Datenschutzrechtliche Anforderungen an die medizinische Forschung unter Berücksichtigung der EU Datenschutz-Grundverordnung (DS-GVO)

Eine Zusammenarbeit von

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

Arbeitsgruppe „Datenschutz und IT-Sicherheit im Gesundheitswesen“

Gesellschaft für Datenschutz und Datensicherheit e. V.

Arbeitskreis „Datenschutz und Datensicherheit im Gesundheits- und Sozialwesen“

Autoren

Holger Koch	Fachberater für Datenschutz und Datensicherheit
Bernd Schütze	Deutsche Telekom Healthcare and Security GmbH
Gerald Spyra	Kanzlei Spyra
Marina Wefer	Konzerndatenschutzbeauftragte Rhön-Klinikum AG

Stand: 16.05.2017

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:

Inhalt

1 Einleitung - Das Ziel dieser Ausarbeitung

Grundsätzlich ist die Freiheit der Forschung als Grundrecht normiert. Im deutschen Recht findet sich dieses Grundrecht in Art. 5 des deutschen Grundgesetzes (GG). Im europäischen Recht in der Europäischen Grundrechtecharta (EuGRC) in Art. 8. Forschung kommt eine Grundrechtsrelevanz u.a. deshalb zu, weil sie letzten Endes für Fortschritt steht, der dem Menschen oder einer bestimmten Personengruppe zu Gute kommen soll. Weil Forschung eng mit dem Begriff „Fortschritt“ gekoppelt und Fortschritt eine wesentliche Bedingung für die Weiterentwicklung der Menschheit aber auch für den nachhaltigen wirtschaftlichen Erfolg ist, kommt der Forschung neben der Bedeutung für die Menschheit oftmals auch eine nicht unerhebliche wirtschaftliche Relevanz zu.

Medizinische Forschung stellt im Rahmen der sonstigen Forschungsbereiche dahingehend einen Sonderfall dar, als dass das beforschte „Objekt“ (z. B. Erforschung einer bestimmten Krankheit) häufig zugleich mit einer Person (dem Subjekt) verbunden ist. Aufgrund der möglichen Eingriffsintensität durch Forschung sind daher die (Grund-) Rechte des Individuums besonders zu beachten. Forschungsfreiheit ist daher nicht schrankenlos. Vielmehr setzen insbesondere etwa die Würde (Art. 1 GG) wie auch das Persönlichkeitsrecht (Art. 2 GG) des jeweiligen Individuums der Forschungsfreiheit Grenzen. Aus diesem Grund gilt es besonders im Bereich der medizinischen Forschung die konkurrierenden Grundrechte bzw. Interessen der Beteiligten im jeweiligen Einzelsachverhalt umfassend zu beleuchten und in einen angemessenen und gerechten Ausgleich zu bringen. In diesem Zusammenhang helfen die forschungsbezogenen Datenschutzgesetze weiter. Diese ziehen durch ihre forschungsbezogenen Regelungen einen (groben) Rahmen für die erlaubte Nutzung medizinischer, personenbezogener Daten.

Unzweifelhaft sind die gesellschaftlich und politisch gewünschten Fortschritte in der Medizin, beispielsweise in der Behandlung von Schlaganfallpatienten oder der von Demenzkranken, nur möglich, wenn im Bereich der medizinischen Versorgung forschende Wissenschaftler - seien es Ärzte, Biologen oder Forscher einer anderen Disziplin - über umfangreiche, aussagekräftige und qualitativ gute Daten von Patienten verfügen. Zur Auswertung dieser Daten ist der Einsatz von moderner Informations- und Kommunikationstechnik unumgänglich. Die Informations- und Kommunikationstechnik (IKT) entwickelt sich rapide. Diese Entwicklung, die stetig zunehmende und für Forschungszwecke zur Verfügung stehende Datenmenge sowie die immer umfangreicheren Datenauswertungsmöglichkeiten haben damit auch einen entsprechenden Einfluss auf die medizinische Forschung.

Die eindrucksvolle Entwicklung der IKT und die damit verbundenen Fortschritte in der Datenverarbeitung, aber auch die mit der Entwicklung der IKT einhergehenden Konsequenzen für die betroffenen Personen, lassen sich eindrucksvoll anhand des 1990 gegründeten „Humangenomprojekts“ verdeutlichen. Dieses Projekt hatte zum Ziel, das Genom eines Menschen vollständig zu entschlüsseln. Die Kosten für das Gesamtprojekt waren aufgrund des hohen Datenverarbeitungsaufwands und der begrenzten Datenverarbeitungsmöglichkeiten mit 3 Milliarden Dollar veranschlagt. 2003 wurde das Ziel erreicht: Die vollständige Sequenzierung des Genoms war abgeschlossen. 2012, nicht einmal 10 Jahre später, ist die vollständige Sequenzierung des menschlichen Erbguts aufgrund der Fortschritte im Bereich der Informationstechnologie für unter 1000 Dollar in weniger als 24 Stunden möglich. Damit eröffnen sich im Bereich der Genomforschung völlig neue, vorher noch nie dagewesene Möglichkeiten im Bereich der individualisierten, personalisierten Therapie. Zugleich steigen mit der Menge der Daten, die für die Forschung zur Verfügung stehen, aber ebenso die Möglichkeiten der Re-Identifizierbarkeit, z. B. anhand der

Genomdaten und damit die Risiken bzgl. der Verletzung von Persönlichkeitsrechten der jeweils betroffenen Personen.

Zusammenfassend erleichtert daher der vorstehend beschriebene technische Fortschritt auf der einen Seite die Forschung. Auf der anderen Seite bedeuten die umfassenden modernen Datenverarbeitungsmöglichkeiten natürlich auch gestiegene Risiken u.a. für die Persönlichkeitsrechte der Menschen, deren Daten die Forschung ermöglichen. Damit steht insbesondere der Schutz personenbezogener Daten in der medizinischen Forschung vor ganz neuen Herausforderungen und kommt mit bisher noch nicht gestellten Fragestellungen einher. Nach der Vorstellung des Europäischen Gesetzgebers soll die neue und im Jahre 2018 europaweit geltende Datenschutz-Grundverordnung (DS-GVO) auch für den Forschungsbereich Antworten auf diese Fragestellungen liefern.

Um den gesellschaftlich und politisch erwünschten Forschungsinteressen Rechnung zu tragen, privilegiert die DS-GVO die Möglichkeiten der Nutzung personenbezogener Daten für diese Zwecke. So stellt etwa die Verarbeitung zu Forschungszwecken nach dem Willen des europäischen Gesetzgebers grundsätzlich keine Zweckänderung dar, die eines separaten Rechtfertigungsgrunds bedarf. Vielmehr geht die DS-GVO davon aus, dass die Datenverarbeitung zu Forschungszwecken, grundsätzlich als mit dem ursprünglichen Zweck, zu dem die Daten erhoben wurden, vereinbar gilt.

Um trotz dieses (Forschungs-) Privilegs dem aus der Grundrechtecharta resultierenden Schutz der Menschenwürde und des Persönlichkeitsrechts gerecht zu werden, stellt die DS-GVO entsprechende Anforderungen an den Schutz der besonders sensiblen personenbezogenen Daten wie Gesundheitsdaten oder genetische Daten, welche gerade bei der medizinischen Forschung verarbeitet werden müssen.

Dabei trägt die DS-GVO auch der Tatsache Rechnung, dass hochwertige medizinische Forschung oftmals die institutionsübergreifende und manchmal auch länderübergreifende Zusammenarbeit erfordert. Grundsätzlich kann deshalb nach dem Willen des Gesetzgebers die zur Forschung erforderliche Datenverarbeitung in jedem EU-Mitgliedsstaat erfolgen. Bei der Verarbeitung außerhalb der EU (sogenannte „Drittländer“) müssen jedoch, aufgrund des damit einhergehenden erhöhten Risikos für den Betroffenen, besondere Anforderungen beachtet werden.

Im Zusammenhang mit den in der DS-GVO enthaltenen Regelungen muss man jedoch berücksichtigen, dass einige dieser Regelungen (für Nicht-Juristen) oftmals schwierig zu lesen und zu interpretieren sind.

Ziel dieser Ausarbeitung ist es daher, sowohl den forschenden Personen als auch den jeweiligen Datenschutzbeauftragten in den forschenden Einrichtungen eine Handlungsempfehlung für den Umgang mit datenschutzrechtlichen Anforderungen an die Hand zu geben. Insbesondere will das vorliegende Dokument aufzeigen, welche datenschutzrechtlichen Rahmenbedingungen von den Forschern mindestens beachtet werden müssen, damit einerseits die Daten der beforschten Personen sicher sind, andererseits auch den jeweils entsprechend dargestellten rechtlichen Rahmenbedingungen genügt wird.

Die Autoren thematisieren in diesem Dokument die ihnen bekannten wesentlichen und für den Forschungsbereich relevanten Fragestellungen und versuchen diese so umfassend wie möglich zu beleuchten. Aufgrund der Komplexität dieses Themas kann die vorliegende Ausarbeitung jedoch nicht alle Themenbereiche abdecken. Somit kann es durchaus vorkommen, dass auch nach Lektüre dieser Ausarbeitung, die eine oder die andere Frage offen bleibt. In diesem Fall stehen dem Forscher verschiedene Möglichkeiten offen, um auf die spezielle Frage eine Antwort zu erhalten: er kann sich

mit dem für ihn zuständigen Datenschutzbeauftragten beraten, weitere Literatur zu Rate ziehen, sich mit anderen Forschern oder zuständigen Institutionen austauschen oder sich an die Datenschutzaufsichtsbehörden wenden. Aber gerne kann er auch die Autoren dieser Ausarbeitung kontaktieren.

2 Abgrenzung

Grundsätzlich dient die Verarbeitung von Patientendaten im Krankenhaus der ärztlichen Versorgung sowie der Behandlungsdokumentation. Darüber hinaus ist der Wissensgewinn aus einer erfolgreichen Behandlung für künftige Behandlungen, auch über das eigene Krankenhaus hinaus, durchaus wünschens- und erstrebenswert. Aus diesem Grunde sollen an dieser Stelle die datenschutzrechtlichen Aspekte und die neuen gesetzlichen Regelungen in der EU zum Thema Forschung besprochen werden.

Der strafrechtliche Aspekt der weiteren Nutzung von Patientendaten zu Forschungszwecken wird hier nicht umfassend thematisiert. Vielmehr sollte jeder Arzt wissen, dass er die Grundregeln der ärztlichen Schweigepflicht auch unter Forschungsgesichtspunkten zu beachten hat. Das bedeutet in der Regel, dass er die Patientendaten nur mit informierter ausdrücklicher Einwilligung der Betroffenen für Forschungszwecke verwenden darf bzw. dass er sie korrekt anonymisieren muss, bevor die Daten für Forschungszwecke eingesetzt werden dürfen.

3 Die Stellung der Forschung innerhalb der Europäischen Union

3.1 Forschung als Grundrecht der EU

Das Grundrecht auf Schutz von personenbezogenen Daten ist im europäischen Recht an zwei zentralen Stellen fixiert: In Art. 8 der Europäischen Grundrechtecharta[1] (GRC) und Art. 16 Abs. 1 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV)[2].

Ähnliches gilt für die Forschung: entsprechend Art. 13 GRC ist die akademische Freiheit zu achten, gemäß Art. 168 Abs. 1 AEUV ergänzt die Tätigkeit der Union

> „die Politik der Mitgliedstaaten und ist auf die Verbesserung der Gesundheit der Bevölkerung, die Verhütung von Humankrankheiten und die Beseitigung von Ursachen für die Gefährdung der körperlichen und geistigen Gesundheit gerichtet. Sie umfasst die Bekämpfung der weit verbreiteten schweren Krankheiten, wobei die Erforschung der Ursachen, der Übertragung und der Verhütung dieser Krankheiten sowie Gesundheitsinformation und -erziehung gefördert werden [...]“

Wenngleich also auch die Forschung ein europäisches Grundrecht ist und im AEUV medizinische Forschung als ein zu fördernder Bereich angesehen wird, muss jegliche Forschung das Grundrecht auf Schutz von personenbezogenen Daten achten: ein „Forschungsvorrang“ existiert dabei nicht. Um hier das Verhältnis dieser oftmals konkurrierenden Grundrechte darzustellen, geht die DS-GVO explizit auch auf datenschutzrechtliche Anforderungen für Forschung ein.

[1] Charta der Grundrechte der Europäischen Union. Online, zitiert 2017-01-22; Verfügbar unter http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex:12016P/TXT

[2] Konsolidierte Fassung des Vertrags über die Arbeitsweise der Europäischen Union. Online, zitiert 2017-01-22; Verfügbar unter http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:12012E/TXT

3.2 Forschung als privilegierte (Daten-) Verarbeitung

Forschung spielt innerhalb der Europäischen Union eine zentrale Rolle. Dementsprechend wird die Rolle der Forschung auch im Vertrag über die Arbeitsweise der Europäischen Union gewürdigt[3]. Diesem europäischen Ansatz, dass Forschung erwünscht ist und gefördert werden soll, trägt die europäische Datenschutz-Grundverordnung (DS-GVO) Rechnung und privilegiert Verarbeitungen personenbezogener Daten zum Zwecke der Forschung an unterschiedlichen Stellen.

Insbesondere enthält die DS-GVO privilegierende Bestimmungen für wissenschaftliche und historische Forschungszwecke, was zur Folge hat, dass festgelegt werden muss, was „wissenschaftliche Forschung" und was „historische Forschung" eigentlich ist.

4 Grundlegende Begriffsbestimmungen

Aufgrund der mannigfaltigen in der DS-GVO zu findenden datenschutzrechtlichen Begrifflichkeiten für den Bereich „Forschung" ist es essenziell, die Bedeutung der Begrifflichkeiten darzustellen, d.h. Begriffsbestimmungen aus datenschutzrechtlicher Sicht vorzunehmen.

4.1 Was ist „Forschung" aus Sicht der DS-GVO?

Der Begriff „Forschung" wird in der DS-GVO selbst nicht definiert. Jedoch vermitteln einige Erwägungsgründe eine Vorstellung, was der europäische Gesetzgeber unter „Forschung" versteht

- Studien, die im öffentlichen Interesse im Bereich der öffentlichen Gesundheit durchgeführt werden (Erwägungsgründe 53, 159)
- Klinische Prüfungen (Erwägungsgrund 156)
- Register (Erwägungsgrund 157)
- Verbesserung der Lebensqualität zahlreicher Menschen (Erwägungsgrund 157)
- Verbesserung der Effizienz der Sozialdienste (Erwägungsgrund 157)
- Grundlagenforschung (Erwägungsgrund 159)
- Angewandte Forschung (Erwägungsgrund 159)
- Privat finanzierte Forschung (Erwägungsgrund 159)

Entsprechend lautet die Definition von Forschung wie folgt:

> *„**Forschung** ist die systematische Suche nach neuen Erkenntnissen sowie deren Dokumentation und Veröffentlichung, wobei Suche sowohl im Bereich der Grundlagenforschung als auch der angewandten Forschung erfolgen kann. Die Ergebnisse der Suche müssen darauf abzielen, dass die Erkenntnisse*
>
> *a) dem öffentlichen Interesse im Bereich der öffentlichen Gesundheit dienen oder*
> *b) der Verbesserung der Lebensqualität zahlreicher Menschen oder der Verbesserung der Effizienz der Sozialdienste dienen oder*
> *c) der klinischen Prüfung therapeutischer Maßnahmen dienen oder*
> *d) der Registerforschung dienen.*
>
> *Die privat finanzierte Forschung ist dabei der öffentlichen Forschung gleichgestellt."*

[3] Vgl. Art. 179 Abs. 1 AEUV (Teil XIX „Forschung, technologische Entwicklung und Raumfahrt"): „Die Union hat zum Ziel, ihre wissenschaftlichen und technologischen Grundlagen dadurch zu stärken, dass ein europäischer Raum der Forschung geschaffen wird […]"

4.2 Was ist „wissenschaftliche Forschung“ aus Sicht der DS-GVO?

Die wissenschaftliche Forschung ist ein spezieller Bereich der Forschung. Im „Hochschul-Urteil[4]“ definierte das Bundesverfassungsgericht: „[…] wissenschaftliche Tätigkeit, d. h. auf alles, was nach Inhalt und Form als ernsthafter planmäßiger Versuch zur Ermittlung der Wahrheit anzusehen ist. […]“.Gemäß vorstehender Ausführungen und unter Berücksichtigung des Urteils des BVerfG lässt sich „wissenschaftliche Forschung“ daher wie folgt definieren:

> *„**Wissenschaftliche Forschung** ist Forschung, die sowohl nach Inhalt als auch der Form entsprechend als ernsthafter planmäßiger Versuch zur Ermittlung der Wahrheit anzusehen ist.“*

4.3 Was ist „historische Forschung“ aus Sicht der DS-GVO?

Historische Forschung ist die methodisch gesicherte Erforschung von Aspekten der Vergangenheit basierend auf einer methodisch gesicherten Analyse bekannter Tatsachen vergangener Epochen unter einer spezifischen Fragestellung durch wissenschaftlich anerkannte Methoden. Dies bedingt insbesondere, dass die Voraussetzungen für das Forschungsergebnis sowie die Methoden, Gedankengänge und Ergebnisse der Forschung nach- bzw. überprüfbar sind. Die Forschung geht dabei stets prüfend und mit dem Streben nach weitgehender Objektivität vor.

Die historische Forschung ist dabei von der Archäologie abzugrenzen. Eine Möglichkeit, diese beiden Bereiche voneinander abzugrenzen, besteht darin, zu prüfen, ob eher schriftliche Zeugnisse im Mittelpunkt stehen (historische Forschung) oder schwerpunktmäßig auf nicht-schriftliche Quellen zurückgegriffen wird (Archäologie).

4.4 Wer darf forschen?

Die eigentliche Teilnahme am Wissenschaftsbetrieb ist grundsätzlich nicht an Voraussetzungen oder Bedingungen geknüpft. Vielmehr steht jedermann die wissenschaftliche Betätigung außerhalb des akademischen oder industriellen Wissenschaftsbetriebs offen[5].

Dies lässt sich ebenfalls aus Art. 5 Abs. 3 Grundgesetz aus der Regelung „Kunst und Wissenschaft, Forschung und Lehre sind frei“ ableiten. Die im Grundgesetz formulierte „Wissenschaftsfreiheit“ richtet sich mithin an jeden. Erforderlich ist jedoch stets eine eigene wissenschaftliche Tätigkeit und damit keine Mittler-, Hilfs- oder Finanzierungsfunktion.

4.5 Öffentliches Interesse

Bei dem Begriff „öffentliches Interesse“ handelt es sich um einen sog. unbestimmten Rechtsbegriff, der sich auf die Belange des Gemeinwohls bezieht. Das öffentliche Interesse ist somit zunächst vom Individualinteresse, also dem Interesse des Einzelnen, abzugrenzen. Analog zu Abschnitt 86 RiStBV[6] kann man von einem öffentlichen Interesse ausgehen, wenn

a) das Vorhaben ein gegenwärtiges Anliegen der Allgemeinheit beinhaltet oder

---

[4] BVerfG, Urteil vom 29.05.1973, AZ.: 1 BvR 424/71 bzw 1 BvR 325/72 (Hochschul-Urteil). Online, zitiert 2016-12-04; Verfügbar unter https://dejure.org/
Kommentierung siehe z.B. Epping/Lenz/Leydecker „Sachlicher Schutzbereich der Wissenschaftsfreiheit“ in Epping. Grundrechte. 6. Auflage 2015, Springer-Verlag, ISBN 978-3-642-54657-0

[5] Bundesverband für Bildung Wissenschaft und Forschung e.V. Was ist Wissenschaft? Online, zitiert 2016-12-04; Verfügbar unter https://www.bbwf.de/

[6] Richtlinien für das Strafverfahren und das Bußgeldverfahren. Abschnitt 86 – Allgemeines. Online, zitiert 2016-12-04; Verfügbar unter https://www.jurion.de/

b) das Vorhaben ein gegenwärtiges Anliegen der Allgemeinheit ist.

Bei der Beurteilung des öffentlichen Interesses stellt sich mithin die zentrale Frage: Nützt das Ergebnis des Vorhabens der Allgemeinheit?

So dürfte die Entdeckung eines Therapieansatzes für eine bestimmte Krebserkrankung sicherlich im Interesse der Allgemeinheit liegen, wenngleich die Anzahl der Erkrankten im Vergleich zum Gesamtkollektiv vergleichsweise gering ist. Jedoch lässt sich durch andere Faktoren wie z. B. dem Spendenaufkommen bei der Deutschen Krebshilfe[7] (356.228 Einzelspenden sowie 7.600 Firmenspenden mit einem Volumen von 26,2 Millionen Euro im Jahr 2015) ein entsprechendes Interesse der Allgemeinheit an der Heilung von Krebserkrankungen ableiten. Ohne die andauernde Spendenbereitschaft der Bevölkerung müsste ein anderer Nachweis für das Interesse der Allgemeinheit („Allgemeininteresse“) vorliegen bzw. erbracht werden, damit von einem „öffentlichen Interesse“ ausgegangen werden kann.

Im Allgemeinen hat das öffentliche Interesse Vorrang vor dem Individualinteresse. Jedoch gilt es auch bei diesen beiden oftmals konkurrierenden Interessen eine Abwägung vorzunehmen (sog. drittschützende Normen[8]).

Diese konkurrierenden Interessen lassen sich z. B. im datenschutzrechtlichen Umfeld darstellen. Gerade im Forschungsbereich kommt es zu einer solchen Konkurrenzsituation, bei welcher das Forschungsinteresse (Interesse der Allgemeinheit) oftmals mit dem Individualinteresse am Schutz der Daten, die sich auf den Betroffenen beziehen, kollidiert. In einem solchen Fall ist eine sachgerechte Abwägung der Interessen erforderlich.

Nicht jedes wissenschaftliche Interesse an der Durchführung eines Forschungsvorhabens hat gegenüber dem Geheimhaltungsinteresse eines Betroffenen Vorrang[9]. Vielmehr ist ein überwiegendes Forschungsinteresse nur dann gegeben, 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 (= Beachtung des Erforderlichkeitsprinzips) und der Grundrechtseingriff gegenüber der betroffenen Person nicht außer Verhältnis zu dem angestrebten Zweck steht.

Ein überwiegendes öffentliches Interesse an der Durchführung des Forschungsvorhabens kann nur dann bejaht werden, wenn verlässliche wissenschaftliche Forschungsergebnisse zu erwarten sind und das Forschungsvorhaben keinen gesetzlichen oder verfassungsrechtlichen Vorgaben widerspricht[9].

4.6 Öffentliches Interesse i. V. m. öffentlicher Gesundheit[10]

Erwägungsgrund 54 referenziert bzgl. des Begriffes „öffentliche Gesundheit“ Verordnung (EG) Nr. 1332/2008 des Europäischen Parlaments und des Rates vom 16. Dezember 2008 über Lebensmittelenzyme und zur Änderung der Richtlinie 83/417/EWG des Rates, der Verordnung (EG)

[7] deutsche Krebshilfe: Geschäftsbericht. Online, zitiert 2016-12-04; Verfügbar unter https://www.krebshilfe.de/

[8] Vgl. z.B. BVerwG, Urteil vom 24.09.1998, AZ.: 4 CN 2.98. Online, zitiert 2016-12-04; Verfügbar unter https://dejure.org/ oder auch BVerfG, Urteil vom 29.06.2016, AZ.: 1 BvR 3487/14. Online, zitiert 2016-12-04; Verfügbar unter https://www.bundesverfassungsgericht.de/

[9] Metschke R, Wellbrock R. (2002) Datenschutz in Wissenschaft und Forschung. Online, zitiert 2016-12-04; Verfügbar unter https://datenschutz-berlin.de/

[10] zitiert aus: GMDS/bvitg: Gemeinsame Empfehlung bzgl. des Umgangs mit der EU Datenschutz-Grundverordnung (DS-GVO) im Gesundheitswesen. Online, zitiert 2016-12-04; Verfügbar unter https://gesundheitsdatenschutz.org/

Nr. 1493/1999 des Rates, der Richtlinie 2000/13/EG, der Richtlinie 2001/112/EG des Rates sowie der Verordnung (EG) Nr. 258/97.

In dieser Verordnung wird der Begriff der öffentlichen Gesundheit hinsichtlich Gemeinschaftsstatistiken über öffentliche Gesundheit und über Gesundheitsschutz und Sicherheit am Arbeitsplatz verwendet. Der Begriff selbst umfasst entsprechend Erwägungsgrund 54 der DS-GVO dabei ein weites Feld:

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

Beachtet werden muss hierbei, dass eine Verarbeitung aufgrund von öffentlichem Interesse auch nur von Institutionen durchgeführt werden darf, die im (nationalen) öffentlichen Interesse handeln, also den direkten Auftrag vom nationalen Gesetzgeber bekamen. Erwägungsgrund 54 schreibt hierzu: „Eine solche Verarbeitung von Gesundheitsdaten aus Gründen des öffentlichen Interesses darf nicht dazu führen, dass Dritte, unter anderem Arbeitgeber, Versicherungs- und Finanzunternehmen, solche personenbezogenen Daten zu anderen Zwecken verarbeiten".

4.7 Erforderlichkeit, Notwendigkeit[10]

Die Begrifflichkeiten „Erforderlichkeit" und „Notwendigkeit" werden oftmals synonym verwendet. Im juristischen Schrifttum besagt der Grundsatz der Verhältnismäßigkeit, dass kollidierende Interessen, Freiheiten oder Rechtsprinzipien nur dann in einem angemessenen Verhältnis zueinander stehen, wenn das zu wahrende Interesse, Freiheitsrecht oder Rechtsprinzip schwerer wiegt als das zu seinen Gunsten geopferte. Auch im Sinne dieses Grundsatzes können die Begrifflichkeiten „Erforderlichkeit" und „Notwendigkeit" synonym verwendet werden.

In der DS-GVO selbst wird der Begriff der „Erforderlichkeit" bzw. „Notwendigkeit" nicht definiert. Allerdings finden sich in den Erwägungsgründen Kriterien, welche die Beurteilung der Erforderlichkeit erleichtern. Die Verarbeitung von Daten ist insbesondere dann erforderlich bzw. notwendig, wenn

- der Zweck der Verarbeitung nicht in zumutbarer Weise durch andere Mittel erreicht werden kann (Erwägungsgrund 39) oder
- der Zweck der Verarbeitung im lebenswichtigen Interesse der betroffenen Person liegt (Erwägungsgrund 112).

D. h. damit eine Maßnahme erforderlich ist, darf es kein milderes (= in die Rechte Betroffener weniger eingreifendes) Mittel geben, welches den gleichen Erfolg mit vergleichbarem Aufwand erreicht. Um die Erforderlichkeit / Notwendigkeit beurteilen zu können, müssen daher drei Fragen beantwortet werden:

1) Gibt es ein anderes Mittel?
2) Ist dieses in gleicher Weise geeignet, den Zweck zu erreichen?
3) Ist dieses Mittel ein milderes, also die Rechte der betroffenen Person weniger belastendes Mittel?

4.8 Interessenabwägung[10]

Der BGH konkretisierte die erforderliche Abwägung, die bei einer Verarbeitung personenbezogener Daten vorgenommen werden muss, in seinem Urteil vom 17.12.1985 (Az. VI ZR 244/84)[11]. Demzufolge ist eine Abwägung des Persönlichkeitsrechts des Betroffenen und des Stellenwerts, den die Offenlegung und Verwendung der Daten für den oder die Betroffenen hat, gegen die Interessen der speichernden Stelle und der Dritten, für deren Zweck die Speicherung erfolgte, erforderlich. „Dabei sind Art, Inhalt und Aussagekraft der beanstandeten Daten an den Aufgaben und Zwecken zu messen, denen ihre Speicherung dient[12].

Diese Abwägung ist für jede Art der Datenverarbeitung (Erhebung, Speicherung, Übermittlung, ...) getrennt, den entsprechenden rechtlichen Regelungen nach zu prüfen. Dabei kann es vorkommen, dass eine Abwägung zum Ergebnis führt, dass die Erhebung und Speicherung von personenbezogenen Daten statthaft ist, eine Übermittlung der Daten an andere Empfänger jedoch nicht legitimiert werden kann.

Grundsätzlich kommen als schutzwürdige Interessen der Betroffenen „alle menschlichen Ziele in Betracht, wie etwa das Streben nach Geld, Anerkennung, nach Privatheit wie nach Kommunikation“, ebenso „das Streben nach Glück“[13]. Dabei gilt, dass die Interessen der Betroffenen als umso schutzwürdiger anzusehen sind,

- je sensitiver die Daten sind und
- je größer die Zahl der die Daten verarbeitenden Personen bzw., bei Übermittlungen, der Abrufberechtigten ist[13].

Bei der Darstellung der Betroffeneninteressen kann die Sphärentheorie[14,15] und ihre Einteilung in die drei Sphären Intim-, Privat- und Sozialsphäre helfen:

- ein Eingriff in die Intimsphäre muss vermieden werden, da hier der Kern der Menschenwürde betroffen ist
- Privat- und Sozialsphäre: hier gilt, je stärker der Eingriff, desto gewichtiger muss das verfolgte Gemeinwohlinteresse (= Verarbeitungszweck) sein.

4.9 Stand der Technik

Die Definition im Bundes-Immissionsschutzgesetz (BImSchG) wurde bei der Überarbeitung dieses Gesetzes im Jahre 2001 an geltende europäischen Vorgaben angepasst, sodass diese Definition (abgesehen von den umweltspezifischen Aspekten) auch maßgeblich für die Auslegung der DS-GVO angesehen werden kann. So heißt es hier:

> „Stand der Technik im Sinne dieses Gesetzes ist der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen, der die praktische Eignung einer Maßnahme zur Begrenzung von Emissionen in Luft, Wasser und Boden, zur Gewährleistung der Anlagensicherheit, zur Gewährleistung einer umweltverträglichen Abfallentsorgung oder

[11] Bundesgerichtshof Urt. v. 17.12.1985, Az.: VI ZR 244/84 Online, zitiert am 2016-12-04; Verfügbar unter http://dejure.org/
[12] Bundesgerichtshof Urt. v. 17.12.1985, Az.: VI ZR 244/84, Rn. 13 Online, zitiert am 2016-12-03; Verfügbar unter https://www.jurion.de/
[13] BeckOK DatenSR/von Lewinski BDSG § 10 Rn. 23-29
[14] BeckOK DatenSR/Wolff BDSG § 28 Rn. 64-70
[15] BVerfG Urteil vom 31.01.1973, AZ.: 2 BvR 454/71 Online, zitiert am 2016-12-04; Verfügbar unter http://dejure.org/ Az.: IV ZR 129/09 Online, zitiert am 2016-12-04; Verfügbar unter https://dejure.org/

sonst zur Vermeidung oder Verminderung von Auswirkungen auf die Umwelt zur Erreichung eines allgemein hohen Schutzniveaus für die Umwelt insgesamt gesichert erscheinen lässt. Bei der Bestimmung des Standes der Technik sind insbesondere die in der Anlage aufgeführten Kriterien zu berücksichtigen."

Diese genannten 13 Kriterien sind:

1. Einsatz abfallarmer Technologie,
2. Einsatz weniger gefährlicher Stoffe,
3. Förderung der Rückgewinnung und Wiederverwertung der bei den einzelnen Verfahren erzeugten und verwendeten Stoffe und gegebenenfalls der Abfälle,
4. vergleichbare Verfahren, Vorrichtungen und Betriebsmethoden, die mit Erfolg im Betrieb erprobt wurden,
5. Fortschritte in der Technologie und in den wissenschaftlichen Erkenntnissen,
6. Art, Auswirkungen und Menge der jeweiligen Emissionen,
7. Zeitpunkte der Inbetriebnahme der neuen oder der bestehenden Anlagen,
8. für die Einführung einer besseren verfügbaren Technik erforderliche Zeit,
9. Verbrauch an Rohstoffen und Art der bei den einzelnen Verfahren verwendeten Rohstoffe (einschließlich Wasser) sowie Energieeffizienz,
10. Notwendigkeit, die Gesamtwirkung der Emissionen und die Gefahren für den Menschen und die Umwelt so weit wie möglich zu vermeiden oder zu verringern,
11. Notwendigkeit, Unfällen vorzubeugen und deren Folgen für den Menschen und die Umwelt zu verringern,
12. Informationen, die von internationalen Organisationen veröffentlicht werden,
13. Informationen, die in BVT-Merkblättern enthalten sind.

Wenngleich natürlich nicht alles aus dem Gesetz 1:1 auf die Regelungen zur Gewährleistung der Anforderungen der DS-GVO übertragen werden kann, bietet das Gesetz eine recht gute Darlegung, was im Sinne des europäischen Gesetzgebers unter Stand der Technik zu verstehen ist.

Auch in der Begründung zum IT-Sicherheitsgesetz[16] findet sich eine Definition zum Stand der Technik, die das in § 3 Abs. 6 BImSchG genannte Prinzip auf die IT(-Sicherheit) adaptiert hat. So heißt es hier:

> „Stand der Technik in diesem Sinne ist der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen, der die praktische Eignung einer Maßnahme zum Schutz der Funktionsfähigkeit von informationstechnischen Systemen, Komponenten oder Prozessen gegen Beeinträchtigungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit gesichert erscheinen lässt. Bei der Bestimmung des Standes der Technik sind insbesondere einschlägige internationale, europäische und nationale Normen und Standards heranzuziehen, aber auch vergleichbare Verfahren, Einrichtungen und Betriebsweisen, die mit Erfolg in der Praxis erprobt wurden."

4.10 Stand der Wissenschaft

Der Terminus „Stand der Wissenschaft" wird zwar von der DS-GVO nicht referenziert, aber bzgl. Forschung wird im Rahmen der Sorgfaltspflichten (siehe auch Kapitel 7.1.4) i. d. R. davon auszugehen sein, dass eine Forschungsarbeit dem für das jeweilige Forschungs-Fachgebiet geltenden „Stand der Wissenschaft" genügen muss. Denn Forschung ist letztlich eine wissenschaftliche Tätigkeit.

[16] Gesetzentwurf der Bundesregierung Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz). S. 14, 15. Online, zitiert am 2017-05-07; Verfügbar unter https://dip21.bundestag.de/

Der Begriff „Stand der Wissenschaft“ umfasst die neuesten technischen und wissenschaftlichen Erkenntnisse. Damit repräsentiert der Stand der Wissenschaft gültige, beweisbare und überprüfbare Erkenntnisse. Das BVerfG schreibt im Kalkar-Beschluss bzgl. Stand der Wissenschaft[17]:

> „[...] übt einen noch stärkeren Zwang dahin aus, dass die rechtliche Regelung mit der wissenschaftlichen und technischen Entwicklung Schritt hält. Es muss diejenige Vorsorge gegen Schäden getroffen werden, die nach den neuesten wissenschaftlichen Erkenntnissen für erforderlich gehalten wird. Lässt sie sich technisch noch nicht verwirklichen, darf die Genehmigung nicht erteilt werden; die erforderliche Vorsorge wird mithin durch das technisch gegenwärtig Machbare begrenzt“.

Der Stand der Wissenschaft folgt dem Grundsatz der bestmöglichen Schadensabwehr und der Risikovorsorge. Dabei muss der Eintritt von Schadensereignissen nicht mit absoluter Sicherheit ausgeschlossen werden, um dem Stand der Wissenschaft zu genügen. Vielmehr muss, dem Urteil des BVerfG folgend, der Eintritt von Schadensereignissen nur soweit „technisch gegenwärtig machbar“ ausgeschlossen werden.

4.11 Pseudonymisierung

Art. 4 Abs. 5 definiert Pseudonymisierung als „die Verarbeitung personenbezogener Daten in einer Weise, dass

- die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können,
- sofern diese zusätzlichen Informationen gesondert aufbewahrt werden
- und technischen und organisatorischen Maßnahmen unterliegen,
- die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden“.

Aus der in der DS-GVO enthaltenen Begriffsbestimmung lassen sich somit verschiedene implizit enthaltene Feststellungen ableiten:

a) Pseudonyme Daten stellen gemäß Art. 4 Abs. 1 personenbezogene oder personenbeziehbare Daten dar, da eine grundsätzliche Möglichkeit zur Identifikation der Person besteht.
b) Der Vorgang der Pseudonymisierung stellt eine Verarbeitung im Sinne von Art. 4 Abs. 2 dar, somit gelten für eine Pseudonymisierung alle Vorgaben bzgl. der Verarbeitung, insbesondere die Vorgaben von Art. 5 und Art. 6 bzw. Art. 9. D. h. auch bei einer Pseudonymisierung der Daten muss immer die Rechtmäßigkeit der Verarbeitung gewährleistet sein. Insbesondere muss bei der Verarbeitung besonderer Kategorien personenbezogener Daten gemäß Art. 9 ein Erlaubnistatbestand zur Pseudonymisierung vorhanden sein.
c) Pseudonyme Daten gelten nur dann als pseudonym, wenn der die Daten Verarbeitende keine Möglichkeit hat, die Zuordnungsvorschrift zwischen Pseudonym und Personenkennung zu erhalten und eine „De-Pseudonymisierung“ mittels dieser Liste vorzunehmen.

Zudem muss festgehalten werden, dass eine Pseudonymisierung keine Anonymisierungstechnik darstellt, wie die Artikel-29-Datenschutzgruppe in WP 216[18] feststellte. Hiernach verringert eine Pseudonymisierung „lediglich die Verknüpfbarkeit eines Datenbestands mit der wahren Identität

[17] BVerfG, Urteil vom 8. August 1978, Az. 2 BvL 8/77. Rn. 116. Online, zitiert am 2017-03-02; Verfügbar unter https://openjur.de/u/166332.html
[18] Artikel-29-Datenschutzgruppe: Stellungnahme 5/2014 zu Anonymisierungstechniken. Online, zitiert am 2017-05-04; Verfügbar unter http://ec.europa.eu/

einer betroffenen Person und stellt somit eine sinnvolle Sicherheitsmaßnahme dar“[18]. Insbesondere sind pseudonymisierte Daten nicht mit anonymisierten Informationen gleichzusetzen[18].

5 Erlaubnistatbestand: Unter welchen Umständen dürfen personenbezogene Daten verarbeitet werden?

Wie vorstehend dargestellt ist für jegliche Verarbeitung personenbezogener oder personenbeziehbarer Daten ein Erlaubnistatbestand erforderlich. Gemäß Art. 9 Abs. 1 DS-GVO ist jegliche Verarbeitung besonderer Kategorien personenbezogener Daten verboten (und damit auch die Verarbeitung zu Forschungszwecken), außer ein in Art. 9 Abs. 2 DS-GVO genannter Umstand liegt vor. Dies gilt grundsätzlich auch für die medizinische Forschung.

5.1 Einwilligung des Betroffenen

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[19].

5.1.1 Die datenschutzrechtliche Aufklärung

Eine datenschutzrechtlich wirksame Aufklärung bedarf einer vollständigen Information, wer zu welchem Zweck wann und wo welche Daten zu verarbeiten beabsichtigt. Auch die Beteiligten und die Speicherdauer sind von Bedeutung. Erst nach einer umfassenden Aufklärung kann der Patient um die Einwilligung gebeten werden, diesem Verfahren zuzustimmen.

Dabei muss dem Patienten bekannt gemacht worden sein, dass er jederzeit das Recht auf Widerruf seiner Einwilligung hat. Diesbezüglich gilt es ihm jedoch auch aufzuzeigen, welche Konsequenzen sein Widerruf hat.

5.1.1.1 Recht auf Nicht-Wissen

In Hinblick auf medizinische Eingriffe besteht nach h.M. die Auffassung, dass von einer selbstbestimmten Entscheidung nur bei zweifelsfreier Kenntnis über das Bestehen eines Aufklärungs- und Verzichtsrechts ausgegangen werden kann, dann aber der Patient auch das Recht besitzt, bewusst auf eine Aufklärung zu verzichten[20]. Analog ist auch bei der datenschutzrechtlichen Aufklärung davon auszugehen, dass die betroffene Person grundsätzlich die Entscheidungshoheit bzgl. einer zu erfolgenden Aufklärung besitzt.

Denn grundsätzlich ist immer auch das Informationsinteresse der betroffenen Person zu berücksichtigen. Dieses leitet sich direkt aus dem Recht auf informationelle Selbstbestimmung ab. Auch Menschen, die nicht mit belastenden Informationen konfrontiert werden wollen, haben deshalb ein Anrecht auf die Entscheidungshoheit bzgl. der Verwendung ihrer personenbezogenen

[19] GMDS (2016): EU DS-GVO: Anforderungen an eine Einwilligung. Online, zitiert am 2016-12-04; Verfügbar unter https://www.gesundheitsdatenschutz.org/(Download als pdf-Datei)
[20] siehe z.B. Schwill F. (2007) Aufklärungsverzicht und Patientenautonomie. Tectum Verlag, 1. Auflage. ISBN 978-3-8288-9292-7

Daten. Eine betroffene Person hat somit immer auch ein Recht auf „Nichtwissen“. Hierauf beruht auch § 8 Abs. 1 S. 2 GenDG, welches bestimmt, dass die betroffene Person selbst frei entscheiden kann, „ob und inwieweit das Untersuchungsergebnis zur Kenntnis zu geben oder zu vernichten ist“[21]. In der Gesetzesbegründung wird diesbezüglich festgehalten, dass im GenDG „das Recht des Patienten auf „Nichtwissen“ festgeschrieben“ ist[22].

Lediglich wenn eine konkrete Gefährdung genau bestimmter anderer Personen oder sogar der Allgemeinheit vorliegt, ist von einer höherrangigen Informationspflicht des Verantwortlichen auszugehen[23]. Um dieses Recht ausüben zu können, müssen „konkrete Konzepte entwickelt werden, wie eine solche Individualbefugnis durch verfahrensrechtlich abgesicherte Strukturen auch in der sozialen Wirklichkeit ermöglicht werden kann“[24]. Denn selbstverständlich ist auch die Entscheidung bzgl. des „Nicht-Wissenwollens“ von der betroffenen Person widerrufbar. D.h., wenn neue Erkenntnisse vorliegen, die möglicherweise die Entscheidung der betroffenen Person beeinflussen könnten, muss die betroffene Person erneut angesprochen werden. Weiterhin muss nachgewiesen werden können, dass die betroffene Person diese Entscheidung wissentlich und aus freiem Willen entschied. Auch muss ggf. nachgewiesen werden, dass Interessen Dritter von dieser Entscheidung nicht betroffen sind (sein können).

Die BMBF-Projektgruppe „Recht auf Nichtwissen“ von der Universität Göttingen erarbeitete Empfehlungen zum anwendungspraktischen Umgang mit dem „Recht auf Nichtwissen“[25]. Obgleich sich diese Hinweise zunächst an die Bereiche Humangenetik und Psychiatrie richten, enthalten diese Empfehlungen auch für andere Fachrichtungen nützliche Hinweise, wie mit diesem Thema umgegangen werden kann. Grundsätzlich muss bedacht werden, dass der die Daten verarbeitende Verantwortliche entsprechend der DS-GVO nachweispflichtig bzw. rechenschaftspflichtig ist. Diese Pflicht gilt somit auch für die Nachweisführung, dass die betroffene Person bzgl. ihrer Einwilligung auf eine Aufklärung bewusst und aus freiem Willen verzichtete.

5.1.2 Sonderfall: Nicht-einwilligungsfähige Patienten

In Deutschland ist bisher weitgehend nicht geregelt, unter welchen Umständen Daten von nicht-einwilligungsfähigen Patienten abseits der Notfallversorgung genutzt werden dürfen. Gesetzliche Regelungen finden sich lediglich in zwei Gesetzen:

- § 41 Abs. 1 S. 2 AMG
- § 21 Nr. 3 S. 3 MPG.

5.1.2.1 Minderjährige Patienten

a) Spezialfall: Dienste der Informationsgesellschaft

[21] Gesetz über genetische Untersuchungen bei Menschen (Gendiagnostikgesetz - GenDG) Online, zitiert am 2017-03-01; Verfügbar unter http://www.gesetze-im-internet.de/gendg/index.html#BJNR252900009BJNE001200000

[22] Drucksache 16/10532: Entwurf eines Gesetzes über genetische Untersuchungen bei Menschen (Gendiagnostikgesetz - GenDG); Begründung Zu § 10 Abs. 1, 2 und 3 Satz 4. Online, zitiert am 2017-03-01; Verfügbar unter http://dip21.bundestag.de/dip21/btd/16/105/1610532.pdf

[23] Duttge G. (2010) Das Recht auf Nichtwissen in der Medizin. DuD: 34-38

[24] Duttge G. (2016) Das Recht auf Nichtwissen in einer informationell vernetzten Gesundheitsversorgung. MedR: 664-669

[25] BMBF-Projektgruppe „Recht auf Nichtwissen“ (2016) Empfehlungen zum anwendungspraktischen Umgang mit dem „Recht auf Nichtwissen“. MedR: 399-405

Art. 8 DS-GVO beinhaltet die zu erfüllenden „Bedingungen für die Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft“. Hiernach darf ein Kind erst nach dem 16. Lebensjahr in die Nutzung der Dienste der Informationsgesellschaft einwilligen, ansonsten wird die Einwilligung bzw. Zustimmung des „Trägers der elterlichen Verantwortung für das Kind“ benötigt.

Aus diesem Grund ist es zunächst für einen Verantwortlichen, der einen solchen Dienst anbietet, essenziell, sich zu vergewissern, ob die Teilnehmer des Dienstes aufgrund ihres Alters wirksam in die Datenverarbeitung einwilligen können. Falls dieses nicht der Fall ist, muss er weitere Überlegungen anstellen. Unterschreitet ein Kind die durch die DS-GVO bzw. nationalstaatliche Regelung festgelegte Altersgrenze, muss ein Verantwortlicher sich entsprechend Art. 8 Abs. 2 DS-GVO unter Berücksichtigung der verfügbaren Technik vergewissern, dass eine Einwilligung bzw. Zustimmung durch den Träger der elterlichen Verantwortung für das Kind erteilt wurde. Generell gilt, dass auch Einwilligungen gemäß Art. 8 DS-GVO den Anforderungen des Art. 7 genügen müssen. Die Beantwortung der Frage, ob ein Kind in eine Datenverarbeitung (in allen übrigen Verarbeitungskonstellationen) rechtswirksam einwilligen kann, hängt damit maßgeblich davon ab, ob das Kind für eine wirksame Einwilligung über die notwendige Einsichts- bzw. Urteilsfähigkeit verfügt oder nicht[26].

a1) Was sind Dienste der Informationsgesellschaft?

Die Definition der Begrifflichkeit „Dienste der Informationsgesellschaft“ ist Erwägungsgrund 21 folgend der Richtlinie 2000/31/EG[27] zu entnehmen. Art. 2 lit. a RL 2000/31/EG verweist bzgl. der Definition der „Dienste der Informationsgesellschaft“ auf Art. 1 Ziff. 2 der Richtlinie 98/34/EG in der Fassung der Richtlinie 98/48/EG. Richtlinie 98/48/EG wurde jedoch im Jahre 2015 durch die Richtlinie 2015/1535[28] ersetzt, weshalb nunmehr die in dieser Richtlinie enthaltenen Definition zur Begriffsbestimmung maßgeblich ist. Aus diesem Grunde verweist auch die Definition in Art. 4 Nr. 25 DS-GVO auf diese Richtlinie. In Art. 1 Abs. 1 lit. b RL 2015/1535 findet sich die folgende Definition:

> „Dienst“ eine Dienstleistung der Informationsgesellschaft, d. h. jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung. Im Sinne dieser Definition bezeichnet der Ausdruck
>
> i. „im Fernabsatz erbrachte Dienstleistung“ eine Dienstleistung, die ohne gleichzeitige physische Anwesenheit der Vertragsparteien erbracht wird;

[26] siehe hierzu auch

1. Unabhängiges Landeszentrum für Datenschutz in Schleswig-Holstein (2009) Praxishandbuch Schuldatenschutz. Abschnitt „Können auch nicht volljährige Schülerinnen und Schüler eine verbindliche datenschutzrechtliche Einwilligungserklärung abgeben? S. 30/31. Online, zitiert am 2016-08-24; Verfügbar unter https://www.datenschutzzentrum.de/schule/praxishandbuch-schuldatenschutz.pdf
2. Unabhängiges Landeszentrum für Datenschutz in Schleswig-Holstein (2015) Datenschutz bei Kindern. Online, zitiert am 2016-08-24; Verfügbar unter https://www.datenschutz.de/datenschutz-bei-kindern/

[27] Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt ("Richtlinie über den elektronischen Geschäftsverkehr") Online, zitiert am 2016-08-06; Verfügbar unter http://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A32000L0031

[28] Richtlinie 2015/1535 des Europäischen Parlaments und des Rates vom 9. September 2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft. Online, zitiert am 2016-08-06; Verfügbar unter http://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1470308288184&uri=CELEX:32015L1535

ii. „elektronisch erbrachte Dienstleistung“ eine Dienstleistung, die mittels Geräten für die elektronische Verarbeitung (einschließlich digitaler Kompression) und Speicherung von Daten am Ausgangspunkt gesendet und am Endpunkt empfangen wird und die vollständig über Draht, über Funk, auf optischem oder anderem elektromagnetischem Wege gesendet, weitergeleitet und empfangen wird;

iii. „auf individuellen Abruf eines Empfängers erbrachte Dienstleistung“ eine Dienstleistung die durch die Übertragung von Daten auf individuelle Anforderung erbracht wird.

Eine Beispielliste der nicht unter diese Definition fallenden Dienste findet sich in Anhang I der Richtlinie. Dementsprechend sind u.a. folgende Dienste nicht als „Dienste der Informationsgesellschaft“ im Sinne der RL 2015/1535 anzusehen:

- Untersuchung oder Behandlung in der Praxis eines Arztes mithilfe elektronischer Geräte, aber in Anwesenheit des Patienten,
- Medizinische Beratung per Telefon/Telefax.

Im Rahmen der Forschung können Portallösungen, in denen beispielsweise Dienstleister die Datensammlung und statistische Auswertung vornehmen, evtl. als „Dienste der Informationsgesellschaft“ im Sinne der RL 2015/1535 angesehen werden.

b) Klinische Studien mit Arzneimitteln und Medizinprodukten

§ 40 Abs. 4 Nr. 3 S. 1 AMG regelt, dass bei minderjährigen Probanden (= Alter unter 18 Jahren) die Einwilligung des gesetzlichen Vertreters vorliegen muss. Hierzu müssen dem gesetzlichen Vertreter die entsprechenden Informationen (§ 40 Abs. 1 S. 3 Nr. 3 lit. c und Abs. 2a AMG) vorliegen. Ist der Minderjährige zudem „in der Lage, Wesen, Bedeutung und Tragweite der klinischen Prüfung zu erkennen und seinen Willen hiernach auszurichten, so ist auch seine Einwilligung erforderlich“.

Die Regelung in § 20 Abs. 4 Nr. 4 MPG ist gleichbedeutend mit der entsprechenden Regelung im AMG, d.h. die Einwilligung des gesetzlichen Vertreters wird benötigt und ggf. muss zusätzlich die Einwilligung des Minderjährigen vorliegen. Eine rechtswirksame Einwilligung verlangt eine vorherige Information bzw. Aufklärung entsprechend § 20 Abs. 1 S. 4 Nr. 2 MPG.

Bzgl. der Einsichtsfähigkeit geht der Gesetzgeber davon aus, dass diese in der Regel vom vollendeten 16. Lebensjahr an gegeben sein kann (siehe Gesetzesbegründung[29]).

c) In allen anderen Fällen

Liegt in anderen als den vorstehend beschriebenen Konstellationen weder eine spezialgesetzliche Regelung vor noch handelt es sich um einen „Dienst der Informationsgesellschaft“ im Sinne der Richtlinie 2000/31/EG[30], so ist nach überwiegender Ansicht in Rechtsprechung und Literatur lediglich die Einsichtsfähigkeit des Minderjährigen entscheidende Zulässigkeitsvoraussetzung für

[29] Entwurf eines Zwölften Gesetzes zur Änderung des Arzneimittelgesetzes vom 2003-12-01. Bundestagsdrucksache 15/2109. Teil B (Besonderer Teil), Nummer 26 (§ 40) zu Abs. 4, S. 31. Online, zitiert am 2017-01-14; Verfügbar unter http://dip21.bundestag.de/doc/btd/15/021/1502109.pdf

[30] Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt ("Richtlinie über den elektronischen Geschäftsverkehr") Online, zitiert am 2016-08-06; Verfügbar unter http://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A32000L0031

die Einwilligung[31]. Ist die Einsichtsfähigkeit des Minderjährigen nicht gegeben, muss die Einwilligung des gesetzlichen Vertreters eingeholt werden[32].

5.1.2.2 Volljährige Patienten

Bei volljährigen Patienten, die nicht einwilligungsfähig sind, wie z. B. komatöse Patienten, ist die Einwilligung des gerichtlich bestellten Betreuers einzuholen, der gemäß § 1902 BGB bzw. § 53 ZPO den Betreuten rechtlich vertreten darf. Insbesondere sind Einwilligungen des Betreuers als rechtlich ebenso bindend anzusehen wie die Einwilligung des Betreuten selbst (§ 164 BGB).

Mitunter wird empfohlen, eine Einwilligung durch einen gemäß § 1896 Abs. 2 S. 2 BGB Bevollmächtigten einzuholen. Auch wenn entsprechend der Bevollmächtigung der Bevollmächtigte die Gesundheitsangelegenheiten des nicht einwilligungsfähigen Patienten wahrnimmt, ist eine entsprechende Einwilligung als ein höchstpersönliches Geschäft anzusehen, für welches § 1896 Abs. 2 S. 2 BGB keine Grundlage bietet.

Sollte mit dem Forschungsvorhaben ein als hoch riskant einzustufender ärztlicher Behandlungseingriff verbunden sein, so bedarf dies der Zustimmung eines Betreuungsgerichts (§ 1904 BGB); eine Zustimmung/Einwilligung eines Betreuers oder Bevollmächtigten alleine reicht nicht aus. Eine Ausnahme hiervon kann bei Vorliegen einer entsprechend § 1901a BGB rechtsgültigen Patientenverfügung vorliegen (§ 1904 Abs. 4 BGB).

Sobald der Patient seine Einwilligungsfähigkeit wiedererlangt hat, ist umgehend dessen Einwilligung einzuholen.

5.1.2.3 Verstorbene Patienten

Personenbezogene Daten Verstorbener werden von den Regelungen der DS-GVO nicht erfasst. Vielmehr beinhaltet die DS-GVO diesbezüglich eine entsprechende „nationale Öffnungsklausel“, von welcher jedoch der deutsche Gesetzgeber bisher noch keinen Gebrauch machte. Vereinzelt finden sich hierzu aber spezialgesetzliche Regelungen, z. B.

- § 27 Abs. 2 S. 2 BbgKHEG [33]
- § 7 Abs. 1 S. 4 HmbKHG[34].

Auch in Kommentaren zum BDSG findet sich die Interpretation, dass das Persönlichkeitsrecht nicht für Verstorbene gilt, da Verstorbene keine natürlichen Personen im Sinne von § 3 Abs. 1 BDSG sind[35].

Indirekt können datenschutzrechtliche Regelungen dennoch zu beachten sein, wenn in den Daten der verstorbenen Person Daten Dritter enthalten sind. Liegen beispielsweise genetische Erkrankungen vor, die auch noch lebende Geschwister oder Kinder betreffen bzw. betreffen könnten, so muss zwar nicht der Datenschutz gegenüber der verstorbenen Person gewahrt werden, wohl aber

---

[31] So z. b: Simitis S. § 4a BDSG Rn. 20,23 in: Simitis (Hrsg.) Bundesdatenschutzgesetz. Nomos Verlagsgesellschaft, 8. Auflage 2014, ISBN 978-3-8487-0593-1

[32] So z. b: Simitis S. § 4a BDSG Rn. 21 in: Simitis (Hrsg.) Bundesdatenschutzgesetz. Nomos Verlagsgesellschaft, 8. Auflage 2014, ISBN 978-3-8487-0593-1

[33] Gesetz zur Entwicklung der Krankenhäuser im Land Brandenburg (Brandenburgisches Krankenhausentwicklungsgesetz - BbgKHEG). Online, zitiert am 2017-01-14; Verfügbar unter http://bravors.brandenburg.de/de/gesetze-212704

[34] Hamburgisches Krankenhausgesetz (HmbKHG). Online, zitiert am 2017-01-14; Verfügbar unter http://www.landesrecht-hamburg.de/jportal/portal/page/bshaprod.psml?showdoccase=1&st=lr&doc.id=jlr-KHGHArahmen

[35] z. B. Dammann U. § 3 BDSG Rn. 17 in: Simitis (Hrsg.) Bundesdatenschutzgesetz. Nomos Verlagsgesellschaft, 8. Auflage 2014, ISBN 978-3-8487-0593-1

der Datenschutz bzgl. der Geschwister/Kinder. Daher darf die Erkrankung oder das genetische Merkmal der betroffenen (verstorbenen) Person nicht ohne weiteres preisgegeben werden.

Weiterhin muss beachtet werden, dass z. B. die Menschenwürde mit dem Tod des Grundrechtsträgers nicht endet. Beim postmortalen Persönlichkeitsrecht, welches ähnlich wie das Datenschutzrecht aus Art. 1 Abs. 1 GG hergeleitet wird, ist bei einem Verstorbenen zumindest dessen allgemeiner Achtungsanspruch zu wahren. Hiervon ist ebenfalls der sittliche wie auch der personale und der soziale Wert des Verstorbenen, den dieser durch die eigene Lebensleistung erlangte, geschützt.

Ferner endet auch die berufliche Schweigepflicht, die aus § 203 StGB resultiert, nicht mit dem Tod. Bzgl. der Schweigepflicht gilt, dass der Wille der verstorbenen Person auf Geheimhaltung der Arzt-Patientenbeziehung nicht durch den Willen eines Dritten (z. B. eines Erben) ersetzt werden darf[36]. Verfügungsberechtigt ist damit alleine der Patient, der sich dem Arzt anvertraut hat, und nicht Dritte[37]. Liegt bei einem Verstorbenen keine Einwilligung (Schweigepflichtentbindung) vor, aber das Interesse des Verstorbenen an der Offenlegung (z. B. durch Äußerungen zu Lebzeiten wie „alles von mir für die Forschung“) ist offensichtlich, so kann damit aus Sicht des § 203 StGB eine legitimierende (mutmaßliche) Einwilligung gegeben sein[36,38].

In einem solchen Fall gilt es durch Analyse des Sachverhalts für den jeweiligen Einzelfall zu entscheiden, ob und - wenn ja - wie die Daten eines Verstorbenen für Forschungszwecke genutzt werden dürfen.

5.2 Verarbeitung ohne Einwilligung des Betroffenen

Hinsichtlich der Nutzung besonderer Kategorien personenbezogener Daten findet sich in Art. 9 Abs. 2 lit. j DS-GVO ein datenschutzrechtlicher Erlaubnistatbestand zur Nutzung von Daten zu Zwecken der wissenschaftlichen Forschung: Hiernach ist eine Verarbeitung gestattet, wenn „die Verarbeitung

- auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats,
- das in angemessenem Verhältnis zu dem verfolgten Ziel steht,
- den Wesensgehalt des Rechts auf Datenschutz wahrt und
- angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht,
- für
    - im öffentlichen Interesse liegende Archivzwecke,
    - für wissenschaftliche oder
    - historische Forschungszwecke oder
    - für statistische Zwecke

  gemäß Artikel 89 Absatz 1 erforderlich (ist).

Dieser Regelung folgend können besondere Kategorien personenbezogener Daten zu „wissenschaftlichen Forschungszwecken“ genutzt werden, wenn fünf Bedingungen erfüllt sind:

[36] so z. B. OLG Naumburg, Urteil vom 09.12.2004, AZ 4 W 43/04. Online, zitiert am 2017-01-14; Verfügbar unter https://dejure.org/dienste/vernetzung/rechtsprechung?Gericht=OLG%20Naumburg&Datum=09.12.2004&Aktenzeichen=4%20W%2043/04

[37] Fischer T, Schwarz O, Dreher E, Tröndle H. (2015) Strafgesetzbuch: mit Nebengesetzen. §203, RN. 34. Beck-Verlag, 59. Auflage 2012, ISBN 978-3-406-62407-0

[38] Fischer T, Schwarz O, Dreher E, Tröndle H. (2015) Strafgesetzbuch: mit Nebengesetzen. §203, RN. 36. Beck-Verlag, 59. Auflage 2012, ISBN 978-3-406-62407-0

a) ein nationales oder europäisches Recht für die Nutzung existiert,
b) dieses Recht steht im angemessenem Verhältnis zum verfolgten (Forschungs-) Ziel,
c) dieses Recht wahrt die datenschutzrechtlichen Anforderungen der DS-GVO,
d) das Gesetz sieht spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vor und
e) die Verarbeitung der Daten ist erforderlich.

Sind diese Bedingungen erfüllt, so müssen darüber hinaus insbesondere die Vorgaben in Art. 89 Abs. 1 berücksichtigt werden:

„Die Verarbeitung zu

- im öffentlichen Interesse liegenden Archivzwecken,
- zu wissenschaftlichen oder historischen Forschungszwecken oder
- zu statistischen Zwecken

unterliegt

- geeigneten Garantien für die Rechte und Freiheiten der betroffenen Person gemäß dieser Verordnung.

Mit diesen Garantien wird sichergestellt, dass

- technische und organisatorische Maßnahmen bestehen,
- mit denen insbesondere die Achtung des Grundsatzes der Datenminimierung gewährleistet wird."

D. h. jedes Forschungsvorhaben muss den Vorgaben der DS-GVO genügen, insbesondere muss es auch

- den Grundsätzen der Verarbeitung genügen (Kapitel II),
- die Betroffenenrechte wahren (Kapitel III) und
- die Sicherheit der Verarbeitung gewährleisten (Kapitel IV).

Insbesondere hat die betroffene Person gemäß Art. 21 Abs. 6 das Recht, der Nutzung „sie betreffender personenbezogener Daten, die zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken gemäß Artikel 89 Absatz 1" verwendet werden sollen, zu widersprechen. Dieses jedoch nur, wenn die Verarbeitung nicht im „öffentlichen Interesse" erfolgt. Sollte Letzteres der Fall sein, geht das öffentliche Interesse dem Individualinteresse (grundsätzlich) vor.

5.2.1 Nationale Erlaubnistatbestände in Deutschland

Art. 9 Abs. 4 DS-GVO enthält eine Öffnungsklausel, welche es den Mitgliedsstaaten erlaubt, „zusätzliche Bedingungen, einschließlich Beschränkungen" einzuführen oder aufrechtzuerhalten, soweit die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten betroffen ist. Dementsprechend sind nationale Erlaubnistatbestände, wie z. B. in einigen Landeskrankenhausgesetzen, oder auch Verarbeitungsverbote, wie sie sich beispielsweise im Sozialgesetzbuch finden, auch nach Wirkeintritt der DS-GVO weiterhin gültig - soweit sie den Rahmenbedingungen der DS-GVO entsprechen bzw. als ergänzende Regelungen entsprechend der Öffnungsklauseln zu interpretieren sind.

5.2.1.1 Krankenhausgesetze der Länder

In mehreren der deutschen krankenhausspezifischen Landesgesetze befinden sich Erlaubnistatbestände zur Nutzung von bei der Patientenbehandlung angefallenen Daten zu Forschungszwecken. Diese gesetzlichen Regelungen sind als Erlaubnistatbestände i. S. v. Art. 9 Abs. 4 DS-GVO anzusehen. Zu diesen landesgesetzlichen Regelungen gehören insbesondere:

- Bayern
  - Art. 27 Abs. 4 BayKrG gestattet die Nutzung von Patientendaten innerhalb des Krankenhauses zu Forschungszwecken oder im Forschungsinteresse des Krankenhauses, ohne dass eine Einwilligung des Patienten hierzu notwendig ist.
- Berlin
  - Ohne Einwilligung ist eine Nutzung der Patientendaten unter den Voraussetzungen von § 25 Abs. 1 S. 2 Nr.1-4 LKG statthaft. Dies bedeutet, dass (mindestens) eine der folgenden Bedingungen erfüllt sein muss:
    - Ärztinnen und Ärzte nutzen innerhalb ihrer Fachrichtung oder sonstigen medizinischen Betriebseinheit verarbeitete Patientendaten für eigene wissenschaftliche Forschungsvorhaben, sofern schutzwürdige Belange der Patientin oder des Patienten dem Forschungsvorhaben nicht entgegenstehen und eine gewerbliche Nutzung ausgeschlossen ist.
    - Die Einwilligung einzuholen ist nicht zumutbar und schutzwürdige Belange der Patientin oder des Patienten werden nicht beeinträchtigt.
    - Das berechtigte Interesse der Allgemeinheit an der Durchführung des Forschungsvorhabens überwiegt das Geheimhaltungsinteresse der Patientin oder des Patienten erheblich.
    - Im Rahmen der Krankenhausbehandlung erhobene und gespeicherte Patientendaten werden vor ihrer weiteren Verarbeitung anonymisiert.
- Brandenburg
  - Entsprechend § 31 BbgKHEG dürfen Patientendaten, die innerhalb ihrer Fachabteilung zulässigerweise gespeichert sind, ohne Einwilligung der jeweiligen Patienten für eigene wissenschaftliche Forschungsvorhaben verarbeiten werden, wenn dabei schutzwürdige Belange der Betroffenen nicht gefährdet sind.
- Bremen
  - Gemäß § 7 Abs. 1 BremKHDSG ist die Verarbeitung von Patientendaten, die im Rahmen der Behandlung gespeichert wurden, für wissenschaftliche medizinische Forschungsvorhaben von Angehörigen eines Heilberufs oder Gesundheitsfachberufs der Behandlungseinrichtung im Krankenhaus sowie in Hochschulen und anderen mit wissenschaftlicher Forschung beauftragten Stellen zulässig, wenn der Patient oder die Patientin eingewilligt hat. Ohne Einwilligung ist die Verarbeitung nur entsprechend den Vorgaben von § 7 Abs. 2 BremKHDSG zulässig.
- Hamburg
  - § 12 HmbKHG erlaubt die Verarbeitung von Patientendaten für eigene wissenschaftliche Forschungsvorhaben, wenn schutzwürdige Interessen der Betroffenen dadurch nicht gefährdet werden.
- Mecklenburg-Vorpommern
  - Entsprechend § 38 Abs. 1 LKHG M-V ist die Verarbeitung von Patientendaten für Forschungszwecke zulässig, wenn die Patientinnen und Patienten hierzu die

entsprechende Einwilligung erteilten. Ohne Einwilligung können Patientendaten unter den Voraussetzungen von§ 38 Abs. 2 LKHG M-V genutzt werden.

- Nordrhein-Westfalen
  - Ohne Einwilligung ist die Nutzung von Patientendaten unter den Voraussetzungen von § 6 Abs. 2 GDSG NRW zulässig. D.h., es muss sich um Patientendaten handeln, auf die das forschende Personal in den Einrichtungen oder öffentlichen Stellen aufgrund seiner Mitwirkung bei der medizinischen Versorgung dieser Patienten ohnehin Zugriff hat („Daten der eigenen Einrichtung“). Oder die nachfolgend dargestellten Bedingungen sind nachgewiesenermaßen erfüllt:
    - Der Zweck eines bestimmten Forschungsvorhabens kann ohne die Verwendung dieser Daten nicht erreicht werden.
    - Das berechtigte Interesse der Allgemeinheit an der Durchführung des Forschungsvorhabens überwiegt das Geheimhaltungsinteresse des Patienten erheblich.
    - Entweder ist nicht möglich ist oder dem Patienten kann aufgrund seines derzeitigen Gesundheitszustandes nicht zugemutet werden, ihn um seine Einwilligung zu bitten.
- Rheinland-Pfalz
  - Patientendaten dürfen gemäß § 37Abs. 1 LKG RP im Rahmen von Forschungsvorhaben durch das Krankenhaus verarbeitet werden, wenn die Patientin oder der Patient hierzu die Einwilligung erteilten. Ohne Einwilligung ist die Verarbeitung nur unter den Bedingungen von § 37Abs. 1 S. 2 LKG RP zulässig.
- Saarland
  - Krankenhausärztinnen und Krankenhausärzte dürfen die innerhalb ihrer Fachabteilung zu Behandlungszwecken aufgezeichneten Patientendaten für eigene medizinische wissenschaftliche Forschung unter den Voraussetzungen von § 14 Abs. 1 SKHG nutzen.
- Sachsen
  - Ärzte dürfen Patientendaten, die innerhalb ihrer Fachabteilung oder bei Hochschulen innerhalb ihrer medizinischen Einrichtungen, in den Universitätsklinika oder in sonstigen medizinischen Einrichtungen gespeichert sind, entsprechend § 34 SächsKHG für eigene wissenschaftliche Forschungsvorhaben verarbeiten.
- Thüringen
  - § 27a Abs. 1 ThürKHG gestattet die Verarbeitung von Patientendaten für Forschungszwecke, wenn die Patientin oder der Patient hierzu die Einwilligung erteilten. Ohne Einwilligung können die Daten unter den Voraussetzungen von § 27a Abs. 2 ThürKHG genutzt werden.

5.2.1.2 Bundesrecht

- § 28 Abs. 6 Ziff. 4 BDSG, ggf. Spezialregelung im Nachfolgegesetz BDSG (neu)
- Klinische Prüfung (AMG, MPG)
- Radioaktive Stoffe, ionisierende Strahlung, Röntgenstrahlung (StrlSchV, RöV)
- Sozialdaten (§§ 287, 303e SGB V, § 206 SGB VII, § 75 SGB X, § 98 SGB XI)

5.3 Privilegierung der Eigenforschung

Unter Eigenforschung wird die Forschung mit personenbezogenen Daten verstanden, die ausschließlich durch das eigene Personal der verantwortlichen Stelle durchgeführt wird. Diese Forschung ist in den Landeskrankenhausgesetzen i. d. R. privilegiert, d. h. dort finden sich spezialgesetzliche Erlaubnistatbestände. Diese finden sich insbesondere in:

- Bundesrecht (§ 28 Abs. 6 Nr. 4 BDSG[39]), ggf. Spezialregelung im Nachfolgegesetz BDSG (neu)
- Bayern (Art. 27 Abs. 4 BayKrG)
- Berlin (§ 25 Abs. 1 Satz 2 Nr. 1 LKG Berlin)
- Hamburg (§12 Abs. 1 HmbKHG)
- Mecklenburg-Vorpommern (§ 38 LKHG M-V)
- Nordrhein-Westfalen (§ 6 Abs. 2 GDSG)
- Rheinland-Pfalz (§ 37 Abs. 1 LKG)
- Sachsen (§ 34 Abs. 1 SächsKHG)
- Thüringen (§ 27 Abs. 4 ThürKHG).

Dem Privileg liegt die Annahme zugrunde, dass zwar eine Zweckänderung, aber keine (weitere) Offenbarung der Patientendaten an nicht an der Behandlung Beteiligte stattfindet.

Andere Krankenhausgesetze erlauben zwar grundsätzlich eine Forschung mit Patientendaten, aber nur, wenn eine Einwilligung vorliegt (z. B. Bremen § 7 Abs. 1 BremKHDSG) oder der Patient nach Information der Nutzung nicht widersprach (z. B. § 14 Saarländisches Krankenhausgesetz).

Die DS-GVO bedingt die Anpassung der nationalen datenschutzrechtlichen Regelungen, was natürlich auch die Regelungen in den Landeskrankenhausgesetzen betrifft. D. h. die künftige Gesetzgebung muss hier verfolgt werden.

6 Zweckanpassung: Privilegierung der Forschung

Mitunter werden für Forschungszwecke personenbezogene Daten benötigt, die ursprünglich für einen anderen Zweck erhoben wurden. Art. 5 Abs. 1 lit. b DS-GVO schreibt hier „eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Art. 89 Abs. 1 DS-GVO nicht als unvereinbar mit den ursprünglichen Zwecken“. D.h. hier findet ggf. zwar eine Zweck*änderung* statt, jedoch sind der „alte“ und der „neue“ Zweck miteinander vereinbar.

Somit können unter den bereits beschriebenen Voraussetzungen von Art. 89 Abs. 1 DS-GVO (siehe Kap. 5.2) z. B. Daten der Routineversorgung grundsätzlich für wissenschaftliche Forschungsvorhaben genutzt werden, wenn ein Erlaubnistatbestand (siehe Kap.5) vorhanden ist.

6.1 Information des Betroffenen

Eine betroffene Person muss grundsätzlich über alle Empfänger „seiner“ personenbezogenen Daten informiert werden. Wenn daher vorhandene Daten zur Forschung genutzt werden sollen und dabei ein der betroffenen Person noch nicht bekannter Empfänger (z. B. Mitarbeiter im Forschungsprojekt, die mit der Versorgung der betroffenen Person nichts zu tun hatten wie beispielsweise

[39] Das Bundesdatenschutzgesetz wird, wie andere Gesetze auch, entsprechend den Vorgaben der DS-GVO angepasst. Derzeit ist noch nicht absehbar, inwieweit sich die Gesetze ändern, welche Erlaubnistatbestände für die Forschung in welchem Gesetz stehen werden. Hier muss in den nächsten Jahren die Gesetzgebung aufmerksam verfolgt werden.

Epidemiologen oder Statistiker) involviert ist, so ist die betroffene Person gemäß Art. 14 DS-GVO hierüber zu informieren, wenn nicht einer der in Art. 14 DS-GVO verankerten Ausnahmetatbestände zutrifft. Bzgl. der Pflichtinhalte der Information siehe Kap. 7.4.1.1 bzw. Kap. 7.4.1.

6.2 Recht auf Widerspruch

Entsprechend Art. 21 Abs. 6 DS-GVO hat eine betroffene Person ein Widerspruchsrecht hinsichtlich der Verarbeitung sie betreffender personenbezogener Daten zu wissenschaftlichen oder historischen Forschungszwecken. Dieses Widerspruchsrecht entfällt nur dann, wenn die Verarbeitung zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe erforderlich ist.

7 Grundlegende Pflichten

Forschungsaktivitäten müssen im datenschutzrechtlichen Sinne ausgestaltet werden (Art. 89 Abs. 1 DS-GVO), dies umfasst insbesondere:

- Beachtung datenschutzrechtlicher Grundsätze, insb. Art. 5 DS-GVO (Transparenz, Zweckbindung, Datenminimierung, Speicherbegrenzung, Rechenschaftspflicht, …)
- Beachtung der Betroffenenrechte, insbesondere Informationspflichten (Erhebung, Zweckänderung) und Widerspruchsrecht (Art. 21 Abs. 6)
- DS-GVO Forschung nur bei Vorhandensein „geeigneter“ technischer und organisatorischer Maßnahmen (insbesondere Artt. 25, 30, 32)

7.1 Rechenschaftspflichten

Aufgrund der in Art. 5 Abs. 2 DS-GVO enthaltenen Rechenschaftspflicht erwachsen Forschern grundsätzliche Nachweispflichten. Demzufolge muss der Verantwortliche (bzw. ggf. die forschende Institution) darlegen können, dass es sich um wissenschaftliche Forschung oder historische Forschung handelt. Die Nachweispflicht beinhaltet ferner die Pflicht zur Nachvollziehbarkeit. Dieses wiederum hat zur Folge, dass eine nachvollziehbare schriftliche oder elektronische Dokumentation, bei der Änderungen unter Berücksichtigung des zeitlichen Verlaufs erkennbar sind, angefertigt werden muss.

7.1.1 Nachweis Forschung

Für den Bereich der Forschung bedeutet dies, dass vor Beginn der Forschung ein objektiv überprüfbarer (d.h. durch einen externen Auditor z. B. eine Datenschutzaufsichtsbehörde) Nachweis geführt werden muss, dass es sich zunächst einmal um eine Forschung im Sinne der DS-GVO handelt. D.h. es muss ein Nachweis erbracht werden, dass der Verarbeitungsvorgang

- eine systematische Suche nach neuen Erkenntnissen beinhaltet und
- eine sorgfältige Dokumentation geplant und durchgeführt wird und
- eine Veröffentlichung der Ergebnisse erfolgen wird und
- die Ergebnisse der Suche
    a) dem öffentlichen Interesse im Bereich der öffentlichen Gesundheit dienen oder
    b) der Verbesserung der Lebensqualität zahlreicher Menschen bedeuten oder
    c) eine Verbesserung der Effizienz der Sozialdienste beinhalten oder
    d) der klinischen Prüfung therapeutischer Maßnahmen dienen oder

e) die Registerforschung unterstützen.

7.1.2 Nachweis „wissenschaftlich“

Auch der Nachweis bzgl. der „Wissenschaftlichkeit“ muss geführt werden. Im Sinne des „Hochschul-Urteils“ des BVerfG[40] bedeutet dies, dass

- nach Inhalt als auch der Form
- ein ernsthafter planmäßiger Versuch zur Ermittlung der Wahrheit

erfolgen muss. D. h. vor Beginn der Forschung muss Zweck und Versuchsplanung unter Berücksichtigung dieser aus dem Gerichtsurteil resultierenden Anforderungen dargelegt werden.

Dazu gehört auch die Darlegung der Forschungsfinanzierung. Denn nur, wenn eine Forschung solide finanziert ist, kann diese auch ernsthaft durchgeführt werden. In allen anderen Fällen muss damit gerechnet werden, dass aufgrund von Finanzierungslücken die Forschung abgebrochen werden muss und damit eine „Ernsthaftigkeit“ der Forschung anzweifelbar wäre.

Wie vorstehend dargestellt, ist die eigentliche Teilnahme am Wissenschaftsbetrieb grundsätzlich nicht den Universitäten vorbehalten, vielmehr steht die wissenschaftliche Betätigung außerhalb des akademischen oder industriellen Wissenschaftsbetriebs jedermann offen[41].

7.1.3 Nachweis „historisch“

Im Sinne der Nachweisbarkeit der DS-GVO, dass es sich um historische Forschung handelt, müssen daher, u.a. aufgrund der für die Forschung bestehenden Privilegien und des damit einhergehenden Risikos für die Betroffenenrechte, insbesondere folgende Nachweise erbracht werden:

1) Es liegt eine spezifische Fragestellung vor.
2) Die Grundlage der Forschung bilden historische Quellen,
3) die Tatsachen darstellen.
4) Die Interpretation der historischen Quellen erfolgt nach den Stand der Wissenschaft.
5) Die Ergebnisse werden zur öffentlichen Diskussion publiziert, sei es in einer Zeitschrift, in einem Buch oder auf einer jedermann verfügbaren und gut auffindbaren Webseite im Internet.

Da die Daten Verstorbener nicht unter das Datenschutzrecht fallen (siehe Kapitel 5.1.2.3), ist es zur datenschutzrechtlichen Bewertung zudem wichtig darzulegen, ob die auszuwertenden historischen Quellen sich auf noch lebende Personen beziehen oder ausschließlich Daten verstorbener Menschen von dem Forschungsvorhaben betroffen sind.

7.1.4 Sorgfaltspflichten

Grundsätzlich ist ferner der Nachweis zu erbringen, dass der oder die Verantwortliche/n den aus der DS-GVO resultierenden Sorgfaltspflichten nachgekommen sind. Dazu gehört auch der Nachweis der in den Kapiteln 7.2, 7.4 und 7.6 dargestellten datenschutzrechtlichen Anforderungen, aber auch der

[40] BVerfG, Urteil v. 29.05.1973, AZ. 1 BvR 424/71B. Online, zitiert 2017-02-10; Verfügbar unter https://dejure.org/dienste/vernetzung/rechtsprechung?Gericht=BVerfG&Datum=29.05.1973&Aktenzeichen=1%20BvR%20424/71; Kommentierung siehe z.B. Epping/Lenz/Leydecker „Sachlicher Schutzbereich der Wissenschaftsfreiheit“ in Epping. Grundrechte. 6. Auflage 2015, Springer-Verlag, ISBN 978-3-642-54657-0

[41] BBWF: Was ist Wissenschaft? Online, zitiert 2017-02-10; Verfügbar unter https://www.bbwf.de/wissenschaft/was-ist-wissenschaft

Nachweis der Einhaltung von grundlegenden Anforderungen wie beispielsweise die Identifizierung von Vertragspartnern.

7.2 Beachtung der Grundsätze für die Verarbeitung personenbezogener Daten

Die zentralen Grundsätze sind in Art. 5 DS-GVO festgelegt. Jegliche Verarbeitung personenbezogener Daten muss diesen Vorgaben entsprechen. Tut sie dieses nicht, ist die Verarbeitung als nicht rechtskonform anzusehen.

Dementsprechend muss auch jede im Forschungsbetrieb durchgeführte Verarbeitung so ausgestaltet sein, dass die nachfolgend vorgestellten grundlegenden und maßgeblichen Anforderungen der DS-GVO erfüllt sind:

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz (Art. 5 Abs. 1 lit. a DS-GVO)
  Die Verarbeitung darf nur auf rechtmäßige Weise und muss in einer für die betroffene Person nachvollziehbaren Weise erfolgen. Um den Nachweis hierfür zu erbringen, können beispielsweise folgende Maßnahmen dienen:
  - Im Verzeichnis der Verarbeitungstätigkeiten werden der Verwendungszweck und die Rechtsgrundlage dargestellt. Diese beiden Aspekte müssen auch der betroffenen Person bei der Datenerhebung mitgeteilt werden.
  - In der Datenschutzerklärung ist dargestellt, wie der Datenschutz im datenverarbeitenden Unternehmen/Behörde/... gelebt wird
  - Im Rollen- und Berechtigungskonzept ist festgeschrieben, wer wann aus welchen Gründen zu welchen Zwecken welche Daten wie verarbeiten darf.
  - Durch eine Protokollierung kann überprüft werden, wer wann zu welchen Zwecken auf welche Daten zugegriffen hat.
  - Der betroffenen Person steht im Rahmen des im Forschungsbereich notwendigen Self-Managements die Möglichkeit zur Verfügung, zu bestimmen, wer wann welche Daten zu welchen Zwecken nutzen darf; zugleich kann die betroffene Person jeglicher Verarbeitung widersprechen, soweit ein Widerspruch rechtlich möglich ist.
  - Etablierung eines „Single Point of Contact“ (SPoC) für die betroffenen Personen bzgl. aller Fragen, die den Datenschutz berühren.
- Zweckbindung (Art. 5 Abs. 1 lit. b DS-GVO)
  Daten dürfen ausschließlich für genau festgelegte, eindeutige und legitime Zwecke erhoben und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden. Zum Nachweis dieser Anforderungen kann z. B. dienen:
  - Dokumentation der Verarbeitungsziele
  - Darstellung aller Verarbeitungsvorgänge inkl. der Datenarten, welche zur Erreichung der Verarbeitungsziele notwendig sind
  - Auditierung der Verarbeitung
- Datenminimierung (Art. 5 Abs. 1 lit. c DS-GVO)
  Verarbeitung von Daten, welche dem Zweck angemessen und auf das für die Erreichung der Zwecke der Verarbeitung notwendige Maß beschränkt sind. Hierzu können u. a. folgende Maßnahmen dienen:

    - Die Dokumentation der Verarbeitungsziele verbunden mit dem Nachweis des Erfordernisses der erhobenen Daten zur Erreichung des Zweckes
    - Kategorisierung der Daten verbunden mit dem Nachweis des Erfordernisses zur Erreichung des Verarbeitungszweckes
- Richtigkeit (Art. 5 Abs. 1 lit. d DS-GVO)
  Die Daten müssen sachlich richtig sein und es müssen alle angemessenen Maßnahmen getroffen werden, damit unrichtige personenbezogene Daten unverzüglich gelöscht oder berichtigt werden. Methoden für den Nachweis dieser Anforderung können bspw. sein:
    - Direkterhebung bei der betroffenen Person,
    - Nutzung von Hashwerten/elektronischen Signaturen zum Nachweis von Änderungen/Manipulationen,
    - 4-Augen-Prinzip bei der Erhebung sowie der Datenverarbeitung.
- Speicherbegrenzung (Art. 5 Abs. 1 lit. e DS-GVO)
  Speicherung der Daten in einer Form, welche die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Erreichung der Verarbeitungszwecke unbedingt erforderlich ist. Zum Nachweis dieser Anforderung können u. a. dienen:
    - Frühestmögliche Anonymisierung oder Löschung der Daten,
    - bei über die Zweckerreichung hinaus andauernder, gesetzlich geforderter Aufbewahrung umfassende Sperrung des Datenzugriffs,
    - Festlegung der maximal notwendigen Speicherdauer.
- Integrität und Vertraulichkeit (Art. 5 Abs. 1 lit. f DS-GVO)
  Die Verarbeitung der Daten muss eine angemessene Sicherheit der personenbezogenen Daten gewährleisten, einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Verarbeitung sowie vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung. Diese Anforderung kann ggfs. nachgewiesen werden durch:
    - Einsatz von Verschlüsselung (Festplattenverschlüsselung, Datenbankverschlüsselung, ...)
    - Nutzung von Hashwerten/elektronischen Signaturen zum Nachweis von Änderungen/Manipulationen
    - Erstellung regelmäßiger Backups
    - Nutzung redundanter Systeme
    - Nachfrage des Systems vor Ausführung einer Änderung bei sensiblen Daten („Wollen sie dies wirklich tun?“)
- Rechenschaftspflicht (Art. 5 Abs. 2 DS-GVO)
  Der Verantwortliche muss nachweisen, dass er den Anforderungen der DS-GVO genügt. Hierzu ist eine entsprechende Dokumentation aller entsprechenden Vorgänge erforderlich.

7.3 Benennung eines Datenschutzbeauftragten

Die Bestellung eines betrieblichen Datenschutzbeauftragten ist entsprechend Art. 37 DS-GVO für

- alle Behörden und öffentliche Einrichtungen (ausgenommen Gerichte)
- Unternehmen, zu deren Kerntätigkeit eine „umfangreiche regelmäßige und systematische Überwachung“ von Betroffenen gehört
- Unternehmen, zu deren Kerntätigkeit die umfangreiche Verarbeitung von besonderen Kategorien von Daten gehört, die in Art. 9 oder 10 DS-GVO beschrieben werden

verpflichtend. Gesundheitsdaten wie auch genetische Daten gehören zu den besonderen Kategorien von Daten.

Bei der Frage, was unter dem Begriff „Kerntätigkeit“ zu verstehen ist, muss auch ErwGr. 97 berücksichtigt werden. Gemäß ErwGr. 97 liegt eine Kerntätigkeit dann vor, wenn sich die Verarbeitung personenbezogener Daten auf die Haupttätigkeiten bezieht, nicht jedoch auf eine Nebentätigkeit. Im Bereich der medizinischen Forschung ist die Kerntätigkeit gerade die Verarbeitung dieser besonderen Daten, so dass auch dieser Punkt erfüllt ist.

In vielen Fällen wird die Bestellung eines entsprechend qualifizierten Datenschutzbeauftragten unumgänglich sein, da im Bereich der medizinischen Forschung immer sensible Daten verarbeitet werden. Da der Verantwortliche zudem die Einhaltung der datenschutzrechtlichen Anforderungen der DS-GVO zu gewährleisten ist, muss bei der datenverarbeitenden Stelle das entsprechende Fachwissen vorhanden sein. Auch aus dieser Sicht erscheint die Benennung eines qualifizieren Datenschutzbeauftragten für Forschungseinrichtungen unumgänglich.

7.4 Wahrung der Betroffenenrechte

(Anm.: Im Rahmen des DSAnpUG werden auf nationaler Ebene die Betroffenenrechte bei der Verarbeitung besonderer Datenkategorien voraussichtlich eingeschränkt. Nach Gesetzesverabschiedung sind in den folgenden Ausführungen Anpassungen vorzunehmen.)

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

7.4.1 Informationspflicht bei Erhebung bzw. Zweckänderung

Der Umfang der Informationspflicht hängt davon ab, ob

- die Daten für das Forschungsvorhaben direkt beim Betroffenen erhoben werden (Direkterhebung) wie z. B. im Anschluss an eine Einwilligung in eine Studienteilnahme. Davon zu unterscheiden ist die Dritterhebung, bei der die Daten bei Dritten und nicht vom Betroffenen bezogen werden, wie z. B. beim Erhalt von Daten aus anderen Quellen, z. B. von Behandlern;

- die Daten im Rahmen einer Zweckänderung aus einer anderen Verarbeitung stammen, wie z. B. einer vorhergehenden ärztlichen Behandlung.

Unabhängig vom Szenario muss die betroffene Person mindestens über die folgenden Informationen verfügen:

- Der Name und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters
- Der Name und die Kontaktdaten des Datenschutzbeauftragten
- Die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen
- Die Rechtsgrundlage, auf welcher die Datenverarbeitung erfolgen darf
- Die Empfänger (bzw. ggfs. die Kategorien von Empfängern) der personenbezogenen Daten
- Die Speicherdauer der personenbezogenen Daten oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer
- Der Hinweis, dass die Betroffenenrechte ausgeübt werden können, d. h. das Bestehen eines Rechts
    - auf Auskunft über die betreffenden personenbezogenen Daten,
    - auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung,
    - auf einen Widerspruch gegen die Verarbeitung,
    - auf Datenübertragbarkeit,
    - auf die Beschwerde bei einer Aufsichtsbehörde.
- Falls die Datenverarbeitung auf Grundlage einer Einwilligung beruht, ist zwingend der Hinweis auf das Bestehen eines Rechts erforderlich, dass die betroffene Person jederzeit die erteilte Einwilligung widerrufen kann, ohne dass dadurch jedoch die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird
- Falls die Datenverarbeitung eine automatisierte Entscheidungsfindung beinhaltet, müssen aussagekräftige Informationen über die involvierte Logik der automatisierten Entscheidungsfindung sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person mitgeteilt werden
- Sofern vorgesehen, die Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln, inklusive der Rechtsgrundlage, welche die Übermittlung legitimiert (z. B. basierend auf einem Angemessenheitsbeschluss der Kommission)

7.4.1.1 Bei Erhebung der Daten bei der betroffenen Person

Werden die Daten bei der betroffenen Person erhoben, müssen ihr die Informationen zum Zeitpunkt der Erhebung vorliegen. Im Rahmen z. B. einer Studienteilnahme würden die Informationen üblicherweise im Rahmen der Einwilligung in die Teilnahme gegeben werden.

Zusätzlich zu den unter 7.4.1 aufgeführten Informationen muss die betroffene Person über Folgendes informiert werden:

- ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist,
- ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche möglichen Folgen die Nichtbereitstellung hätte

Eine Informationspflicht besteht entsprechend Art. 13 Abs. 4 DS-GVO jedoch nicht, wenn die betroffene Person bereits über diese Informationen verfügt. Im Rahmen der Rechenschaftspflicht

sollte der Verantwortliche dafür Sorge tragen, dass er bei Verzicht der Informationsweitergabe an die betroffene Person diesen Umstand auch für Dritte nachvollziehbar belegen kann.

7.4.1.2 Bei Erhebung der Daten nicht bei der betroffenen Person

Die Informationen müssen unter Berücksichtigung der spezifischen Umstände der Verarbeitung innerhalb einer angemessenen Frist nach Erlangung der Daten, längstens jedoch nach einem Monat erteilt werden. Sollten die Daten zur Kommunikation mit der betroffenen Person vor Ablauf dieser Frist herangezogen werden, ist die Information zum Zeitpunkt der ersten Mitteilung zu erteilen. Im Fall der Absicht der Offenlegung gegenüber einem anderen Empfänger ist die Information vor dem Zeitpunkt der Offenlegung zu erteilen.

Zusätzlich zu den unter 7.4.1 aufgeführten Informationen muss die betroffene Person darüber informiert werden, aus welcher Quelle die Daten stammen und ob sie gegebenenfalls aus öffentlich zugänglichen Quellen stammen.

D. h. dass ein Patient vor Verwendung von Daten aus der Routineversorgung (oder anderer Daten, die nicht direkt bei der betroffenen Person erhoben wurden) über die weitere Verwendung dieser Daten zu einem Forschungszweck vom Verantwortlichen (dies ist i.d.R. die Behandler bzw. die den Patienten versorgende Einrichtung) grundsätzlich informiert werden muss.

Eine Informationspflicht besteht jedoch nur dann, wenn nicht ein Ausnahmetatbestand gemäß Art. 14 Abs. 5 DS-GVO vorliegt. Diese Ausnahmetatbestände sind:

a) Die betroffene Person verfügt bereits über alle Informationen.
b) Die Erteilung der Information ist unmöglich. Dies korrespondiert auch mit § 275 BGB: Die Erbringung einer unmögliche Leistung ist ausgeschlossen. Jedoch liegt der Nachweis, dass dies unmöglich ist, bei der Partei, welche die Leistung mit dieser Begründung verweigert. Es muss wirklich unmöglich sein, die Leistung zu erbringen; es genügt nicht, wenn für die Erbringung der Leistung ein sehr hoher Aufwand und/oder hohe finanzielle Beträge erforderlich sind[42].
c) Die Erteilung der Information erfordert einen unverhältnismäßigen Aufwand. ErwGr. 62 gibt als Anhaltspunkte zu diesem Punkt „die Zahl der betroffenen Personen, das Alter der Daten oder etwaige geeignete Garantien“ an. Die Rechtsprechung setzt hohe Maßstäbe bzgl. der Unverhältnismäßigkeit an. Eine Verweigerung ist nur möglich, wenn der erforderliche Aufwand „unter Beachtung des Inhalts des Schuldverhältnisses und der Gebote von Treu und Glauben in einem groben Missverhältnis zu dem Leistungsinteresse des Gläubiger steht[42]“.
   Hierbei ist immer zu beachten, wer das Leistungshindernis zu vertreten hat. Verursachte beispielsweise der Verantwortliche auf Grund eigener Maßnahmen den Aufwand, so ist dies anders zu bewerten als wenn der Aufwand durch Vorgaben von für ihn geltenden gesetzlichen Regelungen verursacht wird. Basiert, wie im vorliegenden Fall, die Auskunftspflicht auf einem Rechtsanspruch, so muss der Verantwortliche schon vor Beginn der Verarbeitung Sorge tragen, dass er der Rechtspflicht entsprechen kann, d. h. selbst verschuldete Leistungshindernisse werden vor Gericht voraussichtlich nicht als „unverhältnismäßiger Aufwand“ angesehen werden.

[42] so z.B. LG Kiel, Urt. v. 04.04.2008 Az. 8 O 50/07: „Krankenhaushaftung: Berufung des Krankenhauses auf die faktische Unmöglichkeit des Auffindens der Originalbehandlungsunterlagen des Patienten“. [Online] 2008 [Zitiert 2017-03-18] Verfügbar unter https://dejure.org/gesetze/BGB/275.html

Was unverhältnismäßiger Aufwand ist, lässt sich letztlich nur im Einzelfall beurteilen[43]. Der Kostenaufwand allein ist keine Begründung für eine Unverhältnismäßigkeit[43]. Vielmehr ist der durch den Vorgang zu erzielende Erfolg ggf. auch der Teilerfolg bei Abwägung aller Umstände des Einzelfalls zu betrachten: steht dieser in keinem vernünftigen Verhältnis zur Höhe des dafür gemachten Geldaufwandes, ist nicht zumutbar, dass die Aufwände vom Verantwortlichen zu tragen sind. In einem solchen Fall würde es Treu und Glauben widersprechen, wenn die betroffene Person die Aufwendungen für die Information dem Verantwortlichen anlasten könnte[44].

d) Rechtsvorschriften der Union oder des Mitgliedstaates, deren Regelungen der Verantwortliche unterliegt, verbieten eine Auskunftserteilung bzw. gestatten die Verweigerung der Informationserteilung.

e) Die betreffenden personenbezogenen Daten unterliegen dem Berufsgeheimnis, welches eine Vertraulichkeit verlangt und eine Information nicht erlaubt. In Deutschland bedeutet dies, dass der von § 203 StGB (und ggf. korrespondierenden Berufsordnungen wie bspw. einer Landes-Berufsordnung für Ärztinnen/Ärzte) adressierte Personenkreis weiterhin der Schweigepflicht unterliegt, hier also keine Offenbarungsbefugnis vorliegt. Beinhaltet die Information durch § 203 StGB geschützte Daten, die durch die Informationserteilung unbefugt offenbart werden, ist daher die Informationsweitergabe zu verweigern. Hierbei ist jedoch zu bedenken, dass i.d.R. § 203 StGB hinsichtlich der die Geheimnis betreffende Person nicht anzuwenden ist.

Ist Letzteres der Fall, muss der Verzicht der Information des Betroffenen gemäß Art. 5 dokumentiert werden, damit bei einer Überprüfung die Entscheidungsfindung bzgl. des Informationsverzichts des Betroffenen dargestellt und von den Prüfern nachvollzogen und beurteilt werden kann.

7.4.2 Recht auf Auskunft

Jeder Betroffene hat das Recht nachzufragen, ob von einem Verantwortlichen seine personenbezogenen Daten verarbeitet werden. Ist dies der Fall, so hat die betroffene Person das Recht zu erfahren, welche Daten dies sind. Weiterhin muss der Verantwortliche dem Betroffenen die Rahmenbedingungen, unter denen die Verarbeitung stattfindet, mitteilen. Zu diesen Informationen gehören insbesondere

- die Verarbeitungszwecke
- die Kategorien personenbezogener Daten
- die Empfänger oder Kategorien von Empfängern (auch geplante)
- die Speicherdauer der personenbezogenen Daten oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer
- alle verfügbaren Informationen über die Herkunft der Daten (nur, wenn die Daten nicht bei der betroffenen Person selbst erhoben wurden)
- das Bestehen der Betroffenenrechte
    - das Recht auf Berichtigung durch den Verantwortlichen

[43] VG Münster, Urt. v. 13.09.2013 Az. 1 K 3312/12 Rn. 45. [Online] 2013 [Zitiert 2017-03-18] Verfügbar unter https://openjur.de/u/647373.html

[44] so z.B.

- BGH, Urt. v. 11.10.2012 Az. VII ZR 179/11, Rn. 17. [Online] 2012 [Zitiert 2017-03-18] Verfügbar unter https://openjur.de/u/557191.html
- BVerwG, Urt. v. 17.03.2016 Az. 7 C 2.15, Rn 24. [Online] 2016 [Zitiert 2017-03-18] Verfügbar unter http://www.bverwg.de/entscheidungen/entscheidung.php?ent=170316U7C2.15.0

    - das Recht auf Löschung oder auf Einschränkung der Verarbeitung der personenbezogenen Daten durch den Verantwortlichen
    - das Recht auf Widerspruch gegen diese Verarbeitung
    - das Recht zur Beschwerde bei einer Aufsichtsbehörde
- wenn eine automatisierte Einzelentscheidung oder ein Profiling unter Nutzung der personenbezogenen Daten durchgeführt wurde
    - aussagekräftige Informationen über die zur Entscheidungsfindung eingesetzte Logik
    - alle benötigten Informationen, damit die betroffene Person die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für sich erkennt
- bei Übermittlung in ein Drittland oder an eine internationale Organisation muss die Person informiert werden, welche Garantien zum Schutz der Daten des Betroffenen existieren.

Diesen Ausführungen folgend hat somit grundsätzlich ein Patient wie auch ein Proband ein Recht auf Einblick in die (Forschungs-) Unterlagen. Der Sponsor bzw. Leiter der klinischen Prüfung ist verpflichtet, dem Probanden Einblick in die Unterlagen zu gewähren und Kopien aller Papiere herauszugeben, die sich auf den Versuch an diesem Probanden beziehen.

7.4.3 Berichtigung der Daten

Ein jeder Betroffene hat das Recht, dass seine Daten beim Verantwortlichen korrekt gespeichert sind. Dazu muss er auch die Möglichkeit haben, seine Daten berichtigen zu lassen. In dem Umfang, wie der Betroffene in die Forschung eingebunden ist und Kenntnis von seinen bei dem konkreten Forschungsprojekt verwendeten Daten hat, hat er auch das Recht erkannte falsche Daten berichtigen zu lassen.

Diesem Gedanken folgt Art. 16 DS-GVO: Danach hat der Patient/Proband das Recht, die unverzügliche Berichtigung unrichtiger Daten zu verlangen. Ebenso besteht, das Recht, die Vervollständigung unvollständiger Daten zu verlangen. Inwieweit diese Rechte in einem Forschungsvorhaben sinnvoll zum Tragen kommen können, hängt von der Betrachtung des Einzelfalls ab.

7.4.4 Löschung der Daten

Grundsätzlich hat jeder das Recht auf Löschung seiner personenbezogenen Daten, wenn die Rechtsgrundlage zur Speicherung bzw. für eine weitere Verarbeitung nicht oder nicht mehr gegeben ist. Dies ist der Fall, wenn entweder der Betroffene seine Einwilligung widerruft oder eine gesetzlich geforderte Aufbewahrungsfrist abgelaufen ist und keine anderen rechtlichen Erlaubnistatbestände vorliegen. Jedoch ist es gerade in der medizinischen Forschung oftmals wichtig, medizinische Daten für einen langen Zeitraum zu speichern. Daher erfolgt im Folgenden eine nähere Betrachtung des Themas „löschen“.

7.4.4.1.1 Begriffsbestimmung „Löschen“

Die Begriffsbestimmungen finden sich in der Richtlinie 95/46/EG[45] des Europäischen Parlaments und des Rates. In Art. 2 lit. b) der RL 95/46/EG[46] wird „Löschen“ der „Verarbeitung personenbezogener Daten“ zugerechnet, selbst jedoch nicht definiert.

[45] 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] 1995 [Zitiert 2015-04-30] Verfügbar unter http://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX:31995L0046

Entsprechend dem Urteil des Europäischen Gerichtshofs vom 13. Mai 2014[47] ist der Begriff „Löschen“ im Sinne von „Löschen im physikalischen Sinn“ oder als irreversibel anonymisieren anzusehen. In gleicher Weise äußert sich die Artikel-29-Gruppe in ihrer Stellungnahme[48] zu Datenschutzfragen im Zusammenhang mit Suchmaschinen. Diese Anonymisierung muss jedoch vollständig unumkehrbar sein, damit die Datenschutzrichtlinie nicht länger greift und dem Begriff des „Löschens“ entsprochen wird.

Diese Auffassung wird auch in anderen Ländern Europas geteilt. Der Oberste Gerichtshof, die oberste Instanz in Zivil- und Strafsachen in Österreich, versteht unter Löschen einen Vorgang, der zu einem unwiderruflichen Beseitigen der Daten führt[49]. Darunter versteht der ÖOGH Maßnahmen, welche bewirken, dass die Daten nicht mehr verfügbar sind.

Aus dem ASNEF/FECEMD-Urteil des EuGH[50] wird ersichtlich, dass Vorgaben einer europäischen Richtlinie, wenn diese hinreichend eindeutig zu interpretieren sind, von einem nationalen Gesetz nicht eingeschränkt werden dürfen. Die Richtlinie 95/46/EG[51] basiert auf der Binnenmarkt-Harmonisierungskompetenz des Art. 114 i.V.m. Art. 26 AEUV[52], dementsprechend können nationale Gesetze keine Änderungen der oder Ergänzungen zur Richtlinie 95/46/EG vornehmen, welche zu einer „unzulässigen Veränderung der Grundsätze des europäischen Datenschutzrechts“[53] führen.

Da die RL 95/46/EG den Begriff „Löschen“ selbst aber nicht definiert, muss von einer entsprechenden Interpretationsmöglichkeit des nationalen Gesetzgebers ausgegangen werden, d.h. eine Definition im Sinne des rein physikalischen Vernichtens als Löschbegriff als Interpretation der RL 95/46/EG ist als rechtmäßig anzusehen.

Mit Wirkeintritt der DS-GVO gilt zudem das harmonisierte europäische Recht, auch für Daten, die vor Wirkeintritt der DS-GVO erhoben wurden. D. h. „Löschen“ ist im Sinne von „Löschen im physikalischen Sinn“ oder als irreversibel anonymisieren anzusehen.

---

[46] 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 (Amtsblatt Nr. L 281 vom 23/11/1995 S. 0031 - 0050). [Online] 1995 [Zitiert 2015-04-30] Verfügbar unter http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:31995L0046&from=DE

[47] EuGH, Urteil vom 13. 5. 2014 - C-131/12. [Online] 2014 [Zitiert 2015-04-30] Verfügbar unter https://dejure.org/dienste/vernetzung/rechtsprechung?Gericht=EuGH&Datum=13.05.2014&Aktenzeichen=C-131/12

[48] Stellungnahme 1/2008 zu Datenschutzfragen im Zusammenhang mit Suchmaschinen. [Online] 2008 [Zitiert 2015-04-30] Verfügbar unter http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_de.pdf

[49] ÖOGH AZ 6 Ob 41/10p, Urteil vom 15.4.2010 [Online] 2008 [Zitiert 2015-04-30] Verfügbar unter http://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Justiz&Dokumentnummer=JJT_20100415_OGH0002_0060OB00041_10P0000_000

[50] EuGH C-468/10, C-469/10, Urteil vom 24.11.2011. [Online] 2011 [Zitiert 2017-05-07] Verfügbar unter http://curia.europa.eu/juris/document/document.jsf?text=&docid=115205&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1

[51] 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] 1995 [Zitiert am 2015-03-27]; Verfügbar unter http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:31995L0046&from=de

[52] Vertrag über die Arbeitsweise der Europäischen Union (AEUV). [Online] 2009 [Zitiert 2015-04-30] Verfügbar unter http://www.aeuv.de/aeuv/dritter-teil/titel-vii/kapitel-3/art-114.html

[53] Kingree T, Kühling J. (2015) Überformende Vorgaben des EU-Sekundärrechts, S. 126. in Thorsten Kingreen/Jürgen Kühling (Hrsg.) Gesundheitsdatenschutzrecht. 1. Auflage. Nomos Verlagsgesellschaft. ISBN 978-3-8487-1680-7

7.4.4.1.2 Begriffsbestimmung „Unkenntlichmachen“

„Unkenntlichmachen“ ist in den Datenschutzgesetzen nicht definiert. In Urteilen[54] wird als Beispiel für „Unkenntlichmachen“ auch das Abdecken von Daten bei Vorlage entsprechender Unterlagen angeführt. Im Standardkommentar zum BDSG (Simitis[55]) wird „Unkenntlichmachen“ als jede Handlung definiert, die irreversibel bewirkt, dass eine Information nicht länger aus gespeicherten Daten gewonnen werden kann. Dazu werden mehrere Möglichkeiten dargestellt, denen aber alle eine Forderung zugrunde liegt: Die Informationen dürfen nicht reproduzierbar sein. Entsprechend Simitis et al. existieren damit vier verschiedene Möglichkeiten, um ein „Unkenntlichmachen zu erreichen[56]:

a) Entfernen oder Überschreiben der Informationen
   Daten werden hierbei durch Entfernung oder Überschreiben der die Daten speichernden Informationen (Referenzen?) gelöscht, ohne dass hierbei jedoch die Integrität des Datenträgers selbst beeinträchtigt wird
b) Zerstörung des Datenträgers
   Daten werden durch das physikalische Zerstören des Datenträgers vernichtet und sind damit unkenntlich
c) Löschung der Verknüpfung
   Ergibt sich eine zu löschende Information aus der Verknüpfung zweier (oder mehrerer) Teilmengen, jedoch nicht aus den unverknüpften Teilmengen, so kann eine datenschutzrechtliche Löschung der Information auch durch eine irreversible Löschung der Verknüpfung erfolgen
d) Beseitigung der Interpretierbarkeit
   Die Daten sind nicht mehr interpretierbar, z. B. weil Angaben zur Speicherorganisation oder Entschlüsselung nicht (mehr) vorhanden sind.

Somit sind Daten im datenschutzrechtlichen Sinn nur dann „unkenntlich“ gemacht, wenn die Kenntnisnahme der den Daten innewohnenden Informationen der verantwortlichen Stelle unmöglich ist.

7.4.4.1.3 Wann muss man löschen?

Entsprechend Art. 17 DS-GVO sind personenbezogene Daten unverzüglich zu löschen, wenn einer der folgenden Tatbestände zutrifft:

a) Die Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig.
b) Die betroffene Person widerruft ihre Einwilligung und es fehlt eine andere Rechtsgrundlage für die Verarbeitung.
c) Die betroffene Person legt entsprechend Art. 21 Abs. 1 DS-GVO Widerspruch gegen die Verarbeitung ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor.

[54] z.B. BGH AZ IVb ZR 374/81 , Urteil vom 13. April 1983. [Online] 1983 [Zitiert 2015-04-30] Verfügbar unter https://www.jurion.de/de/document/show/0:327554,0/ oder auch BGH Az. XII ZB 212/11, Urteil vom 9. November 2011. [Online] 2011 [Zitiert 2015-04-30] Verfügbar unter http://openjur.de/u/258298.html

[55] Prof. Dr. Dres. h. c. Spiros Simitis (Hrsg.) Bundesdatenschutzgesetz. 8. Auflage. Nomos Verlag. ISBN 978-3-8487-0593-1

[56] Dammann U. § 3 BDSG Rn. 172-182 in: Simitis (Hrsg.) Bundesdatenschutzgesetz. Nomos Verlagsgesellschaft, 8. Auflage 2014, ISBN ISBN 978-3-8487-0593-1

d) Die betroffene Person legt gemäß Art. 21 Abs. 2 DS-GVO Widerspruch gegen die Verarbeitung ein.
e) Die personenbezogenen Daten wurden unrechtmäßig verarbeitet.
f) Die Löschung der personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich.
g) Die personenbezogenen Daten wurden in Bezug auf angebotene Dienste der Informationsgesellschaft mit der Einwilligung eines Kindes entsprechend Art. 8 Abs. 1 DS-GVO erhoben.

7.4.4.1.4 Einschränkung der Löschpflicht

Art. 17 Abs. 3 lit. b DS-GVO schränkt das Recht auf Löschung jedoch ein, wenn die Daten zur Erfüllung einer rechtlichen Verpflichtung benötigt werden. Entsprechend §630f BGB[57] gilt:

> *Berichtigungen und Änderungen von Eintragungen in der Patientenakte sind nur zulässig, wenn neben dem ursprünglichen Inhalt erkennbar bleibt, wann sie vorgenommen worden sind. Dies ist auch für elektronisch geführte Patientenakten sicherzustellen.*

Dementsprechend dürfen auch unrichtige Einträge einer Patientenbehandlung während der Zeitdauer der Aufbewahrungsfrist nicht gelöscht werden, vielmehr muss hier eine Sperrung veranlasst werden. Werden daher Patientendaten für die Forschung genutzt und nicht separat von den Behandlungsdaten gespeichert, muss ggf. hierauf geachtet werden. Ebenso müssen ggf. gesetzliche Aufbewahrungsfristen, z. B. resultierend aus dem Arzneimittelgesetz, bei Forschungsdaten beachtet werden. Eine Löschung ist immer erst nach Ablauf einer gesetzlich vorgeschriebenen Aufbewahrungspflicht statthaft.

Weiterhin gilt entsprechend Art. 17Abs. 3 lit. d DS-GVO eine Einschränkung des Rechts auf Löschung, wenn eine Löschung die Verwirklichung von Forschungszielen unmöglich macht oder ernsthaft beeinträchtigt. In diesen Fällen sind die Daten jedoch unmittelbar nach Erreichung des Zieles zu löschen.

7.4.5 Einschränkung der Verarbeitung („Sperren“)

Entsprechend Art. 18 kann eine betroffene Person von einem Verantwortlichen die Einschränkung der Verarbeitung („Sperrung“) verlangen, wenn mindestens eine der nachfolgend genannten Bedingungen zutrifft:

a) Die betroffene Person bestreitet die Richtigkeit der Daten; so sind für die Dauer der Prüfung der Richtigkeit der Daten diese zu sperren.
b) Die betroffene Person legte gemäß Artikel 21 Absatz 1 Widerspruch gegen die Verarbeitung ein; für die Zeitdauer der Prüfung, ob der Widerspruch begründet ist, als auch für den Zeitraum, in welchem der Verantwortliche die Entscheidung herbeiführt, ob dem Widerspruch gefolgt werden muss, sind die Daten zu sperren.
c) Die Daten werden für die Zwecke des Verantwortlichen nicht länger benötigt, die betroffene Person benötigt die Daten jedoch noch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen (z B. innerhalb eines Rechtsprozesses gegen den Verantwortlichen).
d) Die Daten wurden unrechtmäßig erhoben, jedoch lehnt die betroffene Person die Löschung ab und verlangt statt der Löschung eine Sperrung derselben.

[57] Bürgerliches Gesetzbuch (BGB) § 630f Dokumentation der Behandlung. [Online] 2015 [Zitiert 2015-04-30] Verfügbar unter http://www.gesetze-im-internet.de/bgb/__630f.html

D.h., bei einer „Einschränkung der Verarbeitung“ ist die Verarbeitung dieser Daten nicht grundsätzlich unmöglich, wie dies bei gelöschten Daten der Fall ist. Vielmehr ist die Verarbeitung lediglich eingeschränkt (daher der Name). Die „normale“ Verarbeitung ist nicht mehr statthaft, lediglich für die vom Gesetz angesprochenen Prüfzwecke dürfen diese Daten noch verwendet werden. Art. 18 Abs. 2 DS-GVO besagt, dass gesperrte Daten (abgesehen von der eigentlichen Speicherung) nur zu folgenden Zwecken verwendet werden dürfen:

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

Auch ist die Einschränkung zeitlich begrenzt. Je nach Grund für die erfolgte Einschränkung der Verarbeitung endet diese bzgl. der Gründe a) und b) mit dem Prüfergebnis, hinsichtlich Grund c) mit dem Ende des Rechtsstreits der betroffenen Person. Ist die Zeitspanne hinsichtlich der Einschränkung vorbei, sind die Daten zu löschen oder - je nach Ergebnis der Prüfung in den Fällen a) und b) wieder der „normalen“ Verarbeitung zuzuführen.

Ist die Zeitspanne der Einschränkung vorbei, so muss der Verantwortliche gemäß Art. 18 Abs. 3 DS-GVO die betroffene Person hierüber informieren.

7.4.6 Mitteilungspflicht bei Berichtigung, Löschung oder Einschränkung

Werden Daten seitens des Verantwortlichen (also des Forschers bzw. der forschenden Stelle) an Empfänger weitergegeben, so sind diese über jede Berichtigung, Löschung oder Einschränkung der Verarbeitung von personenbezogenen Daten zu informieren. Eine Information darf nur unterbleiben, wenn dies mit einem unverhältnismäßig hohen Aufwand verbunden ist. (Bzgl. Unverhältnismäßigkeit siehe Kapitel 7.4.1.2, Abschnitt c).

7.4.7 Recht auf Datenübertragbarkeit

Die europäische Datenschutz-Grundverordnung (DS-GVO) gewährt Betroffenen ein Recht auf Datenübertragbarkeit. Damit diese es ausüben können, müssen verschiedene (Tatbestands-) Voraussetzungen erfüllt sein. Dazu gehören insbesondere:

- Die personenbezogenen Daten müssen dem Verantwortlichen von der betroffenen Person zur Verarbeitung bereitgestellt worden sein.
- Die Verarbeitung muss auf einer datenschutzrechtlichen Einwilligung oder aufgrund eines Vertrages zwischen Betroffenen und Verantwortlichen erfolgen. Die meisten Forschungsvorhaben werden entweder auf einer Einwilligung oder auf einer vertraglichen Basis beruhen, so dass diese Anforderung bei faktisch allen Forschungsvorhaben erfüllt sein dürfte.

Das Recht auf Datenübertragbarkeit stößt an seine Grenzen, wenn sich in den Datensätzen, die übertragen werden sollen, auch Daten von anderen Betroffenen befinden. In einem solchen Fall sieht ErwGr. 68 vor, dass die Rechte dieser Betroffenen ebenfalls zu berücksichtigen sind. So heißt es:

> „Ist im Fall eines bestimmten Satzes personenbezogener Daten mehr als eine betroffene Person tangiert, so sollte das Recht auf Empfang der Daten die Grundrechte und Grundfreiheiten anderer betroffener Personen nach dieser Verordnung unberührt lassen.“

Sind die vorstehend dargestellten Tatbestandsvoraussetzungen erfüllt, so kann der Betroffene vom Verantwortlichen sowohl den Erhalt (Art. 20 Abs. 1 DS-GVO) als auch die Übermittlung (Art. 20 Abs. 1

und 2 DS-GVO) der Daten an einen Dritten verlangen. Der europäische Gesetzgeber formulierte in der DS-GVO einige Anforderungen bzgl. der Durchführung der Datenübertragbarkeit. Die Anforderungen betreffen insbesondere 3 Themengebiete:

1) Datenübertragung ohne Behinderung
2) Format der Daten
3) Kosten für den Export/Transfer.

7.4.7.1 Bereitstellen durch den Betroffenen

Die DS-GVO selbst enthält keine Legaldefinition des Bereitstellens. In Art. 4 Ziff. 2 DS-GVO finden sich in der Definition der Formulierung „Verarbeitung" Informationen, welche eine Interpretation der Begrifflichkeit „Bereitstellen" erlauben:

> „[…] die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung […]".

Aus der Systematik dieser Definition lässt sich daher zunächst ableiten, dass die Bereitstellung eine Form der Verarbeitung ist. Daraus lässt sich weiter herleiten, dass ein Betroffener ihn betreffende Daten bereitstellt, wenn er einem Anderen (dem Verantwortlichen) eine Zugriffsmöglichkeit auf diese Daten eröffnet[58].

Da die DS-GVO keine eigene Definition zu dem Begriff der Bereitstellung enthält, erscheint es angezeigt, auf die Definition des Vorschlags für die EU-Richtlinie „über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte"[59] zurückzugreifen, der eine Definition der „Bereitstellung" enthält. So heißt es in Art. 2 Ziff. 10 DS-GVO:

> „'Bereitstellung' die Verschaffung des Zugangs zu oder die Zurverfügungstellung von digitalen Inhalten;"

Diese Definition entspricht der obigen Interpretation von Art. 4 Ziff. 2 DS-GVO, sodass davon ausgegangen werden muss, dass der europäische Gesetzgeber diesen Tatbestand bei der Nutzung des Begriffs „Bereitstellung" im Sinn hatte.

Die Bereitstellung der Daten muss - dem Wortlaut von Art. 20 Abs. 1 DS-GVO folgend - durch die betroffene Person selbst erfolgen. Neben der eigentlichen Erhebung beim Betroffenen werden ggf. auch bei Erhebung bei einem Dritten Daten durch den Betroffenen bereitgestellt. Beruht die Datenerhebung auf einer Einwilligung des oder auf einem Vertragsabschluss mit dem Betroffenen, stellt der Betroffene durch seine Einwilligung bzw. durch den Vertragsabschluss die Daten bereit, denn ansonsten dürften die Daten nicht erhoben werden.

---

[58] Siehe hierzu auch Kamlah W Art.20 Rn. 6 in Plath (Hrsg.) BDSG/DSGVO: Kommentar zum BDSG und zur DSGVO sowie den Datenschutzbestimmungen des TMG und TKG. Otto Schmidt Verlag 2016. ISBN 978-3-504-56074-4: „Der Anwendungsbereich ist damit zumindest diesbezüglich weit, da die Formulierung 'jede andere Bereitstellung' in Art. 4 Abs. 2 offenbar meint, dass jedwede davor genannte Verarbeitungsalternative eine Form der Bereitstellung sein kann"

[59] Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte, COM(2015) 634 final. Online, zitiert am 2016-09-12; Verfügbar unter https://ec.europa.eu/transparency/regdoc/rep/1/2015/DE/1-2015-634-DE-F1-1.PDF bzw. auch http://www.ipex.eu/IPEXL-WEB/dossier/document/COM20150634.do

7.4.7.2 Automatisiertes Verarbeitung

Die DS-GVO enthält keine Legaldefinition des Begriffes der „automatisierten Verarbeitung“. Der deutsche Gesetzgeber definierte im Rahmen der Umsetzung der Richtlinie 95/46/EG in § 3 Abs. 2 BDSG automatisierte Verarbeitung wie folgt:

> „Automatisierte Verarbeitung ist die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen. Eine nicht automatisierte Datei ist jede nicht automatisierte Sammlung personenbezogener Daten, die gleichartig aufgebaut ist und nach bestimmten Merkmalen zugänglich ist und ausgewertet werden kann.“

Dieser Definition folgend ist von einer automatisierten Verarbeitung immer dann auszugehen, wenn die Verarbeitung der Daten unter Einsatz einer Datenverarbeitungsanlage[60] erfolgt.

7.4.7.3 Datenübertragung ohne Behinderung

Die Übermittlung der Daten des Betroffenen von einem Verantwortlichen zu einem anderen muss gemäß Art. 20 Abs. 1 DS-GVO ohne Behinderung erfolgen, wenn eine Behinderung nicht technisch impliziert ist und dem Verantwortlichen eine Änderung der technischen Gegebenheiten nicht möglich oder nicht zumutbar ist[61]. Insbesondere ist es daher unzulässig, das Recht auf Datenübertragbarkeit an Bedingungen zu knüpfen, die einer Behinderung gleichkommen. Insbesondere darf eine Datenübertragung nicht verzögert werden, wenn dafür keine zwingenden technischen Gründe existieren.

7.4.7.4 Format der Daten

Die Daten müssen entsprechend Art. 20 Abs. 1 in einem „strukturierten, gängigen und maschinenlesbaren Format” entweder dem Betroffenen übergeben oder an einen anderen Verantwortlichen übermittelt werden, je nach Willen des Betroffenen. ErwGr. 68 führt hierzu ergänzend aus:

> „[…] sollte die betroffene Person außerdem berechtigt sein, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen, maschinenlesbaren und interoperablen Format zu erhalten […]“.

Diesem Erwägungsgrund folgend ist die Interoperabilität eine zusätzliche Anforderung, welche der Verantwortliche bei einem Datenexport berücksichtigen muss. Nach ErwGr. 68 muss jedoch auch beim Recht des Betroffenen auf Datenübertragbarkeit und die damit verbundene Vorhaltung entsprechender technischer Möglichkeiten stets der Verhältnismäßigkeitsgrundsatz gewahrt bleiben. So heißt es in ErwGr. 68:

> „Das Recht der betroffenen Person, sie betreffende personenbezogene Daten zu übermitteln oder zu empfangen, sollte für den Verantwortlichen nicht die Pflicht begründen, technisch kompatible Datenverarbeitungssysteme zu übernehmen oder beizubehalten.“

Diese Ausführungen haben zur Konsequenz, dass bei dem aus Art. 20 resultierendem Recht stets auch die wirtschaftlichen Interessen des Verantwortlichen hinsichtlich der technischen

[60] Unter einer Datenverarbeitungsanlage versteht der Gesetzgeber eine Anlage zum automatisierten Handhaben von Daten. Entscheidend hierbei ist die erleichterte Zugänglichkeit und Auswertbarkeit der Daten in einem Datenbestand. (Dammann U. § 3 Rn. 79 in Simitis (Hrsg.) Bundesdatenschutzgesetz. 8. Auflage 2014. Nomos Verlagsgesellschaft. ISBN978-3-8487-0593-1)

[61] Insbesondere sind technische Maßnahmen, die eine Übermittlung erschweren, unzulässig. Siehe hierzu Paal B. Art. 20 Rn. 21 in Paal/Pauly (Hrsg.) Datenschutz-Grundverordnung. C. h. Beck Verlag 2016. ISBN 978-3-406-69570-4

Umsetzbarkeit berücksichtigt werden müssen, wenngleich bei Vorliegen der gesetzlichen tatbestandlichen Voraussetzungen dem Rechtsanspruch des Betroffenen nachgekommen werden muss[62]. Dieses kann letzten Endes dazu führen, dass der Verantwortliche dem Recht des Betroffenen Rechnung trägt, indem er die Daten in einem weniger optimalen, aber dennoch „strukturierten, gängigen und maschinenlesbaren" Format zur Verfügung stellt[63].

7.4.7.5 Kosten für den Export/Transfer

Erhalt und Übermittlung der Daten erfolgen entsprechend Art. 12 Abs. 5 DS-GVO in der Regel unentgeltlich. Lediglich bei „offenkundig unbegründeten" oder - insbesondere im Fall von häufiger Wiederholung - exzessiven Anträgen einer betroffenen Person kann der Verantwortliche „ein angemessenes Entgelt verlangen" oder sich sogar weigern, aufgrund des Antrags tätig zu werden.

7.4.7.6 Beschränkung des Rechts

Durch die Regelung in Art. 20 Abs. 3 DS-GVO wird das Recht auf Datenübertragbarkeit dahingehend beschränkt, dass ein Betroffener sich nicht auf dieses Recht berufen kann, wenn die Datenverarbeitung durch den Verantwortlichen „für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt". Diese Regelung wird ergänzt von ErwGr. 68, welcher noch die Vorgabe hinsichtlich der „Erfüllung einer rechtlichen Verpflichtung" enthält, der der Verantwortliche unterliegt. Beispiele für diese von der Verordnung vorgesehenen Ausnahmen können Archiv-, Forschungs- oder statistische Zwecke sein[64].

7.4.8 Widerspruchsrecht

Neben dem Recht auf Widerrufung der Einwilligung zur Verarbeitung einer betroffenen Person betreffenden Daten sieht die DS-GVO auch ein eigenständiges Recht auf den Widerspruch gegen die Verarbeitung vor. Ein Widerspruch entsprechend Art. 21 DS-GVO richtet sich gegen eine rechtmäßige, d.h. auf einer gesetzlichen Grundlage stattfindenden Verarbeitung einer betroffenen Person zurechenbaren bzw. zuordenbaren Daten durch einen Verantwortlichen; für unrechtmäßige Verarbeitung ist ein Widerruf nicht erforderlich, hier besteht entsprechend Art. 17 Abs. 1 lit. d DS-GVO eine unmittelbare Verpflichtung zur Löschung der Daten durch den Verantwortlichen.

Dieses Recht auf Widerspruch gilt grundsätzlich auch für Daten, die zu Forschungszwecken eingesetzt werden (sollen). Entsprechend Art. 21 Abs. 6 DS-GVO hat jede betroffene Person das Recht, „aus Gründen, die sich aus ihrer besonderen Situation ergeben, gegen die sie betreffende Verarbeitung sie betreffender personenbezogener Daten, die zu wissenschaftlichen oder historischen Forschungszwecken [...] erfolgt, Widerspruch einzulegen." Diese Vorgabe korrespondiert mit dem

---

[62] Siehe hierzu auch Kamlah W Art.20 Rn. 9 in Plath (Hrsg.) BDSG/DSGVO: Kommentar zum BDSG und zur DSGVO sowie den Datenschutzbestimmungen des TMG und TKG. ottoschmidt Verlag 2016. ISBN 978-3-504-56074-4: „[...] Diese soll die durch Art. 20 intendierte Datenportabilität nicht durch (technische) Restriktionen unterlaufen dürfen und so den Wettbewerb verhindern."

[63] Siehe hierzu auch Kamlah W Art.20 Rn. 10 in Plath (Hrsg.) BDSG/DSGVO: Kommentar zum BDSG und zur DSGVO sowie den Datenschutzbestimmungen des TMG und TKG. ottoschmidt Verlag 2016. ISBN 978-3-504-56074-4: „[...] Im Zweifel wird man dem Verantwortlichen zubilligen müssen, dass er die betreffende Person auf den Weg nach Abs. 1 *[d.h. Daten selbst zu erhalten]* verweist."

[64] siehe z. B. ErwGr. 65: „[...] zur Erfüllung einer rechtlichen Verpflichtung, für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde, aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, für im öffentlichen Interesse liegende Archivzwecke, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist."

Auskunftsrecht, denn eine betroffene Person kann das ihr zustehende Widerspruchsrecht nur ausüben, wenn sie bzgl. der Verarbeitung informiert wird. Somit müssen Verantwortliche, welche aufgrund eines Ausnahmetatbestandes gemäß Art. 14 Abs. 5 DS-GVO von einer Information der betroffenen Person absehen, diesen Umstand bzgl. der Einschätzung der Zumutbarkeit der Informationserteilung berücksichtigen.

Die Widerspruchsmöglichkeit ist hierbei an das Vorliegen von „Gründen, die sich aus ihrer besonderen Situation ergeben," gebunden. Durch die Begrifflichkeit „besondere Situation" wird deutlich, dass es hier einer Einzelfallprüfung bedarf, d.h. der Widerspruch muss begründet sein. Ein „ich will das nicht" seitens der betroffenen Person genügt nicht den regulatorischen Anforderungen. Denkbar sind hier Begründungen wie beispielsweise

- unzureichende Gewährleistung der Sicherheit der Verarbeitung seitens des Verantwortlichen bzw. ggf. existierender Auftragsverarbeiter,
- bereits erfolgte Datenschutzverletzungen verbunden mit der Befürchtung zukünftig erneut auftretender Vorfälle,
- drohende wirtschaftliche oder soziale Nachteile für den Betroffenen, z. B. wenn die verwendeten Daten durch einen potentiell möglichen Datenschutzvorfall der Öffentlichkeit oder einem Teil von dieser bekannt werden.

Erfolgt die Forschung jedoch im öffentlichen Interesse und ist die Erforderlichkeit der Verarbeitung der von dem Widerspruch betroffenen Daten gegeben, so besteht keine Möglichkeit zum Widerspruch (Art. 21 Abs. 6 letzter HS DS_GVO).

7.4.9 Beschränkung der Zulässigkeit automatisierter Entscheidungen im Einzelfall

Art. 22 DS-GVO verbietet, dass die eine natürliche Person betreffende Entscheidung ausschließlich auf einer automatisierten Verarbeitung beruht. Im Rahmen der Forschung könnte dies beispielsweise bedeuten, dass die Auswahl, ob eine Person zu einer Forschung zugelassen wird oder nicht, nicht ausschließlich automatisiert erfolgen darf. Ein Beispiel für eine automatisierte Entscheidung wäre, wenn Patienten ausschließlich auf Grund bestimmter Labordaten automatisiert ausgewählt werden, also alle Patienten im KIS, die den Laborwerten „ABC" genügen, kommen in die Forschung, alle anderen nicht. Eine Vorabauswahl an Hand der entsprechenden Laborwerte ist selbstverständlich möglich, jedoch müsste anschließend ein Mensch die potentiellen Forschungsteilnehmer begutachten und die Endauswahl (also die „Entscheidung") treffen.

Eine Zuordnung entsprechend Zufallsprinzip für „Blind"-Studien ist hiervon nicht betroffen, da die grundlegende Entscheidung „zur Teilnahme an der Forschung geeignet" ja bereits getroffen wurde und die Zuordnung im Rahmen der Informationspflichten bereits mit dem Probanden/Patienten besprochen und diese Person darüber aufgeklärt wurde. Entsprechend Art. 22 Abs. 2 lit. c DS-GVO erfolgt die Zuordnung somit mit deren Einverständnis (siehe auch Art. 22 Abs. 4 S. 1, 2. HS DS-GVO).

Grundsätzlich ist bei automatisierten Entscheidungen jedoch zu beachten, dass immer angemessene Maßnahmen die Rechte und Freiheiten betroffener Personen bzgl. der Entscheidung gewährleisten. Dazu gehört ggf. (siehe Art. 22 Abs. 3 DS-GVO), dass es seitens des Verantwortlichen eine natürliche Person gibt, die - sofern erforderlich - in den Entscheidungsprozess eingreifen kann und welche dem Betroffenen den eigenen Standpunkt darlegen und u.U. auch die Anfechtung der Entscheidung zustellen kann. Hat z. B. eine Person herausgefunden, dass sie in der „Placebo-Gruppe" ist, und diese Person glaubt, dadurch Nachteile in ihrer Behandlung zu haben, so muss der Verantwortliche für

derartige Fälle einen Menschen als Ansprechpartner bereithalten, der mittels seiner Kompetenz auch in der Lage ist, die betroffene Person falls notwendig einer anderen Gruppe zuzuordnen.

7.5 Aufbewahrungsfristen

Für während der Patientenbehandlung angefallene Daten sind grundsätzlich die für diese Daten geltenden gesetzlichen Aufbewahrungszeiträume zu realisieren. Eine Übersicht findet sich in der Ausarbeitung der Deutschen Krankenhausgesellschaft[65].

Für während der Forschung anfallende Daten gelten je nach rechtlicher Grundlage der Forschung die entsprechenden gesetzlichen Aufbewahrungszeiträume. Wesentliche Unterlagen einer klinischen Prüfung, wozu auch die Prüfbögen (CRF) gehören, müssen entsprechend § 13 Abs. 10 GCP-V 10 Jahre aufbewahrt werden.

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 vorgesehen. Hierbei ist jedoch keine unbegrenzte Speicherdauer legitimierbar, denn eine Löschung ist hier entsprechend Art. 17 DS-GVO nach Erreichung des Forschungszweckes 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 Forschungszwecke 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.

7.6 Sicherheit der Verarbeitung

7.6.1 Information bei Datenschutzvorfällen

Wie bisher ist auch in der DS-GVO eine Meldung von Verletzungen des Schutzes personenbezogener Daten (vereinfacht gesagt bei „Datenpannen“) vorgesehen, um physischen, materiellen oder immateriellen Schaden für den Betroffenen zu vermeiden.

Der Begriff „ Verletzung des Schutzes personenbezogener Daten“ ist gemäß Art. 4 Nr. 12 DS-GVO definiert als eine „Verletzung der Sicherheit, die zur Vernichtung, zum Verlust oder zur Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden“.

Der Umgang mit Datenpannen wird in den Artikeln 33 und 34 DS-GVO geregelt, dabei sieht die DS-GVO eine abgestufte Meldepflicht bzgl. Aufsichtsbehörde und Betroffene vor.

7.6.2 Meldung an die Aufsichtsbehörde

Gemäß Art. 33 DS-GVO sind Vorfälle den Datenschutzaufsichtsbehörden unverzüglich möglichst innerhalb 72 Stunden nach Bekanntwerden durch den Verantwortlichen zu melden, wenn

- der Schutz personenbezogener Daten verletzt wurde und
- Risiken für die persönlichen Rechte und Freiheiten natürlicher Personen bestehen

Der Verantwortliche sollte Verzögerungen bzw. Gründe für die Nichteinhaltung der Meldefrist (innerhalb 72 Stunden) aus Nachweisgründen dokumentieren.

Die Informationspflicht bezieht sich auf die unrechtmäßige Kenntniserlangung personenbezogener Daten durch Dritte (z. B. Verlust von Datenträgern, Diebstahl, Hacking) oder die unrechtmäßige

[65] 4KG-Leitfaden Aufbewahrungspflichten und –fristen von Dokumenten im Krankenhaus [Online] 2015 [Zitiert 2017-02-10] Verfügbar unter http://www.dkgev.de/DKG-Leitfaden_Aufbewahrungspflichten

Übermittlung personenbezogener Daten (z. B. durch Fehlversand, illegale Datenweitergabe / -abrufe) sowie Identitätsbetrug und andere Formen des Datenmissbrauchs.

Somit kann die Kompromittierung jedes personenbezogenen Datums eine Meldepflicht auslösen, es sei denn, dass dies voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten der betroffenen natürlichen Personen führt. Folglich hat eine Abwägung der Risiken für den Betroffenen im Ergebnis darzustellen, dass keine Beeinträchtigung ersichtlich ist.

Für die Einschätzung relevant sind Datenarten und ob Maßnahmen ergriffen wurden, um Risiken zu minimieren, das Ergebnis ist zu dokumentieren.

Aufgrund der Nachweispflichten zu beachten sind ferner höhere Dokumentationsanforderungen zu kritischen Vorfällen gemäß Art. 33 Abs. 5 DS-GVO, es empfiehlt sich hierzu einen Reaktionsplan vorzuhalten, der den Meldeprozess und die enthaltenen Anforderungen beschreibt. Auch dies kann risikominimierend wirken. Die Dokumentationsanforderungen sind insgesamt umfangreicher als bisher, daher müssen alle Gegebenheiten, Auswirkungen und Abhilfemaßnahmen enthalten sein.

Die formalen Anforderungen an den Inhalt der Meldung bei meldepflichtigen Vorfällen an die Aufsichtsbehörde enthalten folgende Angaben:

- Art der Datenschutzverletzung,
- Datenkategorien,
- Zahl der betroffenen Personen,
- Anzahl der Datensätze,
- Name/ Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle,
- Beschreibung der möglichen Folgen des Vorfalls,
- ergriffene oder geplante Maßnahmen zur Behebung oder Minimierung der Datenschutzverletzung.

7.6.3 Meldung an den Betroffenen

Anders als die Meldung an die Aufsichtsbehörde setzt eine Informationspflicht der Betroffenen voraus, dass hohe Risiken für die betroffenen Personen vorliegen.

Gemäß Art. 34. Abs. 1 DS-GVO entfällt die Meldepflicht an den Betroffenen, wenn geeignete technische und organisatorische Maßnahmen nachgewiesen werden können, die unbefugten Zugang zu den kompromittierten, personenbezogenen Daten verhindern, etwa durch Verschlüsselung.

Weiterhin ist eine Information an die Betroffenen obsolet, wenn der Verantwortliche dokumentierte wirksame, schadensbegrenzende Maßnahmen ergriffen hat, damit das zum Zeitpunkt der Datenpanne vorliegende hohe Risiko aller Wahrscheinlichkeit nach nicht mehr besteht.

Die Anforderungen an die Meldung der Betroffenen nach Art. 34 DS-GVO unterscheiden sich insoweit von der Meldung an die Aufsichtsbehörde, als die Betroffenen in klarer Sprache und in einer angemessenen Frist informiert werden müssen.

Ist die Benachrichtigung an den Betroffenen mit einem unverhältnismäßigen Aufwand verbunden, kann die Information auch mittels öffentlicher Bekanntmachung (z. B. über eine Pressemeldung) erfolgen, sofern die Betroffenen damit vergleichbar wirksam informiert werden.

Inhalt der Meldung an den Betroffenen:

- Art der Datenschutzverletzung,
- Name und Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle,
- Beschreibung der möglichen Folgen des Vorfalls,

- Beschreibung ergriffener oder geplanter Maßnahmen zur Behebung oder Minimierung der Datenschutzverletzung.

Bei Unsicherheit bezüglich der Meldung oder der Art der Meldung an die Betroffenen ist die zuständige Aufsichtsbehörde zu konsultieren.

7.6.4 Datenschutz-Folgenabschätzung

Grundsätzlich ist eine Datenschutz-Folgenabschätzung erforderlich, wenn Daten der besonderen Art wie z. B. Gesundheitsdaten oder genetische Daten verarbeitet werden; eine Verarbeitung dieser Daten beinhaltet per definitionem ein hohes Risiko für die betroffenen Personen.

Auch Verarbeitungen, welche „neue" Techniken wie beispielsweise RFID und Big Data nutzen, also die Art der Verarbeitung ändern, beinhalten ggfs. entsprechende Risiken und erfordern vermutlich eine Datenschutz-Folgenabschätzung.

Eine Datenschutz-Folgenabschätzung muss gemäß Art. 35 Abs. 7 DS-GVO zumindest die nachfolgend genannten Punkte beinhalten:

- eine systematische Beschreibung
  - der geplanten Verarbeitungsvorgänge,
  - der Zwecke der Verarbeitung,
  - ggfs. die vom Verantwortlichen verfolgten berechtigten Interessen,
- eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck,
- eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen,
- die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren,
  - durch die der Schutz personenbezogener Daten sichergestellt und
  - der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird,
  - wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.

Die Datenschutzbehörde muss dazu entsprechend Art. 35 Abs. 4 DS-GVO eine Positivliste (= wann ist eine Datenschutz-Folgenabschätzung zwingend durchzuführen) veröffentlichen. Desgleichen können die Aufsichtsbehörden entsprechend Art. 35 Abs. 5 DS-GVO eine Negativliste (= wann kann auf eine Datenschutz-Folgenabschätzung verzichtet werden) veröffentlichen. Wenn das in Frage stehende Verfahren nicht gelistet ist, kann eine Datenschutz-Folgenabschätzung ggf. entfallen, wenn die im Kapitel eingangs dargestellten Punkte auf diese Verarbeitungstätigkeit nicht zutreffen.

Im Sinne datenschutzkonformer Abläufe ist unabhängig davon jedoch immer eine Datenschutz-Folgenabschätzung zu empfehlen.

7.6.5 Verzeichnis von Verarbeitungstätigkeiten

Das Verzeichnis von Verarbeitungstätigkeiten entsprechend Art. 30 DS-GVO soll die wesentlichen Informationen zusammenfassen, wie bspw. Angaben zur verantwortlichen Stelle oder zu den verwendeten Daten bzw. Datenarten. Die Inhalte der vorgeschriebenen Dokumentation entsprechen weitestgehend den Inhalten des heutigen Verfahrensverzeichnisses[66]:

[66] Tabelle zitiert aus: GMDS/bvitg: Gemeinsame Empfehlung bzgl. des Umgangs mit der EU Datenschutz-Grundverordnung (DS-GVO) im Gesundheitswesen. Online, zitiert 2016-12-03; Verfügbar unter https://gesundheitsdatenschutz.org/

Art. 30 Abs. 1 DS-GVO	§4e BDSG
a) den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten;	1. Name oder Firma der verantwortlichen Stelle 2. Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen, 3. Anschrift der verantwortlichen Stelle,
b) die Zwecke der Verarbeitung	4. Zweckbestimmungen der Datenerhebung, -verarbeitung oder -nutzung
c) eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;	5. eine Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien
d) die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen;	6. Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können
e) 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;	8. eine geplante Datenübermittlung in Drittstaaten
f) wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;	7. Regelfristen für die Löschung der Daten
g) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1.	8. eine allgemeine Beschreibung, die es ermöglicht, vorläufig zu beurteilen, ob die Maßnahmen nach § 9 zur Gewährleistung der Sicherheit der Verarbeitung angemessen sind

7.6.6 Sicherheit der Verarbeitung

Die Verantwortlichen müssen bei der Verarbeitung von personenbezogenen Daten geeignete Maßnahmen treffen, welche ein dem Risiko angemessenes Schutzniveau gewährleisten. Gesundheitsdaten und genetische Daten gehören gemäß Art. 9 DS-GVO hierbei zu den besonderen Kategorien von Daten, die auf jeden Fall ein hohes Schutzniveau erfordern.

In die Abwägung der zu treffenden technischen und organisatorischen Maßnahmen zur Herstellung eines dem Risiko angemessenen Schutzniveaus sind insbesondere zu berücksichtigen (Art. 32 Abs. 1 DS-GVO):

- Der Stand der Technik
- Die Implementierungskosten
- Art, Umfang, Umstände und Zwecke der Verarbeitung

- Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen.

Diese Maßnahmen schließen u.a. Folgendes ein (Art. 32 Abs. 1 DS-GVO):

- Pseudonymisierung personenbezogener Daten
- Verschlüsselung personenbezogener Daten
- Gewährleistung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten
- Die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen
- Ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Die Anforderungen der DS-GVO stehen damit im Einklang mit den Ausführungen des Bundesverfassungsgerichts im Urteil bzgl. der (heimlichen) Online-Durchsuchung (Urteil bzgl. „Grundrecht auf Vertraulichkeit und Integrität von IT-Systemen“)[67].

8 Anonyme Daten

Wenngleich in den Erwägungsgründen erwähnt wird, dass für anonyme Daten die Grundsätze des Datenschutzes nicht gelten sollten (z. B. Erwägungsgrund 26), findet sich im Gegensatz zum BDSG in der DS-GVO selbst keine Definition bzgl. anonymer Daten. Die Begrifflichkeit der anonymen Daten kann somit nur indirekt aus den Erwägungsgründen abgeleitet werden.

Da die Grundsätze des Datenschutzes nicht gelten, kann es sich bei anonymen Daten nicht um pseudonyme Daten oder andere personenbezogene Daten gemäß Art. 4 Abs. 1 DS-GVO handeln. Somit besteht hier eine Abgrenzung zu den personenbezogenen oder personenbeziehbaren Daten.

Gemäß Erwägungsgrund 26 sind anonyme Daten Informationen, „die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann“. D. h. anonyme Daten dürfen keinen Personenbezug beinhalten. Somit sind anonyme Daten im Sinne der DS-GVO Daten, die wir in Deutschland bisher mit dem Begriff „absolut anonym“ klassifizierten.

Dieses Verständnis bzgl. der Begrifflichkeit „anonyme Daten“ entspricht auch dem bisherigen europäischem Verständnis, wie es beispielsweise von der Artikel-29-Datenschutzgruppe 2014 dargestellt wurde[68]. Werden personenbezogene Daten anonymisiert, so stellt dies eine Weiterverarbeitung[68] dar, für die selbstverständlich zunächst einmal die Erfordernisse der DS-GVO gelten. D. h. für die Anonymisierung ist insbesondere auch ein Erlaubnistatbestand (siehe Kap.5) erforderlich.

[67] Bundesverfassungsgericht Urt. v. 27.02.2008, Az.: 1 BvR 370/07 und 1 BvR 595/07. Online, zitiert am 2016-12-04; Verfügbar unter https://dejure.org/bzw. http://www.bundesverfassungsgericht.de/

[68] Artikel-29-Datenschutzgruppe: Stellungnahme 5/2014 zu Anonymisierungstechniken. Online, zitiert am 2016-12-04; Verfügbar unter http://ec.europa.eu/

9 Spezielle Fragestellungen

9.1 Ethik-Kommissionen

9.1.1 Rechtliche Grundlagen

In Deutschland versteht man unter Ethikkommissionen im Allgemeinen die gesetzlich etablierten Einrichtungen der Ärzteschaft zur Beurteilung von Forschungsvorhaben am Menschen. Die Musterberufsordnung der deutschen Ärzte sah solche Institutionen erstmals 1988 vor[69]. Im deutschen Recht sind gesetzliche Regelungen über Ethik-Kommissionen insbesondere zu finden[70]:

- im Arzneimittelgesetz (§§ 40-42 AMG),
- im Transfusionsgesetz (§§ 8, 9 TFG),
- im Medizinproduktegesetz (§§ 20, 22 MPG),
- im Stammzellgesetz (§§ 6, 8, 9 StzG),
- in der Röntgenverordnung (§ 28 RöV),
- in der Strahlenschutzverordnung (§ 92 StrlSchV)
- in der Durchführungsverordnung des Bundesministeriums zum AMG (GCP-V).

Alle Gesetze – mit Ausnahme des TFG – verlangen, dass eine Ethik-Kommission einzuschalten ist, bevor die Forschungsvorhaben begonnen werden dürfen. Neben diesen bundesrechtlichen Regelungen finden sich aber auch noch solche aus dem Landesrecht, die insbesondere die Zusammensetzung der Ethik-Kommissionen regeln. Untergesetzliche Normen und Richtlinien komplettieren die gesetzlichen Grundlagen.

Die zentrale Ethik-Kommission[71] ist bei der Bundesärztekammer angesiedelt, jedoch gibt es entsprechend des Föderalismus in Deutschland auch rechtliche Rahmenbedingungen sowie Ethikkommissionen in allen Bundesländern:

- Baden-Württemberg
  - § 5 Heilberufe-Kammergesetz
  - Statut der Ethikkommission bei der Landesärztekammer Baden-Württemberg
- Bayern
  - Artt. 29a-g Gesundheitsdienst- und Verbraucherschutzgesetz
  - Anlage A zur Satzung der Bayerischen Landesärztekammer - Geschäfts- und Verfahrensordnung der Ethik-Kommission der Bayerischen Landesärztekammer
- Berlin
  - Ethik-Kommissionsgesetz
  - Ethik-Kommissionsverordnung
  - § 4c Kammergesetz
- Brandenburg
  - § 7 Heilberufsgesetz
  - Satzung der Ethik-Kommission der Landesärztekammer Brandenburg

[69] Kern BR (2008) Standortbestimmung: Ethikkommissionen – auf welchen Gebieten werden sie tätig? MedR 26: 631 – 636

[70] Walter-Sack I (1999) „Zuständigkeit“ medizinischer Ethikkommissionen – (wünschenswerte?) Ausweitung durch Satzungsrecht, dargestellt anhand der Regelungen für die Ethikkommissionen an der Universität Heidelberg und bei der Landesärztekammer Baden-Württemberg. MedR 18: 357 - 360

[71] Zentrale Kommission zur Wahrung ethischer Grundsätze in der Medizin und ihren Grenzgebieten. Online, zitiert am 2017-01-22; Verfügbar unter http://www.zentrale-ethikkommission.de/

- Bremen
    - Ethikkommissions-Verordnung
    - §§30, 30a-c Gesundheitsdienstgesetz
    - Satzung der Ethikkommission der Ärztekammer Bremen
- Hamburg
    - § 9 Hamburgisches Kammergesetz für die Heilberufe (HmbKGH)
    - Satzung der Ethik-Kommission der Ärztekammer Hamburg
- Hessen
    - § 6a Heilberufsgesetz
    - § 53 Hochschulgesetz
    - Satzung der Ethik-Kommission bei der Landesärztekammer Hessen
- Mecklenburg-Vorpommern
    - § 16a Gesetz über den Öffentlichen Gesundheitsdienst
    - Satzung der Ethikkommission an der Medizinischen Fakultät der Universität Rostock
- Niedersachsen
    - § 10 Heilberufe-Kammergesetz
    - Satzung für die Ethikkommission bei der Ärztekammer Niedersachsen
- Nordrhein-Westfalen
    - § 7 Heilberufsgesetz
    - Satzung der Ethikkommission der Ärztekammer Nordrhein
    - Satzung der Ethik-Kommission der Ärztekammer Westfalen-Lippe und der Medizinischen Fakultät der Westfälischen Wilhelms-Universität Münster
- Rheinland-Pfalz
    - § 5a Heilberufsgesetz (HeilBG)
    - Satzung der Ethik-Kommission bei der Landesärztekammer Rheinland-Pfalz
- Saarland
    - § 5 Saarländisches Heilberufekammergesetz
    - Statut der Ethik-Kommission bei der Ärztekammer des Saarlandes
- Sachsen
    - § 5a Sächsisches Heilberufekammergesetz
    - Geschäftsordnung der Ethikkommission bei der Sächsischen Landesärztekammer
- Sachsen-Anhalt
    - Ethik-Kommissionen-Verordnung
    - Geschäftsordnung der Ethik-Kommission des Landes Sachsen-Anhalt
- Schleswig-Holstein
    - § 6 Heilberufekammergesetz
    - Satzung für die Ethikkommissionen der Ärztekammer Schleswig-Holstein
- Thüringen
    - §§17a-g, 86 Heilberufegesetz
    - Satzung der Ethik-Kommission der Landesärztekammer Thüringen

9.1.2 Eine Pflicht der Ethikkommission: Patienten- und Probandenschutz

In erster Linie besteht die Pflicht einer Ethik-Kommission darin, Patienten bzw. Probanden vor gefährlicher oder überraschender Forschung zu bewahren[72]. Zu diesem Zweck muss sie prüfen, ob die Aufklärung der Patienten und Probanden in verständlicher und umfassender Form erfolgt. Des weiteren muss sie dafür Sorge tragen, dass bei den durch die Ethik-Kommission genehmigten Studien die Belastung von Patienten bzw. Probanden auf ein vertretbares Minimum beschränkt bleibt sowie dass gefährliche Versuche nicht oder nur mit Sicherheitsvorkehrungen durchgeführt werden, welche die Gefahr für den Patienten bzw. Probanden entsprechend reduzieren.

9.1.3 Rechtsverbindlichkeit von Entscheidungen einer Ethik-Kommission

Jeder Ethik-Kommission gehört i. d. R. ein Jurist an. Dennoch ist oftmals feststellbar, dass die Stellungnahmen von Ethik-Kommissionen nicht immer juristisch nachvollziehbar sind [73]. Daher wird bereits seit 1981 gefordert, dass neben der zustimmenden Kenntnisnahme durch die Ethik-Kommission auch ein juristisch begründetes Gutachten eingeholt wird[73,74]. Aufgrund der mangelhaften juristischen Nachvollziehbarkeit muss angezweifelt werden, ob durch ein positives Votum eines Forschungsprojektes durch eine Ethik-Kommission beim Projektleiter ein entschuldigender Irrtum erzeugt werden kann[73]. Dies insbesondere deshalb, da positive Bescheide, die nach der Behebung von Mängeln regelmäßig ergehen, oftmals nicht begründet sind und somit die Gründe für diese Entscheidung daher auch nicht nachvollzogen werden können.

Sofern die Ethik-Kommission öffentlich-rechtlich eingerichtet ist, besteht grundsätzlich eine Haftung für eine schuldhafte Verletzung der Amtspflicht durch deren Mitglieder seitens der Institution. Einerseits besteht die Haftung gegenüber einem verletzten Probanden bzw. Patienten hinsichtlich des durch das Forschungsvorhaben entstandenen Schadens, sofern eine bezüglich des Gefährdungspotentials fehlerhafte Beurteilung der Ethik-Kommission vorlag. Andererseits besteht auch eine Haftung gegenüber dem durch Zurückweisung, Verzögerung oder Verletzung der Vertraulichkeit geschädigten Forscher, sofern dessen Recht auf Forschungsfreiheit (Art. 5 Abs. 3 GG) unberechtigt eingeschränkt wurde.

9.1.4 Einsichtnahme in Patienten- bzw. Probandendaten

Da Ethik-Kommissionen vor Beginn eines Forschungsprojektes u.a. das Risiko für die Probanden/Patienten beurteilen sollen, ist eine Einsichtnahme in Patientendaten i. d. R. nicht erforderlich. Grundsätzlich gilt auch in Bezug auf die Zugriffe der Ethik-Kommission auf personenbezogene Daten, dass auch diese Zugriffe stets einer entsprechenden Rechtsgrundlage bedürfen, wie einer Einwilligung der betroffenen Person oder einem anderen gesetzlichen Erlaubnistatbestand.

[72] Deutsch E. (1595) Der Beitrag des Rechts zur klinischen Forschung in der Medizin. NJW: 3019-3024

[73] Deutsch E, Spickhoff A: Ethik-Kommissionen und Rechtsgutachten. in: Deutsch E, Spickhoff A. (2014) Medizinrecht - Arztrecht, Arzneimittelrecht, Medizinprodukterecht und Transfusionsrecht. . Springer Verlag, 7. Auflage, ISBN 978-3-642-38148-5

[74] Samson E. (1981) Über Sinn und Unsinn von Ethik-Kommissionen. DMW: 667-673

9.2 Langfristige Datenarchivierung

9.2.1 Gesetzliche Aufbewahrungspflichten

Bzgl. klinischer Studien hinsichtlich Arzneimitteln gilt eine 10-jährige Aufbewahrungsfrist der wesentlichen Prüfungsunterlagen inklusive der Prüfungsbögen (§ 42 Abs. 3 S. 2 Nr. 4 AMG i. V. m. § 13 Abs. 10 GCP-V).

Die Arzneimittelprüfrichtlinie[75], deren in Anhang I Teil I bis III dargelegten Anforderungen entsprechend in § 26 Abs. 1 S. 1 AMG i. V. m. § 1 AMPV erfüllt werden müssen, verlangt, dass der Inhaber der Genehmigung für das Inverkehrbringen des Arzneimittels gewährleistet:

- Identifizierungscodes müssen für mindestens 15 Jahre nach Abschluss oder Abbrechen der Prüfung aufbewahrt werden.
- Krankenblätter und andere Originaldaten müssen über den längst möglichen Zeitraum, den das Krankenhaus, die Institution oder die private Praxis gestattet, aufbewahrt werden.
- Sponsoren oder spätere Genehmigungsinhaber müssen alle Versuchsunterlagen so lange aufbewahren, wie das Arzneimittel zugelassen ist. Dies umfasst:
    - den Prüfplan,
    - Standard operating procedures (SOP),
    - alle schriftlichen Stellungnahmen zum Prüfplan und zu den Verfahren,
    - Information für Prüfer,
    - Prüfbogen für jede Versuchsperson,
    - Abschlussbericht,
    - gegebenenfalls Audit-Zertifika.
- Der Abschlussbericht wird vom Sponsor oder dem künftigen Genehmigungsinhaber weitere fünf Jahre aufbewahrt, nachdem das Arzneimittel nicht mehr zugelassen ist.

Entsprechend § 12 Abs. 2 S. 2 MPG gilt, dass der Sponsor der klinischen Prüfung

- die Dokumentation nach Nummer 3.2 des Anhangs 6 der Richtlinie 90/385/EWG mindestens 15 Jahre und
- die Dokumentation nach Nummer 3.2 des Anhangs VIII der Richtlinie 93/42/EWG mindestens fünf und im Falle von implantierbaren Produkten mindestens 15 Jahre nach Beendigung der Prüfung aufbewahren muss.

9.3 Genetische Daten

Genetische Daten werden in Art. 4 Nr. 13 DS-GVO wie folgt definiert:

> „'genetische Daten' personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern und insbesondere aus der Analyse einer biologischen Probe der betreffenden natürlichen Person gewonnen wurden“.

Genetische Daten gehören, ebenso wie Gesundheitsdaten, entsprechend Art. 9 Abs. 1 DS-GVO zu den besonderen Kategorien personenbezogener Daten, d. h. zu den Daten mit dem datenschutzrechtlich höchsten Schutzbedarf. Genetische Daten weisen die Besonderheit auf, dass in ihnen der genetische Code von genau einer natürlichen Person enthalten ist, d.h. genetische Daten

[75] Richtlinie 2001/83/EG des Europäischen Parlaments und des Rates vom 6. November 2001 zur Schaffung eines Gemeinschaftskodexes für Humanarzneimittel. Online, zitiert am 2016-12-04; Verfügbar unter http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=uriserv:OJ.L_.2001.311.01.0067.01.DEU

können nicht anonymisiert werden, ohne dass die genetische Information selbst entsprechend verändert wird. Daher sind genetische Daten immer als personenbeziehbare Daten i. S. v. Art. 4 Nr. 1 DS-GVO anzusehen.

9.3.1 Genetische Daten und Einwilligung

Genetische Daten einer betroffenen Person beinhalten immer auch Daten von Dritten, wie beispielsweise der leiblichen Eltern oder Geschwister der betroffenen Person oder auch der eigenen leiblichen Kinder. Eine Einwilligung gemäß Art. 9 DS-GVO (wie auch von Art. 6 DS-GVO) gilt jedoch immer nur für die Daten, die ausschließlich der einwilligenden Person gehören[76]; eine Einwilligung „zu Lasten Dritter" ist nicht möglich.

Mit genetischen Daten werden beispielsweise bei Vorliegen von Erberkrankungen immer Informationen über andere Personen offenbart, ohne dass hierfür eine rechtliche Grundlage existiert. Dies hat zur Konsequenz, dass für die Forschung mit genetischen Daten letztlich auf einen anderen Erlaubnistatbestand als eine Einwilligung zurückgegriffen werden muss.

Die sich hieraus ergebende Problematik für die medizinische Forschung kann letztlich nur der Gesetzgeber lösen.

9.3.2 Die Biomedizin-Konvention des Europarates

Im April 1994 wurde das in Gremien des Europarates in nicht-öffentlichen Sitzungen erarbeitete „Übereinkommen zum Schutz der Menschenrechte und der Menschenwürde im Hinblick auf die Anwendung von Biologie und Medizin: Übereinkommen über Menschenrechte und Biomedizin"[77] - oftmals auch kurz als Bioethikkonvention oder Biomedizin-Konvention (BMK) bezeichnet - „geleakt". Der völkerrechtliche Vertrag trat am 1. Dezember 1999 in Kraft. Auf Grund der Tatsache, dass der Vertrag im April 1994 in Oviedo zur Unterzeichnung vorgelegt wurde, wird der Vertrag auch als „Oviedo-Konvention" bezeichnet. Innerhalb Europas gab es bzgl. der BMK diverse Vorbehalte[78].

Trotz der Möglichkeit, Vorbehalte bezüglich jeder einzelnen Vorschrift auszusprechen (Art. 36 Nr. 1 BMK), haben von den 47 Mitgliedstaaten des Europarates 18 die Konvention nicht oder noch nicht ratifiziert. Auch Deutschland, Liechtenstein und Österreich haben das Übereinkommen bis heute weder ratifiziert noch unterzeichnet[79]. Die BMK wird von einem großen Teil der deutschen (Fach-)

---

[76] z. B. ErwGr. 32 DS-GVO („[...[sie betreffenden personenbezogenen Daten[...["), ErwGR. 40 („Damit die Verarbeitung rechtmäßig ist, müssen personenbezogene Daten mit Einwilligung der betroffenen Person [...[")

[77] Übereinkommen zum Schutz der Menschenrechte und der Menschenwürde im Hinblick auf die Anwendung von Biologie und Medizin: Übereinkommen über Menschenrechte und Biomedizin. Online, zitiert 2017-01-21; Verfügbar unter http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/164?_coeconventions_WAR_coeconventionsportlet_languageId=de_DE bzw. Fulltext http://www.coe.int/de/web/conventions/full-list/-/conventions/rms/090000168007cf98

[78] Vorbehalte und Erklärungen für Vertrag Nr.164. Online, zitiert 2017-01-21; Verfügbar unter https://www.coe.int/de/web/conventions/full-list/-/conventions/treaty/164/declarations?p_auth=jErXFg5z

[79] Unterschriften und Ratifikationsstand des Vertrags 164 (https://www.coe.int/de/web/conventions/full-list/-/conventions/treaty/164/signatures?p_auth=jErXFg5z), Chart of signatures and ratifications of Treaty 168 (http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/168/signatures), Chart of signatures and ratifications of Treaty 186 (http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/186/signatures), Chart of signatures and ratifications of Treaty 195 (http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/195/signatures), Chart of signatures and ratifications of Treaty 203 (http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/203/signatures)

Öffentlichkeit kontrovers diskutiert[80], da die BMK aus deutscher Sicht zu weitreichende Erlaubnistatbestände schafft.

Auf Grund der Tatsache der fehlenden Ratifizierung/Unterzeichnung der BMK spielt diese Konvention im deutschsprachigen Raum - abgesehen von der Schweiz - bzgl. der Erlaubnistatbestände eher eine untergeordnete Rolle. Da die Biomedizinkonvention im Bereich der Biomedizin jedoch einen Mindeststandard zum Schutz der Menschenwürde und Menschenrechte in Europa sicherstellen soll, kann ihre Einhaltung bei in Deutschland erlaubter genetischer Forschung dennoch als Hinweis dienen, dass europarechtliche Vorgaben bzgl. der Einhaltung der Menschenwürde eingehalten werden.

Die Biomedizinkonvention ist ein Rahmenübereinkommen, welches als solches nur die wichtigsten Grundsätze enthält. Zusatzprotokolle enthalten dann ergänzende bzw. detailliertere Regelungen. Hierbei sollen insbesondere durch die Zusatzprotokolle Mindeststandards in verschiedenen Bereichen medizinischer Therapie und biomedizinischer Forschung festlegt werden. Bis heute gibt es vier Zusatzprotokolle:

1) Zusatzprotokoll zum Übereinkommen zum Schutz der Menschenrechte und der Menschenwürde im Hinblick auf die Anwendung von Biologie und Medizin über das Verbot des Klonens von menschlichen Lebewesen (SEV Nr. 168)[81].
2) Zusatzprotokoll zum Übereinkommen über Menschenrechte und Biomedizin bezüglich der Transplantation von menschlichen Organen und Gewebe (SEV Nr. 186)[82].
3) Zusatzprotokoll zum Übereinkommen über Menschenrechte und Biomedizin betreffend biomedizinische Forschung (SEV Nr. 195)[83].
4) Zusatzprotokoll zur Konvention über Menschenrechte und Biomedizin betreffend der Gentests zu gesundheitlichen Zwecken (SEV Nr. 203)[84].

Wie aufgezeigt wurde, muss Forschern hinsichtlich Regelungsanwendung der BMK klar sein, dass es sich hierbei um „Mindeststandards“ handelt. Mithin also der „kleinste gemeinsame Nenner“. Trotzdem wird die Konvention seitens des Vereinigten Königreichs als zu restriktiv und forschungshemmend erachtet und wurde daher bis heute von diesem nicht unterzeichnet. Ferner beinhaltet die BMK für Deutschland keinerlei Erlaubnistatbestände. Mithin kann Forschung, die beispielsweise in Frankreich (BMK ist dort ratifiziert) erlaubt ist, daher in Deutschland verboten sein. Dieser Aspekt ist gerade bei länderübergreifender Forschung zwingend zu beachten.

[80] InteressenGemeinschaft Kritische Bioethik Deutschland (2010) Stellungnahmen und sonstige Texte zur Bioethik-Konvention und den Zusatzprotokollen. Online, zitiert 2017-01-21; Verfügbar unter http://www.bioethik-konvention.de/bioethik-konvention_stellungnahmen.html

[81] Zusatzprotokoll zum Übereinkommen zum Schutz der Menschenrechte und der Menschenwürde im Hinblick auf die Anwendung von Biologie und Medizin über das Verbot des Klonens von menschlichen Lebewesen. Online, zitiert 2017-01-21; Verfügbar unter https://www.coe.int/de/web/conventions/full-list/-/conventions/treaty/168

[82] Zusatzprotokoll zum Übereinkommen über Menschenrechte und Biomedizin bezüglich der Transplantation von menschlichen Organen und Gewebe. Online, zitiert 2017-01-21; Verfügbar unter https://www.coe.int/de/web/conventions/full-list/-/conventions/treaty/186

[83] Zusatzprotokoll zum Übereinkommen über Menschenrechte und Biomedizin betreffend biomedizinische Forschung. Online, zitiert 2017-01-21; Verfügbar unter https://www.coe.int/de/web/conventions/full-list/-/conventions/treaty/195

[84] Zusatzprotokoll zur Konvention über Menschenrechte und Biomedizin betreffend der Gentests zu gesundheitlichen Zwecken. Online, zitiert 2017-01-21; Verfügbar unter https://www.coe.int/de/web/conventions/full-list/-/conventions/treaty/203

9.4 Biobanken

Biobanken sind Sammlungen von Proben menschlicher Körpersubstanzen (z. B. Gewebe, Zellen, Blut oder andere Körperflüssigkeiten [z. B. Harn, Blutserum oder -plasma]). Diese Proben können gekühlt über viele Jahre aufbewahrt werden.

Biobanken haben eine Schlüsselrolle bei der Weiterentwicklung der modernen Medizin. Sie sind Quellen zur Erforschung der Ursachen von Krankheiten und deren Verläufe. Darüber hinaus können sie zur Entwicklung neuer Diagnoseverfahren und Therapien einen wesentlichen Beitrag leisten. Ziel ist die Verbesserung der Diagnostik und Behandlungsmöglichkeiten einer Erkrankung.

Körperbestandteile können als personenbezogene Daten zu qualifizieren sein, da sie zahlreiche Informationen über den Körper und die Gesundheit des jeweiligen Trägers beinhalten. Ermöglichen die Körperstoffe eine Genanalyse, sind diese Körperbestandteile auf jeden Fall als personenbezogene Daten anzusehen (siehe Kapitel 9.3 bzw. Art. 9 Abs. 1 DS-GVO).

Dementsprechend sind für Biobanken die Regelungen der DS-GVO anzuwenden, insbesondere ist ein Schutz der Daten vor unbefugtem Zugriff entsprechend dem Stand der Technik (Art. 32 DS-GVO) zu fordern, ebenso ein entsprechendes Rollen- und Rechtekonzept, welches beschreibt, wer wann unter welchen Umständen aus welchen Gründen auf welche Daten zugreifen darf. Entsprechend den Vorgaben der DS-GVO ist weiterhin der Lebenszyklus der Daten zu beschreiben, d. h. eine Darlegung,

- wie lange die Daten auf Grund welcher Rechtsgrundlage gespeichert werden und
- nach welchem Zeitraum eine Löschung erfolgt.

9.5 Big Data/Smart Data

Viele im Gesundheitswesen etablierte Institutionen / Organisationen / Vereinigungen entdeckten das Thema „Big Data“ als zukunftsrelevantes Thema für sich. In aktuellen Fachveranstaltungen wird es beispielsweise regelmäßig aufgegriffen und thematisiert. In Pubmed brachte eine Suche nach „Big Data“ im Mai 2017 mehr als 3000 Treffer, dies zeigt, wie sehr die Thematik im Gesundheitswesen und in der Gesundheitsforschung angekommen ist.

Das Potential von Big Data liegt nicht nur in der Verwaltung und Speicherung von großen Datenmengen, sondern vor allem in deren Analyse. Big Data eröffnet mit Hilfe modernster Algorithmen die Möglichkeit, in Echtzeit riesige Datenmengen zu analysieren, um hierdurch Antworten auf Fragen zu erhalten, welche zuvor noch nicht gestellt wurden bzw. Fragen zu beantworten, die mit althergebrachten Methoden nicht beantwortet werden konnten.

Im Folgenden werden einige datenschutzrechtliche Aspekte dieser Thematik dargestellt, so dass bei der Planung von Big Data Projekten diese berücksichtigt werden können.

9.5.1 „Big Data“ oder „Smart Data“?

In der Vergangenheit zeigte sich, dass im Rahmen von „Big Data“ eine Datensammlung unabhängig von einer konkreten Fragestellung nicht zielführend ist. Denn die verwendeten Algorithmen ermitteln ohne entsprechende Fragestellungen Korrelationen zwischen Datengruppen, die inhaltlich nichts miteinander zu tun haben. Daher ist es zielführender, den Ansatz von „Smart Data“ zu verfolgen. Dazu muss man über genau die Daten verfügen, die man zur Lösung eines bestimmten Problems oder einer konkreten Fragestellung benötigt; die Datenmenge ist hierbei eigentlich gar nicht entscheidend. (Was letztlich auch dem Datenminimierungsgebot der DS-GVO entspricht.) Der Begriff „Smart Data“ setzt sich immer mehr durch, um auszudrücken, dass man nicht alle möglichen verfügbaren Daten benötigt, sondern nur die Daten, die zur Lösung einer konkreten Frage-

/Problemstellung benötigt werden. Dies setzt natürlich nach wie vor voraus, dass man sich im Vorfeld einer Auswertung Gedanken darüber macht, welche Daten man benötigt - eigentlich eine Selbstverständlichkeit bei jeder wissenschaftlichen Arbeit. Da jedoch der Begriff „Big Data“ der geläufigere ist, wird er auch hier verwendet.

9.5.2 Anonyme Big Data Auswertungen

Die Möglichkeiten, welche sich durch diese Analyse-Techniken bieten, beinhalten aber auch ein potentiell relevantes Risiko: Durch die enormen Datenmengen wird es eher möglich, einzelne Personen anhand ihrer Daten zu re-identifizieren. Das wiederum hat letzten Endes zur Folge, dass etablierte und anerkannte Verfahren wie Pseudonymisierung oder Anonymisierung, die eingesetzt werden, um die Re-Identifizierung des Betroffenen zu verhindern, durch den Einsatz von Big/Smart Data, wirkungslos werden können, zumindest in der Form, wie sie heute genutzt werden.

In den letzten Jahren wurde immer wieder gezeigt, dass bei der Zusammenführung medizinischer Daten eine Re-Identifizierung bei „anonymen“ Daten durchgeführt werden konnte[85,86,87,88,89]. Allein drei demografische Merkmale (Geschlecht, 5-stellige Postleitzahl und Geburtsdatum) reichten aus, um 87% der amerikanischen Bevölkerung zu identifizieren[90].

Daher muss man heute davon ausgehen, dass es im Rahmen von medizinischen Daten keine Anonymität gibt, wenn hinreichend viele Daten zusammengeführt werden. D.h. bei Big Data Anwendungen muss man nach heutigem Stand davon ausgehen, dass man bei Nutzung von Patientendaten immer mit personenbezogenen oder personenbeziehbaren Daten arbeitet[91].

Entsprechend den derzeitigen rechtlichen Vorgaben benötigt man für Big Data Anwendungen in der Medizin somit zwingend entweder eine rechtsgültige Einwilligung der betroffenen Person oder eine andere Rechtsgrundlage.

9.5.3 Zweckbindung

Big Data Anwendungen sollen u.a. verborgene Beziehungen zwischen Informationen entdecken. Damit werden die untersuchten Daten von den Zwecken entkoppelt, zu denen sie ursprünglich einmal erhoben wurden. Die Verarbeitung und Nutzung von Daten ist aber nur für den ursprünglichen Zweck gestattet. Jegliche Zweckänderung benötigt erneut eine Legitimation, d.h. eine Einwilligung der betroffenen Person oder eine andere rechtliche Grundlage. Beides ist aber nur möglich, wenn der Verwendungszweck der Daten bekannt ist.

---

[85] de Montjoye YA, Hidalgo CA, Verleysen M, Blondel VD. (2013) Unique in the Crowd: The privacy bounds of human mobility. Scientific Reports. [Online, zitiert am 2016-11-13]; Verfügbar unter http://www.nature.com/srep/2013/130325/srep01376/full/srep01376.html

[86] Deng B. (2015) People identified through credit-card use alone. [Online, zitiert am 2016-11-13]; Verfügbar unter http://www.nature.com/news/people-identified-through-credit-card-use-alone-1.16817

[87] Franzosa et al. (2015) Identifying personal microbiomes using metagenomic codes. PNAS [Online, zitiert am 2016-11-13]; Verfügbar unter http://www.pnas.org/content/112/22/E2930.abstract

[88] Gymrek M, McGuire AL, Golan D, Halperin E, Erlich Y (2013) Identifying Personal Genomes by Surname Inference. Science 339: 321ff

[89] Milius et al. (2014) The International Cancer Genome Consortium's evolving data-protection policies. Nature Biotechnology (32): 519–523

[90] Sweeney L. (2002) k-anonymity: a model for protecting privacy. International Journal on Uncertainty, Fuzziness and Knowledge-based Systems 10 (5): 557-570. 83 [Online, zitiert am 2016-11-13]; Verfügbar unter http://dataprivacylab.org/dataprivacy/projects/kanonymity/kanonymity.pdf

[91] Tene O, Polonetsky J. (2012) Privacy in the Age of Big Data. Stanford Law Review. [Online, zitiert am 2016-11-13]; Verfügbar unter http://www.stanfordlawreview.org/online/privacy-paradox/big-data

Für Zwecke, die nicht einmal dem Verantwortlichen bei Beginn der Big Data Auswertung bekannt sind, wird die Einholung einer Einwilligung des Betroffenen regelmäßig an einer fehlenden Aufklärungsmöglichkeit scheitern. Eine Datenverarbeitung ohne eine konkrete Zweckbindung ist zudem nach europäischem und deutschem Recht nicht gestattet. Auch eine sehr allgemein gehaltene Zweckdefinition wie „Forschung" entspricht nicht den derzeit, noch den künftig geltenden rechtlichen Anforderungen.

Jedoch besagt Art. 5 Abs. 1 lit. b 2. HS DS-GVO, dass wissenschaftliche oder historische Forschungszwecke, die den Vorgaben von Art. 89 Abs. 1 DS-GVO genügen, nicht als unvereinbar mit den ursprünglichen Zwecken anzusehen sind. Somit lässt sich argumentieren, dass bei der Verarbeitung von Daten für Forschungszwecke (unter Beachtung der Vorgaben von Art. 89) evtl. keine Zweckänderung vorliegt. Dies bedarf jedoch immer der Einzelfallbetrachtung.

9.5.4 Datenminimierung

Art. 8 Abs. 2 der Europäischen Grundrechtecharta verlangt, dass „nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden"[92]. Dieser Vorgabe wird u. a. mit Art. 5 Abs. 1 lit. c DS-GVO Rechnung getragen. Danach dürfen nur dem Zweck angemessene und für die Verarbeitung notwendige Daten erhoben werden.

Daher ist bei Big Data eine Sammlung im Sinne einer „Vorratsdatenspeicherung" nicht statthaft. Entsprechend dem „Smart Data" Ansatz müssen deshalb die für den jeweiligen Forschungszweck benötigten notwendigen Daten erhoben werden.

9.5.5 Big Data und die Erhebung von Daten

Bei Big Data werden Daten aus unterschiedlichen Quellen zusammengeführt. Entsprechend der DS-GVO stellt dies eine Verarbeitung der Daten (im Speziellen einen Akt der Erhebung von Daten) dar. D.h. die Übermittlung der Daten für eine Big Data Anwendung stellt somit regelmäßig eine Verarbeitung dar, wofür die sendende Stelle bzw. der oder die entsprechende(n) Verantwortliche(n) eine Rechtsgrundlage benötigen. Zudem ist entsprechend Art. 14 DS-GVO der Betroffene ggfs. über diese Erhebung seitens der empfangenden Stelle zu informieren.

9.6 Studienzentren

Ein Studienzentrum ist i. d. R. eine zentrale Einrichtung der medizinischen Fakultät einer Universität. Ein Studienzentrum unterstützt Forscher bei der Umsetzung der Forschung, je nach Ausrichtung des Studienzentrums bereits beginnend von der Studien-Idee über die Durchführung, Auswertung und Veröffentlichung, inklusive Forschungsantrags-Bearbeitung.

Ein Studienzentrum ist dabei nicht auf klinische Studien beschränkt. Jedoch stellen klinische Studien häufig einen großen Anteil der Forschungsvorhaben dar, mit denen ein Studienzentrum befasst ist.

Ein Studienzentrum kommt dabei nicht notwendigerweise mit personenbezogenen Daten in Kontakt, da für die administrative Beratung (z. B. *wie* die Daten ausgewertet werden) wohl die Art der Daten (z. B. Alter, Geschlecht), nicht jedoch die konkreten Ausprägungen (Inhalt) bekannt sein müssen. Es gibt jedoch Studienzentren, welche auch eine statistische Auswertung mit anbieten, so dass Personal des Studienzentrums personenbeziehbare Daten verarbeitet. Hier kann es - je nach Konstellation - notwendig sein, dass z. B.

[92] Charta der Grundrechte der Europäischen Union. [Online, zitiert am 2016-11-13]; Verfügbar unter http://www.europarl.de/resource/static/files/europa_grundrechtecharta/_30.03.2010.pdf

- ein Auftragsverarbeitungsvertrag abgeschlossen werden muss (z. B. wenn das Studienzentrum im Auftrag und nach Anweisung des Forschers arbeitet, aber organisatorisch nicht zum datenschutzrechtlichen „Verantwortlichen“ zählt) oder
- eine Einwilligung des Betroffenen diese Verarbeitung durch ein Studienzentrum vorsieht (z. B. im Rahmen einer Verarbeitung durch gemeinsam Verantwortliche).

9.7 Dissertation

Bei einem Doktoranden muss der datenschutzrechtliche Erlaubnistatbestand bzgl. der Nutzung von Patientendaten dargestellt und festgehalten werden, bevor mit der Dissertation begonnen wird. Denn auch im Rahmen dieser Forschungsvorhaben gelten die Vorgaben der DS-GVO. D.h. eine Promotion hat keinerlei „Sonderstatus“, sondern muss, wie die sonstigen Verarbeitungen auch, allen rechtlichen Anforderungen genügen.

Zur Beurteilung, ob die Nutzung der Daten rechtmäßig ist, müssen daher insbesondere folgende Informationen vorliegen:

- Forschungsziel der Promotion
- Welche Forschungsart liegt vor?
    - Ist es eine wissenschaftliche Forschung?
      (Siehe Kapitel 4.2)
    - Ist es eine historische Forschung?
      (Siehe Kapitel 4.3)
    - Liegen die Nachweise hierzu vor?
      (Siehe Kapitel 7.1.2 bzw. Kapitel 7.1.3)
- Existiert ein öffentliches Interesse an dem Forschungsergebnis?
  (Siehe Kapitel 4.5 bzw. 4.7)
- Welche Daten sind zur Erreichung des Forschungszieles erforderlich?
  (Siehe Kapitel 4.7)
- Was ist die Rechtliche Grundlage für die Nutzung der personenbezogenen Daten?
  (Siehe Kapitel 5)
- Entsprechen die Maßnahmen gegen eine unbefugte Verarbeitung der Daten dem „Stand der Technik“?
  (Siehe Kapitel 4.9)
- Erfolgt die Forschung entsprechend dem „Stand der Wissenschaft“?
  (Siehe Kapitel 4.10)
- Sind die grundlegenden datenschutzrechtlichen Anforderungen im Forschungsvorhaben angemessen berücksichtigt?
  (Siehe Kapitel 7)

Dabei müssen diese Nachweise nicht zwingend für jede einzelne Dissertation erfolgen. Gerade im medizinischen Umfeld ist es gängige Praxis, dass - insbesondere in universitären Einrichtungen - immer wieder Promotionsarbeiten vergeben werden. Hierbei können die grundlegenden Aspekte zentral festgehalten werden, z. B. wie die grundsätzlichen Schutzmaßnahmen auszusehen haben oder wie den zentralen datenschutzrechtlichen Anforderungen nachgekommen wird. In diesem Fall müssen nur die individuellen, also die genau für diese Arbeit spezifischen zusätzlichen Informationen (z. B. Forschungsziel oder Art) zusätzlich zu den allgemeinen Beschreibungen dargestellt werden.

Bzgl. der allgemeinen Anforderungen ist dann lediglich eine Verpflichtungserklärung notwendig, dass diese Vorgaben eingehalten werden.

9.8 Zusammenspiel Forschung und Patientenversorgung

Daten der Patientenversorgung sind die größte Datenquelle für die retrospektiv angelegte medizinische Forschung, aber auch in prospektiven Studien stellen diese Daten eine der wertvollsten Forschungsressourcen dar. Diese „Sekundärnutzung" der Daten der Patientenversorgung ist auch politisch gewollt[93]. Aber auch Routinedaten der Gesetzlichen Krankenversicherung, welche primär zu Abrechnungszwecken verarbeitet werden, sind für wissenschaftliche Untersuchungen hoch interessant[94], z. B. für epidemiologische Studien im Bereich der Versorgungsforschung.

Auch wenn die DS-GVO bzgl. der Nutzung von Daten aus der Patientenversorgung eine Privilegierung in Bezug auf den Verwendungszweck beinhaltet, so dass Forschungszwecke entsprechend Art. 5 Abs. 1 lit. b DS-GVO „nicht als unvereinbar mit den ursprünglichen Zwecken" (= Patientenversorgung) gilt, ist grundsätzlich für die Sekundärnutzung ein Erlaubnistatbestand erforderlich. Dieser kann in der (datenschutzrechtlichen) Einwilligung des betreffenden Patienten bestehen oder aus einem anderen gesetzlichen Tatbestand resultieren. Die DS-GVO verweist hier auf den jeweiligen nationalen Gesetzgeber, so dass der deutsche Gesetzgeber entsprechende Erlaubnistatbestände, welche entsprechend Art. 89 Abs. 2 i. V. m. Art. 89 Abs. 1 DS-GVO „geeignete Garantien für die Rechte und Freiheiten der betroffenen Person" aufweisen müssen, schaffen muss.

In den Landes-Krankenhausgesetzen finden sich Regelungen bzgl. der Erlaubnis zur Nutzung von im Krankenhaus angefallenen Patientendaten, für den niedergelassenen Bereich findet sich ein Erlaubnistatbestand in § 28 Abs. 6 Ziff. 4 BDSG und hinsichtlich der Nutzung von Sozialdaten finden sich z. B. in §§ 67b, 67c SGB X entsprechende Erlaubnistatbestände. Prinzipiell gelten die Erlaubnistatbestände als „lex specialis" entsprechend Art. 9 Abs. 4 DS-GVO auch nach dem Wirkeintritt der DS-GVO, jedoch genügen diese Gesetze nicht dem Schutzgedanken der DS-GVO und entsprechen daher nicht den Anforderungen von Art. 89 DS-GVO. Es steht aber zu erwarten, dass der deutsche Gesetzgeber hier zeitnah Abhilfe schafft, so dass mit entsprechenden Anpassungen an den Gesetzen zu rechnen ist. Grundsätzlich gilt, dass ein Gesetz gültig ist, bis es ein Gesetzgeber oder ein entsprechend befugtes Gericht widerruft, d.h. die derzeit vorhandenen Erlaubnistatbestände sollten im Bereich der Forschung weiter genutzt werden, auch wenn sie nicht allen formellen Vorgaben der DS-GVO genügen.

Die gesetzlichen Erlaubnistatbestände unterscheiden häufig zwischen zwei Anwendungsfällen:

1) Nutzung der Patientendaten zu eigenen Forschungszwecken; hierbei werden die Patientendaten ausschließlich von den Personen zu Forschungszwecken genutzt, die auch in die eigentliche Patientenbehandlung integriert waren.
2) Nutzung der Patientendaten durch Dritte bzw. auch durch Dritte. In diesen Fällen werden die Patientendaten auch von Personen zu Forschungszwecken verarbeitet, die nicht in die Patientenbehandlung eingebunden waren. Hierbei ist neben dem Vorhandensein eines

[93] z.B. unterstützte die Europäische Kommission das EU-Projekt „Electronic Health Records for Clinical Research" (EHR4CR, Laufzeit 2011-2016), welches eine europaweite Technologieplattform für die Sekundärnutzung von Daten aus elektronischen Patientenakten für die klinische Forschung etablieren sollte. [Online, zitiert am 2017-03-24] Verfügbar unter http://www.ehr4cr.eu/

[94] Ihle P. (2008) Datenschutzrechtliche und methodische Aspekte beim Aufbau einer Routinedatenbasis aus der Gesetzlichen Krankenversicherung zu Forschungszwecken. Bundesgesundheitsbl - Gesundheitsforsch - Gesundheitsschutz: 1127–1134

datenschutzrechtlichen Erlaubnistatbestands auch darauf zu achten, dass hierbei keine unbefugte Offenbarung im Sinne des § 203 StGB erfolgt - eine datenschutzrechtliche Erlaubnis zur Verarbeitung stellt nicht notwendigerweise eine Befugnis zur Offenbarung von durch § 203 StGB geschützten Daten dar, so dass hier evtl. eine Schweigepflichtentbindung der betroffenen Patienten vorliegen muss.

9.8.1 Eigene Institution

Die Nutzung personenbezogener Daten, die während der in der eigenen Abteilung stattgefundenen Versorgung anfielen, wird von verschiedenen Landes-Krankenhaus-Gesetzen erlaubt

	Baden-Württemberg	Bayern	Berlin	Brandenburg	Bremen	Hamburg	Hessen	Mecklenburg-Vorpommern	Niedersachsen	Nordrhein-Westfalen	Rheinland-Pfalz	Saarland	Sachsen	Sachsen-Anhalt	Schleswig-Holstein	Thüringen	Bundesrecht
Forschung	-	x[1)]	x[2)]	x[1)]	x	x[1)]	x	x[1)]	x	x[1)]	x[1)]	x[1)]	x[1)]	x[1)]	x	x[1)]	x

Legende:

- \- keine spezielle Regelung
- x Nutzung erlaubt, ggf. unter Berücksichtigung zusätzlicher Bedingungen (1/2)
- 1) Nutzung ohne Einwilligungserklärung möglich
- 2) Nutzung ohne Einwilligungserklärung bei Anonymisierung möglich

Die Kirchenrechtlichen Bestimmungen beinhalten ebenfalls eine Erlaubnis zur Nutzung personenbezogener Daten zu Forschungszwecken.

9.8.2 Institutionsübergreifende Forschung

Eine institutionsübergreifende Forschung beinhaltet - sofern keine Auftragsverarbeitung vorliegt - immer eine Übermittlung der Daten an Stellen außerhalb der eigenen Institution. Für diese Weitergabe ist grundsätzlich ein Erlaubnistatbestand erforderlich. Dabei existiert im Datenschutzrecht kein Konzernprivileg. D. h. jegliche Weitergabe an Stellen außerhalb der eigenen Legaleinheit ist davon betroffen.

So ist bei entsprechender Konstellation die Zusammenarbeit zwischen dem versorgendem Universitätsklinikum und Beschäftigten eines Instituts für Medizinische Biometrie der Universität hiervon betroffen, wenn Universitätsklinikum und Universität eigene Legaleinheiten sind. Gleiches gilt selbstverständlich ebenso, wenn zwei oder mehr Krankenhäuser zusammen forschen oder Beschäftigte aus anderen Legaleinheiten in die eigene Institution zu Forschungszwecken kommen.

Möglichkeiten, dies datenschutzrechtlich zu gestalten, sind insbesondere:

- Die Bildung eines Konstrukts entsprechend Art. 26 DS-GVO („Gemeinsam für die Verarbeitung Verantwortliche“)
- Auftragsverarbeitung
- Arbeitsnehmerüberlassung.

9.9 Forschung mit Patientendaten außerhalb Deutschlands

Im Gegensatz zum BDSG erlaubt die DS-GVO eine Verarbeitung inklusive einer Auftragsverarbeitung überall auf der Welt. Es geht hierbei aus Datenschutzsicht ausschließlich darum, dass das von der DS-GVO definierte Schutzniveau am Ort der Verarbeitung gewährleistet wird.

9.9.1 Verarbeitung innerhalb der EU

Der freie Verkehr personenbezogener Daten, zu denen auch die vom Landesrecht adressierten Patientendaten gehören, darf aus Gründen des Schutzes betroffener Personen bei der Verarbeitung ihrer Daten weder eingeschränkt noch verboten werden (Art. 1 Abs. 3 DS-GVO[95]). Somit dürfen auch datenschutzrechtliche Bestimmungen keine Grundlage für innereuropäische Verkehrsbeschränkungen darstellen[96].

Unter dem Aspekt, dass die DS-GVO das Datenschutzniveau innerhalb ihres Geltungsbereichs auf ein gleich hohes, einheitliches Niveau hebt, ist diese Regelung auch nachvollziehbar. ErwGr. 6 der DS-GVO stellt diesbezüglich fest, dass „private Unternehmen und Behörden im Rahmen ihrer Tätigkeiten in einem noch nie dagewesenen Umfang auf personenbezogene Daten zurückgreifen“ und „auch natürliche Personen Informationen öffentlich weltweit zugänglich“ machen. Diese Entwicklungen „erfordern einen soliden, kohärenteren und klar durchsetzbaren Rechtsrahmen im Bereich des Datenschutzes in der Union“ (ErwGr. 7). Wird dieser Rechtsrahmen innerhalb der EU jedoch gewährleistet, ist eine Beschränkung der (legitimen) Verarbeitung personenbezogener Daten auf bestimmte Örtlichkeiten aus Gründen des Datenschutzes nicht notwendig, da schon von Gesetzes wegen alle Stellen in Europa dasselbe Datenschutzniveau aufweisen (müssen). Entsprechend führt ErwGr. 13 aus, dass „der freie Verkehr personenbezogener Daten in der Union nicht aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten eingeschränkt oder verboten“ werden darf.

Unter Berücksichtigung von Art. 26 Abs. 2 AEUV[97] ist auch offensichtlich, dass aus Sicht des europäischen Gedankens eine (unnötige) Beschränkung innerhalb der europäischen Binnengrenzen nicht mit dem Vertrag über die Arbeitsweise der Europäischen Union vereinbar ist: der „freie Verkehr von Waren, Personen, Dienstleistungen und Kapital“ muss gewährleistet sein.

9.9.2 Verarbeitung in einem Drittland

Entsprechend ErwGr. 10 ist eines der Ziele der DS-GVO, in allen Mitgliedstaaten den Schutz personenbezogener Daten auf einem Mindestniveau zu gewährleisten („[…] sollte das Schutzniveau für die Rechte und Freiheiten von natürlichen Personen bei der Verarbeitung dieser Daten in allen Mitgliedstaaten gleichwertig sein“). Demgemäß muss insbesondere die Übermittlung personenbezogener Daten an Drittländer oder international tätige Organisationen aus Sicht der DS-GVO geregelt werden, damit auch die in diesen Ländern erfolgende Verarbeitung diesem (Mindest-) Schutzniveau entspricht.

---

[95] EUR-Lex: 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 2017-01-02] Verfügbar unter http://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1483339883994&uri=CELEX:32016R0679

[96] Paal B, Pauly D. (2017) Datenschutz-Grundverordnung: DS-GVO. Art. 1 Rn. 13 C.H.Beck Verlag, 1. Auflage. ISBN 978-3-406-69570-4

[97] Vertrag über die Arbeitsweise der Europäischen Union: Art. 26 [Online, zitiert am 2017-01-02] Verfügbar unter https://dejure.org/gesetze/AEUV/26.html

Die Artt. 44 bis 50 in Kapitel V widmen sich der Thematik der Datenverarbeitung in einem Drittland und beschreiben, welche Voraussetzungen geschaffen sein müssen, damit eine dort stattfindende Verarbeitung rechtskonform erfolgen kann.

Art. 44 DS-GVO beschreibt die grundlegenden Erfordernisse. Entsprechend Art. 44 DS-GVO ist für die Einhaltung der Vorgaben neben dem Verantwortlichen ggfs. auch der Auftragsverarbeiter verantwortlich. D. h. wenn ein Verstoß durch den Auftragsverarbeiter verursacht wurde, dann wird ggfs. auch dieser mit einem Bußgeld bestraft, welches bis zu 20 000 000 Euro oder im Fall eines Unternehmens bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs betragen kann. Dies gilt gemäß Art. 44 DS-GVO auch für die etwaige Weiterübermittlung personenbezogener Daten durch das betreffende Drittland oder die betreffende internationale Organisation an ein anderes Drittland oder eine andere internationale Organisation. D. h., wenn aufgrund der in einem Drittland geltenden Regelungen personenbezogene Daten unrechtmäßig im Sinne der DS-GVO weitergegeben werden, sind dafür der Verantwortliche und ggfs. auch der Auftragsverarbeiter verantwortlich.

Art. 45 DS-GVO räumt der Europäischen Kommission das Recht ein, Länder, Gebiete oder Sektoren in einem Drittland zu benennen, die ein angemessenes Schutzniveau haben. Die Kommission kann somit ein angemessenes Datenschutzniveau auch für ein Gebiet oder ein oder mehrere spezifische Sektoren eines Drittlands feststellen. Somit kann ggfs. die Übermittlung in einem Teilbereich statthaft sein, auch wenn das Drittland als Ganzes als „unsicher“ eingestuft bleibt.

Sollte für das Land kein (pauschaler) Angemessenheitsbeschluss vorliegen, können entsprechend **Art. 46 DS-GVO** über einen Vertrag nach den Standarddatenschutzklauseln oder über verbindliche interne Datenschutzvorschriften die für die Übermittlung notwendigen Garantien gegeben werden. Die derzeit geltenden Standardvertragsklauseln [98] behalten entsprechend ErwGr. 171 ihre Gültigkeit, bis sie entweder von der Kommission oder dem EuGH für ungültig erklärt werden. Hierbei muss beachtet werden, dass in den aktuellen Standardvertragsklauseln in Klausel 5 die Pflichten des Datenimporteurs (also die Stelle im Drittland) beschrieben werden. Bei Anwendung der vorliegenden Standardvertragsklausen garantiert der Datenimporteur, dass

- er die personenbezogenen Daten nur im Auftrag des Datenexporteurs und in Übereinstimmung mit dessen Anweisungen und den vorliegenden Klauseln verarbeitet; dass er sich, falls er dies aus irgendwelchen Gründen nicht einhalten kann, bereit erklärt, den Datenexporteur unverzüglich davon in Kenntnis zu setzen,
- er seines Wissens keinen Gesetzen unterliegt, die ihm die Befolgung der Anweisungen des Datenexporteurs und die Einhaltung seiner vertraglichen Pflichten unmöglich machen.

D. h. die rechtlichen Rahmenbedingungen im Drittland müssen dergestalt sein, dass der Datenimporteur diesen Vertragsanforderungen genügen kann.

Das bisher bekannte Instrument „Binding Corporate Rules“ wurde in **Art. 47 DS-GVO** aufgenommen. Binding Corporate Rules (BCR) sind ein Konstrukt für verbindliche Richtlinien

[98] EU-Kommission: Beschluss der Kommission vom 5. Februar 2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern. [Online, zitiert am 2016-05-26]; Verfügbar unter http://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1445851652852&uri=CELEX:32010D0087

zum Umgang mit den eigenen personenbezogenen Daten innerhalb der eigenen Konzernstruktur[99,100]. Basierend auf diesen Richtlinien dürfen internationale Institutionen, Organisationen und Firmen nach geltendem europäischem Recht personenbezogene Daten in Drittstaaten mit nicht angemessenem Datenschutzniveau transferieren, sofern die BCR von der zuständigen Aufsichtsbehörde genehmigt wurden.

Entsprechend **Art. 48 DS-GVO** sind Gesetze von Drittländern, Entscheidungen von Behörden oder auch in einem Drittland gefällte Gerichtsurteile, welche von einem Verantwortlichen die Übermittlung oder Offenlegung personenbezogener Daten fordern, nur dann statthaft, wenn die Aufforderung aus dem Drittland auf eine in Kraft befindliche internationale Übereinkunft (z. B. ein Rechtshilfeabkommen) zwischen dem Drittland und der Union oder bzw. dem Mitgliedsstaat, in welchem der Verantwortliche tätig ist und dessen Rechtsprechung er unterliegt, gestützt ist. Ohne entsprechende Übereinkunft ist eine Übermittlung oder Offenbarung personenbezogener Daten nicht statthaft und kann gemäß Art. 83 Abs. 5 Lit. c DS-GVO mit einem Bußgeld bis zu 20 000 000 Euro oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs sanktioniert werden.

Gemäß **Art 49 Abs. 1 lit. a DSGVO** ist es möglich, personenbezogene Daten auf Basis einer Einwilligung oder zur Erfüllung eines Vertrages zu übermitteln, auch wenn für das jeweilige Drittland das Vorliegen eines Angemessenheitsbeschlusses der Kommission nicht gegeben ist und das Drittland auch keine geeigneten Garantien für die Sicherheit der personenbezogenen Daten aufweist. Entsprechend Art. 49 Abs. 1 Lit. b DS-GVO ist die Übermittlung statthaft, wenn sie für die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen oder zur Durchführung von vorvertraglichen Maßnahmen auf Antrag der betroffenen Person erforderlich ist. Weiterhin ist die Übermittlung personenbezogener Daten eines Betroffenen in ein Drittland statthaft, wenn dies zum Abschluss oder zur Erfüllung eines im Interesse der betroffenen Person von dem Verantwortlichen mit einer anderen natürlichen oder juristischen Person geschlossenen Vertrags erforderlich ist. Im Sinne der Behandlung eines Betroffenen durch einen Arzt kann somit die Übermittlung medizinischer Daten in ein Drittland im Rahmen eines Behandlungsvertrages statthaft sein, wenn beispielsweise die bestmögliche medizinische Versorgung nur durch die Verarbeitung in einem Drittland gewährleistet werden kann und Alternativen nicht gegeben sind. Diesbezüglich gilt es jedoch den Patienten entsprechend zu informieren.

10 Sanktionierung

Die DS-GVO sieht zwei Abstufungen bei der Bußgeldhöhe vor:

1) Geldbußen von bis zu 10.000.000 EUR oder im Fall eines Unternehmens von bis zu 2% seines gesamten weltweit erzielten Jahresumsatzes (Art. 83 Abs. 4)
   Z. B. bei Verstoß gegen

[99] EU-Kommission: Letters and other documents. [Online, zitiert am 2016-05-26]; Verfügbar unter http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/index_en.htm

[100] EU-Kommission: Binding Corporate rules. [Online, zitiert am 2016-05-26]; Verfügbar unter http://ec.europa.eu/justice/data-protection/article-29/bcr/index_en.htm

- 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)

2) Geldbußen von bis zu 20.000.000 EUR oder im Fall eines Unternehmens von bis zu 4% seines gesamten weltweit erzielten Jahresumsatzes (Art. 83. Abs. 5)
   Z. B. bei Verstoß gegen
   - Artt. 5, 6, 7, 9 (z. B. 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
3) Geldbußen von bis zu 20.000.000 EUR oder im Fall eines Unternehmens von bis zu 4% seines gesamten weltweit erzielten Jahresumsatzes (Art. 83. Abs. 6)
   Bei Nichtbefolgung einer Anweisung der Aufsichtsbehörde gemäß Art. 58 Abs. 2

Bei der Verhängung des Bußgeldes sind auch die Vorgaben von Art. 83 Abs. 2 lit. a-k DS-GVO zu berücksichtigen, insbesondere sind zu beachten:

Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde	Hierzu ist z. B. zu betrachten: - 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	Hierzu ist z. B. zu betrachten: - 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	Hierzu ist z. B. 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	Hierzu ist z. B. zu betrachten: - Wurden der Aufsichtsbehörde unverzüglich alle benötigten Informationen gegeben?

Aufsichtsbehörde	- Wurden Anstrengungen unternommen, um nachteilige Auswirkungen zu mildern? - Wurden Anstrengungen unternommen, damit künftig Verstöße dieser Art nicht mehr vorkommen?
Etwaige einschlägige frühere Verstöße	Ist es Wiederholungstatbestand?
Kategorien personenbezogener Daten	Im Kontext der Gesundheitsversorgung/-forschung handelt es sich immer um besondere Kategorien von Daten, sodass ein Verstoß schwerer wiegt.

Es ist nicht damit zu rechnen, dass ein Verantwortlicher bei einem ersten Vergehen, welches auch nur darin bestehen kann, einem einzelnen Betroffenen sein Recht verweigert zu haben, die Höchststrafe angesetzt wird. Allerdings muss die Aufsichtsbehörde bei der Verhängung der Höhe des Bußgeldes auch bedenken, dass der europäische Gesetzgeber hier bewusst die höhere Version des Bußgeldes anordnete und nicht den kleineren Betrag aus Art. 83 Abs. 4 DS-GVO.

Weiterhin muss sich die Höhe der Geldbuße bei einem Verstoß „europäisch“ einordnen lassen. D. h. für einen Verstoß muss theoretisch in allen Ländern ein den Umständen entsprechendes, einheitliches Bußgeld verhängt werden. Diesbezüglich müssen sich die Aufsichtsbehörden abstimmen, womit die derzeitige Artikel-29-Datenschutzgruppe eine eigene Arbeitsgruppe beauftragte[101]. Dabei muss natürlich auch die Wirtschaftslage des Verantwortlichen berücksichtigt werden. So dürfte ein Bürger voraussichtlich in allen Ländern ein wirtschaftlich gleich hohes Bußgeld erhalten, welches sich vom absoluten Betrag jedoch von Land zu Land unterscheiden kann. Ein globales Unternehmen hingegen wird voraussichtlich nach seiner Gesamt-Wirtschaftsleistung beurteilt, unabhängig von der einzelnen Leistung im Land, in welchem das Bußgeld verhängt wird. Die Aufsichtsbehörden planen hier einen Bußgeldkatalog zu erstellen, sodass die Einordnung erleichtert wird.

[101] Article 29 Working Party: Adoption of 2017 GDPR Action Plan. Online, zitiert am 2017-03-23; Verfügbar unter http://ec.europa.eu/newsroom/document.cfm?doc_id=41387

11 Abkürzungsverzeichnis

Abs	Absatz
Art	Artikel
Artt	Artikel (Mehrzahl)
DSB	Datenschutzbeauftragter
DS-GVO	Datenschutz-Grundverordnung
EG	Europäische Gemeinschaft
ErwGr	Erwägungsgrund
EU	Europäische Union
lit	Literal
RL	Richtlinie
Rn	Randnote, -nummer, -zahl, -ziffer
WP	Working Paper

12 Glossar

Auftragsverarbeiter	Art. 4 Ziff. 8 DS-GVO „'Auftragsverarbeiter' eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet“
Automatische Verarbeitung	Verarbeitung unter Nutzung von EDV; also z. B. Word- oder Excel-Datei, aber auch KIS, RIS, PACS, unabhängig ob Client-Server-Lösung oder Stand-alone PC, Tablet oder anderweitige Hardware genutzt wird
Betroffener/ betroffene Person	Genau genommen „betroffene Person“, in der gesamten Literatur aber als "Betroffener" aufgeführt; Art. 4 Ziff. 1 DS-GVO „'Personenbezogene Daten' alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann“
Datei	Im informationstechnischem Sinn: Gruppe von gespeicherten oder als eine Einheit bearbeiteten Aufzeichnungen (Quelle: ISO/IEC 2382:2015)
Daten/Datum	Im Informationstechnischem Sinn: Die re-interpretierbare Darstellung von Information in einer formalisierten, für Kommunikation, Interpretation, oder Bearbeitung geeigneten Weise (Quelle: ISO/IEC 2382:2015)
Datenintegrität	Eigenschaft, dass Daten nicht auf unautorisierte Art geändert oder zerstört worden sind. (Quelle: DIN EN ISO 27799)
Datenlöschung	Arbeitsgang, der zur dauerhaften, unwiderruflichen Entfernung der Informationen über die betreffende Person oder den Gegenstand aus dem betreffenden Speicher oder Speichermedium führt. (Quelle: DIN CEN ISO/TS 14265)
Datenschutzverletzung	Situation, in der Daten einer Person auf illegale Weise oder unter Verletzung einer oder mehrerer relevanter Datenschutzbestimmungen verarbeitet wurde (Quelle: DIN CEN ISO/TS 14265)
Dritter	Art. 4 Ziff. 10 DS-GVO „'Dritter' eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt

	sind, die personenbezogenen Daten zu verarbeiten“
Drittland	Land, welches nicht an die gesetzlichen Anforderungen der EU-Datenschutz-Direktive gebunden ist (Land außerhalb des EWR) (Quelle: DIN EN 14484)
Empfänger	Art. 4 Ziff. 9 DS-GVO „’Empfänger’ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht. Behörden, die im Rahmen eines bestimmten Untersuchungsauftrags nach dem Unionsrecht oder dem Recht der Mitgliedstaaten möglicherweise personenbezogene Daten erhalten, gelten jedoch nicht als Empfänger; die Verarbeitung dieser Daten durch die genannten Behörden erfolgt im Einklang mit den geltenden Datenschutzvorschriften gemäß den Zwecken der Verarbeitung“
Format	Im Informationstechnischem Sinn im Bereich der textuellen Verarbeitung spezifizierte Festsetzung oder Lay-out von Text in gedruckter oder angezeigter Form oder auf einem Datenträger gespeichert (Quelle: ISO/IEC 2382:2015)
Genetische Daten	Art. 4 Ziff. 13 DS-GVO „’Genetische Daten’ personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern und insbesondere aus der Analyse einer biologischen Probe der betreffenden natürlichen Person gewonnen wurden“
Gesundheitsdaten	Art. 4 Ziff. 15 DS-GVO „’Gesundheitsdaten’ personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen“
Nicht-Abstreitbarkeit	Fähigkeit, das Auftreten eines behaupteten Ereignisses oder einer Handlung und die verursachenden Einheiten nachzuweisen, um Streitigkeiten über das Auftreten oder Nichtauftreten des Ereignisses oder der Handlung und die Beteiligung von Einheiten an dem Ereignis zu entscheiden. (Quelle: DIN ISO IEC 27000)
Normadressat	Rechtssubjekt (z. B. natürliche Person, juristische Person, Personenvereinigung), an die sich die Regelung eines Gesetzes (= einer Norm) richtet
Notfallzugriff	Zugriff auf Daten für einen angemessenen und festgelegten Zweck, wenn eine bestehende Verletzungs- oder Todesgefahr spezielle Genehmigungen oder die Außerkraftsetzung anderer Steuerungseinrichtungen erfordert, um die Verfügbarkeit von Daten in unterbrechungsloser und dringlicher Art und Weise sicherzustellen. (Quelle: DIN CEN ISO/TS 14265)
Offenlegung	Preisgabe von Daten an Personen, die nicht routinemäßig über die

	entsprechende Berechtigung verfügen. (Quelle: DIN CEN ISO/TS 14265)
Pseudonymisierung	Pseudonymisierung ist „die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden“. (Quelle: Art. 4 Ziff. 5 DS-GVO)
Restrisiko	nach der Risikobehandlung verbleibende Risiko (Quelle: DIN ISO IEC 27001)
Revisionssicherheit	Der Begriff „Revisionssicherheit“ bezieht sich auf die Anforderungen a) des Handelsgesetzbuches (§§ 239, 257 HGB) b) der Abgabenordnung (§§ 146, 147 AO), c) der Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS) d) ... d. h., auf praktisch ausnahmslos steuerrechtliche bzw. handelsrechtliche Vorgaben. Andere gesetzlichen Vorgaben werden hierbei nicht beachtet. Die revisionssichere Archivierung ist nur ein Bestandteil der rechtssicheren Archivierung. So beinhaltet eine revisionssichere Archivierung beispielsweise keine datenschutzrechtlichen Vorgaben, z. B. bzgl. des Zugriffs auf die archivierten Daten. Hingegen beinhaltet eine revisions- und rechtssichere Archivierung auch alle rechtlichen Anforderungen.
Risiko	Kombination aus der (Eintritts-) Wahrscheinlichkeit eines Ereignisses und dessen Auswirkungen (Quelle: DIN ISO IEC 27000)
Signaturen, elektronische	Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen (Quelle: §2 Abs.1 SigG)
Verantwortlicher	Art. 4 Ziff. 7 DS-GVO „’Verantwortlicher’ die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden“
Verarbeitung	Art. 4 Ziff. 2 DS-GVO „’Verarbeitung’ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die

	Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung“
Verfahren	festgelegte Art und Weise, eine Tätigkeit oder einen Prozess auszuführen (Quelle: DIN ISO IEC 27000)
Verfügbarkeit	Eigenschaft, auf Anforderung einer autorisierten Entität zugänglich und nutzbar zu sein (Quelle: DIN EN ISO 22600-1)
Vertraulichkeit	Eigenschaft, die dazu führt, dass die betreffende(n) Information(en) keinen Personen, Entitäten oder Prozessen, die nicht über die entsprechende Autorisation verfügen, verfügbar gemacht oder diesen gegenüber offengelegt wird (Quelle: DIN EN ISO 22600-1)

13 Literatur

13.1 Bücher

- Antonow K. (2006) Der rechtliche Rahmen der Zulässigkeit für Biobanken zu Forschungszwecken. Nomos Verlagsgesellschaft; 1. Auflage, ISBN 978-3-832-91709-8
- Boos J, Spranger TM, Heinrichs B. (2010) Forschung mit Minderjährigen: Medizinische, rechtliche und ethische Aspekte. Verlag Karl Alber, 1. Auflage, ISBN 978-3-495-48436-4
- Deutsch E, Spickhoff A. (2014) Medizinrecht - Arztrecht, Arzneimittelrecht, Medizinprodukterecht und Transfusionsrecht. Springer Verlag, 7. Auflage, ISBN 978-3-642-38148-5
- Deutsch et al. (2011) Die Implementierung der GCP-Richtlinie und ihre Ausstrahlungswirkungen. Springer Verlag, 1. Auflage, ISBN 978-3-642-13176-9
- Forgó et al. (2010) Ethical and Legal Requirements of Transnational Genetic Research. Nomos Verlagsgesellschaft; 1. Auflage, ISBN 978-3-848-72489-5
- Freier F. (2009) Recht und Pflicht in der medizinischen Humanforschung – Zu den rechtlichen Grenzen der kontrollierten Studie. Springer Verlag, 1. Auflage, ISBN 978-3-540-95876-5
- Harnischmacher et al. (2006) Checkliste und Leitfaden zur Patienteneinwilligung: Grundlagen und Anleitung für die klinische Forschung. Medizinisch Wissenschaftliche Verlagsgesellschaft; 1. Auflage, ISBN 978-3-939-06925-6
- Kandler HC. (2008) Rechtliche Rahmenbedingungen biomedizinischer Forschung am Menschen. Springer Verlag, 1. Auflage, ISBN 978-3-540-75515-9
- Karaalp RN. (2016) Der Schutz von Patientendaten für die medizinische Forschung in Krankenhäusern: Eine rechtsvergleichende Untersuchung der Regelungen in Deutschland und Frankreich. Springer Verlag, 1. Auflage, ISBN 978-3-658-16184-2
- Magnus D. (2006) Medizinische Forschung an Kindern: Rechtliche, ethische und rechtsvergleichende Aspekte der Arzneimittelforschung an Kindern. Mohr Siebeck Verlag, 1. Auflage, ISBN 978-3-161-49033-0
- Plomer O. (2005) The Law and Ethics of Medical Research: International Bioethics and Human Rights. Verlag Routledge-Cavendish, 1. Auflage, ISBN 978-1-859-41687-7
- Pommerening et al. (2014) Leitfaden zum Datenschutz in medizinischen Forschungsprojekten: Generische Lösungen der TMF 2.0. Medizinisch Wissenschaftliche Verlagsgesellschaft, 1. Auflage, ISBN 978-3-95466-123-7
- Pöttgen N. (2008) Medizinische Forschung und Datenschutz. Peter Lang Verlag, 1. Auflage, ISBN 978-3-631-58050-9
- Reimer F. (2017) Die Forschungsverfügung - Eine Untersuchung zu antizipierten Verfügungen in der Humanforschung unter besonderer Berücksichtigung der Arzneimittelforschung mit Demenz- und Notfallpatienten. Springer Verlag, 1. Auflage, ISBN 978-3-662-53261-4
- Schriever KH, Schröder M. (2014) G3P - Good Privacy Protection Practice in Clinical Research: Principles of Pseudonymization and Anonymization. De Gruyter Verlag, 1. Auflage, ISBN 978-3-110-36764-5
- Simon et al. (2006) Biomaterialbanken - Rechtliche Rahmenbedingungen. Medizinisch Wissenschaftliche Verlagsgesellschaft, 1. Auflage, ISBN 978-3-939-06914-0
- Söns U. (2008) Biobanken im Spannungsfeld von Persönlichkeitsrecht und Forschungsfreiheit: Eine Gefahr für Selbstbestimmungsrecht und Datenschutz? Verlag Dr. Kovac, 1. Auflage, ISBN 978-3-830-03915-0

- Sprecher F. (2007) Medizinische Forschung mit Kindern und Jugendlichen: nach schweizerischem, deutschem, europäischem und internationalem Recht. Springer Verlag, 1. Auflage, ISBN 978-3-540-73757-5

13.2 Journals

- Arning M, Forgó N, Krügel T. (2006) Datenschutzrechtliche Aspekte der Forschung mit genetischen Daten. DuD: 700-705
- Bender S, Elias P. (2015) Forschung mit Big Data - die europäische Perspektive. Bundesgesundheitsbl: 799-805
- Burgardt C. (2006) Rechtliche Rahmenbedingungen der Arzneimittelforschung. Onkologe: 309-319
- Cornelius K. (2017) Die Bereitstellung humaner Alt-Bioproben durch eine Biobank zu Zwecken der medizinischen Genomforschung. MedR: 15-20
- Desoi M, Jandt S. (2012) Zulässige Erhebung von Daten zu Forschungszwecken. DuD: 895-901
- Deutsch E. (2013) Aufklärung und Einwilligung bei klinischer Forschung: Einfluss der allgemeinen Regeln des Völkerrechts. MedR: 243-244
- Freier F. (2005) Getrennte Körperteile in der Forschung zwischen leiblicher Selbstverfügung und Gemeinbesitz. MedR: 321-328
- Freund G, Weiss N. (2004) Zur Zulässigkeit der Verwendung menschlichen Körpermaterials für Forschungs- und andere Zwecke. MedR: 315-319
- Gerling RW. (2008) Einwilligung und Datenweitergabe in der Forschung. DuD: 733-735
- Hase F. (2011) Forschung mit Sozialdaten. DuD: 875-878
- Herbst T. (2009) Die Widerruflichkeit der Einwilligung in die Datenverarbeitung bei medizinischer Forschung. MedR: 149–152
- Hoff L. (2015) Forschungs- und Entwicklungskooperation zwischen Industrie und Lehre. 43-46
- Lippert HD. (2001) Forschung an und mit Körpersubstanzen – wann ist die Einwilligung des ehemaligen Trägers erforderlich? MedR: 406-410
- Lippert HD. (2013) Das Patientenrechtegesetz und die biomedizinische Forschung – wird die Forschung etwa stiefmütterlich behandelt? MedR: 714-718
- Mand E. (2005) Biobanken für die Forschung und informationelle Selbstbestimmung. MedR: 565-575
- Menzel HJ. (2006) Datenschutzrechtliche Einwilligungen in medizinische Forschung. MedR: 702-707
- Molnár-Gábor F, Korbel JO. (2016) Verarbeitung von Patientendaten in der Cloud - Die Freiheit translationaler Forschung und der Datenschutz in Europa. ZD: 274-281
- Nitz G, Dierks C. (2002) Nochmals: Forschung an und mit Körpersubstanzen - wann ist die Einwilligung des ehemaligen Trägers erforderlich? MedR: 400-403
- Rittner C. (2007) Ein Modell für die Forschung am einwilligungsunfähigen (bewusstlosen) Notfallpatienten. MedR: 340-344
- Roßnagel A, Hornung G. (2008) Forschung à la Card? Grenzen und Vorschläge für eine Nutzung der elektronischen Gesundheitskarte zur medizinischen Forschung. MedR: 538-543
- Rütsche B. (2014) Das Recht der biomedizinischen Forschung am Menschen: Nationales Recht im Spiegel internationaler Prinzipien. MedR: 725-732
- Spickhoff A. (2006) Forschung an nicht-einwilligungsfähigen Notfallpatienten. MedR: 707-715

- Spindler G. (2016) Big Data und Forschung mit Gesundheitsdaten in der gesetzlichen Krankenversicherung. MedR: 691-699
- Taupitz J. (2012) Medizinische Forschung an jungen und alten Patienten. MedR: 583-588
- Timm J. (2016) Digitalisierung und Big Data in der Medizin. MedR: 681-686
- Watteler O, Kinder-Kurlanda KE. (2015) Anonymisierung und sicherer Umgang mit Forschungsdaten in der empirischen Sozialforschung. DuD: 515-519
- Wellbrock R. (2003) Datenschutzrechtliche Aspekte des Aufbaus von Biobanken für Forschungszwecke. MedR: 77-82