Klinische Register und Datenschutz

Eine Zusammenarbeit von

Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V.
Arbeitskreis „Datenschutz und IT-Sicherheit im Gesundheitswesen“

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

ZTG Zentrum für Telematik und Telemedizin GmbH (ZTG)

Autoren

David Koeppe	Vivantes - Netzwerk für Gesundheit GmbH
Bernd Schütze	Deutsche Telekom Healthcare and Security GmbH
Lars Treinat	ZTG Zentrum für Telematik und Telemedizin GmbH
Eric Wichterich	ZTG Zentrum für Telematik und Telemedizin GmbH

Stand: 13. Dezember 2019

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:

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, Männern und Frauen.
>
> Im folgenden Text wird, 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.

Inhaltsverzeichnis

Zusammenfassung

Mit Hilfe eines klinischen Registers werden patientenbezogen medizinische Daten in einem vordefinierten medizinischen Bereich wie beispielsweise Brustkrebs gesammelt. Klinische Register können dabei auf einer gesetzlichen Grundlage basieren, wie beispielsweise Krebsregister basierend auf den jeweiligen Landeskrebsregistergesetzen, oder sie sind nicht gesetzlich geregelt. Nicht gesetzlich geregelte Register werden häufig von medizinischen Fachgremien oder von diesen gegründeten privatwirtschaftlichen Institutionen betreiben.

Klinische Register benötigen zur Verarbeitung personenbezogener Daten, zu denen auch pseudonyme Daten gehören, einen Erlaubnistatbestand. Bei den Erlaubnistatbeständen zur Verarbeitung von Gesundheitsdaten wie auch genetischen Daten bietet Art. 9 Abs. 4 DS-GVO den nationalen Gesetzgebern viel Gestaltungsspielraum, so dass der deutsche Bundes- und auch Landesgesetzgeber hier eigene Erlaubnistatbestände in Gesetzen wie z.B. den Sozialgesetzbüchern oder dem Arzneimittelgesetz schaffen kann.. Im Falle gesetzlich geregelter Register findet sich der Erlaubnistatbestand daher im jeweiligen Registergesetz, bei nicht gesetzlich geregelten Registern stellt häufig die Einwilligung der jeweiligen Patienten den Erlaubnistatbestand dar.

Art. 5 Abs. 1 DS-GVO beinhaltet Grundsätze, die bei jeder Verarbeitung personenbezogener Daten immer gewährleistet sein müssen, also auch bei klinischen Registern: Diese Grundsätze beinhalten u. a. die Zweckbindung, die Datenminimierung und die Speicherbegrenzung. Somit dürfen personenbezogene Daten von einem klinischen Register nur auf rechtmäßige Weise zu genau definierten Zwecken verarbeitet werden, es dürfen nur die zur Erreichung dieser (vor Erhebung) definierten Zwecke unbedingt erforderlichen Daten verarbeitet werden und der Zeitraum der Speicherung der Daten muss definiert sein: Daten müssen nach Erreichen des Zweckes gelöscht werden, wenn keine gesetzlichen Aufbewahrungsfristen einzuhalten sind. Bei einem klinischen Register darf man zu Recht die Frage stellen, wann der Zweck erreicht ist. Jedoch verlangt der Grundsatz der Erforderlichkeit der Daten, dass man auch die Notwendigkeit des Personenbezugs nachweisen muss. Denn die DS-GVO verlangt grundsätzlich, dass man die Einhaltung der Vorgaben der DS-GVO nachweist.

Klinische Register „leben“ von Patientendaten. Die Patientendaten werden in den versorgenden Einrichtungen jedoch zu Zwecken der Patientenversorgung erhoben, nicht um die Daten in einem Register zu speichern. Daher spricht man hier von einer „Sekundärnutzung“ der Daten; der primäre Zweck der Datenverarbeitung war ja die Patientenversorgung. Art. 5 Abs. 1 lit. b DS-GVO beinhaltet die Regelung, dass „eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke“ gemäß Art. 89 Abs. 1 DS-GVO nicht als „unvereinbar mit den ursprünglichen Zwecken“ gilt, man spricht hier von „Zweckkompatibilität“. Aber gleichwohl liegt natürlich eine Zweckänderung vor, aus der entsprechende Pflichten resultieren.

Die Verarbeitung personenbezogener Daten in einem klinischen Register muss für die betroffenen Personen/Patienten transparent erfolgen, allen in Kapitel II DS-GVO genannten Betroffenenrechten und insbesondere den Informationspflichten muss genügt werden. Jeder Patient hat das Recht auf Auskunft bzgl. der in einem klinischen Register verarbeiteten bzw. gespeicherten Daten. Weiterhin ist u. a. zu beachten, dass nach Art. 15 Abs. 3 DS-GVO der Verantwortliche betroffenen Personen auch eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung

stellen muss. Dementsprechend sollten klinische Register die Möglichkeit haben, alle zu einem Patienten gehörenden Daten in eine pdf-Datei exportieren zu können, um diese Datei anfragenden betroffenen Patienten übergeben zu können.

Die DS-GVO verlangt zudem eine „sichere“ Verarbeitung der Daten. Dies beginnt schon bei der Planung: Privacy by Design (Art. 25 DS-GVO) verlangt eine datenschutzgerechte Planung, Privacy by Default (ebenfalls Art. 25 DS-GVO) dass die „datenschutzfreundlichste“ Variante die Voreinstellung bei der Verarbeitung ist. Bestehen erhöhte Risiken, was bei klinischen Registern häufig zutreffen wird, ist eine Datenschutz-Folgenabschätzung (Art. 35 DS-GVO) durchzuführen. Der Einsatz angemessener technischer und organisatorischer Maßnahmen muss dabei für den gesamten Lebenszyklus der Daten die Sicherheit der Verarbeitung gewährleisten, Art. 32 DS-GVO gibt hier die Beachtung des jeweils geltenden „Stands der Technik“ vor.

Die DS-GVO enthält Regelungen bzgl. der Verletzung des Schutzes personenbezogener Daten. Eine Verletzung des Schutzes personenbezogener Daten liegt daher nicht nur dann vor, wenn Unberechtigte Zugang zu diesen Daten bekommen, sondern auch, wenn diese Daten unbeabsichtigt oder unrechtmäßig vernichtet, verändert oder verloren gehen. Je nach Höhe des aus der Verletzung des Schutzes personenbezogener Daten resultierenden Risikos muss die datenschutzrechtliche Aufsichtsbehörde und ggf. auch die betroffenen Patienten selbst über diese Verletzung inklusive der aus der Verletzung resultierenden Risiken und der zur Begrenzung der Risiken sowie der Verhinderung künftiger Verletzungen getroffenen Maßnahmen informiert werden.

Bei Verstößen gegen die Vorgaben können die Aufsichtsbehörden einerseits ein Bußgeld verhängen, andererseits auch von „Abhilfebefugnissen“ Gebrauch machen. Diese Abhilfebefugnisse können eine Verwarnung darstellen, eine Anweisung Anträgen einer betroffenen Person auf Ausübung der ihr nach der DS-GVO zustehenden Rechte wie beispielsweise Löschung der Daten zu entsprechen, aber letztlich auch die Anweisung zur Beendigung der Verarbeitung beinhalten. D. h. Aufsichtsbehörden können bei entsprechenden Verstößen auch die Arbeit eines Registers beenden, zumindest für den Zeitraum, bis alle aus Sicht der Aufsichtsbehörden relevanten Verstöße beseitigt sind.

Gemäß Art. 38 Abs. 1 DS-GVO muss ein Datenschutzbeauftragter „ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden“ werden. Dies beinhaltet natürlich auch die Erstellung und den Betrieb eines klinischen Registers, insbesondere auch Forschungsprojekte innerhalb des klinischen Registers. Daher ist der Datenschutzbeauftragte schon bei der Planung eines klinischen Registers einzubeziehen und es sind ihm sowohl während der Planung als auch während der Laufzeit alle zur Prüfung der Verarbeitung benötigten Informationen bereitzustellen.

1 Einführung

In einem klinischen Register werden Patientendaten aus versorgenden Einrichtungen gesammelt. Diese Datensammlung kann je nach Ausrichtung des Registers zu folgenden Zwecken dienen:

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

Klinische Register entwickeln sich nicht nur in Deutschland immer stärker zu einem wichtigen Werkzeug, welches die Beurteilung des Therapieverhaltens unter Realbedingungen ermöglicht. D. h. es kann dargestellt werden, wie die Versorgungslage in Deutschland aussieht, aber auch, wo ggf. noch Verbesserungspotential besteht. Ein gutes Beispiel hierzu ist das Traumaregister, welches die Verbesserung der Versorgung Unfallverletzter in den letzten zwanzig Jahren maßgeblich beeinflusste.[1]

Eine hohe Validität der mittels des klinischen Registers getroffenen Aussagen kann natürlich nur dann erzielt werden, wenn im Register eine möglichst vollzählige Erfassung behandelten Patienten erfolgt: je vollständiger die Erfassung, desto genauer und zutreffender können die Aussagen sein.

Somit ist es häufig erforderlich, dass im Register weniger Daten erfasst werden als beispielsweise in Forschungsdatenbanken. Denn es sollen möglichst alle versorgenden Einrichtungen Daten liefern können, aber die für spezielle Forschungsfragen erforderlichen Daten wie beispielsweise spezielle biochemische Marker werden nicht überall erhoben. Daher werden in Registern i. d. R. nur Basisdatensätze erhoben, wie z. B. bei den klinischen Krebsregistern der Basisdatensatz[2] von ADT/GEKID.

Der vorliegende Leitfaden nimmt die Zielsetzung von Registern in den Fokus und führt durch seinen strukturellen Aufbau durch die wesentlichen Datenschutzaspekte, die bei der Errichtung und beim Betrieb von Registern zu beachten sind.

1.1 Register zur Forschung

Mit Hilfe eines klinischen Registers werden patientenbezogen medizinische Daten in einem vordefinierten medizinischen Bereich wie beispielsweise Brustkrebs gesammelt. Die gesammelten Daten können gezielt hinsichtlich definierter klinischer Fragestellungen, die natürlich mit dem medizinischen Bereich des Registers zusammenhängen müssen, ausgewertet und so Fragestellungen der epidemiologischen, sehr viel häufiger jedoch der klinischen Forschung angegangen werden.

[1] Deutschen Gesellschaft für Unfallchirurgie: Traumaregister. [Online, zitiert am 2019-10-01]; Verfügbar unter http://www.traumaregister-dgu.de/

[2] ADT, GEKID: Gemeinsamer einheitlicher onkologischer Basisdatensatz. [Online, zitiert am 2019-10-01]; Verfügbar unter https://www.tumorzentren.de/onkol-basisdatensatz.html

1.2 Register zur Qualitätssicherung

Mit Hilfe eines klinischen Registers werden patientenbezogene medizinische Daten in einem vordefinierten Arbeitsbereich gesammelt und können hinsichtlich der Qualitätssicherung der medizinischen Versorgung der Bevölkerung ausgewertet und so die Versorgungsqualität beurteilt werden, in der Regel sogar vergleichend, so dass einzelne Versorgungseinrichtungen individuelle Bewertungen erhalten, welche die eigene Versorgungsqualität im Vergleich zu allen am Register teilnehmenden Versorgungseinrichtungen abbildet.

Insbesondere kann ein gutes klinisches Register Fragen hinsichtlich der Sicherheit der Patientenbehandlung, der Wirksamkeit therapeutischer Maßnahmen und nicht zuletzt auch zur Kosteneffektivität der medizinischen Versorgung adressieren. Ebenfalls ist es möglich, neue Behandlungsmethoden mit bereits etablierten Verfahren zu vergleichen und so Vor- und Nachteile, d. h. die Nützlichkeit wie auch Nebenwirkungen dieser neuen Behandlungsmethoden, unter Realbedingungen zu evaluieren.

2 Datenschutz: Europarecht vs. Landesrecht

Entsprechend Art. 288 Abs. 2 AEUV[3] besitzt unmittelbar anwendbares Unionsrecht Vorrang gegenüber nationalem Recht, dies gilt sowohl gegenüber einfachgesetzlichem innerstaatlichen Recht als auch gegenüber dem Verfassungsrecht. Nur wenn ein nationaler Verfassungsgrundsatz wie beispielsweise der in den Artt. 1-20 GG beschriebene Kern der deutschen Verfassung von einer europäischen Regelung verletzt wird, können nationale Gerichte davon abweichen[4].

Unmittelbar anwendbares Unionsrecht ist immer dann gegeben, wenn es keines Transformationsakts eines Mitgliedstaats bedarf. EU-Verordnungen sind verbindliche Rechtsakte, welche unmittelbar gelten und in allen ihren Teilen verbindlich sind. EU-Richtlinien sind europäische Rechtsakte, in denen ein zu erreichendes Ziel festgelegt wird. EU-Richtlinien müssen von den Mitgliedsstaaten in eigene Rechtsvorschriften umgesetzt werden und daher werden EU-Richtlinien nicht zu detailliert formuliert; den Mitgliedstaaten soll bei der Umsetzung ein ausreichender Ermessensspielraum bleiben. EU-Richtlinien sind somit auch nicht unmittelbar anwendbare europäische Rechtsakte.

EU-Rechtsakte sind abgeleitetes Recht[5] und müssen dem gemeinsamen Leitfaden[6] genügen. Bezüglich der Erwägungsgründe findet sich im zitierten gemeinsamen Leitfaden des Europäischen Parlaments, des Rates und der Kommission:

- Leitlinie 10.1: „Die ‘Erwägungsgründe’ sind jener Teil des Rechtsakts, der die Begründung enthält und zwischen den Bezugsvermerken und dem verfügenden Teil des Rechtsakts steht. […] Die Erwägungsgründe werden im Gegensatz zum verfügenden Teil so formuliert, dass ihre Unverbindlichkeit deutlich wird.“

[3] Konsolidierte Fassung des Vertrags über die Arbeitsweise der Europäischen Union. [Online, zitiert am 2019-11-11]; Verfügbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A12012E%2FTXT

[4] EuGH, Urt. V. 05.12.2017 Az. C-42/17. [Online, zitiert am 2019-11-11]; Verfügbar unter https://dejure.org/2017,46354

[5] Abgeleitetes Recht. [Online, zitiert am 2019-11-11]; Verfügbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=LEGISSUM%3Aai0032

[6] Gemeinsamer Leitfaden des Europäischen Parlaments, des Rates und der Kommission für Personen, die an der Abfassung von Rechtstexten der Europäischen Union mitwirken. [Online, zitiert am 2019-11-11]; Verfügbar unter https://publications.europa.eu/de/publication-detail/-/publication/3879747d-7a3c-411b-a3a0-55c14e2ba732/language-de

- Leitlinie 10.5: „Die Erwägungsgründe müssen in möglichst knapper Form die Gründe für die wesentlichen Vorschriften des verfügenden Teils des Rechtsakts angeben."
- Leitlinie 10.5.2: „Erwägungsgründe, mit denen ohne Angabe der Gründe lediglich festgestellt wird, dass es geboten sei, bestimmte Vorschriften zu erlassen, dürfen nicht aufgenommen werden."

Erwägungsgründe begründen Rechtsvorschriften und haben keinerlei Gesetzescharakter. Erwägungsgründe können insbesondere die in den Richtlinien und Verordnungen enthaltenen Regelungen nicht ändern. Erwägungsgründe dienen der Erläuterung, was der europäische Gesetzgeber mit den zu den Erwägungsgründen gehörenden Regelungen erreichen wollte und stellen somit die wichtigste Quelle zur Interpretation europäischer Rechtsakte dar; die teleologische Auslegung durch Berücksichtigung der Erwägungsgründe genießt Vorrang in der europäischen Rechtsprechung und insbesondere beim EuGH.

Erwägungsgründe können aber nie den Regelungsinhalt ändern, welcher sich aus dem Wortlaut ergibt; der Interpretationsspielraum endet bei dem Wortlaut eines Gesetzes: Bietet der Wortlaut keinen Interpretationsspielraum, können Erwägungsgründe dem Wortlaut der Regelung keinen anderen Sinn zuweisen.

Seit 25.05.2018 wirkt europaweit die europäische Datenschutzgrundverordnung (DS-GVO)[7] unmittelbar und gilt für jede Verarbeitung von personenbezogenen Daten von Personen, die sich in der EU aufhalten, sowie auf Verarbeitungen selbst, welche in der EU erfolgen (Art. 3 DS-GVO: sog. „Marktortprinzip"). Somit stellt insbesondere die DS-GVO unmittelbar anwendbares Unionsrecht dar und ist bezüglich der Rechtswirkung gegenüber nationalem deutschen Recht vorrangiges Recht: die Regelungen der europäischen Datenschutz-Grundverordnung sind Art. 288 Abs. 2 AEUV gegenüber deutschem Datenschutzrecht höherrangiges Recht.

Jedoch enthält die DS-GVO diverse Öffnungsklausen, die dem jeweiligen nationalen Gesetzgeber die „Anpassung" der DS-GVO erlauben. Hinweise für Öffnungsklauseln finden sich in der DS-GVO, wenn beispielsweis „…dem Recht eines Mitgliedstaats…" oder „…den Vorschriften nationaler zuständiger Stellen…" im Text zu finden ist. Bei der Nutzung der Öffnungsklauseln gilt:

- Ein nationaler Gesetzgeber darf nur im Rahmen der Vorgaben der DS-GVO Regelungen treffen.
- Insbesondere kann ein nationaler Gesetzgeber nicht die Regeln der DS-GVO außer Kraft setzen, wenn keine Öffnungsklausel dafür vorgesehen ist.

Beispiele für Öffnungsklauseln sind:

- Definition „Verantwortlicher" (Art. 4 Abs. 7)
- Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten (Art. 9 Abs. 4)
- Bestellung eines Datenschutzbeauftragten (Art. 37 Abs. 4)

Weiterhin enthält die DS-GVO Vorgaben, dass nationale Regelungen der EU Kommission gemeldet werden müssen (sog. „Notifizierungspflicht"). In der DS-GVO werden diese Regelungen i. d. R. mit „teilen der Kommission" bzw. „teilt der Kommission" dargestellt. Notifizierungspflichten bestehen beispielsweise in:

[7] 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). Online zitiert am 2019-11-12; verfügbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=DE.

- Art. 49 Abs. 5: Bestimmungen, die Beschränkungen der Übermittlung bestimmter Kategorien von personenbezogenen Daten an Drittländer oder internationale Organisationen darstellen
- Art. 51 Abs. 4: Aufsichtsbehörde, die im Datenschutzausschuss mitwirkt
- Art. 83 Abs. 9: Rechtsbehelfe statt Geldbußen bei Verstößen gegen die DS-GVO
- Art. 84 Abs. 2: Festgelegte Sanktionen gegen Verstöße gegen die DS-GVO
- Art. 85 Abs. 3: Abweichungen von den Vorgaben der DS-GVO bzgl. Verarbeitungen, die zu journalistischen Zwecken oder zu wissenschaftlichen, künstlerischen oder literarischen Zwecken erfolgen
- Art. 88 Abs. 3: Rechtsvorschriften bzgl. Beschäftigtendatenschutz
- Art. 90 Abs. 2: Regelungen bzgl. Umgang mit Daten, die einem Berufsgeheimnis unterliegen

Deutschland meldete im Oktober 2018 verschiedene Gesetze[8]. Die Bundesregierung beabsichtigt im Rahmen einer jährlichen Abfrage (jeweiliger Stichtag: 1. Juli) eine jährliche Notifizierungsmeldung abzugeben[9].

Die Frage bzgl. der vorrangigen Anwendbarkeit der DS-GVO ist daher nicht ganz so einfach, wie man es auf Grund von Art. 288 Abs. 2 AEUV meinen könnte. Natürlich ist die DS-GVO vorrangiges Recht, aber auf Grund der Vielzahl der Öffnungsklauseln sowie der Delegation verschiedener Regelungen an den nationalen Gesetzgeber muss ein sehr genauer Blick auf die jeweilige Regelung geworfen werden um zu ersehen, ob nationales oder europäisches Recht anzuwenden ist. Bei den Erlaubnistatbeständen zur Verarbeitung von Gesundheitsdaten wie auch genetischen Daten bietet Art. 9 Abs. 4 DS-GVO den nationalen Gesetzgebern beispielsweise viel Gestaltungsspielraum, bei der Sicherheit der Verarbeitung hingegen so gut wie keinen Spielraum. Somit kann nur eine fachkundige Beurteilung bei der Beantwortung der Frage „DS-GVO vs. deutsches Recht“ weiterhelfen.

3 Grundsätze für die Verarbeitung personenbezogener Daten

Art. 5 Abs. 1 DS-GVO beinhaltet Grundsätze, die bei jeder Verarbeitung personenbezogener Daten immer gewährleistet sein müssen, also auch von jedem klinischen Register. Diese Grundsätze beinhalten:

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz (Art. 5 Abs. 1 lit. a DS-GVO):
  Personenbezogene Daten dürfen ausschließlich auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden. Dies beinhaltet:
  1. Die Verarbeitung muss einem legitimen Zweck dienen und ein Erlaubnistatbestand zur Verarbeitung der Daten liegt vor. Desgleichen müssen im Falle der Verarbeitung der personenbezogenen Daten in einem Drittstaat die Vorgaben von Kapitel V DS-GVO erfüllt sein. Werden Auftragsverarbeiter eingesetzt, sind die Vorgaben zur Auftragsverarbeitung einzuhalten, bei Zusammenarbeit mit Partnern muss ggf. ein Vertrag zur gemeinsamen Verarbeitung abgeschlossen werden.

[8] Anlage zu Bundestagsdrucksache 19/5155 vom 19.10.2018. [Online, zitiert am 2019-11-01]; Verfügbar unter http://dipbt.bundestag.de/dip21/btd/19/051/1905155.pdf

[9] Antwort des Parlamentarischen Staatssekretärs Dr. Günter Krings vom 10. Oktober 2018, S. 16. [Online, zitiert am 2019-11-01]; Verfügbar unter http://dipbt.bundestag.de/dip21/btd/19/051/1905155.pdf

2. Was genau der Verordnungsgeber unter der Regelung einer „Verarbeitung nach Treu und Glauben“ versteht, wird an keiner Stelle in der DS-GVO präzisiert. Jedoch findet sich in ErwGr. 38 RL 95/46[10] hierzu Folgendes:

   > „Datenverarbeitung nach Treu und Glauben setzt voraus, dass die betroffenen Personen in der Lage sind, das Vorhandensein einer Verarbeitung zu erfahren und ordnungsgemäß und umfassend über die Bedingungen der Erhebung informiert zu werden, wenn Daten bei ihnen erhoben werden.“

   D. h. die Verarbeitung muss „fair“ erfolgen.
3. Die Verarbeitung der Daten muss für die betroffenen Personen transparent erfolgen. Dies erfordert insbesondere die Gewährleistung der in Kapitel II DS-GVO dargestellten Betroffenenrechte.

- Zweckbindung (Art. 5 Abs. 1 lit. b DS-GVO):
  Die Verarbeitung personenbezogener Daten darf nur im Rahmen von festgelegten, eindeutigen und legitimen Zwecken erfolgen. Somit scheidet insbesondere eine Verarbeitung für noch unbekannte Zwecke aus, eine „Vorratsdatenspeicherung“ ist nicht mit den Vorgaben der DS-GVO vereinbar.
  Eine Änderung des Zweckes bedarf wiederum eines eigenen Erlaubnistatbestandes. Dabei gilt eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke nicht als unvereinbar mit dem ursprünglichen Zweck, was ggf. für andere Zweckänderungen nachgewiesen werden muss.
- Datenminimierung (Art. 5 Abs. 1 lit. c DS-GVO):
  Die Verarbeitung personenbezogener Daten muss für den verfolgten Zweck *erforderlich* und *angemessen* sein. Erforderlich ist die Verarbeitung personenbezogener Daten nur dann, wenn ohne diese Datenverarbeitung der verfolgte Zweck nicht erreicht werden kann. D. h. die Daten sind für die Erreichung der verfolgten Zwecke unverzichtbar.
  Angemessenheit liegt vor, wenn es zu der Verarbeitung kein „milderes“ Mittel gibt, welches weniger in die Rechte und Freiheiten natürlicher Personen eingreift.
  Datenminimierung beinhaltet daher keine Beschränkung der absoluten Datenmenge, es kann durchaus die Verarbeitung einer sehr große Menge personenbezogener Daten erforderlich und angemessen sein.
- Richtigkeit (Art. 5 Abs. 1 lit. d DS-GVO):
  Die Daten müssen für die Dauer der Verarbeitung, die von der Erhebung der Daten bis zu deren Löschung andauert („Lebenszyklus“ der Daten), sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein.
  Es müssen alle „angemessenen“ Maßnahmen getroffen werden, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden.
  Während eine Berichtigung falscher Daten immer erfolgen muss, ist eine Aktualisierung der Daten nur erforderlich, wenn die Aktualisierung für die Verarbeitung der Daten erforderlich ist. Wenn ein Patient vor zwei Jahren in Behandlung war und dieser Patient heute nach zwei

[10] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr. [Online, zitiert am 2019-11-01]; Verfügbar unter https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A31995L0046

Jahren umzieht, so liegt kein falsches Datum vor, denn zum Zeitpunkt der Behandlung stimmte die Adresse. Daher ist eine Korrektur nicht erforderlich. Kommt dieser Patient jedoch zur erneuten Behandlung ins Krankenhaus, so muss die neue Adresse erfasst werden.

- Speicherbegrenzung (Art. 5 Abs. 1 lit. e DS-GVO):
  Personenbezogene Daten dürfen nur so lange in einer die Identifizierung der betroffenen Personen erlaubenden Form gespeichert werden, wie es für die erfolgten Zwecke erforderlich ist.
  Dabei erlauben auch pseudonymisierte Daten die Identifizierung einer Person. Art. 5 Abs. 1 lit. e DS-GVO verlangt also, dass personenbezogene Daten schnellstmöglich gelöscht oder anonymisiert werden. D. h. entweder direkt nach Zweckerreichung oder nach Ablauf der gesetzlichen Aufbewahrungspflichten, wenn diese für die Verarbeitung bestehen, muss die Anonymisierung oder Löschung erfolgen.
  Erfolgt die Verarbeitung ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke, so dürfen diese Daten länger gespeichert werden, wenn geeignete technische und organisatorische Maßnahmen zum Schutz der Rechte und Freiheiten der betroffenen Personen durchgeführt werden. Dies beinhaltet insbesondere, dass das Verarbeitungsverfahren gemäß den Vorgaben von Art. 25 DS-GVO (s. Kap. 6.1.1.1) entwickelt und durchgeführt wird.
- Integrität und Vertraulichkeit (Art. 5 Abs. 1 lit. f DS-GVO):
  Bei jeder Verarbeitung muss die Integrität der Daten sowie der Schutz vor unbefugter Kenntnisnahme und Verarbeitung gewährleistet werden. Dies wird insbesondere durch die Umsetzung der Anforderungen von Art. 32 DS-GVO („Sicherheit personenbezogener Daten“) gewährleistet.

Art. 5 Abs. 2 DS-GVO verlangt, dass die Einhaltung dieser Grundsätze nachgewiesen werden muss. D. h. bei jeder Verarbeitung besteht eine Rechenschaftspflicht, welche letztlich die Erfüllung aller Anforderungen der DS-GVO umfasst.

4 Erlaubnistatbestand zur Speicherung von Patientendaten in einem Register

4.1 Gesetzlich geregelte Register

Registergesetze beinhalten Regelungen sowohl bzgl. der Aufgaben als auch Angaben bzgl. der zu verarbeitenden Daten wie auch der Erlaubnistatbestände. Dabei können Registergesetze sowohl eigene Erlaubnistatbestände enthalten als auch Regelungen bzgl. Einwilligung bzw. Widerspruchsrecht beinhalten. So enthält beispielsweise

- die sächsische Regelung zum Krebsregister eine Pflicht zur Meldung an das Krebsregister, wobei ein Widerspruch des Patienten nicht vorgesehen ist,
- die Regelung in Bremen zwar auch eine Meldepflicht, sieht aber eine Möglichkeit zum Widerspruch inklusive Löschung der Daten vor,
- die landesrechtliche Regelung in Nordrhein-Westfalen wiederum sieht lediglich einen Widerspruch gegenüber der Speicherung des identifizierenden Chiffrats vor, nicht aber bzgl. der eigentlichen Datenverarbeitung.

I. d. R. sind bei gesetzlich geregelten Registern zudem die Vorgaben bzgl. Datenverarbeitung abschließend geregelt. D. h. diese Register dürfen ausschließlich die im Gesetz angegebenen Daten verarbeiten und keine zusätzlichen Daten verarbeiten. Insbesondere in den Sozialgesetzbüchern gesetzlich normierte Vorgaben sind abschließend und können nicht erweitert werden.

D. h. es muss bei den gesetzlich geregelten Registern genau auf die Inhalte der Regelungen geachtet werden.

4.2 Nicht-gesetzlich geregelte Register

Bei nicht-gesetzlich geregelten Registern wird der Zweck allein von dem bzw. den Verantwortlichen entschieden. Die Daten, die verarbeitet werden dürfen, richten sich dann wiederum nach dem Zweck: entsprechend den Vorgaben der DS-GVO dürfen allein die Daten verarbeitet werden, die zur Erreichung des Zweckes des Registers erforderlich sind; der Nachweis bzgl. der Notwendigkeit der Daten zur Zweckerreichung liegt beim Register, entsprechend Art. 5 DS-GVO muss eine entsprechende Dokumentation vorhanden sein.

Der Erlaubnistatbestand bei nicht-gesetzlichen Registern ist regelhaft die Einwilligung der betroffenen Person, d. h. des Patienten. Da Register i. d. R. mit pseudonymen Daten arbeiten, haben die Register keinen eigenen Kontakt zum Patienten. Daher sind klinische Register i. d. R. darauf angewiesen, dass die Einwilligungen durch die versorgenden Einrichtungen eingeholt werden. Da eine Verarbeitung der Daten durch das klinische Register ohne Vorliegen einer rechtsgültigen Einwilligung nicht erlaubt ist, andererseits die Speicherung der Einwilligungen durch das Register selbst letztlich die De-Pseudonymisierung bedeuten könnte, ist die beste Lösung eine vertragliche Vereinbarung mit den datenliefernden versorgenden Einrichtungen, dass diese nur Daten meldet, bei denen eine Einwilligung vorliegt, und dass die Einrichtung die Einwilligung für die Dauer der Verarbeitung der Daten für das Register aufbewahrt.

4.3 Nationale Erlaubnistatbestände zur Forschung

Art. 9 Abs. 2 lit. j DS-GVO enthält einen auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats beruhenden Erlaubnistatbestand zur Verarbeitung von Gesundheitsdaten sowie genetischen Daten zu Forschungszwecken. Dabei müssen deutsche Gesetze, welche die Nutzung von Gesundheitsdaten sowie genetischen Daten zu Forschungszwecken erlauben, die Vorgaben der DS-GVO berücksichtigen, d.h. die deutschen Gesetze müssen

- in angemessenem Verhältnis zu dem verfolgten (Forschungs-) Ziel stehen,
- den Wesensgehalt des Rechts auf Datenschutz wahren und
- angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsehen.

D.h., der deutsche Bundes- und Landesgesetzgeber ist nicht völlig frei in der Gestaltung der gesetzlichen Rahmenbedingungen hinsichtlich bzgl. der Forschung mit Gesundheitsdaten oder genetischen Daten.

Die meisten Landesgesetze enthalten Regelungen zur Nutzung von im Krankenhaus angefallenen Patientendaten zu Forschungszwecken:

- Baden-Württemberg: § 46 Abs. 1 Ziff. 2a LKHG
- Bayern: Art. 27 Abs. 4 BayKrG
- Berlin: § 25 LKG
- Brandenburg: § 31 BbgKHEG

- Bremen: § 7 BremKHDSG
- Hamburg: § 12 HmbKHG
- Hessen: § 12 Abs. 3 HKHG 2011 i.V.m. § 24 HDSIG
- Mecklenburg-Vorpommern: § 37 LKHG M-V
- Nordrhein-Westfalen: § 6 GDSG NW
- Rheinland-Pfalz: § 37 LKG
- Saarland: § 14 SKHG
- Sachsen: § 34 SächsKHG
- Sachsen-Anhalt: § 17 KHG LSA
- Thüringen: § 27 Abs. 4 ThürKHG, § 27a ThürKHG

Außer in Niedersachsen und Schleswig-Holstein[11] existieren somit in jedem Land spezialgesetzliche Regelungen zur Nutzung von Patientendaten zu Forschungszwecken. I. d. R. legitimieren die Regelungen aber nur „Eigenforschung", d. h. man darf nur die Daten von Patienten, an deren Behandlung die Institution beteiligt war, zu Forschungszwecken der eigenen Institution nutzen, aber nicht weitergeben zu Forschungszwecken anderer. Was als „Institution" anzusehen ist, unterscheidet sich dabei von Bundesland zu Bundesland: in einem Bundesland ist darunter das Krankenhaus zu verstehen, im anderen Bundesland hingegen nur die jeweilige versorgende Fachabteilung des Krankenhauses. Somit müssen die Regelungen im jeweiligen Bundesland bzgl. der Nutzung von Patientendaten zu Forschungszwecken geprüft werden.

Geprüft werden muss auch, ob die jeweiligen bundes- oder landesgesetzlichen Regelungen den Anforderungen von Art. 9 Abs. 2 lit. j DS-GVO genügt, d. h. die landesspezifische Regelung „in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht". Denn bisher wurden die landesspezifischen Regelungen bzgl. des Gesundheitsdatenschutzes nur in acht Bundesländern an die DS-GVO angepasst: Brandenburg, Hamburg, Hessen, Mecklenburg-Vorpommern, Rheinland-Pfalz, Saarland, Sachsen-Anhalt und Thüringen. D. h., man kann nicht grundsätzlich davon ausgehen, dass die landesspezifischen Regelungen den Anforderungen der DS-GVO genügen.

4.3.1 Interessenabwägung bei Forschung

Obwohl Art. 9 DS-GVO keine Interessensabwägung bei der Verarbeitung besonderer Kategorien personenbezogener Daten wie Gesundheitsdaten oder genetischen Daten vorsieht, beinhalten einige deutsche Regelungen zur Nutzung dieser Daten zu Forschungszwecken eine Interessensabwägung, wie bspw. § 27 BDSG. Ein Nachweis des „überwiegenden Interesses" des Forschers ist nicht immer leicht zu führen und kann auch nicht allgemeingültig abgebildet werden. Im Nachfolgenden werden daher nur Hinweise gegeben, wie eine Darstellung des überwiegenden Interesses erfolgen könnte.

Kann ein Nachweis erbracht werden, dass ein starkes öffentliches Interesse an den Ergebnissen der Forschung vorliegt, so kann dies ein starkes Indiz sein, dass ein überwiegendes Interesse der Allgemeinheit an der Verarbeitung gegenüber dem Interesse der Einzelperson an der Nicht-

[11] Am 08. Oktober 2019 erfolgte die Unterrichtung des Schleswig-Holsteinischen Landtags bezüglich des Entwurfs eines Landeskrankenhausgesetzes (LKHG). Der Entwurf sieht in Teil 7 (§§ 35 bis 40) auch datenschutzrechtliche Regelungen vor, § 38 betrifft die Datenverarbeitung im Rahmen von Forschungsvorhaben; Forschung mit Patientendaten ist gemäß § 38 Abs. 1 LKHG-Entwurf nur mit Einwilligung erlaubt. [Online, zitiert am 2019-11-21]; Verfügbar unter http://www.landtag.ltsh.de/infothek/wahl19/unterrichtungen/00100/unterrichtung-19-00184.pdf

Verarbeitung vorliegt. Analog zu Abschnitt 86 Richtlinien für das Strafverfahren und das Bußgeldverfahren (RiStBV) liegt ein öffentliches Interesse dann vor, wenn

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

Die zentralen Fragen, die beantwortet werden müssen, lauten also:

- Interessiert das Vorhaben die Allgemeinheit?
- Nützt das Ergebnis des Vorhabens der Allgemeinheit?

Im Allgemeinen kann postuliert werden, dass ein entsprechendes öffentliches Interesse immer Vorrang vor dem Individualinteresse hat. Jedoch ist immer eine Abwägung erforderlich. Überwiegendes Forschungsinteresse kann insbesondere nur dann als gegeben angenommen werden, wenn

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

Hinweise für ein öffentliches Interesse an der Durchführung des Forschungsvorhabens können insbesondere sein:

- Eine hohe Zahl erkrankter Patienten, welche von dem Forschungsergebnis profitieren. Hier bieten beispielsweise die Informationen des statistischen Bundesamtes eine gute Grundlage für die Argumentation.
- Eine Reduzierung der Kosten für die Allgemeinheit, z. B. weil durch das Forschungsergebnis die Behandlungskosten der untersuchten Erkrankung deutlich reduziert werden und die Allgemeinheit dementsprechend weniger Steuergeld in die erforderliche Behandlung dieser Erkrankung investieren muss.
- Die Bedeutung des Forschungsergebnisses für die nähere Umgebung der Patienten, wie beispielsweise dem Ehepartner. Erkrankungen und deren Auswirkungen können auch für nahe Angehörige zu enormen psychischen Belastungen führen, welche ggf. professionell behandelt werden müssen und deren Behandlungskosten volkswirtschaftlich betrachtet werden sollten. Bei vererbbaren Erkrankungen gehören zum Umfeld beispielsweise auch Nachkommen hinzu, auch die Auswirkungen auf diese Personen sollten betrachtet werden. Weiterhin können auch Arbeitgeber involviert sein, wenn man an Ausfälle bei der Arbeit mit entsprechenden wirtschaftlichen Verlusten denkt. Bei einer Einzelperson ist dieser wirtschaftliche Verlust vermutlich überschaubar, aber über die Summe der Patienten kann hier ein für die Volkswirtschaft relevanter Anteil zustande kommen.
- Die Bedeutung des Forschungsergebnisses für die betroffenen Patienten selbst ist immer von Bedeutung. Je größer die Auswirkung des Forschungsergebnisses für die betroffenen Patienten selbst sind, wie beispielsweise eine Behandlung bisher nur schwer oder gar nicht behandelbarer Erkrankungen, desto geringer wird ihr Interesse an einer Nicht-Verarbeitung ihrer Daten anzunehmen sein.

Kann ein entsprechendes öffentliches Interesse dargestellt werden, so können technisch-organisatorische Maßnahmen, welche das Risiko für die betroffenen Patienten reduzieren, ebenfalls dazu führen, dass bei einer Interessabwägung davon ausgegangen werden kann, dass das Interesse

der betroffenen Person an einer Nicht-Verarbeitung geringer ist als wenn keine entsprechenden Maßnahmen ergriffen werden.

4.4 Nationale Erlaubnistatbestände zur Qualitätssicherung

Art. 9 Abs. 2 lit. i DS-GVO enthält einen Erlaubnistatbestand zur Verarbeitung von Gesundheitsdaten sowie genetischen Daten auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats zu Zwecken der Qualitätssicherung. Dabei müssen deutsche Gesetze, welche die Nutzung von Gesundheitsdaten sowie genetischen Daten zu Zwecken der Qualitätssicherung erlauben, „angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Personen“ beinhalten und insbesondere die Wahrung des Berufsgeheimnisses berücksichtigen. D.h., der deutsche Bundes- und Landesgesetzgeber ist nicht völlig frei in der Gestaltung der gesetzlichen Rahmenbedingungen hinsichtlich der Forschung mit Gesundheitsdaten oder genetischen Daten.

Die meisten Landesgesetze enthalten Regelungen zur Nutzung von im Krankenhaus angefallenen Patientendaten zu Zwecken der Qualitätssicherung:

- Baden-Württemberg: § 45 Abs. 3 Ziff. 1 LKHG:
  Patientendaten dürfen zur Qualitätssicherung in der stationären Versorgung gespeichert, verändert und genutzt, soweit diese Zwecke nicht mit anonymisierten Daten erreicht werden können und nicht überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen.
- Berlin: § 24 Abs. 5 Ziff. 7 LKG:
  Patientendaten dürfen an Stellen außerhalb des Krankenhauses übermittelt und offenbart werden, soweit dies zur Qualitätssicherung der Behandlung im Krankenhaus erforderlich ist, soweit der Zweck nicht mit anonymisierten oder pseudonymisierten Daten erreicht werden kann, die Übermittlung an eine Ärztin, einen Arzt oder eine ärztlich geleitete Stelle erfolgt und nicht überwiegende schutzwürdige Interessen der Patientin oder des Patienten entgegenstehen.
- Brandenburg: § 28 Abs. 2 Ziff. 1 BbgKHEG:
  Patientendaten dürfen mit Ausnahme der Offenlegung zur Qualitätssicherung der Behandlung durch das Krankenhaus verarbeitet werden, soweit diese Zwecke nicht mit anonymisierten Daten erreicht werden können und nicht überwiegende schutzwürdige Interessen der betroffenen Personen entgegenstehen. § 24 BbgDSG gilt entsprechend, soweit nicht besondere Rechtsvorschriften vorgehen.
- Bremen: § 2 Abs. 5 Ziff. 1 BremKHDSG:
  Patientendaten dürfen zur Qualitätssicherung in der stationären Versorgung gespeichert und genutzt werden, soweit diese Zwecke nicht mit pseudonymisierten oder anonymisierten Daten erreicht werden können und nicht überwiegende schutzwürdige Interessen des oder der Betroffenen entgegenstehen.
- Hamburg: § 10 Abs. Ziff. 7 HmbKHG:
  Im Krankenhaus dürfen Patientendaten für die Qualitätskontrolle der Leistungen des Krankenhauses verwendet werden, soweit dies erforderlich ist, dies mit anonymisierten Daten nicht möglich ist und im Einzelfall überwiegende Interessen der betroffenen Person der Verarbeitung nicht entgegenstehen.
- Hessen: § 12 Abs. 2 Ziff. 7 i.V.m. § 12 Abs. 3 HKHG 2011 und § 24 HDSIG
  § 12 Abs. 2 Ziff. 7 HKHG 2011: Die Übermittlung von Patientendaten an Personen oder Stellen außerhalb des Krankenhauses ohne die Einwilligung der oder des Betroffenen ist zulässig, soweit dies erforderlich ist zur Qualitätssicherung in der stationären Versorgung,

wenn der Empfänger eine Ärztin oder ein Arzt oder eine ärztlich geleitete Stelle ist und der genannte Zweck nicht mit anonymisierten oder pseudonymisierten Daten erreicht werden kann und nicht überwiegende schutzwürdige Interessen der Betroffenen entgegenstehen,
§ 12 Abs. 3 HKHG 2011: Abs. 2 und § 24 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes gelten in Krankenhäusern mit Behandlungseinrichtungen verschiedener Fachrichtungen auch zwischen diesen.

- Mecklenburg-Vorpommern: § 34 Abs. 1 Ziff. 2 LKHG M-V:
  Eine Verarbeitung personenbezogener Daten von Patientinnen und Patienten zu einem anderen als in § 33 Absatz 1 genannten Zweck ist nur zulässig, wenn dies zur Durchführung qualitätssichernder Maßnahmen erforderlich ist.
- Nordrhein-Westfalen: § 11 Abs. 2 GDSG NW:
  Für die Qualitätssicherung im Krankenhaus ist der Zugriff auf Patientendaten nur insoweit zulässig, als diese Zwecke nicht mit anonymisierten Daten erreicht werden können.
- Rheinland-Pfalz: § 36 Abs. 2 Ziff. 2 LKG:
  Patientendaten dürfen nur verarbeitet werden, soweit dies zur Durchführung qualitätssichernder Maßnahmen in der Krankenversorgung erforderlich ist und dieser Zweck nicht in vertretbarer Weise mit anonymisierten oder pseudonymisierten Daten erreicht werden kann.
- Saarland: § 13 Abs. 4 Ziff. 10 SKHG:
  Die Übermittlung von Patientendaten an Personen und Stellen außerhalb des Krankenhauses ist nur zulässig, wenn die Patientin oder der Patient eingewilligt hat oder eine Rechtsvorschrift die Übermittlung erlaubt oder soweit dies erforderlich ist zur Qualitätssicherung in der stationären Versorgung, wenn der Empfänger eine Ärztin oder ein Arzt oder eine ärztlich geleitete Stelle ist und der genannte Zweck nicht mit anonymisierten oder pseudonymisierten Daten erreicht werden kann und nicht überwiegende schutzwürdige Interessen der Betroffenen entgegenstehen.
- Sachsen: § 33 Abs. 3 Ziff. 4 SächsKHG:
  Eine Übermittlung von Patientendaten an Personen und Stellen außerhalb des Krankenhauses ist nur zulässig, soweit sie erforderlich ist zur Durchführung qualitätssichernder Maßnahmen in der Krankenversorgung, wenn das Interesse der Allgemeinheit an der Durchführung der beabsichtigten Maßnahme die schutzwürdigen Belange des Patienten erheblich überwiegt.
- Sachsen-Anhalt: § 16 Abs. 3 Ziff. 6 KHG LSA:
  Das Krankenhaus darf Patientendaten verarbeiten, soweit dies erforderlich ist zur Qualitätskontrolle der Leistungen des Krankenhauses und zur Durchführung qualitätssichernder Maßnahmen, soweit diese durch einen Arzt oder eine ärztlich geleitete Stelle durchgeführt werden und der Zweck nicht mit anonymisierten oder pseudonymisierten Daten erreicht werden kann.
- Thüringen: § 27 Abs. 6 Ziff. 4 ThürKHG
  Eine Übermittlung von Patientendaten an Empfänger außerhalb des Krankenhauses ist nur zulässig, soweit sie erforderlich ist zur Durchführung qualitätssichernder Maßnahmen in der Krankenversorgung, wenn bei der beabsichtigten Maßnahme das Interesse der Allgemeinheit an der Durchführung die schutzwürdigen Belange der Patienten erheblich überwiegt.

Zusammenfassend kann man bzgl. Qualitätssicherung folgende Anforderungen für die Übermittlung der Daten an ein klinisches Register zu Zwecken der Qualitätssicherung aufstellen, wenn keine spezielle gesetzliche Regelung wie beispielsweise ein Krebsregistergesetz existiert:

1) Es muss ein Nachweis erbracht werden, dass die Daten zum Erreichen der qualitätssichernden Zwecke erforderlich sind.
2) Es muss nachgewiesen werden, dass das Interesse der Allgemeinheit an der Durchführung der qualitätssichernden Maßnahmen die schutzwürdigen Belange der Patienten erheblich überwiegt
3) Die Daten müssen anonymisiert, falls nicht möglich pseudonymisiert an das Register übermittelt werden. Bei pseudonymer Übermittlung muss dargestellt werden, warum eine anonyme Verarbeitung nicht möglich ist.
4) Das klinische Register muss die qualitätssichernden Maßnahmen durch einen Arzt oder eine ärztlich geleitete Stelle durchführen lassen.
5) Ergänzend zu den Vorgaben der DS-GVO bzgl. Sicherheit der Verarbeitung (insbesondere Artt. 25, 35, 32 DS-GVO) sind nationale Vorgaben zur Sicherheit der Verarbeitung wie beispielsweise § 24 BbgDSG oder § 22 Abs. 2 BDSG zu berücksichtigen.

4.5 Einwilligung

Gemäß Art. 9 Abs. 2 lit. a ist eine Verarbeitung besonderer Kategorien personenbezogener Daten gestattet, wenn

a) die betroffene Person einwilligt und
b) Unionsrecht oder das Recht von Mitgliedstaaten die Verarbeitung nicht verbieten.

Für eine wirksame Einwilligung müssen die Vorgaben der DS-GVO eingehalten werden. Näheres zur rechtskonformen Einwilligung findet sich z. B. in der Ausarbeitung „EU DS-GVO: Anforderungen an eine Einwilligung“ der GMDS[12].

5 Rechte der betroffenen Patienten

Die Betroffenenrechte sind datenschutzrechtlich im Kapitel III der DS-GVO (Artt. 12 - 22) festgelegt. Im Überblick handelt es sich um folgende Rechte des Betroffenen bzw. Pflichten gegenüber dem Betroffenen:

- Informationspflicht bei Erhebung bzw. Zweckänderung von personenbezogenen Daten, unterschieden nach:
  - Erhebung bei der betroffenen Person
  - Erhebung nicht bei der betroffenen Person („Dritterhebung“)
- Auskunftsrecht der betroffenen Person
- Recht auf Berichtigung
- Recht auf Löschung
- Recht auf Einschränkung der Verarbeitung
- Mitteilungspflicht bei Berichtigung, Löschung oder Einschränkung
- Recht auf Datenübertragbarkeit
- Widerspruchsrecht
- Beschränkung der Zulässigkeit automatisierter Entscheidungen im Einzelfall.

[12] GMDS (2016): EU DS-GVO: Anforderungen an eine Einwilligung. [Online, zitiert am 2019-10-01]; Verfügbar unter https://www.gesundheitsdatenschutz.org/(Download als pdf-Datei)

Entsprechend Art. 12 Abs. 1 muss der Verantwortliche, also auch jedes Register, geeignete Maßnahmen treffen, um diesen Pflichten nachzukommen. D.h., es muss von Anfang an ein Prozess etabliert sein, der sicherstellt, dass jeder Betroffene seine Rechte wahrnehmen kann und das Register ohne schuldhaftes Verzögern den Verpflichtungen nachkommt.

Kann ein Verantwortlicher nachweisen, dass er eine Person nicht identifizieren kann, darf ein Verantwortlicher sich weigern, den Betroffenenrechten nachzukommen (Art. 12 Abs. 2 S. 2 i. V. m. Art. 11 Abs. 2 DS-GVO), ausgenommen die betroffene Person stellt zusätzliche Informationen zur Identifikation bereit. In Fällen, in denen der Verantwortliche, also das Register, die Identifikation nicht durchführen und dementsprechend die Betroffenenrechte nicht umsetzen kann, muss er dies den ihre Rechte ausübenden Personen mitteilen.

Existieren hingegen nur begründete Zweifel an der Identität der Person, so kann der Verantwortliche gemäß Art. 12 Abs. 6 DS-GVO zusätzliche Informationen anfordern, die zur Bestätigung der Identität der betroffenen Person erforderlich sind. Die Datenschutzkonferenz nennt hier als Beispiel für zusätzliche Informationen eine Postadresse bei elektronischem Auskunftsantrag[13].

Allerdings stellt sich die Frage, wann Zweifel an der Identität „begründet" sind. Existiert ein Nutzerkonto mit einer verifizierten E-Mail-Adresse z.B. in einem Patientenportal, liegt beim Verantwortlichen bereits eine Bestätigung der Mailadresse vor. Gleichermaßen muss man von der Richtigkeit der Mailadresse ausgehen, wenn zuvor per E-Mail mit der betroffenen Person kommuniziert wurde; wäre die Mailadresse nicht die der betroffenen Person gewesen, läge hier sonst vermutlich schon ein Verstoß gegen § 203 StGB vor. Begründete Zweifel können vorliegen, wenn dem Verantwortlichen weder E-Mail noch Postadresse vorliegen oder wenn die im Antrag zur Wahrnehmung der Betroffenenrechte angegebene Adresse nicht mit der bekannten übereinstimmt. Gerade in Bezug auf klinische Register kann man eher regelhaft von begründeten Zweifeln ausgehen, da Register i. d. R. mit pseudonymen Daten arbeiten, d.h. hier sollten Mechanismen vorgesehen werden, wie die Identität der ihre Betroffenenrechte wahrnehmenden Personen geklärt werden können[14].

Hinweis: Oftmals werden die Verantwortlichen der klinischen Register nur pseudonymisierte Daten erhalten. Jedoch gelten die Vorgaben der DS-GVO hinsichtlich der Betroffenenrechte auch für diese Daten. Da der Verantwortliche keinen Kontakt zu den betroffenen Personen hat, empfiehlt es sich, dass die Ärztinnen und Ärzte in den versorgenden Einrichtungen, in welchen die für die Registermeldung benötigten klinischen Daten erhoben werden, als ausführende Organe des bzw. der Verantwortlichen agieren. D. h., dass diese einerseits die Informationspflichten erfüllen, andererseits aber auch als Ansprechpartner der Patienten bzgl. der Wahrnehmung der Betroffenenrechte wie bspw. Auskunftsrecht oder Berichtigung der Daten fungieren.

5.1 Informationspflichten

Bei Aufnahme in ein klinisches Register muss den aus Artt. 13 und 14 DS-GVO resultierenden Informationspflichten genügt werden.

[13] Datenschutzkonferenz: Kurzpapier Nr. 6 - Auskunftsrecht der betroffenen Person, Art. 15 DS-GVO. [Online, zitiert am 2019-11-27]; Verfügbar unter https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_6.pdf

[14] Das LfDI BW gab bzgl. Auskunftsverfahren Hinweise zur Identitätsprüfung (Abschnitt 3 „Methoden der Identifizierung"). [Online, zitiert am 2019-11-27]; Verfügbar unter https://www.baden-wuerttemberg.datenschutz.de/identitaetspruefung-bei-elektronischen-auskunftsersuchen-nach-art-15-ds-gvo/

Idealerweise erhält jeder Patient bei Aufnahme in das Register ein Informationsschreiben, in welchem die notwendigen Angaben entsprechend Art. 13 resp. Art. 14 DS-GVO enthalten sind. In dieser Broschüre sollte sich dann auch ein Link auf die Internetseite des Registers befinden, in welcher die Angaben zu den Auftragsverarbeitern gelistet sind:

- Namen des Auftragsverarbeiters
- die Tätigkeit (z. B. Betreuung Krankenhausinformationssystem)
- wann das Vertragsverhältnis begann
- ggfs. wann das Vertragsverhältnis endete (offenes Enddatum = Vertragsverhältnis dauert an).

Grundsätzlich können die Angaben natürlich auch in dem Informationsschreiben enthalten sein. Aber um dem aus Art. 12 DS-GVO resultierenden Transparenzgedanken zu folgen, erscheint es angebracht, diese Informationen auszulagern. Letztlich ist es für den Patienten weniger von Interesse, ob die Verarbeitung der personenbezogenen Daten durch einen Auftragsverarbeiter oder den Verantwortlichen selbst erbracht wird; ein Einspruchsrecht haben die Patienten nicht. Und je nach Anzahl der Auftragsverarbeiter könnte der Gedanke aufkommen, dass andere Informationen durch diese Angaben eher „versteckt“ werden. Zuletzt gilt es zu bedenken, dass sich bei den eingesetzten Auftragsverarbeitern Änderungen ergeben können und ohne Nutzung des Internets die gesetzlich geforderte Information bzgl. der Empfängerliste sich als schwierig oder sogar als undurchführbar erweisen kann.

Die Informationen müssen dabei stets in einer klaren und einfachen Sprache vermittelt werden, wie es Art. 12 DS-GVO fordert.

5.2 Auskunftsrecht

Jeder Patient hat das Recht auf Auskunft bzgl. der über ihn in einem klinischen Register verarbeiteten bzw. gespeicherten Daten. Dies sollte ihm im Rahmen der im Abschnitt 5.1 genannten Information mitgeteilt werden. Idealerweise wird in dieser Information weiterhin eine Telefonnummer als auch eine spezielle nicht-personalisierte E-Mailadresse, die somit auch bei einem Wechsel des zuständigen Sachbearbeiters erhalten bleibt, genannt.

Nach Art. 15 Abs. 3 DS-GVO muss der Verantwortliche betroffenen Personen auch eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung stellen. Dementsprechend sollten klinische Register die Möglichkeit haben, alle zu einem Patienten gehörenden Daten in eine pdf-Datei zu exportieren, um diese Datei anfragenden betroffenen Patienten übergeben zu können.

5.3 Recht auf Berichtigung

Nach Art. 16 hat jeder Patient das Recht, dass unrichtige Daten berichtigt werden. Da Daten die Grundlage jeder medizinischen Behandlung und Forschung darstellen, liegt die Korrektur unrichtiger Daten selbstverständlich auch im ureigenen Interesse der datenverarbeitenden Stelle.

Allerdings hat nach Art. 16 DS-GVO jeder Patient auch das Recht, dass unvollständige Daten vervollständigt werden, ggf. auch mittels einer ergänzenden Erklärung. Hier kann es zu unterschiedlichen Interpretationen seitens des klinischen Registers und der betroffenen Person bzgl. der Interpretation von „unvollständig“ kommen. Der europäische Gesetzgeber verlangt daher, dass dieses Recht „unter Berücksichtigung der Zwecke der Verarbeitung“ zu erfolgen hat. D. h. die Beurteilung bzgl. Unvollständigkeit muss aus Sicht des Verarbeitungszweckes erfolgen. Entsprechend dem aus Art. 5 Abs. 1 lit. c DS-GVO resultierendem Gebot der Datenminimierung dürfen hier also nur

für den Verarbeitungszweck erforderliche Daten ergänzt werden. Dass diese Daten ergänzt werden, liegt aber wiederum im Interesse des klinischen Registers und wird daher jederzeit möglich sein.

Jeder Patient muss darauf hingewiesen werden, dass für ihn diese Rechte bestehen. Dies erfolgt idealerweise in dem in Abschnitt 5.1 erwähnten Informationsschreiben.

5.4 Recht auf Einschränkung der Verarbeitung („Sperrung“)

Gemäß Art. 18 DS-GVO hat jeder Patient das Recht, unter den Voraussetzungen von Art. 18 Abs. 1 DS-GVO von dem Verantwortlichen die Einschränkung der Verarbeitung (= „Sperrung“) zu verlangen. Durch das in Abschnitt 5.1 beschriebene Informationsschreiben sollte jeder Patient darauf hingewiesen werden, dass er ein Recht auf die Einschränkung der Verarbeitung seiner Daten hat. Zugleich sollte er darauf hingewiesen werden, dass dieses Recht ggf. durch gesetzliche Bestimmungen eingeschränkt wird.

Der Verantwortliche muss dabei beachten, dass gemäß Art. 18 Abs. 2 DS-GVO eine derartige Sperrung nur mit Einwilligung der betroffenen Person rückgängig gemacht werden darf. Ansonsten darf eine Verarbeitung, von einer Speicherung abgesehen, nur

- zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder
- zum Schutz der Rechte einer anderen natürlichen oder juristischen Person oder
- aus Gründen eines wichtigen öffentlichen Interesses der Union oder eines Mitgliedstaats

erfolgen. Weiterhin muss der Verantwortliche entsprechend den Vorgaben von Art. 18 Abs. 3 DS-GVO die betroffene Person, die eine Sperrung erwirkte, unterrichten, bevor die Einschränkung aufgehoben wird.

5.5 Recht auf Löschung

Nach Art. 17 DS-GVO hat jede betroffene Person das Recht, dass sie betreffende Daten gelöscht werden, wenn die Umstände aus Art. 17 Abs. 1 DS-GVO zutreffen und die Ausnahmetatbestände aus Art. 17 Abs. 3 DS-GVO nicht anzuwenden sind.

Durch das in Abschnitt 5.1 beschriebene Informationsschreiben sollte jeder Patient darauf hingewiesen werden, dass er ein Recht auf Löschung seiner Daten hat. Zugleich sollte er darauf hingewiesen werden, dass dieses Recht ggf. durch gesetzliche Bestimmungen wie z. B. durch die Vorgabe gesetzlicher Aufbewahrungsfristen eingeschränkt wird.

5.6 Widerspruchsrecht

Nach Art. 21 Abs. 6 DS-GVO hat jede betroffene Person das Recht, aus Gründen, „die sich aus ihrer besonderen Situation ergeben“, gegen eine Verarbeitung sie betreffender Daten zu wissenschaftlichen oder historischen Forschungszwecken zu widersprechen. Entsprechend Art. 21 Abs. 4 DS-GVO muss jede betroffene Person ausdrücklich auf dieses Recht hingewiesen werden.

Jeder Proband resp. Patient sollte daher in dem in Abschnitt 5.1 erwähnten Informationsschreiben auf sein Recht zum Widerspruch gegen eine Datenverarbeitung hingewiesen werden. Dabei ist zu berücksichtigen, dass der Proband bzw. Patient auch darauf hingewiesen wird, dass ein Widerspruchsrecht ggf. durch gesetzliche Regelungen eingeschränkt wird, z. B. eine Speicherung aufgrund gesetzlicher Bestimmungen trotz seines Widerspruchs erfolgen muss.

5.7 Recht auf Datenübertragbarkeit

Gemäß Art. 20 DS-GVO hat jeder Patient unter den Voraussetzungen von Art. 20 Abs. 1 lit. a, b DS-GVO das Recht, von ihm bereitgestellte Daten

- vom Verantwortlichen in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten

sowie

- sie einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, dem die personenbezogenen Daten bereitgestellt wurden, zu übermitteln bzw. sie übermitteln zu lassen.

Jeder Patient sollte in dem in Abschnitt 5.1 genannten Informationsschreiben auf diese Rechte hingewiesen werden. Es sollte dabei aber auch darauf hingewiesen werden, dass kein Empfänger dieser Daten gesetzlich dazu verpflichtet ist, diese Daten überhaupt oder in dem vom Verantwortlichen bereitgestellten Format anzunehmen.

6 Sicherheit der Verarbeitung

Die Überschrift von Art. 25 DS-GVO lautet „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“, im englischen findet sich „Data protection by design and by default“. In der Literatur zum Thema finden sich überwiegend die Begriffe „Privacy by Design“ bzw. „Privacy by Default“, weswegen diese Begrifflichkeiten auch hier im Text verwendet werden.

„Data Privacy“ und „Data Protection“ sind sehr eng miteinander verbunden, so dass die Begriffe oft synonym benutzt werden. Schaut man in die Literatur zu den Begrifflichkeiten, so finden sich jedoch Unterschiede bei der Zielrichtung. Der Begriff „Data Protection“ adressiert den Schutz von Daten vor unbefugtem Zugriff, bei „Data Privacy geht es hingegen um den autorisierten Zugriff, d.h. um die Festlegung von Fragestellungen wie „wer definiert, was ein autorisierter Zugriff ist“ oder „wer bestimmt, wer autorisiert auf Daten zugreifen darf“. Während „Data Protection“ im Wesentlichen technische Aspekte anspricht, geht es bei „Data Privacy“ überwiegend um rechtliche Fragestellungen.

„Datenschutz“ kann nur umgesetzt werden, wenn „Data Privacy“ durch „Data Protection“ ergänzt wird. In dem Konzept des „Privacy by Design“, das eng mit dem Konzept der „Privacy enhancing technologies[15]“ oder PET verbunden ist, wird daher ein integrativer Ansatz verstanden. Im Folgenden finden sich daher zu den Ausführungen bzgl. „Privacy by Design“ Hinweise zur Umsetzung von „Datenschutz“, d.h. auch Beschreibungen, die eher einen technischen Aspekt ansprechen.

6.1 Privacy by Design/Default

Grundlegendes zum Thema Privacy by Design/Default findet man in der Praxishilfe von bvitg, GDD und GMDS[16]. Während Privacy by Design schon auf die konzeptionelle Phase zielt, verlangt Privacy by Design, das zu Anfang immer eine datenschutzfreundliche Grundeinstellung existiert. Der

[15] Privacy-Enhancing Technologies: The Path to Anonymity. Verlag „Information and Privacy Commissioner/Ontario“ 1995. ISBN 978-9034632029. [Online, zitiert am 2019-12-10]; Verfügbar unter http://govdocs.ourontario.ca/node/14782 bzw. http://www.ontla.on.ca/library/repository/mon/10000/184530.pdf

[16] bvitg, GDD, GMDS: Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Art. 25 DS-GVO). [Online, zitiert am 2019-09-30]; Verfügbar unter https://ds-gvo.gesundheitsdatenschutz.org/html/privacy_design_default.php

europäische Datenschutzausschuss veröffentlichte im November 2019 Leitlinien zum Thema zur öffentlichen Kommentierung, d. h. der Text ist noch nicht final[17]. Dennoch empfiehlt es sich, den Text zu lesen, um die Sicht der europäischen Aufsichtsbehörden zum Thema kennenzulernen.

6.1.1.1 Privacy by Design: 7 grundlegende Prinzipien

Privacy by Design wird i. d. R. mit der Umsetzung der „7 grundlegenden Prinzipien", aufgestellt von der ehemaligen kanadischen Datenschutzbeauftragten Ann Cavoukian[18,19], gleichgesetzt:

1. Proaktiv, nicht reaktiv; als Vorbeugung und nicht als Abhilfe
2. Datenschutz als Standardeinstellung
3. Datenschutz ist in das Design eingebettet
4. Volle Funktionalität – eine Positivsumme, keine Nullsumme
5. Durchgängige Sicherheit. Schutz während des gesamten Lebenszyklus
6. Sichtbarkeit und Transparenz – Für Offenheit sorgen
7. Wahrung der Privatsphäre der Nutzer: Für nutzerzentrierte Gestaltung sorgen

1,2,4,5,6,7 ist immer (auch) projekt-/umsetzungsspezifisch. 3 und 5 hängen vom System ab: was bietet das IT-System, was stellt der Hersteller zur Verfügung.

6.1.1.2 Umsetzung von Privacy by Design

Die damalige kanadische Datenschutzbeauftragte Ann Cavoukian, die „Privacy by Design" ins Leben rief, empfahl 2011 Unternehmen[20]:

1) Ein Unternehmen muss einen Privacy by Design-Leiter und/oder ein Team einrichten, indem es die geeigneten Personen identifiziert.
2) Proaktive Prozesse und Praktiken zum Datenschutz durch Design einführen, umsetzen und einhalten:
    a) Anwendung auf das Design und die Architektur von Infrastruktur, IT-Systemen und Geschäftspraktiken, die mit personenbezogenen Daten interagieren oder deren Verwendung beinhalten;
    b) Beschreibung aller Kernzwecke und Hauptfunktionen, die von diesen Infrastrukturen, Systemen und Praktiken erfüllt werden, einschließlich, aber nicht beschränkt, auf die Gewährleistung der Sicherheit und den Schutz der Privatsphäre bei personenbezogenen Daten;
    c) Datenminimierung einbeziehen und den höchstmöglichen Grad an Datenschutz für personenbezogene Daten bieten, während diese gleichzeitig den anderen Kernzwecken dienen und die anderen Hauptfunktionen erfüllen;
    d) Bereitstellung dieses Grades an Datenschutz durch den Einsatz der maximal möglichen Mittel, die erforderlich sind, um die Sicherheit, Vertraulichkeit und Integrität personenbezogener Daten während des gesamten Lebenszyklus der Daten

[17] EDPB: Guidelines 4/2019 on Article 25 Data Protection by Design and by Default. [Online, zitiert am 2019-12-10]; Verfügbar unter https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_de

[18] Ann Cavoukian: Privacy by Design - The 7 Foundational Principles. [Online, zitiert am 2019-10-01]; Verfügbar unter https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf

[19] Ann Cavoukian: Privacy by Design: Strong Privacy Protection - Now, and Well into the Future. [Online, zitiert am 2019-10-01]; Verfügbar unter https://www.ipc.on.ca/wp-content/uploads/Resources/PbDReport.pdf

[20] Ann Cavoukian: Privacy by Design in Law, Policy and Practice - A White Paper for Regulators, Decision-makers and Policy-makers. (2011) [Online, zitiert am 2019-10-01]; Verfügbar unter http://www.ontla.on.ca/library/repository/mon/25008/312239.pdf

zu gewährleisten, von der ursprünglichen Erhebung über die Verwendung, Speicherung, Verbreitung bis zur sicheren Vernichtung am Ende des Lebenszyklus;

e) Wann immer dies angemessen ist, ist dieser Datenschutz automatisch vorzusehen, so dass keine Maßnahmen für einzelne Benutzer oder Kunden erforderlich sind, um die Privatsphäre ihrer personenbezogenen Daten zu schützen;

f) Sicherstellen, dass Infrastruktur, IT-Systeme und Geschäftspraktiken, die mit personenbezogenen Daten interagieren oder deren Verwendung beinhalten, angemessen transparent bleiben und einer unabhängigen Überprüfung durch alle relevanten Interessengruppen, einschließlich Aufsichtsbehörden, betroffener Personen, Nutzer und Kunden sowie Partnerorganisationen, unterliegen; und

g) Förderung der Gestaltung und Aufrechterhaltung benutzerzentrierter Systeme und Praktiken, einschließlich starker Datenschutzvorgaben, angemessener Datenschutzhinweise und anderer benutzerfreundlicher Funktionen.

Zur Unterstützung eines umfassenden Privacy by Design-Programms muss ein Unternehmen nach Ansicht von einigen internationalen Datenschutz-Aufsichtsbehörden:

(1) Angemessene Schulungen zum Thema Datenschutz und Sicherheit für seine Mitarbeiter durchführen;

(2) Ein System zur Überwachung aller Projekte, die regelmäßig personenbezogene Daten verarbeiten, einführen;

(3) Von den Projektleitern verlangen, dass sie für alle Projekte Dokumente zum Datenschutz entwerfen, pflegen, einreichen und aktualisieren, um sicherzustellen, dass Produkt-, Programm- oder Serviceteams die Auswirkungen ihrer Produkte, Programme und Dienstleistungen auf den Datenschutz von der ersten Stunde an bis zur endgültigen Einführung bewerten; und

(4) Ein internes Auditteam mit der Durchführung regelmäßiger Audits beauftragen, um die vollständige Umsetzung ausgewählter Dokumente zum Datenschutz und deren Überprüfung durch die zuständigen Manager zu verifizieren.

Eine Umsetzung von Privacy by Design könnte in Anlehnung an die von Ann Cavoukian aufgestellten Prinzipien z. B. beinhalten:

- Richtlinien/Policy zum Datenschutz festlegen, also beispielsweise:
  - Das Unternehmen sollte den Datenschutz im gesamten Unternehmen und in jeder Phase der Entwicklung seiner Produkte und Dienstleistungen fördern.
  - Der Schutz der Privatsphäre sollte zu Beginn des Planungsprozesses in die Geschäftspraktiken einbezogen werden.
  - Umfassende Datenschutzmanagementverfahren sollten während des gesamten Lebenszyklus von Produkten und Dienstleistungen aufrechterhalten werden.
- Verantwortlichkeiten definieren, z. B.
  - Datenverarbeitung im Büro, Home Office usw.
  - Geschäftsprozessverantwortliche
  - Produktentwickler
  - Technische Lösungsentwickler / Manager
  - Datenschutzbeauftragter
  - …
- Weiterbildung für die an der Verarbeitung beteiligten Personen anbieten/ermöglichen, was u.a. nachfolgende Punkte beinhalten sollte:

    - Integration von Datenschutzschulungen und Sensibilisierungsprogrammen
    - Rollen- und aufgabenspezifische Inhalte für alle Beteiligten
    - Interdisziplinäres Publikum beachten: Geschäftsprozessverantwortliche, Softwareentwickler, Projektmanager, Vertriebsmitarbeiter...
- Rahmenwerk für ein Datenschutzmanagement implementieren, welches u.a. beinhaltet
    - Festlegung der Verwaltungsstruktur und Beibehaltung während des Verarbeitungszeitraum
    - Erstellung und Pflege einer Bestandsaufnahme, welche personenbezogenen Daten verarbeitet werden und welche Datenübertragungsmechanismen erfolgen
    - Einhaltung interner Datenschutzrichtlinien und Überprüfung der Einhaltung entsprechend der festgelegten Vorgaben
    - Durchführung von Schulungen und Sensibilisierungsprogrammen mit den an der Verarbeitung beteiligten Personen
    - Management von Informationssicherheitsrisiken
    - Management der Risiken bei der Datenverarbeitung durch Dritte
    - Festlegung des Umgangs mit Hinweisen/Meldungen (z. B. Whistleblower)
    - Festlegung des Umgangs mit und der Reaktion auf Anfragen und Beschwerden von Personen und Überprüfung der Einhaltung dieser Vorgaben
    - Festlegung eines Monitorings für neue betriebliche Praktiken und Überprüfung der Umsetzung der Festlegung sowie der Durchführung des Monitorrings
    - Festlegung eines Verfahrens zur Verwaltung von Datenschutzverletzungen und Überprüfung der Einhaltung des Verfahrens
    - Monitoring der Datenverarbeitung
    - Verfolgung externe Kriterien (z. B. Gesetzesänderungen)
- Überprüfungen bzgl. Umsetzung der Policy, Wahrnehmung von Verantwortlichkeiten, Durchführung von Weiterbildungen usw.
- Und natürlich: Dokumentation.

Speziell für den Einsatz von Oracle®-Datenbanken wurde 2013 eine Empfehlung für den Umgang mit Privacy by Design veröffentlicht[21]; da diese Datenbank im Gesundheitswesen oft eingesetzt wird, ist diese Empfehlung vermutlich auch von Interesse. Und grundsätzlich sind die Empfehlungen auf den Einsatz von anderen Enterprise-Strukturen sehr gut übertragbar.

6.1.1.3 Privacy by Design: der Europäischen Agentur für Netz- und Informationssicherheit (ENISA)

Es gibt Empfehlungen der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) zum Thema[22]:

- Vier eher technische Empfehlungen:
    - Datenminimierung (Minimize): Beschränken Sie die Verarbeitung personenbezogener Daten so weit wie möglich.

[21] Ann Cavoukian, Mark Dixon: Privacy and Security by Design: An Enterprise Architecture Approach (2013) [Online, zitiert am 2019-10-01]; Verfügbar unter https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-privacy-and-security-by-design-oracle.pdf

[22] Europäischen Agentur für Netz-und Informationssicherheit (ENISA): Privacy and Data Protection by Design – from policy to engineering (2014) [Online, zitiert am 2019-10-01]; Verfügbar unter https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design

    - Datentrennung (Separate): Trennen Sie die Verarbeitung personenbezogener Daten so weit wie möglich, insbesondere von/nach unterschiedlichen Verarbeitungszwecken.
    - Pseudonymisierung (Abstract): Beschränken Sie so weit wie möglich die Details, in denen personenbezogene Daten verarbeitet werden.
    - Verbergen (Hide): Personenbezogene Daten schützen oder nicht verlinkbar oder nicht beobachtbar machen. Stellen Sie sicher, dass es nicht öffentlich oder bekannt wird.
- Vier eher organisatorische Anforderungen:
    - Informieren (Inform): Informieren Sie die betroffenen Personen rechtzeitig und angemessen über die Verarbeitung ihrer personenbezogenen Daten.
    - Kontrolle (Control): Geben Sie den betroffenen Personen eine angemessene Kontrolle über die Verarbeitung ihrer personenbezogenen Daten.
    - Durchsetzen (Enforce): Verpflichten Sie sich, personenbezogene Daten datenschutzgerecht zu verarbeiten und dies angemessen durchzusetzen.
    - Demonstrieren (Demonstrate): Zeigen Sie, dass Sie personenbezogene Daten datenschutzgerecht verarbeiten.

Die ENISA-Empfehlungen sind vielleicht „greifbarer“ als die 7 grundlegenden Prinzipien von Ann Cavoukian, adressieren aber letztlich identische Anforderungen.

6.2 Datenschutz-Folgenabschätzung

Eine Datenschutz-Folgenabschätzung (abgekürzt DSFA) soll in den Fällen, in denen eine Verarbeitung wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringt, helfen, die Risiken zu minimieren und durch Darstellung der Maßnahmen zur Reduzierung der Risiken auch für Dritte nachvollziehbar aufzeigen, wie Verantwortliche für die Datenverarbeitung mit diesen Risiken umgehen.

Dabei beschreibt Art. 35 DS-GVO verschiedene Fälle, in denen eine DSFA erfolgen muss. Weiterhin *dürfen* nationale Datenschutz-Aufsichtsbehörden Listen veröffentlichen, wann eine DSFA nicht erforderlich ist (sog. „Whitelist“), und sie *müssen* Listen veröffentlichen, wann eine DSFA erforderlich ist. Alle Listen müssen, sofern diese Verarbeitungstätigkeiten umfassen, welche mit dem Angebot von Waren oder Dienstleistungen in mehreren Mitgliedstaaten im Zusammenhang stehen, dem Kohärenzverfahren nach Art. 63 DS-GVO unterworfen werden, D. h. dem europäischen Datenschutz-Ausschuss vorgelegt werden. Die Entscheidung zur deutschen Liste findet sich auf der EDSA-Homepage[23], die Liste selbst ist auf der Homepage der Datenschutzkonferenz verfügbar[24].

Unabhängig davon steht es jedem Verantwortlichen selbstverständlich frei, auch in anderen Fällen eine DSFA durchzuführen, beispielsweise zur Darstellung der Einhaltung der Vorgaben der DS-GVO hinsichtlich der Sicherheit der Verarbeitung.

[23] EDPB: Opinion 5/2018 on the draft list of the competent supervisory authorities of Germany regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR). [Online, zitiert am 2019-09-30]; Verfügbar unter https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-52018-draft-list-competent-supervisory_en

[24] DSK: Anwendungshinweise - Liste von Verarbeitungsvorgängen nach Art. 35 Abs. 4 DS-GVO für den nicht-öffentlichen Bereich. [Online, zitiert am 2019-09-30]; Verfügbar unter https://www.datenschutzkonferenz-online.de/anwendungshinweise.html bzw. direkt pdf-Datei unter https://www.datenschutzkonferenz-online.de/media/ah/20181017_ah_DSK_DSFA_Muss-Liste_Version_1.1_Deutsch.pdf

Die Verbände bvitg, DKG und GMDS veröffentlichten eine Praxishilfe[25], in welcher der Umfang wie auch die Durchführung einer DSFA ausführlich beschrieben wird. Daher finden sich hier nur Hinweise, die speziell für klinische Register zu beachten sind.

Entsprechend der DSK-Liste ist eine DSFA insbesondere erforderlich (Nummerierung entspricht der Nummerierung in der DSK DSFA-Muss-Liste) bei:

2) Verarbeitung von genetischen Daten, wenn zugleich mindestens eines der nachfolgenden Kriterien erfüllt wird:
    a. Daten zu schutzbedürftigen Betroffenen wie Patienten,
    b. Innovative Nutzung oder Anwendung neuer technologischer organisatorischer Lösungen wie z. B. im Bereich der medizinischen Forschung,
    c. Bewerten oder Einstufen (Scoring),
    d. Abgleichen oder Zusammenführen von Datensätzen wie z. B. Zusammenführen von Datensätzen aus mehreren Versorgungseinrichtungen,
    e. Betroffene werden an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags gehindert, wie beispielsweise dem Recht auf Löschung, da die Daten aus Forschungsinteresse vorerst nicht gelöscht werden sollten.

    Auch in klinischen Registern werden mitunter genetische Daten gespeichert, so dass hier ggf. eine DSFA erforderlich sein kann.
10) Zusammenführung von personenbezogenen Daten aus verschiedenen Quellen und der Verarbeitung der so zusammengeführten Daten, sofern
    - die Zusammenführung oder Verarbeitung in großem Umfang vorgenommen werden,
    - für Zwecke erfolgen, für welche nicht alle der zu verarbeitenden Daten direkt bei den betroffenen Personen erhoben wurden,
    - die Anwendung von Algorithmen einschließen, die für die betroffenen Personen nicht nachvollziehbar sind, und
    - der Entdeckung vorher unbekannter Zusammenhänge zwischen den Daten für nicht im Vorhinein bestimmte Zwecke dienen

    Klinische Register führen i. d. R. Daten aus verschiedenen Versorgungseinrichtungen (= Quellen) zusammen, die Daten werden zudem i. d. R. nicht direkt beim Patienten erhoben, sondern bei den Versorgungseinrichtungen. Weiterhin werden Register häufig eingesetzt, um eine hinreichend große Datenmenge zu erhalten, mit der bisher unbekannte Mechanismen der Erkrankung entdeckt und somit neue oder verbesserte Behandlungsmethoden entdeckt werden können. Daher kann hier auch dieser Punkt zutreffen, insbesondere, wenn KI-Ansätze integriert werden.
15) Anonymisierung von personenbezogenen Daten besonderer Kategorien (Art. 9 Abs. 1 DS-GVO) nicht nur in Einzelfällen (in Bezug auf die Zahl der betroffenen Personen und die Angaben je betroffener Person) zum Zweck der Übermittlung an Dritte.
    Letztlich führt dies dazu, dass bei der Anonymisierung von aus der Versorgung stammenden Patientendaten zu Zwecken der Weitergabe der Daten an ein klinisches Register regelhaft eine DSFA erforderlich ist.

[25] Bvitg, DKG, GMDS: Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO. [Online, zitiert am 2019-09-30]; Verfügbar unter https://ds-gvo.gesundheitsdatenschutz.org/html/dsfa.php

6.3 IT-Sicherheit

Art. 1 Abs. 1 DS-GVO beschreibt, dass die DS-GVO insbesondere dem „Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten“ dient. Hierzu verfolgt die DS-GVO einen risiko-orientierten Ansatz: Art. 32 DS-GVO fordert nicht die Gewährleistung des höchstmöglichen Niveaus hinsichtlich der Sicherheit der Verarbeitung, sondern es muss ein *angemessenes* Schutzniveau sichergestellt werden.

Art. 32 DS-GVO schreibt vor, dass unter Berücksichtigung

- des Stands der Technik,
- der Implementierungskosten,
- der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie
- der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die persönlichen Rechte und Freiheiten

geeignete technische und organisatorische Maßnahmen getroffen werden müssen, um ein dem *Risiko angemessenes Schutzniveau* zu gewährleisten. Verantwortlich für die Gewährleistung ist nach Art. 32 DS-GVO sowohl der für die Verarbeitung Verantwortliche als auch – sofern vorhanden - der Auftragsverarbeiter. Letzterer natürlich nur für den Teil, den der Auftragsverarbeiter zu verantworten hat. Aus Art. 5 DS-GVO folgt eine Nachweispflicht, die aber indirekt auch von Art. 32 Abs. 3 DS-GVO verlangt wird.

Weiterhin verlangt die DS-GVO, dass dieser dem Risiko der Verarbeitung angemessene Schutz auf Dauer sicherzustellen ist. D. h. die

- Vertraulichkeit,
- Integrität,
- Verfügbarkeit und
- Belastbarkeit

für Systeme und Dienste im Zusammenhang mit der Verarbeitung der personenbezogenen Daten ist für den gesamten Lebenszeitraum zu gewährleisten.

Dabei müssen die Schutzmaßnahmen gegebenenfalls eine Pseudonymisierung und eine Verschlüsselung der personenbezogenen Daten beinhalten. Ferner muss ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen, welche die Sicherheit der Verarbeitung gewährleisten, existieren.

Eine ausführliche Darstellung der Thematik findet sich in der Praxishilfe[26] von bvitg und GMDS.

7 Datenschutzbeauftragter

7.1 Pflicht zur Benennung

Gemäß Art. 37 Abs. 1 lit. c DS-GVO muss ein Datenschutzbeauftragter benannt werden, wenn „die Kerntätigkeit in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Art. 9 besteht“. Die Kerntätigkeit eines klinischen Registers besteht in der Verarbeitung von Gesundheits- und/oder genetischen Daten, die beide in Art. 9 Abs. 1 DS-GVO genannt sind.

[26] Bvitg, GMDS: Sicherheit personenbezogener Daten: Umgang mit Art. 32 DS-GVO. (2018) [Online, zitiert am 2019-10-01]; Verfügbar unter https://ds-gvo.gesundheitsdatenschutz.org/html/sicherheit_verarbeitung.php

In den ErwGr. 75 bzw. 91 ist zu finden, dass im Bereich des „Umfangs der Datenverarbeitung“ zwei Einflussgrößen zu berücksichtigen sind: Zum einen die Anzahl der Personen, zum anderen die Menge der verarbeiteten Daten. Entsprechend ErwGr. 91 ist bzgl. des Umfangs auch zu berücksichtigen, ob große Mengen personenbezogener Daten auf regionaler, nationaler oder supranationaler Ebene verarbeitet werden, was letztlich auch wiederum den Umfang der Datenmenge („große Mengen“) adressiert.

In den „Leitlinien in Bezug auf Datenschutzbeauftragte[27]“ des europäischen Datenschutzausschusses wird empfohlen, bei der Klärung der Frage, ob sich von einer umfangreichen Verarbeitung sprechen lässt, die folgenden Faktoren zu berücksichtigen:

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

Da der Anspruch eines Registers darin besteht,

- einen möglichst umfassenden Anteil der erkrankten Personen zu umfassen
- alle relevanten Daten zur Beurteilung der Erkrankung zu erheben
- die Daten langfristig zu speichern und die gespeicherten Daten regelmäßig auszuwerten
- den gesamten Einzugsbereich des Registers abzudecken,

wird man zumindest bei deutschlandweit arbeitenden klinischen Registern, welche mit personenbezogenen oder pseudonymen Daten arbeiten, davon ausgehen müssen, dass diese einen Datenschutzbeauftragten benennen müssen. Dies kann auch für ein lokal, z. B. nur in einem Bundesland, arbeitendes klinisches Register gelten; eine entsprechende Prüfung der Pflicht zur Benennung ist immer erforderlich. Im Zweifelsfall sollte die zuständige Datenschutz-Aufsichtsbehörde um eine Stellungnahme gebeten werden.

7.2 Information des und Prüfung durch den Datenschutzbeauftragten

Gemäß Art. 38 Abs. 1 DS-GVO muss ein Datenschutzbeauftragter „ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden“ werden. Dies beinhaltet natürlich auch die Sammlung von Gesundheits- oder genetischen Daten in einem klinischen Register.

Entsprechend Art. 39 Abs. 1 lit. a DS-GVO ist der Datenschutzbeauftragte zur Überwachung der Einhaltung der Vorgaben aller datenschutzrechtlichen Bestimmungen verpflichtet. Der Datenschutzbeauftragte muss daher nicht nur informiert werden, sondern es müssen alle Informationen bereitgestellt werden, damit der Datenschutzbeauftragte seinen Prüfpflichten genügen kann.

D. h. der Datenschutzbeauftragte muss sowohl bei Planung als auch bei inhaltlichen Änderungen der Registerarbeit (z. B. Änderung der Art der Datenerhebung oder der zu erhebenden Daten) hinzugezogen werden.

[27] Europäischer Datenschutzausschuss: von der Artikel-29-Datenschutzgruppe übernommene Papiere „Guidelines on Data Protection Officers ('DPOs') (wp243rev.01)“. [Online, zitiert am 2019-11-05]; Verfügbar unter https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048

8 Verzeichnis der Verarbeitungstätigkeiten

Das Verzeichnis der Verarbeitungstätigkeiten wird in Art. 30 DS-GVO von allen Verantwortlichen (Art. 30 Abs. 1 DS-GVO) und Auftragsverarbeitern (Art. 30 Abs. 2 DS-GVO) gefordert, welche eine Verarbeitung besonderer Datenkategorien gemäß Art. 9 Abs. 1 DS-GVO durchführen. Da Gesundheitsdaten wie auch genetische Daten unter diese Regelung fallen, muss jedes klinische Register zwingend ein Verzeichnis der Verarbeitungstätigkeiten führen. Zum Thema „Verzeichnis der Verarbeitungstätigkeiten“ wird bzgl. der Interpretation der rechtlichen Regelungen auf die Praxishilfe der GMDS[28] verwiesen.

Die DS-GVO beschreibt die Mindestinhalte des Verzeichnisses in im Art. 30 Abs. 1 (Verantwortlicher) bzw. im Art. 30 Abs. 2 (Auftragsverarbeiter), Tabelle 1 gibt die Inhalte stichpunktartig wieder.

Art. 30 Abs. 1 DS-GVO (Verantwortlicher)	**Art. 30 Abs. 2 DS-GVO (Auftragsverarbeiter)**
	Namen und die Kontaktdaten des Auftragsverarbeiters, sowie gegebenenfalls des Vertreters des Auftragsverarbeiters
Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen	Namen und die Kontaktdaten eines jeden Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie gegebenenfalls des Vertreters des Verantwortlichen
Namen und die Kontaktdaten eines etwaigen Datenschutzbeauftragten	Namen und die Kontaktdaten eines etwaigen Datenschutzbeauftragten des Auftragsverarbeiters und des Verantwortlichen
Zwecke der Verarbeitung	Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden
Beschreibung der Kategorien betroffener Personen	
Beschreibung der Kategorien personenbezogener Daten	
Kategorien von Empfängern […], einschließlich Empfänger in Drittländern oder internationalen Organisationen	gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien
die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien	
eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gem. Art. 32	eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32

Tabelle 1: Mindestinhalte des Verzeichnisses der Verarbeitungstätigkeiten

[28] GMDS: Verzeichnis von Verarbeitungstätigkeiten: Hinweise zur Erstellung (2016). [Online, zitiert am 2019-10-01]; Verfügbar unter https://ds-gvo.gesundheitsdatenschutz.org/html/verarbeitungsverzeichnis.php

Das Verzeichnis ist schriftlich zu führen, wobei dies eine elektronische Form einschließt. Vorlagen für ein Verzeichnis der Verarbeitungstätigkeiten werden von verschiedenen Stellen angeboten[29].

9 Zusammenarbeit

Mitunter arbeiten in klinischen Registern mehr als eine juristische Person zusammen. Die Form der Zusammenarbeit bestimmt dabei das datenschutzrechtliche Vertragsverhältnis: sind es gleichberechtigte Partner, wird es sich um eine gemeinsame Verarbeitung handeln, handelt jedoch ein Partner auf Weisungen des anderen, wird eher eine Auftragsverarbeitung vorliegen. Die Unterschiede zeigt die folgende Tabelle:

Kriterium	Auftragsverarbeitung	Gemeinsame Verarbeitung
Grundsatz	Weisungsgebundene Verarbeitung von Daten durch Auftragnehmer	(Gleichberechtigte) Partnerschaft mit gemeinsamer Verantwortung
Erlaubnistatbestand	Verantwortlicher verfügt über einen Erlaubnistatbestand	Die gemeinsam an der Verarbeitung Beteiligten haben einen (gemeinsamen) Erlaubnistatbestand
Voraussetzung für Verarbeitung	Vertrag oder sonstiges Rechtsinstrument	Aufteilung der Pflichten gemäß Art. 26 (und entsprechende vertragliche Regelung / Vereinbarung)

Tabelle 2: Unterscheidung "Auftragsverarbeitung" und "Gemeinsame Verarbeitung"

9.1 Auftragsverarbeitung

Die Auftragsverarbeitung ist eine „privilegierte“ Form der Verarbeitung, für die der europäische Gesetzgeber vertragsrechtliche Anforderungen (Art. 28 DS-GVO) aufstellt. „Privilegiert“ ist die Auftragsverarbeitung dahingehend, dass kein Erlaubnistatbestand benötigt wird, um einem Auftragnehmer Daten zur Verarbeitung zu geben; die Tatsache, dass der Auftragnehmer die Daten ausschließlich entsprechend den Weisungen des Auftraggebers verarbeiten darf, wird dahingehend gewertet, dass der Auftragnehmer als „dem Auftraggeber zugehörend“ gewertet wird: Der Auftragnehmer zählt datenschutzrechtlich wie Personal des Auftraggebers.

Beispiel für eine Auftragsverarbeitung:

> Ein Register nutzt die Software eines Herstellers. Der Hersteller führt regelmäßig Wartungsarbeiten durch, spielt Funktionserweiterungen sowie Anpassungen an die Registersoftware ein. Bei diesen Arbeiten kann ein Zugriff auf die im Register gespeicherten personenbezogenen Daten erfolgen.

Die angesprochene Weisungsgebundenheit und einige andere Vereinbarungen, die in Art. 28 DS-GVO beschrieben sind, müssen bei Vorliegen einer Verarbeitung personenbezogener Daten im Auftrag in Form eines Vertrages verbindlich festgelegt werden. Zur Erstellung dieses Vertrages gibt es eine Praxishilfe, auf die an dieser Stelle verwiesen wird[30].

[29] Z.B. Datenschutzkonferenz

- Muster [Online, zitiert am 2019-10-19]; Verfügbar unter: https://www.datenschutzkonferenz-online.de/media/ah/201802_ah_muster_verantwortliche.pdf
- Hinweise zu Verzeichnis [Online, zitiert am 2019-10-19]; Verfügbar unter: https://www.datenschutzkonferenz-online.de/media/ah/201802_ah_verzeichnis_verarbeitungstaetigkeiten.pdf

[30] BvD, bvitg, DKG, GDD, GMDS: Mustervertrag zur Auftragsverarbeitung (2018). [Online, zitiert am 2019-10-01]; Verfügbar unter https://ds-gvo.gesundheitsdatenschutz.org/html/adv-vertrag.php

9.2 Gemeinsame Verantwortung

Art. 4 Ziff. 7 DS-GVO definiert einen (gemeinsamen) Verantwortlichen als jemanden, der allein oder *gemeinsam mit anderen über die Zwecke und Mittel* der Verarbeitung von personenbezogenen Daten entscheidet. Dies findet sich so auch in Art. 26 Abs. 1 S.1 DS-GVO wieder, in dem es heißt: „Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie gemeinsam Verantwortliche."

Dabei kommt es bei der Beurteilung der Tatsache, ob die Parteien gemeinsam über Zwecke und Mittel bestimmen können, weniger auf die vertragliche Ausgestaltung an, sondern vielmehr ist für diese Beurteilung entscheidend, dass eine solche Entscheidungsbefugnis in der Realität auch tatsächlich gegeben ist. Damit kommt es hinsichtlich der Beurteilung maßgeblich auf die Betrachtung und Bewertung anhand der tatsächlichen Gegebenheiten an[31].

Gemäß der Interpretation der Artikel-29-Datenschutzgruppe muss der Begriff „gemeinsam" „im Sinne von ‚zusammen mit' oder ‚nicht alleine' in unterschiedlichen Spielarten und Konstellationen ausgelegt werden"[32]. Wie der EuGH in seinem Facebook-Urteil feststellte, muss nicht jeder der Verantwortlichen gleich viel Verantwortung haben und über alle Daten verfügen, damit von einer gemeinsamen Verantwortung gesprochen werden kann[33].

In der GMDS-Praxishilfe „Art. 26 DS-GVO: Gemeinsam Verantwortliche" findet sich sowohl eine ausführliche Interpretation der Regelungen als auch Hinweise zur Vertragsgestaltung[34].

9.3 Berufsgeheimnisträger als „Datenlieferant"

Keine Zusammenarbeit im eigentlichen Sinne liegt vor, wenn von patientenversorgenden Stellen Daten einem Register lediglich bereitgestellt werden, die Berufsgeheimnisträger gleichsam als „Datenlieferant" für das Register dienen.

Hier sind zwei unabhängig agierende Verantwortliche:

1) Die den Patienten versorgende Einrichtung (z.B. Krankenhaus oder Arztpraxis)
2) Das Register

Sofern die Verarbeitung auf einer Einwilligung des Patienten beruht, werden dementsprechend auch zwei Einwilligungen benötigt:

1) Die den Patienten versorgende Einrichtung benötigt eine Einwilligung, damit die Patientendaten an ein Register weitergegeben werden dürfen
2) Das Register benötigt eine Einwilligung, damit die Patientendaten durch das Register verarbeitet werden dürfen.

[31] Hartung J. Art. 26 Rn. 14 in Kühling/Buchner (Hrsg.) DS-GVO Datenschutz-Grundverordnung Kommentar. C.H.Beck Verlag, 2. Auflage 2018. ISBN 978-3-406-719325

[32] Artikel-29-Datenschutzgruppe. (2010) WP 169 Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", Abschnitt III.1.d) Zweites Element: „allein oder gemeinsam mit anderen", S. 22. [Online, zitiert am 2019-09-30]; Verfügbar unter http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_de.pdf

[33] Europäischer Gerichtshof (EuGH). Urt. V. 05. Juni 2018, AZ: C-210/16. Rn. 38. [Online, zitiert am 2019-09-30]; Verfügbar unter http://curia.europa.eu/juris/document/document.jsf?text=&docid=202543&pageIndex=0&doclang=d &mode=lst&dir=&occ=first&part=1&cid=568857

[34] GMDS: Art. 26 DS-GVO: Gemeinsam Verantwortliche (2018). [Online, zitiert am 2019-10-01]; Verfügbar unter https://ds-gvo.gesundheitsdatenschutz.org/download/Art.26-Gemeinsam_Verantwortliche.pdf

Da entsprechend Art. 7 DS-GVO der Verantwortliche die Einwilligung nachweisen muss und in diesem Fall zwei unabhängig voneinander agierende Verantwortliche vorhanden sind, müssen zwingend auch zwei Einwilligungen des Patienten vorliegen. Dabei kann natürlich das Register die versorgende Einrichtung mit der Einholung der vom Register benötigten Einwilligung beauftragen.

10 Datenpannen und Meldepflicht[35]

Die DS-GVO enthält Regelungen bzgl. der Verletzung des Schutzes personenbezogener Daten. Art. 4 Ziff. 12 DS-GVO enthält die Definition einer „Verletzung des Schutzes personenbezogener Daten“: Demnach handelt es sich um eine Verletzung der Sicherheit, welche

- ob **unbeabsichtigt** oder **unrechtmäßig**,
- zur **Vernichtung**, zum **Verlust**, zur **Veränderung**, oder zur **unbefugten Offenlegung**
- von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt,
- die **übermittelt, gespeichert** oder auf **sonstige Weise verarbeitet wurden**.

Eine Verletzung des Schutzes personenbezogener Daten liegt daher nicht nur dann vor, wenn Unberechtigte Zugang zu diesen Daten bekommen, sondern auch, wenn diese Daten unbeabsichtigt oder unrechtmäßig vernichtet oder verändert werden oder verloren gehen.

10.1 Verzeichnis der Datenpannen

Art. 33 Abs. 5 DS-GVO verlangt, dass der Verantwortliche Verletzungen des Schutzes personenbezogener Daten einschließlich aller im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten stehenden Fakten, von deren Auswirkungen und der ergriffenen Abhilfemaßnahmen dokumentiert. Diese Dokumentation muss der zuständigen Aufsichtsbehörde die Überprüfung der Einhaltung der Bestimmungen von Art. 33 ermöglichen, d. h. auf Anforderung der Aufsichtsbehörde zur Verfügung gestellt werden. Insbesondere kann die Aufsichtsbehörde an Hand dieses Verzeichnisses prüfen, ob alle meldepflichtigen Vorfälle auch gemeldet wurden.

Grundsätzlich müssen in diesem Verzeichnis alle Datenpannen dokumentiert werden.

10.2 Meldepflicht bei Datenpannen: Aufsichtsbehörde

Art. 33 Abs. 1 DS-GVO verlangt, dass der Verantwortliche, in diesem Fall das jeweilige Register, im Falle einer Verletzung des Schutzes personenbezogener Daten diese Verletzung unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, der Aufsichtsbehörde meldet. D. h., es meldet nie der Auftragsverarbeiter, immer nur der Verantwortliche. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden nach Bekanntwerden der Verletzung, so ist ihr eine Begründung für die Verzögerung beizufügen.

Die Meldung an die Aufsichtsbehörden muss dabei mindestens die folgenden Informationen beinhalten:

1. eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe
   - der Kategorien der Daten (z. B. Bankdaten, Gewerkschaftsdaten oder Gesundheitsdaten) und

[35] Grundsätzlich sei hier auf die „Leitlinien für die Meldung von Verletzungen des Schutzes personenbezogener Daten“ der Artikel-29-Datenschutzgruppe verwiesen, welche von EDSA auf seiner ersten Sitzung anerkannt wurden. [Online, zitiert am 2019-10-19]; Verfügbar unter https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052

- der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien der Personen (z. B. Patienten oder Beschäftigte) und
- der ungefähren Zahl der betroffenen personenbezogenen Datensätze

2. den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen
3. eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten
4. eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Es müssen daher neben der Verletzung selbst noch diverse Informationen bereitgestellt werden, so dass selbst eine Zeitspanne von 72 Stunden nur schwierig einzuhalten sein kann. Insbesondere die Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen bedingt letztlich eine vollständige Analyse des Vorfalls, welche ja auch einiges an Zeit kosten wird.

Bei der EU-Vorgabe von 72 Stunden ist zu beachten, dass die EU-Verordnung 1182/71[36] Regeln für die Fristen, Daten und Termine beinhaltet, die bei allen europäischen Regelungen, die selbst keine abweichenden Vorgaben beinhalten, anzuwenden sind. Da die DS-GVO keine eigenen Regelungen hinsichtlich des Umgangs mit Fristen, Daten und Termine beinhaltet, gelten somit die Vorgaben der Verordnung 1182/71. Hierbei sind bei der Vorgabe von den in Art. 33 DS-GVO vorgegebenen 72 Stunden insbesondere zu beachten:

- Art. 3 Abs. 1 VO 1182/71: Ist für den Anfang einer nach Stunden bemessenen Frist der Zeitpunkt maßgebend, wann ein Ereignis eintritt oder eine Handlung vorgenommen wird, so wird bei der Berechnung dieser Frist die Stunde nicht mitgerechnet, in die das Ereignis oder die Handlung fällt.
- Art. 3 Abs. 2 lit. a VO 1182/71: Eine nach Stunden bemessene Frist beginnt am Anfang der ersten Stunde und endet mit Ablauf der letzten Stunde der Frist.
- Art. 3 Abs. 3 VO 1182/71: Die Fristen umfassen die Feiertage, die Sonntage und die Sonnabende, soweit diese nicht ausdrücklich ausgenommen oder die Fristen nach Arbeitstagen bemessen sind.

Somit zählen Wochenenden und Feiertage bei der Fristberechnung hinzu. Die ergänzende Regelung von Art. 3 Abs. 5 VO 1182/7, dass jede Frist von zwei oder mehr Tagen mindestens zwei Arbeitstage umfassen muss, gilt nur bei nach Tagen bemessenen Fristen.

Die Meldefrist/-Zeit beginnt ab dem Zeitpunkt, ab welchem dem Verantwortlichen die Verletzung bekannt wurde. Hierbei ist zu beachten, dass zum Kreis des Verantwortlichen alle Beschäftigten gehören: Nimmt ein Beschäftigter die Verletzung zur Kenntnis, so hat der Verantwortliche die Verletzung zur Kenntnis genommen. Daher ist es erforderlich, dass einerseits Prozesse bzgl. der Weitergabe der Informationen etabliert werden, andererseits alle Beschäftigten hinsichtlich der Weitergabe der Information bzgl. der Verletzung des Schutzes personenbezogener Daten geschult werden.

[36] Verordnung (EWG, Euratom) Nr. 1182/71 des Rates vom 3. Juni 1971 zur Festlegung der Regeln für die Fristen, Daten und Termine. [Online, zitiert am 2019-10-19]; Verfügbar unter https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A31971R1182

Auftragsverarbeiter gelten als der „verlängerte“ Arm des Verantwortlicher, d. h. es gilt: hat der Auftragsverarbeiter Kenntnis von der Verletzung erhalten, so gilt dies als Kenntnisnahme des Verantwortlichen und die Zeitspanne, in welcher eine Meldung zu erfolgen hat, beginnt ab Kenntnisnahme durch den Auftragsverarbeiter zu laufen. Grundsätzlich ist der Auftragsverarbeiter durch Art. 33 Abs. 2 DS-GVO gesetzlich verpflichtet, eine Verletzung unverzüglich dem Verantwortlichen zu melden. Je nach vertraglicher Gestaltung können bei einer „unverzüglichen“ (= ohne schuldhaftes Verzögern) Meldung aber 2-3 Tage vergehen, man denke nur an Freitag Nachmittag und anschließendes Wochenende. Bekommt der Verantwortliche die Meldung aber ggf. mit 48 Stunden Verzögerung, bleibt kaum noch Zeit zur Bearbeitung des Vorfalls durch den Verantwortlichen. Daher sollten vertragliche Regelungen eine Pflicht zu einer entsprechend schnellen Meldung des Auftragsverarbeiters an den Verantwortlichen beinhalten, wobei der Verantwortliche in diesen Fällen natürlich auch die Verarbeitung an Wochenenden und Feiertagen gewährleisten muss.

Ausnahme von der Meldepflicht: Art. 33 Abs. 1 DS-GVO enthält einen Ausnahmetatbestand von der grundsätzlich zu erfolgenden Meldung aller Verletzungen. Wenn eine Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt, muss keine Meldung erfolgen. Die Bewertung kann für den Verantwortlichen mitunter schwierig sein; auf Grund der Tatsache, dass ein Verstoß gegen die Meldepflicht bußgeldbewehrt (Art. 83 Abs. 4 lit. b DS-GVO) ist, empfiehlt es sich, im Zweifelsfall eine Meldung abzugeben.

10.3 Meldepflicht bei Datenpannen: Betroffene Personen

Art. 34 Abs. 1 DS-GVO verlangt, dass eine Verletzung des Schutzes personenbezogener Daten der bzw. den betroffenen Personen unverzüglich gemeldet wird, wenn die Verletzung voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat. D. h. es muss nicht zwingend ein hohes Risiko vorhanden sein: Es reicht, wenn die Verletzung voraussichtlich ein hohes Risiko darstellen *könnte*.

Eine Benachrichtigung betroffener Personen hinsichtlich der Verletzung des Schutzes personenbezogener Daten muss mindestens beinhalten:

1. den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen
2. eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten
3. eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Dabei ist zu beachten, dass Art. 34 Abs. 2 DS-GVO fordert, dass die Informationen in „klarer und einfacher Sprache“ zu erfolgen haben: Die Vorgaben von Art. 12 DS-GVO bzgl. transparenter Information müssen bei der Information nach Art. 34 DS-GVO eingehalten werden.

Ausnahme von der Meldepflicht: Art. 34 Abs. 3 DS-GVO enthält einen Ausnahmetatbestand von der Meldepflicht. Eine Meldung an die betroffene Person muss nicht erfolgen, wenn mindestens eine der nachfolgenden Bedingungen erfüllt ist:

1. Der Verantwortliche hat geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen, dass die betroffenen personenbezogenen Daten für alle

unbefugten/unberechtigten Personen unzugänglich sind. Dies kann z. B. durch den Einsatz von dem Stand der Technik entsprechender Verschlüsselung gewährleistet sein.

2. Der Verantwortliche durch der Verletzung nachfolgende Maßnahmen sichergestellt hat, dass das hohe Risiko aller Wahrscheinlichkeit nach nicht mehr besteht. Dies kann z. B. dadurch geschehen, wenn beim Diebstahl eines mobilen Datenträgers unmittelbar nach dem Diebstahl ein „Remote Wipe[37]“ erfolgte.
3. Die Meldung mit einem unverhältnismäßigen Aufwand verbunden wäre. In diesem Fall hat stattdessen eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden. In diesen Fällen kann beispielsweise eine Veröffentlichung des Vorfalles in regionalen oder überregionalen (je nach Gruppe betroffener Personen) Tageszeitungen erfolgen. Ein bloßes Bekanntgeben auf der eigenen Homepage allein wird i. d. R. nicht ausreichen, da man nicht davon ausgehen kann, dass die betroffenen Personen zeitnah die Homepage aufsuchen. Eine Darstellung auf der eigenen Homepage kann nur eine ergänzende Maßnahme darstellen, z. B. um ergänzend zum Zeitungsartikel weitere Informationen bereitzustellen.

10.4 Umgang mit Datenpannen: Was ist zu tun?

Es muss ein Team gebildet werden, welches Datenpannen abarbeitet. Zum Team sollten mindestens gehören:

- Der Datenschutzbeauftragte. Wenn kein Datenschutzbeauftragter benannt wurde, ein Jurist mit entsprechendem datenschutzrechtlichem Fachwissen
- Ein Mitglied der Geschäftsführung, welches
  a) den Vorfall aus Unternehmenssicht bewerten und insbesondere die Entscheidung bzgl. Meldepflicht treffen kann
  b) eine Entscheidung hinsichtlich der Kosten, welche zu ergreifende Maßnahmen i. d. R. beinhalten, beschließen kann
- Ein IT-Sicherheitsexperte, welcher
  a) den Vorfall aus IT-Sicht bewerten kann
  b) Maßnahmen zur Behebung der Verletzung vorschlagen kann
  c) Maßnahmen, soweit möglich, zur Abmilderung der möglichen nachteiligen Auswirkungen für die betroffenen Personen vorschlagen kann
- Ein Fachexperte aus dem betrieblichen Umfeld, aus welchem die Daten stammen, welcher die Bedeutung des Vorfalls für betroffene Personen beurteilen kann. Im Umfeld der Fragestellung dieser Ausarbeitung wird dies regelhaft ein entsprechendes medizinisches Fachwissen voraussetzen.

Weiterhin muss ein Prozess zum Umgang mit Datenpannen etabliert werden. Dieser Prozess muss mindestens beinhalten:

- Welche Vorfälle werden zu welchen Zeitpunkten durch wen an wen gemeldet?
- Wer hat welche Zuständigkeiten?
  - Wie erfolgt durch wen bis wann eine Risikobewertung?

[37] Remote Wipe ist ein Sicherheitsfeature, welches erlaubt, aus der Ferne Daten auf einem Computer, Smartphone oder Tablet zu löschen. Allerdings funktioniert Remote Wipe nur mit existierender Verbindung zu einem Netzwerk (Internet oder Mobilfunknetz, je nach eingesetzter IT-Lösung). Daher kann man von einem erfolgreichen Löschen der Daten erst dann ausgehen, wenn das Gerät den Erhalt des Löschbefehls sowie die durchgeführte Löschung bestätigte. Die Abgabe des Remote Wipe Löschbefehles alleine reicht nicht aus um davon ausgehen zu können, dass das Risiko aller Wahrscheinlichkeit nach nicht mehr besteht.

    - Wer darf der Aufsichtsbehörde melden?
    - Wer meldet betroffenen Personen? Oder führt eine entsprechende öffentliche Bekanntgabe durch?
    - Wenn kein Datenschutzbeauftragter existiert: Wer ist Ansprechpartner für die zuständige Aufsichtsbehörde?
- Wie sind die Regelungen bzgl. Auftragsverarbeiter?
    - Wer ist Anlaufstelle für Auftragsverarbeiter?
    - Wann muss/kann ein Auftragsverarbeiter melden?
    - Welche Zuarbeit muss ein Auftragsverarbeiter in welchem Zeitraum leisten? Nur innerhalb der vereinbarten Servicezeiten oder ggf. auch außerhalb? Letzteres kann mit zusätzlichen Kosten verbunden sein.
- Wer führt das gesetzlich geforderte Verzeichnis?

Dieser Prozess muss in das vorhandene Risikomanagement integriert werden. Insbesondere müssen alle Beschäftigten in einer Schulung bzgl. des Umgangs mit entsprechenden Vorfällen unterwiesen werden; man kann ja nicht im Vorfeld wissen, welcher Beschäftigte eine (mögliche) Verletzung des Schutzes personenbezogener Daten entdeckt und daher das Wissen um den Prozess kennen muss. Desgleichen sollte eine entsprechende vertragliche Vereinbarung mit dem Auftragsverarbeiter existieren.

11 Befugnisse der Datenschutz-Aufsichtsbehörden

11.1 Abhilfebefugnisse

Gemäß Art. 58 Abs. 2 DS-GVO haben Datenschutz-Aufsichtsbehörden insbesondere folgende Abhilfebefugnisse:

- Aufsichtsbehörden können Verantwortliche oder Auftragsverarbeiter warnen, dass beabsichtigte Verarbeitungsvorgänge voraussichtlich gegen datenschutzrechtliche Bestimmungen verstoßen.
- Aufsichtsbehörden können Verantwortliche oder Auftragsverarbeiter verwarnen, wenn diese mit Verarbeitungsvorgängen gegen datenschutzrechtliche Bestimmungen verstoßen haben.
- Aufsichtsbehörden können Verantwortliche oder Auftragsverarbeiter anweisen, den Anträgen einer betroffenen Person auf Ausübung der ihr nach der DS-GVO zustehenden Rechte wie beispielsweise Löschung der Daten zu entsprechen.
- Aufsichtsbehörden können die Berichtigung oder Löschung von personenbezogenen Daten oder die Einschränkung der Verarbeitung und die Unterrichtung der Empfänger der Daten über die angeordneten Maßnahmen anordnen.
- Aufsichtsbehörden können Verantwortliche oder Auftragsverarbeiter anweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DS-GVO zu bringen.
- Aufsichtsbehörden können eine vorübergehende oder endgültige Beschränkung einer Verarbeitung, einschließlich eines Verbots, verhängen.

Insbesondere die letzten beiden Möglichkeiten können dazu führen, dass ein Register seine Arbeit einstellen muss. Daher sind Hinweise von Aufsichtsbehörden, in denen Zweifel an der Rechtmäßigkeit der Verarbeitung geäußert werden, sehr ernst zu nehmen. Spätestens wenn eine

Verwarnung seitens der Aufsichtsbehörden ausgesprochen wurde, sollte die Verarbeitung in der vorliegenden Form eingestellt und in Absprache mit der Aufsichtsbehörde angepasst werden.

11.2 Bußgelder

Bei Verstößen bzgl.

- Artt. 5, 6, 7, 9 (fehlende oder fehlerhaft eingeholte Einwilligung)
- Artt. 12-22 (Verstoß gegen die Rechte der/des Betroffenen)
- Artt. 44 bis 49 (Unrechtmäßige Übermittlung in ein Drittland oder int. Organisation)
- Nichtbefolgung einer Anweisung oder einer vorübergehenden oder endgültigen Beschränkung oder Aussetzung der Datenübermittlung durch die Aufsichtsbehörde

können Aufsichtsbehörden das sogenannte „hohe“ Bußgeld (Geldbußen bis zu 20 Millionen Euro bzw. 4 % des Vorjahresumsatzes, je nachdem, welche Summe höher ist) verhängen. Bei Verstößen bzgl.

- Art. 25 (Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen)
- Art. 28 (Auftragsverarbeiter)
- Art. 29 (Verarbeitung unter der Aufsicht des Verantwortlichen oder des Auftragsverarbeiters)
- Art. 30 (Verzeichnis von Verarbeitungstätigkeiten)
- Art. 31 (Zusammenarbeit mit der Aufsichtsbehörde)
- Art. 32 (Sicherheit der Verarbeitung)
- Artt. 33 u. 34 (Meldung von Datenpannen an Aufsichtsbehörde und Betroffenen)
- Art. 35 (Datenschutzfolgenabschätzung)
- Artt. 36 bis 39 (Datenschutzbeauftragter)

können Aufsichtsbehörden das sogenannte „kleine“ Bußgeld (Geldbußen bis zu 10 Millionen Euro bzw. 2 % des Vorjahresumsatzes, je nachdem, welche Summe höher ist) verhängen.

Grundsatz: Immer, wenn die betroffene Person direkt selbst betroffen ist (unrechtmäßige Verarbeitung, Verstoß gegen Betroffenenrechte), droht das „hohe“ Bußgeld, in anderen Fällen i. d. R. das „kleine“ Bußgeld.

Bei Verhängung von Bußgeldern müssen Aufsichtsbehörden entsprechend Art. 83 Abs. 2 DS-GVO insbesondere berücksichtigen:

- Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde, z. B.
  - Meldete der Verantwortliche bzw. der Auftragsverarbeiter selbst das Vergehen an die Aufsichtsbehörde?
  - Erfuhr die Aufsichtsbehörde vom Betroffenen davon? Ggfs. aufgrund der Tatsache, dass der Verantwortliche den Betroffenen auf diese Möglichkeit hinwies?
  - Wurde die Aufsichtsbehörde erst über Dritte (z. B. Presse) informiert?
- Art, Schwere und Dauer des Verstoßes wie beispielsweise
  - Liegt ein genereller Verstoß vor, d. h. man kann generell der gesetzlichen Pflicht nicht genügen?
  - Sind es nur die konkreten Umstände des Einzelfalles, die ein Genügen der gesetzlichen Pflicht verhindern?
  - Wie groß ist der potentielle Schaden für jeden einzelnen Betroffenen? Wie groß ist der Schaden insgesamt?

- Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes, d. h. insbesondere ist zu betrachten:
  - Wurde die gesetzliche Pflicht vom Verantwortlichen im Ablauf seiner Prozesse ignoriert?
  - Wurde fahrlässig einem einzelnen Betroffenen sein Recht verweigert?
- Umfang der Zusammenarbeit mit der Aufsichtsbehörde, z. B.
  - Wurden der Aufsichtsbehörde unverzüglich alle benötigten Informationen gegeben?
  - Wurden Anstrengungen unternommen, um nachteilige Auswirkungen zu mildern?
  - Wurden Anstrengungen unternommen, damit künftig Verstöße dieser Art nicht mehr vorkommen?
- Sind etwaige einschlägige frühere Verstöße bekannt?
  - Ist es Wiederholungstatbestand?
- Die Kategorien personenbezogener Daten
  - Im Kontext der Gesundheitsversorgung/-forschung handelt es sich immer um die besonders schützenswerten Daten der in Art. 9 Abs. 1 DS-GVO genannten besonderen Kategorien, sodass ein Verstoß i. d. R. schwerer wiegt.

Bei der Verhängung von Bußgeldern müssen Aufsichtsbehörden gemäß Art. 83 Abs. 1 DS-GVO dem Grundsatz folgen, dass die Verhängung von Geldbußen in jedem Einzelfall wirksam, verhältnismäßig und abschreckend sein muss. Dabei ist insbesondere ErwGr. 148 zu beachten:

> „Im Falle eines geringfügigeren Verstoßes oder falls voraussichtlich zu verhängende Geldbuße eine unverhältnismäßige Belastung für eine natürliche Person bewirken würde, kann anstelle einer Geldbuße eine Verwarnung erteilt werden."

Allerdings gilt ErwGr. 148 gilt nicht für juristische Personen wie beispielsweise ein klinisches Register.

Die Datenschutzkonferenz verabschiedete im September 2019 ein Konzept zur Bußgeldzumessung in Verfahren gegen Unternehmen[38]. Verstöße gegen die DS-GVO müssen europaweit einheitlich sanktioniert werden, daher ist das deutsche Konzept zunächst als Diskussionsentwurf für Europa anzusehen; die Datenschutzkonferenz brachte ihren Entwurf auch schon in den entsprechenden Arbeitskreis des EU Datenschutzausschusses ein. Unabhängig von der Rechtsgültigkeit des Konzeptes zeigt der Entwurf, wie deutsche Aufsichtsbehörden planen, bei Verstößen zu sanktionieren und ist daher sicherlich für alle Verantwortlichen von Interesse.

12 Besondere Fragestellungen

12.1 Datenverarbeitung in Drittstaaten

12.1.1 Auftragsverarbeitung

Bei sog. Drittländern (= Land ohne ein als hinreichend anerkanntes Datenschutzniveau) ist gemäß Art. 44 DS-GVO ebenfalls die Sicherstellung eines angemessenen Datenschutzniveaus beim Datenempfänger zu gewährleisten. Um dies zu bewerkstelligen, hat die Europäische Kommission sogenannte „Standardvertragsklauseln" bereitgestellt, welche beim Einsatz eines Auftragsverarbeiters in einem solchen Drittland verwendet werden müssen, wenn unter dem Aspekt

[38] Datenschutzkonferenz: Konzept zur Bußgeldzumessung in Verfahren gegen Unternehmen. [Online, zitiert am 2019-10-19]; Verfügbar unter Anwendungshinweisen (https://www.datenschutzkonferenz-online.de/anwendungshinweise.html bzw. direkt pdf-Datei unter https://www.datenschutzkonferenz-online.de/media/pm/20190917_bu%C3%9Fgeldkonzept.pdf

der Auftragsverarbeitung ein Auftragnehmer eines derartigen Landes von einem Auftraggeber mit Sitz in der EU beauftragt werden soll (Art. 46 Abs. 2 lit. c DS-GVO). Diese Vertragsvorgaben ergänzen und präzisieren die Vertragsbedingungen über die eigentliche Leistungserbringung hinsichtlich der datenschutzrechtlich geforderten Mindeststandards[39]. Die Rechte und Pflichten der Parteien werden geregelt und müssen unverändert übernommen werden. Seit dem 15.5.2010 müssen die neuen EU-Standardvertragsklauseln genutzt werden[40].

Eine Beauftragung von Auftragnehmern in Ländern, denen die Europäische Kommission bereits ein angemessenes Datenschutzniveau gemäß Art. 45 DS-GVO attestiert hat, sog. sichere Drittstaaten, ist rechtlich zulässig; die Liste der Länder steht online zur Verfügung[41].

12.2 Zweckänderung und Erlaubnis zur Verarbeitung

Klinische Register „leben“ von Patientendaten. Die Patientendaten werden in den versorgenden Einrichtungen jedoch zu Zwecken der Patientenversorgung erhoben, nicht, um die Daten in einem Register zu speichern. Daher spricht man hier von einer „Sekundärnutzung“ der Daten; der primäre Zweck der Datenverarbeitung war ja die Patientenversorgung.

Art. 5 Abs. 1 lit. b DS-GVO beinhaltet die Regelung, dass „eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke“ gemäß Art. 89 Abs. 1 DS-GVO nicht als „unvereinbar“ mit den ursprünglichen Zwecken gilt. D. h. hier findet ggf. zwar eine Zweck*änderung* statt, jedoch können der „alte“ und der „neue“ Zweck miteinander vereinbar sein. Art. 5 Abs. 1 lit. b DS-GVO beinhaltet jedoch nicht, dass dies immer der Fall ist; vielmehr muss im Einzelfall nachgewiesen werden, dass der Forschungszweck vereinbar mit dem ursprünglichen Zweck (i. d. R. Patientenversorgung) ist[42]. Dieser Nachweis der Vereinbarkeit ist entsprechend den Vorgaben von Art. 6 Abs. 4 DS-GVO zu führen. Dazu muss der Forscher unter anderem folgende Kriterien berücksichtigen:

a) „Jede Verbindung zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung“
   Beispielsweise ist der Patient an Prostatakrebs erkrankt und das Forschungsprojekt dient der Verbesserung dieser Behandlung, was man als starken Hinweis für einen kompatiblen Zweck ansehen könnte. Hingegen wäre eine Forschung bzgl. nächtlichen Harndrangs trotz des gemeinsamen urologischen Fachgebietes nicht so ein offensichtlicher Hinweis.
b) „Den Zusammenhang, in dem die personenbezogenen Daten erhoben wurden, insbesondere hinsichtlich des Verhältnisses zwischen den betroffenen Personen und dem Verantwortlichen“
   Werden die Daten zur Forschung von denselben Menschen genutzt, die auch in die Behandlung involviert waren, so besteht einerseits ein starkes Vertrauensverhältnis

[39] Bzgl. Möglichkeiten der Verarbeitung von Daten in einem Drittland siehe Artt. 44-50 EU DS-GVO sowie entsprechende Kommentierungen

[40] Beschluss der Kommission vom 5. Februar 2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates. [Online, zitiert am 2019-10-19]; Verfügbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32010D0087

[41] Commission decisions on the adequacy of the protection of personal data in third countries. [Online, zitiert am 2019-10-19]; Verfügbar unter http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/ index_en.htm

[42] Roßnagel Art. 5 Rn 106, 109 in: Simitis/Hornung/Spieker (hrsg.) Datenschutzrecht DSGVO mit BDSG. Nomos Verlag, 1. Auflage 2019. ISBN978-3-8487-3590-7

resultierend aus der Arzt-Patienten-Beziehung, zudem werden die Daten keinen weiteren Personen offenbart. Dies ist bei Nutzung der Daten durch Personen, die nicht an der Behandlung beteiligt waren, nicht der Fall.

c) „Die Art der personenbezogenen Daten, insbesondere ob besondere Kategorien personenbezogener Daten gemäß Artikel 9 verarbeitet werden“
Gesundheits- und genetische Daten haben einen besonders hohen Schutzbedarf, daher muss die Kompatibilität zwischen dem neuen (Forschungs-) Zweck und dem primären Zweck entsprechend deutlich ausgeprägt sein.

d) „Die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen“
Hier ist insbesondere zu betrachten, welche Bedeutung eine weitergehende Offenbarung der aus der Erkrankung resultierenden Daten für den Patienten haben können, wie z. B. Stigmatisierung, Verlust von Ehepartner, Freunden oder auch des Jobs usw.

e) „Das Vorhandensein geeigneter Garantien, wozu Verschlüsselung oder Pseudonymisierung gehören kann“
Je sensibler die Daten und je höher der Schutzbedarf der Daten, desto besser müssen die technisch-organisatorischen Maßnahmen zum Schutz dieser Daten sein.

Kann die Kompatibilität des neuen Zweckes mit dem ursprünglichen Zweck nachgewiesen werden, so können unter den Voraussetzungen von Art. 89 Abs. 1 DS-GVO Daten der Routineversorgung grundsätzlich für Forschungszwecke genutzt werden. Entsprechend ErwGr. 50 S. 2 DS-GVO wäre auch kein neuer Erlaubnistatbestand erforderlich: „In diesem Fall ist keine andere gesonderte Rechtsgrundlage erforderlich als diejenige für die Erhebung der personenbezogenen Daten“. Jedoch gilt dies nur im Rahmen des ursprünglichen Erlaubnistatbestandes, d. h., dass beispielsweise zur Weitergabe der Daten an Dritte, deren Verarbeitung nicht durch den ursprünglichen Erlaubnistatbestand legitimiert wurde, daher ggf. ein neuer Erlaubnistatbestand benötigt wird.

Hier muss also darauf geachtet werden, welchen Zwecken das Register dient, denn die Privilegierung gilt keiner Qualitätssicherung. Für Forschung und Statistik können jedoch Umstände gelten, die eine Nutzung der Patientendaten erlauben.

12.2.1 Zweckkompatibel, aber trotzdem Zweckänderung

Auch wenn alter und neuer Zweck kompatibel sind, handelt es sich trotzdem um eine Zweckänderung. D. h. entsprechend Art. 13 Abs. 3 DS-GVO bzw. Art. 14 Abs. 4 DS-GVO muss eine Information der betroffenen Person stattfinden, inklusive des Hinweises auf sein Widerspruchsrecht. Dies kann nur unterlassen werden, wenn einer der in Art. 13 Abs. 4 bzw. Art. 14 Abs. 5 DS-GVO genannten Ausnahmetatbestände zutrifft.

12.3 Strafrechtliches Offenbarungsverbot (§ 203 StGB)

Zweck der Regelung von § 203 StGB ist es, das sensible Vertrauensverhältnis zwischen Geheimnisträgern wie Ärzten und ihren Patienten zu schützen. Insbesondere soll § 203 StGB verhindern, dass dieses Vertrauensverhältnis durch eine unbefugte Offenbarung an Dritte geschädigt bzw. gestört wird.

Der Tatbestand des § 203 StGB setzt voraus, dass einer der dort genannten Geheimnisverpflichteten („Berufsgeheimnisträger“) ein **fremdes** Geheimnis, welches ihm in seiner **beruflichen** Eigenschaft anvertraut worden ist, unbefugt offenbart. Damit dient diese strafrechtliche Vorschrift primär des

Schutzes der Geheimsphäre des Einzelnen, daneben aber auch dem des Allgemeininteresses an der Verschwiegenheit einzelner Berufsgruppen[43].

Die Regelungen von § 203 StGB gelten dabei unabhängig vom Datenschutzrecht: Eine Offenbarung kann datenschutzrechtlich erlaubt, strafrechtlich jedoch verboten sein. Auch gibt es Unterschiede zwischen einer datenschutzrechtlichen Einwilligung in die Verarbeitung personenbezogener Daten und der strafrechtlichen Offenbarungsbefugnis durch den Patienten:

Strafrechtliche Einwilligung		Datenschutzrechtliche Einwilligung
Einverständnis zur Offenbarung („Befugnis zur Offenbarung)	≠	Einwilligung bzgl. Datenverarbeitung (Befugnis zur beschriebenen Verarbeitung)
Klauselmäßige Einwilligung: Grundsätzlich möglich, aber nur in Kenntnis und ausdrücklich; konkludente oder gar mutmaßliche Einwilligung kommt klauselmäßig grundsätzlich nicht in Frage	≠	Klauselmäßige Einwilligung: Grundsätzlich möglich, aber Art. 9 Abs. 2 lit. a DS-GVO verlangt im Gegensatz zu Art.6 Abs. 1 lit. a DS-GVO eine ausdrückliche Einwilligung
Einsichts- und Urteilsfähigkeit muss gegeben sein = Bedeutung und Tragweite müssen überblickt werden können	=	Einsichts- und Urteilsfähigkeit muss gegeben sein = Bedeutung und Tragweite müssen überblickt werden können
Unterrichtung bzgl. Art und Umfang der Einschaltung Dritter (konkrete Bezeichnung erforderlich)	≠	Unterrichtung bzgl. Art und Umfang der Einschaltung Dritter (aber Kategorien möglich, bei „broad consent“ ggf. keine konkrete Bezeichnung)
Generalvollmachten ungültig	=	Generalvollmachten ungültig (Aber „broad consent“?)
Willensmängel können zur Unwirksamkeit führen (z. B. Drohungen, Täuschungen oder Irrtümer)	=	Willensmängel können zur Unwirksamkeit führen (z. B. Drohungen, Täuschungen oder Irrtümer)
Rückwirkende Einwilligung nicht möglich	=	Rückwirkende Einwilligung nicht möglich
Offenbarungsbefugnis widerrufbar	=	Einwilligung widerrufbar
Konkludente Einwilligung möglich	≠	Konkludente Einwilligung nicht möglich

Das Vorliegen einer datenschutzrechtlichen Einwilligung kann daher nicht mit einer Befugnis zur Offenbarung nach § 203 StGB gleichgesetzt werden, vielmehr muss im Einzelfall geprüft werden, ob die datenschutzrechtliche Einwilligung auch den Erfordernissen einer strafrechtlichen Offenbarungsbefugnis genügt.

12.4 Berufsrechtliches Offenbarungsverbot für Ärztinnen und Ärzte

Die ärztliche Schweigepflicht, der jede approbierte Ärztin und jeder approbierte Arzt als Mitglied der jeweiligen Landesärztekammer unterliegt, gilt vom Grundsatz her zunächst einmal gegenüber jedermann, der nicht in das Arzt-Patienten-Verhältnis einbezogen ist. Der Kreis der Schweigepflichtigen entspricht dem Kreis der Personen, die auch unter § 203 StGB fallen[44]. Auch der

[43] Bräutigam P. (2011) §203 StGB und der funktionale Unternehmensbegriff - Ein Silberstreif am Horizont für konzerninternes IT-Outsourcing bei Versicherern. CR: 411-416

[44] Lippert. § 9 MBO-Ä, Rn: 18-20. In: Ratzel/Lippert/Prütting´: Kommentar zur (Muster-)Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte – MBO-Ä 1997. 7. Auflage 2018. ISBN 978-3-662-55164-6

Tatbestand des Offenbarens ist analog zu dem von § 203 StGB adressierten Umständen zu sehen[45]. Vom Grundsatz her stellt somit eine § 203 StGB genügende Offenbarungsbefugnis auch eine Offenbarungsbefugnis aus berufsrechtlicher Sicht dar.

Dies gilt auch für die am 30.10.2017 stattgefundene Neuregelung des § 203 StGB[46], denn die (Muster-)Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte mit Stand 14. Dezember 2018 entspricht bzgl. der Schweigepflicht weitestgehend den Regelungen des § 203 StGB. In § 9 Abs. 4 MBO-Ä findet sich:

> „Gegenüber den Mitarbeiterinnen und Mitarbeitern von Dienstleistungsunternehmen sowie sonstigen Personen, die an der beruflichen Tätigkeit mitwirken, sind Ärztinnen und Ärzte zur Offenbarung befugt, soweit dies für die Inanspruchnahme der Tätigkeit der mitwirkenden Personen erforderlich ist.
> Ärztinnen und Ärzte haben dafür zu sorgen, dass die mitwirkenden Personen schriftlich zur Geheimhaltung verpflichtet werden.
> Diese Verpflichtung zur Geheimhaltung haben Ärztinnen und Ärzte vorzunehmen oder auf das von ihnen beauftragte Dienstleistungsunternehmen zu übertragen."

Allerdings sollte beachtet werden, dass § 203 Abs. 4 StGB lediglich eine Verpflichtung fordert („[…] zur Geheimhaltung verpflichtet wurde[…]"), § 9 Abs. 4 MBO-Ä jedoch die schriftliche Verpflichtung („[…] schriftlich zur Geheimhaltung verpflichtet […]"). D. h. beim Einsatz von Dienstleistern wie Auftragsverarbeitern sollte, wann immer ein berufsrechtliches Offenbarungsverbot für Ärztinnen und Ärzte existiert, auf eine schriftliche Verpflichtung geachtet werden.

Die Umsetzung der Beschlüsse des 121. Deutschen Ärztetages 2018 in Erfurt durch die Bundesländer ist jedoch nicht überall erfolgt, auch entsprechen nicht alle Regelungen der Länder denen der MBO-Ä, so dass die Betrachtung der jeweiligen Landesberufsordnungen der Ärztinnen und Ärzte bzgl. Offenbarungsverbot bzw. Offenbarungserlaubnis leider unerlässlich ist.

12.5 Anonymisierung

Grundsätzlich muss eine Unterscheidung zwischen dem datenschutzrechtlichen Begriff des „anonymen" Datums sowie der strafrechtlichen Bedeutung der Personenbeziehbarkeit unterschieden werden.

12.5.1 Unbefugte Offenbarung i.S.v. § 203 StGB bei der Nutzung anonymer oder pseudonymer Daten

Strafrechtlich gesehen erfüllen Mitteilungen, aus denen die Person des Betroffenen nicht ersichtlich ist, mangels Personenbeziehbarkeit, nicht den Tatbestand der Offenbarung[47]. Daraus folgt, dass die Weitergabe von Informationen, welche keine Möglichkeit der Identifizierung beinhalten, somit insbesondere auch keine unbefugte Offenbarung darstellen kann.

Dementsprechend stellt auch die Weitergabe von anonymen Daten keine Offenbarung i. S. d. § 203 StGB dar[47].

---

[45] Lippert. § 9 MBO-Ä, Rn: 53, 54. In: Ratzel/Lippert/Prütting´: Kommentar zur (Muster-)Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte – MBO-Ä 1997. 7. Auflage 2018. ISBN 978-3-662-55164-6

[46] „Gesetz zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger *Personen"* vom 30.10.2017, BGBl. I, Seite 3618. [Online, zitiert am 2019-11-11]; Verfügbar unter http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl117s3618.pdf

[47] Siehe z. B.

Art. 4 Ziff. 5 S-GVO definiert pseudonyme Daten als Daten, welche „ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können“, d. h. auch bei der Weitergabe von pseudonymen Daten i. S. d. DS-GVO erfolgt keine Offenbarung im Sinne des § 203 StGB[48], wenn die Zuordnungsvorschrift, also der Schlüssel, beim (Berufs-)Geheimnisträger selbst verbleibt und der Empfänger der Daten somit keinerlei Möglichkeit der Identifikation der Person des Betroffenen hat.

12.5.2 Datenschutzrecht und der Begriff der Anonymisierung

Entsprechend ErwGr. 26 DS-GVO sollten die Vorgaben der DS-GVO nicht für anonyme Daten gelten. D. h. für anonyme Daten gelten die Anforderungen der DS-GVO nicht. Jedoch muss der Verantwortliche, u. a. der Rechenschaftspflicht aus Art. 5 Abs. 2 DS-GVO folgend, zu jedem Zeitpunkt der Verarbeitung (und damit insbesondere auch während der gesamten Speicherdauer) nachweisen können, dass es sich um anonyme Daten handelt.

Daraus ergibt sich im Umkehrschluss, dass anonyme Daten weder direkt personenbezogene Daten noch pseudonymisierte Daten sein können. D. h., anonyme Daten sind Daten, bei denen keine Zuordnungsmöglichkeit zu einer spezifischen betroffenen Person existiert[49]. Im Umkehrschluss gilt daher, dass, wenn auch nur eine Möglichkeit der Zuordnung der Daten zu einer spezifischen betroffenen Person existiert, die Daten keine anonymen Daten sind.

Anonymisierung ist dementsprechend die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten nicht mehr einer spezifischen betroffenen Person zugeordnet werden können.

Sowohl pseudonyme als auch anonyme Daten sind daher für den Verantwortlichen keiner spezifischen betroffenen Person zuordenbar. Der Unterschied zwischen anonymen und pseudonymen Daten liegt darin, dass bei pseudonymen Daten außerhalb der Zugriffsmöglichkeiten des Verantwortlichen grundsätzlich eine Zuordnungsmöglichkeit besteht oder bestehen könnte, bei anonymen Daten hingegen für niemanden eine Zuordnungsmöglichkeit vorhanden ist.

Da es sich sowohl bei der Pseudonymisierung als auch bei der Anonymisierung um eine Verarbeitung gemäß Art. 4 Ziff. 2 DS-GVO handelt, ist daher auch für eine Anonymisierung bzw. Pseudonymisierung von Gesundheitsdaten ein Erlaubnistatbestand gem. Art. 9 Abs. 2,4 DS-GVO bzw. Art. 6 Abs. 1, 2 DS-GVO für Daten, die nicht zu den besonderen Kategorien zählen, erforderlich.

- Weidemann § 203 Rn. 33 in Heintschel-Heinegg (Hrsg.) BeckOK StGB 38. Ed. vom 1. Mai 2018
- Kargl § 203 Rn. 8 in Kindhäuser / Neumann / Paeffgen (Hrsg.) Strafgesetzbuch. 5. Auflage 2017. ISBN 978-3-8487-3106-0
- Fischer § 203 Rn. 33 in Fischer. Strafgesetzbuch: StGB. 65. Auflage 2018. ISBN 978-3-406-70874-9

[48] So z. B. zu finden in:

- Cierniak/Niehaus § 203 Rn. 51,109 in Münchener Kommentar zum Strafgesetzbuch Band 4: § § 185-262, 3. Aufl. 2017, ISBN 978-3-406-68554-5
- Lenckner/Eisele § 203 Rn. 19b5 in Schönke / Schröder (Hrsg.) Strafgesetzbuch: StGB. 29. Auflage 2014. ISBN 978-3-406-65226-4

[49] Voigt P, von dem Bussche A. The EU General Data Protection Regulation (GDPR) - A Practical Guide. Springer Verlag, 2017. ISBN 978-3-319-57958-0. PP 13-16, chapter „2.1.2.2 Anonymisation and Pseudonymisation“: „Anonymised data is either information that does not relate to an identified or identifiable individual or personal data that was rendered anonymous in such a manner that the person is not or no longer identifiable.“

Bzgl. der Thematik Pseudonymisierung/Anonymisierung wird auf die Praxishilfe der GMDS verwiesen[50].

12.6 Speicherdauer

Ausnahmen von der Pflicht zur „Speicherbegrenzung“ (Art. 5 Abs. 1 lit. e DS-GVO), d. h. von der Löschpflicht personenbezogener Daten, sind für wissenschaftliche und historische Forschungszwecke sowie für statistische Zwecke vorgesehen.

Hierbei ist jedoch keine unbegrenzte Speicherdauer legitimierbar, denn eine Löschung ist hier entsprechend Art. 17 DS-GVO nach Erreichung des Zweckes zwingend erforderlich, wenn keine rechtlichen Gründe dagegensprechen. Vielmehr gestattet diese Ausnahmeregelung, Daten, die zu anderen Zwecken erhoben wurden und eigentlich zu löschen sind (z. B. Daten aus der Patientenversorgung), aufzubewahren und für einen oder mehrere zuvor definierte (Forschungs-) Zwecke zu verwenden. Hierbei sind die Schutzziele der DS-GVO zu beachten, d. h. wann immer möglich, ist mit anonymen oder wenigstens pseudonymen Daten zu arbeiten.

Weiterhin ist die betroffene Person gemäß Art. 13 Abs. 2 lit. a DS-GVO (Direkterhebung, d. h. das Register erhebt die Daten bei der Person) bzw. gemäß Art. 14 Abs. 2 lit. a DS-GVO (Dritterhebung, das Register erhebt die Daten z. B. bei einem Krankenhaus) über „die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer“ zu informieren. D. h. es muss grundsätzlich eine Löschung der Daten vorgesehen werden, die Speicherdauer richtet sich ausschließlich nach dem Erreichen des Zweckes.

Hierbei muss insbesondere berücksichtigt werden, dass bei Zwecken des Registers, die ja mehrere Jahrzehnte andauern können, nicht für die gesamte Dauer eine Personenidentifizierbarkeit gegeben sein muss. Hier muss konzeptionell beachtet werden, ab wann eine Anonymisierung der Daten möglich ist. Nach einem Beschluss der österreichischen Datenschutzaufsichtsbehörde[51] kann eine Anonymisierung eine Form der Löschung darstellen, so dass auch eine Anonymisierung der Daten eine Speicherbegrenzung i. S. d. DS-GVO darstellen kann.

12.7 Datenerhebung bei Verstorbenen

12.7.1 Datenschutz bei Verstorbenen?

Datenschutzrechtliche Regelungen sollen Menschen die Wahrnehmung ihrer Rechte ermöglichen. Daher enden datenschutzrechtliche Regelungen regelhaft mit dem Tod der betroffenen Personen, da mit dem Tod die Verfügungsgewalt endet. Erben (oder auch nahe Angehörige) können die in der DS-GVO garantierten Betroffenenrechte weder anstelle der verstorbenen Person noch aus eigenem Recht geltend machen.

In ErwGr. 27 DS-GVO heißt es dementsprechend auch: „Diese Verordnung gilt nicht für die personenbezogenen Daten Verstorbener. Die Mitgliedstaaten können Vorschriften für die Verarbeitung der personenbezogenen Daten Verstorbener vorsehen.“ Der Schutzbereich der DS-GVO endet also mit dem Tod der betroffenen Person. Jedoch muss immer beachtet werden, dass

[50] GMDS: Arbeitshilfe zur Pseudonymisierung/Anonymisierung (2018) [Online, zitiert am 2019-10-01]; Verfügbar unter https://ds-gvo.gesundheitsdatenschutz.org/html/pseudonymisierung_anonymisierung.php

[51] Datenschutzbehörde: GZ: DSB-D123.270/0009-DSB/2018 vom 5.12.2018. [Online, zitiert am 2019-10-01]; Verfügbar unter https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT_20181205_DSB_D123_270_0009_DSB_2018_00/DSBT_20181205_DSB_D123_270_0009_DSB_2018_00.html

Patientendaten auch Daten von noch lebenden Personen beinhalten können (z. B. erbliche Erkrankungen), für die die DS-GVO immer noch gilt.

Weiterhin können Mitgliedstaaten Regelungen bzgl. des Umgangs mit den Daten Verstorbener erlassen. Der deutsche Gesetzgeber entfernte jedoch bei der Überarbeitung des BDSG den Schutz Verstorbener, desgleichen geschah beim dem Berliner Datenschutz-Anpassungs- und Umsetzungsgesetz EU. Grundsätzlich kann in bereichsspezifischen Gesetzen sowohl vom Bundes- wie auch vom Landesgesetzgeber der Umgang mit den Daten Verstorbener geregelt werden. Im Bereich von klinischen Registern muss daher immer auch die Überarbeitung der landesrechtlichen Vorgaben für Krankenhäuser beobachtet und auf Regelungen bzgl. des Umgangs mit Daten Verstorbener geprüft werden. Eine bundeseinheitliche Regelung ist leider nicht in Sicht, so dass in einem Bundesland etwas erlaubt, derselbe Tatbestand in einem anderen Bundesland verboten sein kann.

§ 7 Abs. 1 S. 3 HmbKHG lautet beispielsweise: „Der Datenschutz endet nicht mit dem Tode der Patientin oder des Patienten."

12.7.2 Straf- und berufsrechtliches Offenbarungsverbot bei Toten

Weder die ärztliche Schweigepflicht nach § 9 MBO-Ä noch die aus § 203 StGB endet mit dem Tod des Patienten: Die gesetzliche Schweigepflicht gilt auch über den Tod des Betroffenen hinaus[52]. Auch ist nach dem Tod des Patienten eine mutmaßliche Einwilligung ausgeschlossen, da eine mutmaßliche Einwilligung immer voraussetzt, dass die Person in der Lage ist, die Einwilligung zu erteilen[53]. Weiterhin ist ein Übergang auf die Erben kraft Erbrechts regelmäßig ausgeschlossen, da die Verfügungsbefugnis höchstpersönlicher Natur und daher mit dem Tod des Berechtigten erlischt.[54]

12.8 Genetische Daten und Einwilligung

Biomaterial enthält prinzipiell immer auch Daten über verwandte Personen wie beispielsweise Kinder, Eltern, Enkel. Im Rahmen der Vorgabe der DS-GVO kann eine Einwilligung immer nur für die eigenen Daten, nicht aber für die Daten Dritter gegeben werden kann. Zugleich ist eine Anonymisierung nicht möglich, da genetische Daten immer den eindeutigen Code für die betroffene Person beinhalten; bestenfalls eine Pseudonymisierung scheint realisierbar zu sein.

Gibt eine Person heute beispielsweise Biomaterial ab, so kann ein heute noch nicht geborenes Enkelkind aufgrund der Kenntnis dieses gespendeten Biomaterials in der Zukunft durch eine Erkrankung diskriminiert werden, die heute noch gar nicht bekannt ist, die aber dem Erbgut innewohnt. Weiterhin liegt für die Verarbeitung der Daten jedoch auch kein Erlaubnistatbestand zugrunde.

Daher wird für die Verarbeitung derartiger personenbezogener bzw. personenbeziehbarer Daten ein gesetzlicher Erlaubnistatbestand benötigt, wenn seitens der Gesellschaft ein Konsens besteht, dass die Vorratsdatenspeicherung von Biomaterial mit recht allgemeiner Zweckbindung („medizinische Forschung") gewünscht ist. Hier ist der nationale Gesetzgeber gefragt, im Rahmen der Öffnungsklausel von Art. 9 Abs. 4 DS-GVO tätig zu werden.

[52] Kargl § 203 Rn. 10 in Kindhäuser / Neumann / Paeffgen (Hrsg.) Strafgesetzbuch. 5. Auflage 2017. ISBN 978-3-8487-3106-0

[53] Kargl § 203 Rn. 63 in Kindhäuser / Neumann / Paeffgen (Hrsg.) Strafgesetzbuch. 5. Auflage 2017. ISBN 978-3-8487-3106-0

[54] Lenckner/Eisele § 203 StGB Rn. 25. In: Schönke/Schröder (Hrsg.) Strafgesetzbuch. 29. Aufl. 2014. ISBN 978-3-406-65226-4

12.9 Datenschutz- und IT-Sicherheitskonzept

Datenschutz und IT-Sicherheit nutzen ähnliche Begrifflichkeiten:

Datenschutz (Art. 32)	IT-Sicherheit	Deutsche Begriffe
Confidentiality	Confidentiality	Vertraulichkeit
Integrity	Integrity	Integrität
Availability	Availability	Verfügbarkeit
Resilience	Business Continuity/ Business Resilience	Belastbarkeit vs. Ausfallsicherheit, Geschäftsbeständigkeit

Bei der Betrachtung von Schutzobjekt und Angreifermodell sieht man jedoch Unterschiede. Aus Sicht der IT-Sicherheit ist die betroffene Person der (potentielle) Angreifer auf die Daten der Organisation resp. des Unternehmens, beim Datenschutz ist (u.a.) die Organisation resp. das Unternehmen Angreifer auf die personenbezogenen Daten der betroffenen Person, z. B. durch eine rechtswidrige Zweckänderung. Eine Gegenüberstellung der Schutzziele zeigt daher die Unterschiede auf:

	Datenschutz	IT-Sicherheit
Was wird geschützt?	Schutz personenbezogener Daten	Schutz aller (Unternehmens-) Daten
Schutzziele	Schutz der informationellen Selbstbestimmung im Interesse der Betroffenen	Schutz von Daten im Interesse des Unternehmens/des Verantwortlichen
Wovor wird geschützt?	Schutz vor Datenmissbrauch und –pannen	Schutz vor (aus Unternehmenssicht) unbefugter Veränderung, Löschung/Zerstörung ...
Rechtliche Grundlage	Datenschutzrecht (DS-GVO, BDSG, LKHG, …)	Unternehmensrecht (KonTraG, Aktiengesetz, GmbH-Gesetz, HGB, …)
Wie wird geschützt?	Technische und organisatorische Maßnahmen	Technische und organisatorische Maßnahmen

Datenschutz und IT-Sicherheit nutzen zur Erreichung ihrer Ziele dabei die gleichen Werkzeuge wie z. B. ein Berechtigungskonzept. Jedoch hat der Datenschutz einen anderen Fokus als IT-Sicherheit: das eine schützt die Sicherheit der Daten betroffener Personen, das andere schützt die Daten des Unternehmens – beides kann identisch sein, muss es aber nicht. So gibt es beispielsweise auch Unterschiede beim Umgang mit den technischen und organisatorischen Maßnahmen, was am Beispiel der Protokollierung dargestellt wird:

Datenschutz	IT-Sicherheit
„Du darfst nur protokollieren, was für den jeweiligen Verwendungszweck erforderlich ist, also nur das absolut Notwendige“	„Ich muss alles protokollieren. Nur so kann ich herausfinden, was passierte und künftigen Vorfällen vorbeugen“
„Protokolle müssen nach 6 Monaten gelöscht werden, spätestens nach 1 Jahr“	„Protokolle muss ich aufbewahren. Mitunter wird ein Vorfall erst nach Monaten oder Jahren bemerkt und dann muss ich rekonstruieren können, was passierte“
Sicherheitsvorfälle werden dokumentiert und ggf. an die Datenschutz-Aufsicht gemeldet; ein Prozess zur Gewährleistung muss etabliert werden	Sicherheitsvorfälle werden dokumentiert und ggf. ans BSI gemeldet; ein Prozess zur Gewährleistung muss etabliert werden

Datenschutzkonzept und IT-Sicherheitskonzept ergänzen sich daher, aber es gibt auch Abgrenzungen:

Datenschutzkonzept	IT-Sicherheitskonzept
Alle notwendigen Informationen für die datenschutzrechtliche Beurteilung der Verarbeitung personenbezogener Daten, z. B. – Art und Umfang der Daten – Rechtmäßigkeit der Verarbeitung	Alle (notwendigen) Informationen, unabhängig ob personenbezogen oder nicht, die zur Gewährleistung der Informationssicherheit benötigt werden
Digitale und analoge Verarbeitung	Digitale und analoge Verarbeitung

Um die von der DS-GVO geforderte Sicherheit der Verarbeitung zu gewährleisten, wird beides benötigt: Datenschutz- und IT-Sicherheitskonzept. Dies heißt aber nicht, dass zwei Papiere existieren müssen: In einer Beschreibung können die Gemeinsamkeiten zusammen beschrieben werden, ergänzend in den jeweiligen Abschnitten die Besonderheiten von Datenschutz- und IT-Sicherheitskonzept dargestellt werden. Im Hinblick auf die Erstellung von Datenschutz- und IT-Sicherheitskonzepten wird hier auf zwei vertiefende Leitfäden der GMDS verwiesen[55].

[55] GMDS, ZTG: „Leitfaden für die Erstellung von Datenschutzkonzepten im Gesundheitswesen“ (Stand 2016-1212). [Online, zitiert am 2019-12-10]; Verfügbar unter https://www.gesundheitsdatenschutz.org/html/datenschutzkonzept.php
Bvitg, GMDS, ZTG: Leitfaden für die Erstellung eines IT-Sicherheitskonzeptes (Stand 2017-09-29) [Online, zitiert am 2019-12-10]; Verfügbar unter https://www.gesundheitsdatenschutz.org/html/itsicherheitskonzept.php

13 Abkürzungen

Abs	Absatz
ADT	Arbeitsgemeinschaft Deutscher Tumorzentren e. V.
Art	Artikel
Artt	Artikel (Mehrzahl)
BDSG	Bundesdatenschutzgesetz
BvD	Berufsverband der Datenschutzbeauftragten Deutschlands e. V.
BVerfG	Bundesverfassungsgericht
bvitg	Bundesverband Gesundheits-IT e. V.
DKG	Deutsche Krankenhausgesellschaft e. V.
DSFA	Datenschutz-Folgenabschätzung
DSG	Datenschutzgesetz
DSK	Datenschutzkonferenz
DS-GVO	Datenschutz-Grundverordnung
EDPB	European Data Protection BOARD (=EDSA)
EDSA	Europäischer Datenschutz-Ausschuss (= EDPB)
EDV	Elektronische Datenverarbeitung
ENISA	Europäische Agentur für Netz-und Informationssicherheit (European Union Agency for Cybersecurity)
ErwGr	Erwägungsgrund/Erwägungsgründe
EU	Europäische Union
GDD	Gesellschaft für Datenschutz und Datensicherheit e. V.
GEKID	Gesellschaft der Epidemiologischen Krebsregister in Deutschland
GG	Grundgesetz
GMDS	Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V.
IT	Informationstechnik, informationstechnisches…
Kap	Kapitel
LDSG	Landesdatenschutzgesetz
LKG	Landeskrankenhausgesetz
lit	littera (lat. „Buchstabe“)
LKHG	Landeskrankenhausgesetz
Ziff	Ziffer
ZTG	Zentrum für Telematik und Telemedizin GmbH

14 Ergänzende Literaturhinweise

14.1 Fachzeitschriften

1) Antes et al. (2009) Register für klinische Studien. Einführung in das Thema und Hintergründe. Bundesgesundheitsbl 52:459–462
2) Behrendt et al. (2017) Klinische Register im 21. Jahrhundert. Ein Spagat zwischen Datenschutz und Machbarkeit? Chirurg 88:944–949
3) Bestehorn K. (2005) Medizinische Register: ein Beitrag zur Versorgungsforschung. Med Klin 100: 722–728
4) Bestehorn et al. (2006) Register für klinische Studien – eine kritische Bestandsaufnahme. Med Klin 101: 120-126
5) Jacobs S, Stallmann C, Pigeot I. (2015) Verknüpfung großer Sekundär- und Registerdatenquellen mit Daten aus Kohortenstudien. Bundesgesundheitsbl 58: 822–828
6) Mathis-Edenhofer S, Piso B. (2011) Formen medizinischer Register – Definitionen, ausgewählte methodische Aspekte und Qualität der Forschung mit Registern. Wien Med Wochenschr 161/23–24: 580–590
7) Petersen et al. (2019) Sichere und datenschutzgerechte Umsetzung medizinischer Register. DuD: 507-512
8) Schraven S, Mlynski R (2019) Register – Auswertung von multizentrischen Daten. Laryngo-Rhino-Otol 98: S1–S12
9) Storf et al. (2017) Register für seltene Erkrankungen. OSSE – ein Open-Source-Framework für die technische Umsetzung. Bundesgesundheitsbl 60:523–531
10) Strangfeld A, Richter A. (2015) Wie unterstützen Registerdaten die klinische Entscheidungsfindung? Z Rheumatol 74:119–124
11) Swart E, Stallmann C, Powietzka J, March S. (2014) Datenlinkage von Primär- und Sekundärdaten. Bundesgesundheitsbl 57:180–187

14.2 Bücher

1) Karaalp RM. Der Schutz von Patientendaten für die medizinische Forschung in Krankenhäusern. Eine rechtsvergleichende Untersuchung der Regelungen in Deutschland und Frankreich. Springer Fachmedien Wiesbaden GmbH, 1. Auflage 2017. ISBN 978-3-658-16184-2
2) Lenk C, Duttge G, Fangerau H. (Hrsg.) Handbuch Ethik und Recht der Forschung am Menschen. Springer-Verlag Berlin Heidelberg, 1. Auflage 2014. ISBN 978-3-642-35098-6
3) Reimer F. Die Forschungsverfügung. Eine Untersuchung zu antizipierten Verfügungen in der Humanforschung unter besonderer Berücksichtigung der Arzneimittelforschung mit Demenz- und Notfallpatienten. Springer-Verlag Berlin Heidelberg, 1. Auflage 2017. ISBN 978-3-662-53261-4
4) Weigel J. Das Biobankgeheimnis. Tectum Baden-Baden, 1. Auflage 2018. ISBN 978-3-8288-3990-8

Anhang 1. Liste von klinischen Registern in Deutschland

Das Deutsche Register Klinischer Studien (DRKS) ist für die Registrierung aller in Deutschland durchgeführten patientenorientierten klinischen Studien zuständig.[56]

Anhang 1.1. Beispiele für gesetzlich geregelte klinische Register

Register	Gesetzliche Regelung	Fundort im Internet
Hämophilieregister	Hämophilieregister-Verordnung (DHRV)	http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl119s0744.pdf
Implantateregister	Implantateregister-Errichtungsgesetz (EIRD) (Gesetzesentwurf)	http://dip21.bundestag.de/dip21/btd/19/105/1910523.pdf
Samenspenderregister	Samenspenderregistergesetz	https://www.gesetze-im-internet.de/saregg/index.html
Krebsregister	Bundeskrebsregisterdatengesetz (BKRG)	http://www.gesetze-im-internet.de/bkrg/
Landeskrebsregister Baden-Württemberg	Gesetz über die Krebsregistrierung in Baden-Württemberg (Landeskrebsregistergesetz - LKrebsRG)	http://www.landesrecht-bw.de/jportal/?quelle=jlink&query=KrebsRegG+BW&psml=bsbawueprod.psml&max=true
Landeskrebsregister Bayern	Bayerisches Krebsregistergesetz (BayKRegG)	https://www.gesetze-bayern.de/Content/Document/BayKRegG/true?AspxAutoDetectCookieSupport=1
Landeskrebsregister Berlin	Staatsvertrag zwischen dem Land Berlin und dem Land Brandenburg über die Einrichtung und den Betrieb eines klinischen Krebsregisters nach § 65c des Fünften Buches Sozialgesetzbuch	http://gesetze.berlin.de/jportal/?quelle=jlink&query=KlKrebsRegBE%2FBBStVtr+BE&psml=bsbeprod.psml&max=true
Landeskrebsregister Brandenburg	Gesetz zur Änderung des Staatsvertrages über das Gemeinsame Krebsregister der Länder Berlin, Brandenburg, Mecklenburg-Vorpommern, Sachsen-	https://bravors.brandenburg.de/gesetze/krebsregisterstv_g_2017

[56] Deutsches Register Klinischer Studien (DRKS). [Online, zitiert am 2019-11-11]; Verfügbar unter https://www.drks.de bzw. beim DIMDI unter https://www.dimdi.de/dynamic/de/weitere-fachdienste/deutsches-register-klinischer-studien/

Register	Gesetzliche Regelung	Fundort im Internet
	Anhalt und der Freistaaten Sachsen und Thüringen	
Landeskrebsregister Bremen	Gesetz über das Krebsregister der Freien Hansestadt Bremen (Krebsregistergesetz - BremKRG)	https://www.transparenz.bremen.de/vorschrift_detail/bremen2014_tp.c.126648.de
Landeskrebsregister Hamburg	Hamburgisches Krebsregistergesetz (HmbKrebsRG)	http://www.landesrecht-hamburg.de/jportal/portal/page/bshaprod.psml?doc.id=jlr-KrebsRegGHArahmen&st=lr&doctyp=BSBayern&showdoccase=1&paramfromHL=true#focuspoint
Landeskrebsregister Hessen	Hessisches Krebsregistergesetz	https://www.rv.hessenrecht.hessen.de/bshe/document/VB-HE-AD-GVBl2014-18-241
Landeskrebsregister Mecklenburg-Vorpommern	Gesetz über die Krebsregistrierung in Mecklenburg-Vorpommern (Krebsregistrierungsgesetz - KrebsRG M-V)	http://www.landesrecht-mv.de/jportal/portal/page/bsmvprod.psml?nid=0&showdoccase=1&doc.id=jlr-KrebsRGMVrahmen&st=lr
Landeskrebsregister Niedersachsen	Gesetz über das Klinische Krebsregister Niedersachsen (GKKN)	http://www.nds-voris.de/jportal/?quelle=jlink&query=KlKrebsRegG+ND&psml=bsvorisprod.psml&max=true
Landeskrebsregister Nordrhein-Westfalen	Gesetz über die klinische und epidemiologische Krebsregistrierung im Land Nordrhein – Westfalen (Landeskrebsregistergesetz - LKRG NRW)	https://recht.nrw.de/lmi/owa/br_bes_text?sg=0&menu=1&bes_id=34084&aufgehoben=N&anw_nr=2
Landeskrebsregister Rheinland-Pfalz	Landeskrebsregistergesetz (LKRG)	http://landesrecht.rlp.de/jportal/?quelle=jlink&query=KrebsRegG+RP&psml=bsrlpprod.psml
Landeskrebsregister Saarland	Saarländisches Krebsregistergesetz (SKRG)	http://sl.juris.de/cgi-bin/landesrecht.py?d=http://sl.juris.de/sl/KrebsRegG_SL_2015_rahmen.htm
Landeskrebsregister Sachsen	Staatsvertrag über das Gemeinsame Krebsregister der Länder Berlin, Brandenburg, Mecklenburg-Vorpommern, Sachsen-Anhalt und der Freistaaten Sachsen und Thüringen	https://www.revosax.sachsen.de/vorschrift/5369-StV-Gemeinsames-Krebsregister
Landeskrebsregister	Gesetz zum Staatsvertrag über das	http://www.landesrecht.sachsen-

Register	Gesetzliche Regelung	Fundort im Internet
Sachsen-Anhalt	Gemeinsame Krebsregister der Länder Berlin, Brandenburg, Mecklenburg-Vorpommern, Sachsen-Anhalt und der Freistaaten Sachsen und Thüringen	anhalt.de/jportal/?quelle=jlink&query=KrebsRegBEuaStVtrG+ST&psml=bssahprod.psml&max=true
Landeskrebsregister Schleswig-Holstein	Gesetz über das Krebsregister des Landes Schleswig-Holstein (Krebsregistergesetz - KRG SH)	http://www.gesetze-rechtsprechung.sh.juris.de/jportal/?quelle=jlink&query=LKRG+SH&psml=bsshoprod.psml&max=true
Landeskrebsregister Thüringen	Thüringer Gesetz zu dem Staatsvertrag über das Gemeinsame Krebsregister der Länder Berlin, Brandenburg, Mecklenburg-Vorpommern, Sachsen-Anhalt und der Freistaaten Sachsen und Thüringen	http://landesrecht.thueringen.de/jportal/?quelle=jlink&query=KrebsRegBEuaStVtrG+TH&psml=bsthueprod.psml&max=true

Anhang 1.2. Beispiele für nicht gesetzlich geregelte klinische Register

Register	Gründer/Fachgesellschaft	Fundort im Internet
Traumaregister	Akademie der Unfallchirurgie GmbH	http://www.traumaregister-dgu.de
MDS Register	Gesellschaft für Medizinische Innovation – Hämatologie und Onkologie mbH	http://www.mds-register.de/
Deutsches Hepatitis C-Register	Leberstiftungs-GmbH Deutschland	http://www.deutsches-hepatitis-c-register.de/
RABBIT-SpA	Deutsches Rheuma-Forschungszentrum	https://rabbit-spa.de/
B_2HIR	Berlin-Brandenburger Herzinfarktregister e. V.	https://herzinfarktregister.de
DMD- und SMA-Patientenregister	Friedrich-Baur-Institut Klinikum der Universität München	https://www.treat-nmd.de/register/index.de.html
FKRP-Patientenregister	Friedrich-Baur-Institut Klinikum der Universität München	https://www.fkrp-registry.org/index.de.html
Register Morbus Adamantiades-Behçet	Deutsches Register Morbus Adamantiades-Behçet e.V.	http://www.behcet.de/
Zentralregisters Kutane Lymphome	Deutsche Dermatologische Gesellschaft (DDG)	http://www.ddg-lymphomregister.de/
Deutsches Reanimationsregister	Deutsche Gesellschaft für Anästhesiologie und Intensivmedizin e.V.	https://www.reanimationsregister.de/
Deutsches Qualitätsbündnis Sepsis - DQS	Universitätsklinikum Jena	https://www.uniklinikum-jena.de/dqs
Deutsches Wirbelsäulenregister	Deutsche Wirbelsäulengesellschaft DWG e.V.	https://dwg.memdoc.org/
Multiple Sklerose Register	MS Forschungs- und Projektenwicklungs-gGmbH	https://www.msregister.de/

Anhang 2. DS-GVO Checkliste

	Ja	Nein	Nachweis vorhanden und überprüfbar
(Verarbeitungs-) Zweck des klinischen Registers beschrieben?			
Lässt sich die Erforderlichkeit aller verarbeiteten Daten aus dem Zweck ableiten und wurde dies dokumentiert?			
Ist die Rechtsgrundlage für die Verarbeitung geklärt und dokumentiert?			
Wird „Broad Consent“ genutzt? Wenn ja: Sind alle Voraussetzungen erfüllt und insbesondere entsprechende technische und organisatorische Maßnahmen vorhanden?			
Sind alle Betroffenenrechte berücksichtigt worden?			
Existiert ein Informationsschreiben, welches alle gesetzlich geforderten Informationen enthält und ist ein Prozess etabliert und dokumentiert, welcher gewährleistet, dass jede Person dieses Schreiben erhält?			
Ist ein Prozess etabliert und dokumentiert, welcher den Umgang mit Auskunftsanfragen regelt?			
Ist ein Prozess etabliert und dokumentiert, welcher den Umgang mit Anfragen bzgl. Korrektur der Daten regelt?			
Ist ein Prozess etabliert und dokumentiert, welcher den Umgang mit einem Widerspruch bzgl. der Verarbeitung personenbezogener Daten regelt?			
Ist ein Prozess etabliert und dokumentiert, welcher den Umgang mit Aufforderungen zur Einschränkung der Verarbeitung („Sperrung“) regelt?			
Ist ein Prozess etabliert und dokumentiert, welcher den Umgang mit Löschanfragen regelt?			
Ist ein Prozess etabliert und dokumentiert, welcher den Umgang mit Anfragen bzgl. der Wahrnehmung des Rechts auf Datenübertragbarkeit regelt?			
Existiert ein Verzeichnis der Verarbeitungstätigkeiten?			
Sind alle Auftragsverarbeiter gelistet und existieren die erforderlichen Verträge?			
Sind alle Auftragsverarbeiter ggf. vertraglich verpflichtet, die berufliche Schweigepflicht und das strafrechtliche Offenbarungsverbot einzuhalten?			
Sind die Anforderungen bzgl. der Sicherheit der Verarbeitung erfüllt?			
Ist Privacy by Design für das klinische Register berücksichtigt und kann nachgewiesen werden?			
Ist Privacy by Default für das klinische Register			

	berücksichtigt und kann nachgewiesen werden?			
	Wurde die Notwendigkeit bzgl. einer DSFA geprüft und das Ergebnis festgehalten? Wurde bei positivem Ergebnis eine DSFA durchgeführt?			
	Wurde der Lebenszyklus der Daten beschrieben? Inklusive Löschzeitpunkt?			
	Existiert ein Datenschutzkonzept? Wenn nein: Wurde nachvollziehbar dargelegt und dokumentiert, warum dies nicht erforderlich ist?			
	Existiert ein Berechtigungskonzept für den Zugriff auf die Daten? Wenn nein: Wurde nachvollziehbar dargelegt und dokumentiert, warum dies nicht erforderlich ist?			
	Existiert ein Archivierungskonzept? Wenn nein: Wurde nachvollziehbar dargelegt und dokumentiert, warum dies nicht erforderlich ist?			
	Existiert ein Löschkonzept? Wenn nein: Wurde nachvollziehbar dargelegt und dokumentiert, warum dies nicht erforderlich ist?			
	Existiert ein IT-Sicherheitskonzept? Wenn nein: Wurde nachvollziehbar dargelegt und dokumentiert, warum dies nicht erforderlich ist?			
	Existiert ein Backupkonzept? Wenn nein: Wurde nachvollziehbar dargelegt und dokumentiert, warum dies nicht erforderlich ist?			
	Existiert ein Protokollierungskonzept? Wenn nein: Wurde nachvollziehbar dargelegt und dokumentiert, warum dies nicht erforderlich ist?			
	Sind interne Audits zur Überprüfung der Einhaltung der Vorgaben der DS-GVO vorgesehen? Existiert ein Zeitplan und werden die Audits dokumentiert?			
	Sind externe Audits zur Überprüfung der Einhaltung der Vorgaben der DS-GVO vorgesehen? Existiert ein Zeitplan und werden die Audits dokumentiert?			
Erfolgt eine Verarbeitung in einem Drittstaat?				
	Existiert für die Verarbeitung im Drittstaat eine Grundlage aus Kap. V der DS-GVO?			
	Ist dies dokumentiert?			
Ist der Umgang mit Datenpannen geregelt?				
	Werden alle Datenpannen dokumentiert?			
	Ist der Prozess bzgl. Meldung an die Aufsichtsbehörden etabliert und dokumentiert?			
	Ist der Prozess bzgl. Meldung an die betroffene Person etabliert und dokumentiert?			
Ist bei Publikationen und Veröffentlichungen gewährleistet, dass keine personenbezogenen Daten i.S.v. Art. 4 Abs. 1 DS-GVO enthalten sind?				