rechtsprechung.sh.juris.de/perma?j=RettDG_SH>
  + § 9 Abs. 3 Weitere Aufgaben, Dokumentation, Datenverarbeitung   
    <https://www.gesetze-rechtsprechung.sh.juris.de/bssh/document/jlr-RettDGSH2017V1P9><https://www.gesetze-rechtsprechung.sh.juris.de/bssh/document/jlr-RettDGSH2017rahmen>  
    (Verweis auf § 12 Landesdatenschutzgesetz)
  + § 12 LDSG: Verarbeitung besonderer Kategorien personenbezogener Daten  
    <https://www.gesetze-rechtsprechung.sh.juris.de/bssh/document/jlr-DSGSH2018pP12>
    1. Thüringen
* Thüringer Rettungsdienstgesetz (ThürRettG)  
  <https://landesrecht.thueringen.de/perma?j=RettDG_TH>
  + § 30 Datenschutz  
    <https://landesrecht.thueringen.de/bsth/document/jlr-RettDGTH2008V2P30>

1. Siehe insbesondere BVerfG, Urteil des Ersten Senats vom 15. Dezember 1983, Az. 1 BvR 209/83. Online, zitiert am 2024-01-15; verfügbar unter [https://www.bundesverfassungsgericht.de/SharedDocs/ Entscheidungen/DE/1983/12/rs19831215\_1bvr020983.html](https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/1983/12/rs19831215_1bvr020983.html) [↑](#footnote-ref-1)
2. EuGH, Urt. v. 2023-12-21, Rechtssache C-667/21, Rn. 79. Online, zitiert am 2024-01-15; verfügbar unter <https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:62021CJ0667> [↑](#footnote-ref-2)
3. EuGH, Urt. v. 2022-08-01, Rechtssache C-92/09, C-93/09, Rn. 119, 120, 125. Online, zitiert am 2024-01-15; verfügbar unter <https://dejure.org/2010,236> bzw. Volltext abrufbar unter <https://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1698904362512&uri=CELEX%3A62020CJ0184> [↑](#footnote-ref-3)
4. EuGH, Urt. v. 2023-07-04, Rechtssache C‑252/21, Rn. 89 sowie Leitsatz 2. Online, zitiert am 2024-01-15; verfügbar unter <https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:62021CJ0252> [↑](#footnote-ref-4)
5. Z. B. GMDS, GDD (2021): Die datenschutzrechtliche Einwilligung: Freund (nicht nur) des Forschers. Online, zitiert am 2024-01-15; verfügbar unter <https://gesundheitsdatenschutz.org/html/einwilligung.php> [↑](#footnote-ref-5)
6. EuGH Urt. v. 2021-01-18, Rechtssache C-61/19, zu finden im Tenor des Urteils. Online, zitiert am 2024-01-15; verfügbar unter <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A62019CA0061&qid=1703360472835> [↑](#footnote-ref-6)
7. Zu beachten: Der BGH erklärte mit seiner Postbank-Entscheidung Zustimmungsfiktionsklauseln in den AGB der Kreditinstitute für missbräuchlich, dies sollte im Kontext der Einwilligung ebenfalls beachtet werden, wenngleich es im Urteil nicht um eine Einwilligung i. S. d. DS-GVO ging, sondern um Art. 54 Abs. 1 i. V. m. Art. 52 Nr. 6 Buchst. a Richtlinie (EU) 2015/2366. BGH, Urt. v. 2021-04-27, Az.  XI ZR 26/20. Online, zitiert am 2024-01-15; verfügbar unter <https://dejure.org/2021,10415> bzw. Volltext Urteil unter <https://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&nr=118834&pos=0&anz=1> [↑](#footnote-ref-7)
8. EuGH, Urt. v. 2023-07-04, Rechtssache C-252/21. Rn. 150. Online, zitiert am 2024-03-22; verfügbar unter <https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:62021CJ0252> [↑](#footnote-ref-8)
9. Eine Abrechnungsgesellschaft kann im Rahmen einer Auftragsverarbeitung vom Krankenhaus eingesetzt werden. In diesem Fall zählt die Abrechnungsgesellschaft als interne Stelle des Verantwortlichen, eine Einwilligung zur Abrechnung durch die Abrechnungsgesellschaft ist dann nicht nötig. Zu beachten ist hierbei, dass die gesamte Abrechnung in diesen Fällen immer auch im Namen des jeweiligen Krankenhauses erfolgen muss, nie die Abrechnungsgesellschaft selbst Forderungen stellen darf. [↑](#footnote-ref-9)
10. Albers M, Veit RD.: Art. 6 DS-GVO, Rn. 44. In: Wolff/Brink/v. Ungern-Sternberg (Hrsg.) BeckOK Datenschutzrecht. 46. Edition, Stand: 01.08.2023 [↑](#footnote-ref-10)
11. So z. B.:

    Buchner B, Petri T.: Art. 6, Rn. 77. In: Kühling / Buchner (Hrsg.) Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO / BDSG. C. H. Beck, 3. Auflage 2020. ISBN: 978-3-406-74994-0

    Kremer P.: Art. 6. Rn. 53. In: Eßer / Kramer / von Lewinski (Hrsg.) DSGVO / BDSG: Datenschutz-Grundverordnung, Bundesdatenschutzgesetz und Nebengesetze (Auernhammer). Wolters Kluwer, 7. Auflage 2020. ISBN 978-3-452-295-26-2

    Roßnagel A.: Art. 6, Rn. 57. In: Simitis / Hornung / Spiecker gen. Döhmann (Hrsg.) Datenschutzrecht. Nomos, 1. Auflage 2019. ISBN 978-3-8487-3590-7 [↑](#footnote-ref-11)
12. EuGH, Urt. v-2023-07-04, Rechtssache C‑252/21, Rn. 93. Online, zitiert am 2024-01-15; verfügbar unter <https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:62021CJ0252> [↑](#footnote-ref-12)
13. Heberlein H.: Art. 6, Rn. 21. In: Ehmann/Selmayr (Hrsg.) Datenschutz-Grundverordnung. C. H. Beck Verlag, 2. Auflage, 2018. ISBN 978-3-406-72006-2 [↑](#footnote-ref-13)
14. Wiesner R.: § 76 SGB VIII, Rn. 12. In: Wiesner / Wapler (Hrsg.) SGB VIII - Kinder- und Jugendhilfe. C. H. Beck Verlag, 6. Auflage 2022. ISBN 978-3-406-75040-3 [↑](#footnote-ref-14)
15. Graulich K.: E. Das Handeln von Polizei- und Ordnungsbehörden zur Gefahrenabwehr, Rn. 10. In: Lisken/Denninger, Handbuch des Polizeirechts. C. H. Beck Verlag, 7. Auflage 2021. ISBN 978-3-406-74370-2 [↑](#footnote-ref-15)
16. Katzenmeier C.: XI. Passivlegitimation und Beweisrecht, Rn. 43. In: Laufs/Katzenmeier/Lipp (Hrsg.) Arztrecht. C. H. Beck Verlag, 8. Auflage 2021. ISBN 978-3-406-73675-9 [↑](#footnote-ref-16)
17. Katzenmeier C.: XI. Passivlegitimation und Beweisrecht, Rn. 44. In: Laufs/Katzenmeier/Lipp (Hrsg.) Arztrecht. C. H. Beck Verlag, 8. Auflage 2021. ISBN 978-3-406-73675-9 [↑](#footnote-ref-17)
18. Greiner H-P.: § 839 BGB, Rn. 492-498. In: Spickhoff (Hrsg.) Medizinrecht. C. H. Beck Verlag, 4. Auflage 2022. ISBN 978-3-406-78835-2 [↑](#footnote-ref-18)
19. Katzenmeier C.: XI. Passivlegitimation und Beweisrecht, Rn. 45. In: Laufs/Katzenmeier/Lipp (Hrsg.) Arztrecht. C. H. Beck Verlag, 8. Auflage 2021. ISBN 978-3-406-73675-9 [↑](#footnote-ref-19)
20. Schantz P.: Art. 6, Rn. 99. In: Simitis / Hornung / Spiecker gen. Döhmann (Hrsg.) Datenschutzrecht. Nomos, 1. Auflage 2019. ISBN 978-3-8487-3590-7 [↑](#footnote-ref-20)
21. Schulz S.: Art. 6, Rn. 62. In: Gola/Heckmann, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz. C. H. Beck Verlag, 3. Auflage, 2022. ISBN 978-3-406-78266-4 [↑](#footnote-ref-21)
22. Albers M, Veit RD.: Art. 6 DS-GVO, Rn. 71. In: Wolff/Brink/v. Ungern-Sternberg (Hrsg.) BeckOK Datenschutzrecht. 46. Edition, Stand: 01.08.2023 [↑](#footnote-ref-22)
23. Art. 3 lit. f Richtlinie 2011/24/EU. Online, zitiert am 2024-01-15; verfügbar unter <https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:02011L0024-20140101#tocId6> [↑](#footnote-ref-23)
24. Art. 3 Abs. 1 lit. a der Richtlinie 2005/36/EG verweist auf „reglementierte Berufe“, bei welchen die Aufnahme oder Ausübung oder eine der Arten der Ausübung direkt oder indirekt durch Rechts- und Verwaltungsvorschriften an den Besitz bestimmter Berufsqualifikationen gebunden ist. Online, zitiert am 2024-01-15; verfügbar unter <https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:02005L0036-20231009#tocId25> [↑](#footnote-ref-24)
25. Ein Hinweis hierzu findet sich z. B. in Schütze B, Spyra G. (2018) Schweigepflicht und die Einbindung externer Kräfte: endlich geregelt. Online, zitiert am 2024-01-15; verfügbar unter <https://gesundheitsdatenschutz.org/html/schweigepflicht_05.php> [↑](#footnote-ref-25)
26. Hierbei sollten die Ausführungen des EuGH bzgl. des Meta-Falles beachtet werden: EuGH, Urt. v. 2023-07-04, Rechtssache C-252/21. Rn. 140ff, insbesondere Rn. 154. Online, zitiert am 2024-01-15; verfügbar unter <https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:62021CJ0252> [↑](#footnote-ref-26)
27. Siehe

    § 5 Abs. 3 DiPAV: „[…] dürfen nur aufgrund einer Einwilligung nach Artikel 9 Absatz 2 Buchstabe a der Verordnung (EU) 2016/679 […} und ausschließlich zu den folgenden Zwecken verarbeitet werden […]“. Online, zitiert am 2024-01-15; verfügbar unter <https://www.gesetze-im-internet.de/dipav/__5.html>

    § 4 Abs. 2 DiGAV: „[…] dürfen personenbezogene Daten nur aufgrund einer Einwilligung der Versicherten nach Artikel 9 Absatz 2 Buchstabe a der Verordnung (EU) 2016/679 […] und ausschließlich zu den folgenden Zwecken verarbeitet werden […]“. Online, zitiert am 2024-01-15; verfügbar unter <https://www.gesetze-im-internet.de/digav/__4.html> [↑](#footnote-ref-27)
28. So z. B. zu finden in:

    EuGH, Urt. v. 2020-07-06, Rechtssache C‑311/18. Rn. 172 bis 175. Online, zitiert am 2024-01-15; verfügbar unter <https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:62018CJ0311>

    EuGH, Urt. v. 2022-08-01, Rechtssache C-184/20. Rn. 70. Online, zitiert am 2024-01-15; verfügbar unter <https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:62020CJ0184> [↑](#footnote-ref-28)
29. So z. B. zu finden in:

    EuGH, Urt. v. 2020-07-06, Rechtssache C‑311/18. Rn. 176. Online, zitiert am 2024-01-15; verfügbar unter <https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:62018CJ0311>

    EuGH, Urt. v. 2021-06-22, Rechtssache C-439/19. Rn. 105. Online, zitiert am 2024-01-15; verfügbar unter <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=ecli%3AECLI%3AEU%3AC%3A2021%3A504> [↑](#footnote-ref-29)
30. EuGH, Urt. v. 2023-03-30, Rechtssache C-34/21. Rn. 65, 71. Online, zitiert am 2024-01-15; verfügbar unter <https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:62021CJ0034> [↑](#footnote-ref-30)
31. EuGH, Urt. v. 2022-02-24, Rechtssache C-175/20. Rn. 83. Online, zitiert am 2024-01-15; verfügbar unter <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A62020CJ0175> [↑](#footnote-ref-31)
32. Ablehnend:

    Albers M, Veit RD.: Art. 9, Rn. 110. In: Wolff/Brink/v. Ungern-Sternberg (Hrsg.). BeckOK Datenschutzrecht. 46. Edition, Stand: 01.08.2023

    Greve H.: Art. Rn. 38. In: Eßer / Kramer / von Lewinski (Hrsg.). DSGVO / BDSG: Datenschutz-Grundverordnung, Bundesdatenschutzgesetz und Nebengesetze. Verlag Carl Heymanns. 7. Auflage. 2020. ISBN 978-3-452-29526-2

    Petri: Art. 9 Rn. 101. In: Simitis / Hornung / Spiecker gen. Döhmann (Hrsg.). Datenschutzrecht. Nomos Verlag, 1. Auflage 2019. ISBN 978-3-8487-3590-7

    Schiff A.: Art. 9, Rn. 64. In: Ehmann/Selmayr. Datenschutz-Grundverordnung. C. H. Beck Verlag, 2. Auflage 2018. ISBN 978-3-406-70215-0

    Schulz S.: Art. 9, Rn. 49. In; Gola/Heckmann (Hrsg.). Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, C. h. Beck Verlag, 3. Auflage 2022. ISBN 978-3-406-78266-4

    Zustimmend:

    Weichert: Art. 9, Rn. 159. In: Kühling / Buchner (Hrsg.). Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO / BDSG. C. H. Beck Verlag, 3. Auflage 2020. ISBN 978/3-406-74994-0 [↑](#footnote-ref-32)
33. So z. B. in

    EuGH, Urt. v. 2023-07-04, Rechtssache C-252/21. Online, zitiert am 2024-01-15; verfügbar unter <https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:62021CJ0252>

    EuGH, Urt. v. 2022-04-05, Rechtssache C-140/20. Online, zitiert am 2024-01-15; verfügbar unter <https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:62020CJ0140> [↑](#footnote-ref-33)
34. Siehe stellvertretend: Weichert T. (2023-11-14) Stellungnahme GDNG. Online, zitiert am 2024-01-15; verfügbar unter <https://www.netzwerk-datenschutzexpertise.de/dokument/medizinische-forschung-und-datenschutz> bzw. pdf-Datei unter <https://www.netzwerk-datenschutzexpertise.de/sites/default/files/2023_stn_gdng.pdf> [↑](#footnote-ref-34)
35. Wissenschaftliche Dienste Deutscher Bundestag. (2019) Gesetzgebungskompetenzen im Bereich des Krankenhausrechts. Online, zitiert am 2024-03-21; verfügbar unter <https://www.bundestag.de/resource/blob/648488/7920b181e85756ccdedff0334a18145b/WD-3-094-19-pdf-data.pdf> [↑](#footnote-ref-35)
36. Wissenschaftliche Dienste Deutscher Bundestag. (2022) Verfassungsrechtlicher Rahmen für die Regelung der stationären medizinischen Versorgung. Online, zitiert am 2024-03-21; verfügbar unter <https://www.bundestag.de/resource/blob/899852/e48e78cfe536ee972862bab82b8618e9/WD-3-054-22-pdf-data.pdf> [↑](#footnote-ref-36)
37. Wissenschaftliche Dienste Deutscher Bundestag. (2019) Zur Frage der Gesetzgebungskompetenz des Bundes für den Öffentlichen Gesundheitsdienst. Online, zitiert am 2024-03-21; verfügbar unter <https://www.bundestag.de/resource/blob/657236/c82ba2db1cd763e2f46439828d73c4e0/WD-9-043-19-pdf-data.pdf> [↑](#footnote-ref-37)
38. Wollenschläger F. (2023) Verfassungskonformität der Reform der Krankenhausplanung auf der Basis der dritten Stellungnahme und Empfehlung der Regierungskommission für eine moderne und bedarfsgerechte Krankenhausversorgung „Grundlegende Reform der Krankenhausvergütung“. Online, zitiert am 2024-03-21; verfügbar unter <https://www.stmgp.bayern.de/wp-content/uploads/2023/04/gutachten_verfassungskonformitaet_krankenhausplanung.pdf> [↑](#footnote-ref-38)
39. Oeter S, Münkler l.: Art. 74, Rn. 140. In: Huber/Voßkuhle (Hrsg.) Grundgesetz, Band 2. C. H. Beck Verlag, 8. Auflage 2024. ISBN 978-3-406-79230-4 [↑](#footnote-ref-39)
40. Siehe

    Wissenschaftliche Dienste Deutscher Bundestag. (2022) Verfassungsrechtlicher Rahmen für die Regelung der stationären medizinischen Versorgung, Seite 3. Online, zitiert am 2024-03-21; verfügbar unter <https://www.bundestag.de/resource/blob/899852/e48e78cfe536ee972862bab82b8618e9/WD-3-054-22-pdf-data.pdf>

    Wissenschaftliche Dienste Deutscher Bundestag. (2019) Gesetzgebungskompetenzen im Bereich des Krankenhausrechts; Seite 3. Online, zitiert am 2024-03-21; verfügbar unter <https://www.bundestag.de/resource/blob/648488/7920b181e85756ccdedff0334a18145b/WD-3-094-19-pdf-data.pdf>

    Wollenschläger, Seite 16/17. Online, zitiert am 2024-03-31; verfügbar unter <https://www.stmgp.bayern.de/wp-content/uploads/2023/04/gutachten_verfassungskonformitaet_krankenhausplanung.pdf> [↑](#footnote-ref-40)
41. Wollenschläger F, Schmidl A. (2016) Kompetentielle Grundfragen des Krankenhausstrukturgesetzes: das neue Qualitätsziel in der Krankenhausplanung. GesR: 542-550 (545) [↑](#footnote-ref-41)
42. Halbe B, Orlowski U.: § 13Krankenhausrecht, Rn. 19. In: Clausen/Schroeder-Printzen (Hrsg.) Münchener Anwaltshandbuch Medizinrecht. C. h. Beck Verlag, 3. Auflage 2020. ISBN: 978-3-406-72937-9 [↑](#footnote-ref-42)
43. BVerfG, Urt. v. 1991-02-07, Az. 2 BvL 24/84, Rn. 72. Online, zitiert am 2024-03-31; verfügbar unter <https://dejure.org/1991,41>, Volltext unter <https://openjur.de/u/176784.html> [↑](#footnote-ref-43)
44. Wissenschaftliche Dienste Deutscher Bundestag. (2022) Verfassungsrechtlicher Rahmen für die Regelung der stationären medizinischen Versorgung, Seite 4. Online, zitiert am 2024-03-21; verfügbar unter <https://www.bundestag.de/resource/blob/899852/e48e78cfe536ee972862bab82b8618e9/WD-3-054-22-pdf-data.pdf> [↑](#footnote-ref-44)
45. Oeter S, Münkler l.: Art. 74, Rn. 142. In: Huber/Voßkuhle (Hrsg.) Grundgesetz, Band 2. C. H. Beck Verlag, 8. Auflage 2024. ISBN 978-3-406-79230-4 [↑](#footnote-ref-45)
46. BVerfG, Urt. v. 1993-05-28, Az. 2 BvF 2/90, 2 BvF 4/90, 2 BvF 5/92. Online, zitiert am 2024-03-31; verfügbar unter <https://dejure>.org/1993,2 [↑](#footnote-ref-46)
47. Wissenschaftliche Dienste Deutscher Bundestag. (2019) Zur Frage der Gesetzgebungskompetenz des Bundes für den Öffentlichen Gesundheitsdienst, S. 8. Online, zitiert am 2024-03-21; verfügbar unter https://www.bundestag.de/resource/blob/657236/c82ba2db1cd763e2f46439828d73c4e0/WD-9-043-19-pdf-data.pdf [↑](#footnote-ref-47)
48. Ratzel R, Lippert H.\_D., Prütting J.: § 9, Rn. 6. Kommentar zur (Muster-)Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte – MBO-Ä 1997. Springer Verlag, 8. Auflage, 2022. ISBN 978-3-662-64723-3 [↑](#footnote-ref-48)
49. Ratzel R, Lippert H.\_D., Prütting J.: § 9, Rn. 52. Kommentar zur (Muster-)Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte – MBO-Ä 1997. Springer Verlag, 8. Auflage, 2022. ISBN 978-3-662-64723-3 [↑](#footnote-ref-49)
50. BVerfG, Urt. v. 19\*83-12-1983, Az.  1 BvR 209/83, 1 BvR 269/83, 1 BvR 362/83, 1 BvR 420/83, 1 BvR 440/83, 1 BvR 484/83. Online, zitiert am 2024-04-07; verfügbar unter [https://www.bundesverfassungsgericht.de/ SharedDocs/Entscheidungen/DE/1983/12/rs19831215\_1bvr020983.html](https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/1983/12/rs19831215_1bvr020983.html) [↑](#footnote-ref-50)
51. BVerfG, Urt. v. 1973-05-29, Az. 1 BvR 424/71, 1 BvR 325/72, Rn. 113. Online, zitiert am 2024-03-31; verfügbar unter <https://dejure.org/1973,10> [↑](#footnote-ref-51)
52. Oeter S, Münkler l.: Art. 74, Rn. 109. In: Huber/Voßkuhle (Hrsg.) Grundgesetz, Band 2. C. H. Beck Verlag, 8. Auflage 2024. ISBN 978-3-406-79230-4 [↑](#footnote-ref-52)
53. Jarass HD: Art. 140/Art. 137 WRV, Rn. 8. In: Jarass/Pieroth, Grundgesetz für die Bundesrepublik Deutschland. C. H. Beck Verlag, 18. Auflage 2024. ISBN 978-3-406-81527-0 [↑](#footnote-ref-53)
54. BVerfG, Urt. v. 1985-06-04, Az. 2 BvR 1703/83, 2 BvR 1718/83, 2 BvR 856/84. Online, zitiert am 2024-04-13; verfügbar unter https://dejure.org/1985,13 [↑](#footnote-ref-54)
55. BVerfG, Urt. v. 1986-05-14, Az. 2 BvL 19/84. Online, zitiert am 2024-04-13; verfügbar unter <https://dejure.org/1986,346> [↑](#footnote-ref-55)
56. BVerfG, Urt. v. 1977-10-11, Az. 1 BvR 96/77. Online, zitiert am 2024-04-13; verfügbar unter <https://dejure.org/1977,797> [↑](#footnote-ref-56)
57. BVerfG, Urt. v. 1971-01-23, Az. 2 BvR 59/71. Online, zitiert am 2024-04-13; verfügbar unter <https://dejure.org/1971,73> [↑](#footnote-ref-57)
58. Jarass HD: Art. 140/Art. 137 WRV, Rn. 6. In: Jarass/Pieroth, Grundgesetz für die Bundesrepublik Deutschland. C. H. Beck Verlag, 18. Auflage 2024. ISBN 978-3-406-81527-0 [↑](#footnote-ref-58)
59. BVerfG, Urt. v. 1983-12-13, Az. 2 BvL 13/82, 2 BvL 14/82, 2 BvL 15/82, Rn. 63: „Zu den ' für alle geltenden Gesetzen ' können nur solche rechnen, die für die Kirche dieselbe Bedeutung haben wie für jedermann“. Online, zitiert am 2024-04-13; verfügbar unter <https://openjur.de/u/193654.html> [↑](#footnote-ref-59)
60. BVerfG, Urt. v. 1980-03-25, Az. 2 BvR 208/76. Online, zitiert am 2024-04-13; verfügbar unter <https://dejure.org/1980,16> [↑](#footnote-ref-60)
61. Konsolidierte Fassung des Vertrags über die Arbeitsweise der Europäischen Union. Online, zitiert am 2024-04-13; verfügbar unter <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:12012E/TXT> [↑](#footnote-ref-61)
62. EuGH, Urt. V. 2018-04-17, Az. C-414/16. Insbesondere Rn. 47, 53, 55, 58, 62, 63. Online, zitiert am 2024-04-14; verfügbar unter <https://dejure.org/2018,8713> bzw. Urteil unter <https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:62016CJ0414> [↑](#footnote-ref-62)
63. Bzgl. Datenschutzrecht gibt es noch keine Entscheidungen des EuGH, jedoch sind die Anmerkungen hinsichtlich des zu beachtenden europäischen Rechts in der Rechtssache C-68/17 (Urt. v. 2018-09-11) in dieser Hinsicht hilfreich. Online, zitiert am 2024-04-13; verfügbar unter <https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:62017CJ0068> [↑](#footnote-ref-63)
64. So z. B. zu finden in:

    EuGH, Urt. V. 2018-04-17, Rechtssache C-414/16, Leitsatz 3. Online, zitiert am 2024-04-14; verfügbar unter <https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:62016CJ0414>

    EuGH, Urt. v. 2018-09-11, Rechtssache C-68/17, Leitsatz 2. Online, zitiert am 2024-04-14; verfügbar unter <https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:62017CJ0068> [↑](#footnote-ref-64)
65. Zu § 26 Abs. 4 BDSG ist anzumerken, dass der BAG dem EuGH am 8. Februar 2023 Fragen vorlegte, die letztlich auch eine Bewertung der Zulässigkeit von Betriebsvereinbarungen als Erlaubnistatbestand zur Verarbeitung personenbezogener Daten beinhaltet.

    Vorlagefragen: <https://curia.europa.eu/juris/document/document.jsf?text=&docid=273715&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1>

    Verfahrensdokumentation: <https://curia.europa.eu/juris/liste.jsf?oqp=&for=&mat=or&jge=&td=%3BALL&jur=C%2CT%2CF&num=C%2D65%2F23> [↑](#footnote-ref-65)
66. Z.B. EuGH, Urt. v. 2023-03-30, Rechtssache C-34/21: Hier wird u.a. die europäisch auszulegenden Begriffe „Beschäftigte“ und „Beschäftigungskontext“ besprochen [↑](#footnote-ref-66)
67. So z.B.

    Kommentarliteratur

    Greiner S.: § 16 SGB IX, Rn. 12b bis 12f- In: Neumann/Pahlen/Greiner/Winkler/Westphal/Krohne (Hrsg.) Sozialgesetzbuch IX: SGB IX. C. H. Beck Verlag, 15. Auflage 2024. ISBN 978-3-406-79269-4

    Gutzeit M.: § 167 SGB IX, Rn. 6, 12. In: Rolfs/Giesen/Meßling/Udsching (Hrsg.) BeckOK Sozialrecht, 72. Edition. Stand: 01.03.2022

    Kossens M.: § 167 SGB IX, Rn. 29. In: Kossens/von der Heide/Maaß (Hrsg.) SGB IX Rehabilitation und Teilhabe von Menschen mit Behinderungen mit Behindertengleichstellungsgesetz. C. H. Beck Verlag, 5. Auflage. 2023. ISBN 978-3-406-71436-8

    Rolfs C.: § 167 SGB IX, Rn. 7. In: Erfurter Kommentar zum Arbeitsrecht. C. H. Beck Verlag, 24. Auflage 2024 ISBN 978-3-406-80415-1

    Fachzeitschriften

    Fuhlrott M. (2024)

    Glatzel B. (2023) Aktuelle Rechtsprechung zum betrieblichen Eingliederungsmanagement. NZA-RR: 113 – 116 (113)

    Löser A. (2021) Rechte der Schwerbehindertenvertretung. öAT: 155 – 158 (156)

    Stück V. (2021) BEM-Verfahren – Voraussetzungen, Beteiligte, Rollen und Aufgaben. ArbRAktuell: 339 – 342 (341) [↑](#footnote-ref-67)
68. Kein Recht auf Einsichtnahme besteht hingegen auf die Teile der Bewerbungsunterlagen, auf die der AG seine Entscheidung nicht gestützt hat. (siehe z. B. Rolfs: § 178 SGB IX, Rn. 6. In: Erfurter Kommentar zum Arbeitsrecht, 24. Auflage 2024. ISBN 978-3-406-80415-1) D. H. Es dürfen keine Unterlagen weitergegeben werden, die vom Arbeitgeber nicht als entscheidungsrelevant angesehen werden. Somit ist eine Darstellung erforderlich, welche Unterlagen entscheidungsrelevant sind und warum diese entsprechend bewertet sind. Die Nachwollziehbarkeit muss auch hier gegeben sein, ein Bewerber hat im Rahmen seines Auskunftsrechts auch hierauf Anspruch. [↑](#footnote-ref-68)
69. BAG, Urt. v. 2018-12-19, Az. 7 ABR 80/16, Rn. 22. Online, zitiert am 2024-05-11; verfügbar unter <https://dejure.org/2018,42738> bzw. Urteil beim BAG <https://www.bundesarbeitsgericht.de/entscheidung/7-abr-80-16/> [↑](#footnote-ref-69)
70. Bremische evangelische Kirche: Patientendatenverordnung. Online, zitiert am 2024-05-09; verfügbar unter <https://www.kirchenrecht-bremen.de/document/13864> [↑](#footnote-ref-70)
71. Gesetz zum Schutz von Patientendaten bei der Seelsorge in katholischen Einrichtungen des Gesundheitswesens in der (Erz-)Diözese (SeelsorgePatDSG). Online, zitiert am 2024-05-09; verfügbar unter <https://kirchlicher-datenschutz.org/seelsorgepatdsg/> [↑](#footnote-ref-71)
72. Wissenschaftlichen Dienste dt. Bundestag: WD 9 - 020/22 Gesetzgebungskompetenzen im Bereich des Rettungswesens (2022-03-07). Online, zitiert am 2024-06-18; verfügbar unter <https://www.bundestag.de/resource/blob/897344/b02aad2f6e6f696144af1a86966f5d94/WD-9-020-22-pdf.pdf> [↑](#footnote-ref-72)
73. Gesetz über den Beruf der Notfallsanitäterin und des Notfallsanitäters. Online, zitiert am 2024-06-18; verfügbar unter <https://www.gesetze-im-internet.de/notsang/index.html> [↑](#footnote-ref-73)
74. Wissenschaftlichen Dienste dt. Bundestag: WD 9 - 049/22 Ausbildung und Berufsausübung von Rettungssanitätern (2022-09-20). Online, zitiert am 2024-06-18; verfügbar unter <https://www.bundestag.de/resource/blob/912896/e896cc1c5c4599645ff6b1cbb4fd3deb/WD-9-049-22-pdf.pdf> [↑](#footnote-ref-74)
75. Im Koalitionsvertrag für die 20. Legislaturperiode des Bundestages ist vorgesehen, das Rettungswesen als integrierten Leistungsbereich in das SGB V aufzunehmen. Siehe „Koalitionsvertrag zwischen SPD, Bündnis 90/Die Grünen und FDP“, S. 66, 3. Absatz. Online, zitiert am 2024-06-18; verfügbar unter <https://www.bundesregierung.de/breg-de/aktuelles/koalitionsvertrag-2021-1990800>, pdf-Datei Vertrag unter <https://www.spd.de/fileadmin/Dokumente/Koalitionsvertrag/Koalitionsvertrag_2021-2025.pdf> [↑](#footnote-ref-75)
76. EuGH, Urt. v-2023-07-04, Rechtssache C‑252/21, Rn. 93. Online, zitiert am 2024-01-15; verfügbar unter <https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:62021CJ0252> [↑](#footnote-ref-76)
77. Buchner B, Petri T.: Art. 6, Rn. 153. In: Kühling / Buchner (Hrsg.) Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO / BDSG. C. H. Beck, 3. Auflage 2020. ISBN: 978-3-406-74994-0 [↑](#footnote-ref-77)
78. Schantz P.: Art. 6, Rn. 101. In: Simitis / Hornung / Spiecker gen. Döhmann (Hrsg.) Datenschutzrecht. Nomos, 1. Auflage 2019. ISBN 978-3-8487-3590-7 [↑](#footnote-ref-78)
79. Schantz P.: Art. 6, Rn. 107. In: Simitis / Hornung / Spiecker gen. Döhmann (Hrsg.) Datenschutzrecht. Nomos, 1. Auflage 2019. ISBN 978-3-8487-3590-7 [↑](#footnote-ref-79)
80. BVerfG, Urt. v. 1973-01-31, AZ.: 2 BvR 454/71. Rn. 34, 35. Online, zitiert am 2024-03-22; verfügbar unter <https://dejure.org/1973,7>, Volltext unter <https://openjur.de/u/180606.html> [↑](#footnote-ref-80)
81. So zu finden in

    Albers M, Veit RD.: Art. 6 DS-GVO, Rn. 71. In: Wolff/Brink/v. Ungern-Sternberg (Hrsg.) BeckOK Datenschutzrecht. 46. Edition, Stand: 01.08.2023

    Buchner B, Petri T.: Art. 6, Rn. 155. In: Kühling / Buchner (Hrsg.) Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO / BDSG. C. H. Beck, 3. Auflage 2020. ISBN: 978-3-406-74994-0

    Schantz P.: Art. 6, Rn. 112. In: Simitis / Hornung / Spiecker gen. Döhmann (Hrsg.) Datenschutzrecht. Nomos, 1. Auflage 2019. ISBN 978-3-8487-3590-7 [↑](#footnote-ref-81)
82. EuGH, Urt. v. 2023-12-07, Rechtssache C-26/22, C-64/22. Rn. 75 bis 80. Online, zitiert am 2024-01-15; verfügbar unter <https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:62022CJ0026> [↑](#footnote-ref-82)
83. EuGH, Urt. v, 2016-10-19, Rechtssache C-582/14, Rn. 62: „[…] der im konkreten Einzelfall einander gegenüberstehenden Rechte und Interessen […]“. Online, zitiert am 2024-01-15; verfügbar unter <https://dejure.org/2016,33959> bzw. Volltext unter <https://curia.europa.eu/juris/document/document.jsf?text=&docid=184668&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1> [↑](#footnote-ref-83)
84. EuGH Urt. v. 2023-12-07, Rechtssache C-26/22, C-64/22, Rn. 94. Online, zitiert am 2024-03-22; verfügbar unter <https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:62022CJ0026> [↑](#footnote-ref-84)
85. EuGH, Urt. v. 2019-12-11, Rechtssache C-708/18, Rn. 55. Online, zitiert am 2024-03-22; verfügbar unter <https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:62018CJ0708> [↑](#footnote-ref-85)
86. EuGH Urt. v. 2023-12-07, Rechtssache C-26/22, C-64/22, Rn. 79. Online, zitiert am 2024-03-22; verfügbar unter <https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:62022CJ0026> [↑](#footnote-ref-86)
87. EuGH, Urt. V. 2019-12-11, Rechtssache C-708/18, Rn. 44. Online, zitiert am 2024-03-22; verfügbar unter <https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:62018CJ0708> [↑](#footnote-ref-87)
88. EuGH, Urt. v. 2023-07-04, Rechtssache C-252/21. Rn. 126. Online, zitiert am 2024-03-22; verfügbar unter <https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:62021CJ0252> [↑](#footnote-ref-88)
89. Quelle: Bevölkerungsstand vom 31.12.2015, entnommen offizieller Statistik veröffentlicht vom Statistischen Bundesamt [↑](#footnote-ref-89)
90. Quelle: Brustkrebsfrüherkennung durch Mammographie-Screening, Onkologe 2017, 23:701–710, DOI 10.1007/s00761-017-0261-3 [↑](#footnote-ref-90)
91. Quelle: <https://www.frauenaerzte-im-netz.de/de_brustkrebs-risikofaktoren-vorbeugung_367.html> [↑](#footnote-ref-91)
92. Wissenschaftliche Dienste Deutscher Bundestag. (2022) Verfassungsrechtlicher Rahmen für die Regelung der stationären medizinischen Versorgung. Online, zitiert am 2024-03-21; verfügbar unter <https://www.bundestag.de/resource/blob/899852/e48e78cfe536ee972862bab82b8618e9/WD-3-054-22-pdf-data.pdf> [↑](#footnote-ref-92)
93. Siehe z. B.

    Jandt S.: Art. 32 Rn. 40. In: Kühling/Buchner (Hrsg.) DS-GVO Bundesdatenschutzgesetz Kommentar. C. H. Beck Verlag, 3. Auflage 2020. ISBN 978-3-406-74994-0

    John N, Schaller J. (2022) Keine Disponibilität der technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO. CR: 156-159

    Lotz B, Wendler J. (2016) Datensicherheit als datenschutzrechtliche Anforderung: Zur Frage der Abdingbarkeit des § 9 BDSG. CR: 31-36

    Schwartmann R, Hermann T.: Teil 10.5 Datenschutz und Datensicherheit im (I)IoT, Rn. 79. In: Leupold/Wiebe/Glossner (Hrsg.) IT-Recht. C. H. Beck Verlag, 4. Auflage 2021. ISBN 978-3-406-74458-7 [↑](#footnote-ref-93)
94. Siehe z. B. Bleckat A. (2021) Abdingbarkeit des Art. 32 DS-GVO durch Einwilligung. RDV: 206-208 (207) [↑](#footnote-ref-94)
95. Verordnung des Europäischen Parlaments und des Rates über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnung (EU) 2019/1020: Konsolidierter Text. Online, zitiert am 2024-04-25; verfügbar unter <https://www.europarl.europa.eu/doceo/document/TA-9-2024-0130_DE.html> [↑](#footnote-ref-95)
96. Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie). Online, zitiert am 2024-04-25; verfügbar unter <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32022L2555> [↑](#footnote-ref-96)
97. Bisher existiert nur ein geleakter Referentenentwurf des BMI vom 2023-12-23; ob die Frist seitens des deutschen Gesetzgebers eingehalten oder wieder einmal überschritten wird, ist derzeit nicht sicher zu sagen. Online, zitiert am 2024-04-25; verfügbar unter

    Geleakter Referentenentwurf: <https://ag.kritis.info/2024/03/07/referentenentwurf-des-bmi-nis-2-umsetzungs-und-cybersicherheitsstaerkungsgesetz-nis2umsucg/>

    Diskussion zum Umsetzungstand: <https://intrapol.org/2024/03/04/update-zum-neuen-refe-fuer-ein-nis2umsucg/> [↑](#footnote-ref-97)
98. Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die Resilienz kritischer Einrichtungen und zur Aufhebung der Richtlinie 2008/114/EG des Rates. Online, zitiert am 2024-04-25; verfügbar unter <https://eur-lex.europa.eu/eli/dir/2022/2557/oj> [↑](#footnote-ref-98)
99. Referentenentwurf des BMI vom 2023-07-28 stand zur Verbändekommentierung zur Verfügung, sowohl der Referentenentwurf wie auch die Stellungnahmen sind im Internet abrufbar. Online, zitiert am 2024-04-25; verfügbar unter <https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/KRITIS-DachG.html> [↑](#footnote-ref-99)
100. Bundestag - Drucksache 19/13438 vom 2019-09-23, Seite 48 (Zu Nummer 10). Online, zitiert am 2024-04-23; verfügbar unter <https://dserver.bundestag.de/btd/19/134/1913438.pdf> [↑](#footnote-ref-100)
101. Z. B.: GMDS, GDD: „Die datenschutzrechtliche Einwilligung: Freund (nicht nur) des Forschers. Stand: 30. April 2021. Online, zitiert am 2024-04-23; verfügbar unter [https://gesundheitsdatenschutz.org/html/ einwilligung.php](https://gesundheitsdatenschutz.org/html/einwilligung.php) [↑](#footnote-ref-101)
102. OLG Düsseldorf, Urt. v. 2021-10-28, Az. 16 U 275/20, Rn. 73. Online, zitiert am 2024-04-23; verfügbar unter <https://dejure.org/2021,55418> bzw. Volltext unter <https://openjur.de/u/2384847.html> [↑](#footnote-ref-102)
103. SG Hamburg, Urt. v. 2023-06-30, Az.  S 39 AS 517/23, Rn. 43. Online, zitiert am 2024-04-23; verfügbar unter <https://www.landesrecht-hamburg.de/bsha/document/NJRE001547745> [↑](#footnote-ref-103)
104. SG Hamburg, Urt. v. 2023-06-30, Az.  S 39 AS 517/23, Rn. 90. Online, zitiert am 2024-04-23; verfügbar unter <https://www.landesrecht-hamburg.de/bsha/document/NJRE001547745> [↑](#footnote-ref-104)
105. EuGH, Urt. v. 2023-12-14, Rechtssache C-340/21, Rn. 42. Online, zitiert am 2024-04-23; verfügbar unter <https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:62021CJ0340> [↑](#footnote-ref-105)
106. EuGH, Urt. v. 2023-12-14, Rechtssache C-340/21, Rn. 57. Online, zitiert am 2024-04-23; verfügbar unter <https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:62021CJ0340> [↑](#footnote-ref-106)
107. Bayrisches Landesamt für Datenschutzaufsicht: 7. Tätigkeitsbericht von 2015/2016, S. 99. Online, zitiert am 2024-04-23; verfügbar unter https://www.lda.bayern.de/media/baylda\_report\_07.pdf [↑](#footnote-ref-107)
108. Bayrisches Landesamt für Datenschutzaufsicht: 8. Tätigkeitsbericht von 2017/2018, S. 137 u. 138. Online, zitiert am 2024-04-23; verfügbar unter <https://www.lda.bayern.de/media/baylda_report_08.pdf> [↑](#footnote-ref-108)
109. Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit: Abdingbarkeit von technisch-organisatorischen Maßnahmen (Art. 32 DSGVO). Online, zitiert am 2024-04-23; verfügbar unter <https://datenschutz-hamburg.de/fileadmin/user_upload/HmbBfDI/Vermerke_und_Stellungnahmen/Vermerk-Abdingbarkeit_TOMs.pdf> [↑](#footnote-ref-109)
110. Sächsische Datenschutz- und Transparenzbeauftragte: Tätigkeitsbericht 2019, Abschnitt 4.1.7, S. 87. Online, zitiert am 2024-04-23; verfügbar unter [https://www.datenschutz.sachsen.de/download/ taetigkeitsberichte/Taetigkeitsbericht\_2019.pdf](https://www.datenschutz.sachsen.de/download/taetigkeitsberichte/Taetigkeitsbericht_2019.pdf) [↑](#footnote-ref-110)
111. Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche Deutschland: Dispositionsrecht zur Einwilligung in die Nichtanwendung von technischen und organisatorischen Maßnahmen. Beschluss der Sitzung vom 2022-06-15. Online, zitiert am 2024-04-23; verfügbar unter <https://www.kath-datenschutzzentrum-ffm.de/wp-content/uploads/2022-06-15-Beschluss-Dispositionsrecht-Nichtanwendung-TOM.pdf> [↑](#footnote-ref-111)
112. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit: : Stellungnahme zur steuerlichen Förderung der Elektromobilität, S. 3 und 4. (Stand 2019-10-11) Online, zitiert am 2024-04-23; verfügbar unter <https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Stellungnahmen/2019/StgN_steuerliche_F%C3%B6rderung_eMobilit%C3%A4t.pdf?__blob=publicationFile&v=5> [↑](#footnote-ref-112)
113. Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg: Tätigkeitsbericht Datenschutz 2020, S. 43. Online, zitiert am 2024-04-23; verfügbar unter <https://www.lda.brandenburg.de/sixcms/media.php/9/TB_2020_web.pdf> [↑](#footnote-ref-113)
114. Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein: 37. Tätigkeitsbericht 2019, Abschnitt 5.4.9 auf S. 99. Online, zitiert am 2024-04-23; verfügbar unter <https://www.datenschutzzentrum.de/tb/tb37/uld-37-taetigkeitsbericht-2019.pdf> [↑](#footnote-ref-114)
115. Datenschutzkonferenz: Beschluss vom 2021-11-24 zur Möglichkeit der Nichtanwendung technischer und organisatorischer Maßnahmen nach Art. 32 DSGVO auf ausdrücklichen Wunsch betroffener Personen. Online, zitiert am 2024-04-23; verfügbar unter [https://www.datenschutzkonferenz-online.de/media/dskb/ 20211124\_TOP\_7\_Beschluss\_Verzicht\_auf\_TOMs.pdf](https://www.datenschutzkonferenz-online.de/media/dskb/20211124_TOP_7_Beschluss_Verzicht_auf_TOMs.pdf) [↑](#footnote-ref-115)
116. Österreichische Datenschutzbehörde, B. v. 2018-11-16 Geschäftszahl DSB-D213.692/0001-DSB/2018, Abschnitt D 3.2.2. Online, zitiert am 2024-04-23; verfügbar unter <https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Dsk&Entscheidungsart=Undefined&Organ=Undefined&SucheNachRechtssatz=True&SucheNachText=True&GZ=DSB-D213.692%2f0001-DSB%2f2018&VonDatum=01.11.2018&BisDatum=01.12.2018&Norm=&ImRisSeitVonDatum=&ImRisSeitBisDatum=&ImRisSeit=Undefined&ImRisSeitForRemotion=Undefined&ResultPageSize=100&Suchworte=&Position=1&SkipToDocumentPage=true&ResultFunctionToken=6f146701-3dee-4023-9b80-1be58056518f&Dokumentnummer=DSBT_20181116_DSB_D213_692_0001_DSB_2018_00> [↑](#footnote-ref-116)
117. EuGH, Urt. v. 2014-08 04, Rechtssachen C-293/12 und C-594/12. Rn. 42, S. 3: „Im Übrigen ist insoweit festzustellen, dass nach Art. 6 der Charta jeder Mensch nicht nur das Recht auf Freiheit, sondern auch auf Sicherheit hat.“ Online, zitiert am 2024-04-23; verfügbar unter <https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:62012CJ0293> [↑](#footnote-ref-117)