Datenschutz bei Klinischen Studien

Eine Zusammenarbeit von

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

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

Autoren

Susanne Jendges	Universitätsklinikum Giessen und Marburg GmbH
David Koeppe	Vivantes - Netzwerk für Gesundheit GmbH
Michael Letter	5medical management GmbH
Johannes Moenter	CURACON GmbH Wirtschaftsprüfungsgesellschaft
Susanne Pelka	Sana Kliniken AG
Mark Rüdlin	Rechtsanwalt + Datenschutzbeauftragter
Bernd Schütze	Deutsche Telekom Healthcare and Security GmbH

Stand: 10. Dezember 2019

Haftungsausschluss

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

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

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

Copyright

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

Geschlechtergerechte Sprache

Hinweis bzgl. geschlechtsneutraler Formulierung im gesamten Text:

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

Inhaltsverzeichnis

Zusammenfassung

Bei jeder klinischen Studie werden personenbezogene Daten von Patienten, mitunter auch von Probanden verarbeitet. Selbst wenn Studien mit anonymisierten Daten arbeiten, müssen zunächst personenbezogene Daten erfasst und anschließend anonymisiert werden. Daher sind in jeder klinischen Studie datenschutzrechtliche Rahmenbedingungen zu beachten.

Bei klinischen Studien werden grundsätzlich die in Art. 9 Abs. 1 DS-GVO beschriebenen besonderen Kategorien von Daten verarbeitet, insbesondere Gesundheitsdaten oder auch genetische Daten. Die Verarbeitung dieser Daten beinhaltet stets erhebliche Risiken für die Grundrechte und Grundfreiheiten der betroffenen Personen. Daher ist die Verarbeitung grundsätzlich verboten, d.h. für die Verarbeitung derartiger Daten muss ein Erlaubnistatbestand vorliegen, welcher entsprechend ErwGr. 52 DS-GVO angemessene Garantien zum Schutz der personenbezogenen Daten und anderer Grundrechte aufweisen muss. Im Rahmen von klinischen Studien stellt i.d.R. die Einwilligung der betroffenen Personen die Rechtsgrundlage für die Verarbeitung dar, jedoch bedingen die Vorgaben der DS-GVO, dass für eine rechtlich gültige Einwilligung gemäß den Anforderungen von ErwGr. 51 DS-GVO auch entsprechend angemessene Schutzmaßnahmen zur Verarbeitung dieser sensiblen Daten vorhanden sein müssen.

ErwGr. 53 DS-GVO betont, dass besondere Kategorien personenbezogener Daten, die ja eines höheren Schutzes bedürfen, nur dann für gesundheitsbezogene Zwecke verarbeitet werden sollen, wenn die Verarbeitung für das Erreichen dieser Zwecke im Interesse einzelner natürlicher Personen und der Gesellschaft insgesamt erforderlich ist. D.h.: Bei jeder klinischen Studie muss entsprechend den Vorgaben von Art. 5 DS-GVO nachgewiesen werden, dass die Studie entweder im Interesse einzelner natürlicher Personen oder die Studie im Interesse der Gesellschaft insgesamt erforderlich ist.

Bei jeder Verarbeitung sind die in Art. 5 DS-GVO aufgeführten Grundsätze für die Verarbeitung personenbezogener Daten zu beachten. Diese müssen bei jeder Verarbeitung personenbezogener Daten immer gewährleistet sein müssen, also auch bei jeder Form einer klinischen Studie. Diese Grundsätze beinhalten u. a. die Zweckbindung, die Datenminimierung und die Speicherbegrenzung. Somit dürfen personenbezogene Daten bei einer klinischen Studie nur auf rechtmäßige Weise zu genau definierten Zwecken verarbeitet werden, es dürfen nur die zur Erreichung dieser (vor Erhebung) definierten Zwecke unbedingt erforderlichen Daten verarbeitet werden und der Zeitraum der Speicherung der Daten muss definiert sein: Daten müssen nach Erreichen des Zweckes gelöscht werden, wenn keine gesetzlichen Aufbewahrungsfristen einzuhalten sind. Die DS-GVO verlangt grundsätzlich, dass man die Einhaltung der Vorgaben der DS-GVO nachweist.

Insbesondere bei retrospektiven Studien findet die Datenerhebung vor Beginn der Studie statt, denn hier werden ausschließlich Patientendaten aus in der Vergangenheit stattgefundenen Behandlungen genutzt. Die Patientendaten werden in den versorgenden Einrichtungen jedoch zu Zwecken der Patientenversorgung erhoben, nicht um die Daten für eine Studie zu nutzen. Daher spricht man hier von einer „Sekundärnutzung“ der Daten; der primäre Zweck der Datenverarbeitung war ja die Patientenversorgung. Art. 5 Abs. 1 lit. b DS-GVO beinhaltet die Regelung, dass „eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Art. 89 Abs. 1 DS-GVO nicht als

unvereinbar mit den ursprünglichen Zwecken“, man spricht hier von „Zweckkompatibilität“. Aber gleichwohl liegt natürlich eine Zweckänderung vor, aus der entsprechende Pflichten resultieren.

Die Verarbeitung personenbezogener Daten in einer klinischen Studie muss für die betroffenen Personen/Patienten transparent erfolgen, alle in Kapitel II der DS-GVO genannten Betroffenenrechte und insbesondere den Informationspflichten muss genügt werden. Jeder Patient hat das Recht auf Auskunft bzgl. der in einem klinischen Studie verarbeiteten bzw. gespeicherten Daten. Weiterhin ist u. a. zu beachten, dass nach Art. 15 Abs. 3 DS-GVO muss der Verantwortliche betroffenen Personen auch eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung stellen. Dementsprechend sollte die Möglichkeit existieren, alle zu einem Patienten gehörenden Daten in eine pdf-Datei exportieren zu können, um diese Datei anfragenden betroffenen Patienten übergeben zu können.

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

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

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

Gemäß Art. 38 Abs. 1 DS-GVO muss ein Datenschutzbeauftragte „ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden“ werden. Dies beinhaltet natürlich auch Forschungsprojekte mit personenbezogenen Daten, insbesondere auch klinische Studien. Daher ist der Datenschutzbeauftragte schon bei der Planung einer klinischen Studie einzubeziehen und ihm sowohl während der Planung als auch während der Laufzeit alle zur Prüfung der Verarbeitung benötigten Informationen bereitzustellen.

1 Vorwort

Klinische Studien dienen der stetigen Verbesserung von Diagnose- und Therapiemethoden und bilden daher einen wichtigen und unverzichtbaren Pfeiler des medizinischen Fortschritts. Anders als bei anderen Forschungen erfolgen bei klinischen Studien Prüfungen und Untersuchungen direkt an einem Patienten oder Probanden, d.h. es werden bei jeder klinischen Studie sensible Gesundheitsdaten oder auch genetische Daten verarbeitet.

Diese Praxishilfe will sowohl den Forscher als auch den Datenschutzbeauftragten beim Umgang mit den datenschutzrechtlichen Anforderungen bei klinischen Studien unterstützen.

2 Einführung

Wissenschaftliche Studien sind die wichtigste Entscheidungsgrundlage in der Medizin. Klinische Studien werden zur Prüfung der Wirksamkeit, der Verträglichkeit und der Sicherheit von Untersuchungs- und Behandlungsmethoden durchgeführt, aber auch um verschiedene Behandlungs- oder Untersuchungsmöglichkeiten miteinander zu vergleichen.

Eine Ethikkommission muss jede Studie im Vorfeld genehmigen. Die Zusammensetzung von Ethikkommissionen wird sowohl im Landesrecht (z. B. im niedersächsischen Kammergesetz für die Heilberufe[1] oder im baden-württembergischen Heilberufe-Kammergesetz[2]), als auch in den Spezialgesetzen des Bundes wie beispielsweise dem AMG oder dem MPG geregelt. In den Landesgesetzen wird in der Regel darauf verwiesen, dass in den Landesärzteordnungen die Zusammensetzung geregelt wird, in den Bundesgesetzen wird i.d.R. das Bundesministerium ermächtigt, in Rechtsverordnungen Aufgaben und Zusammensetzung von Ethikkommissionen zu bestimmen. Zu den Mitgliedern von Ethikkommissionen zählen i.d.R. aber immer Ärzte, Naturwissenschaftler, Juristen, Philosophen und Laien, statt Philosophen werden mitunter auch Theologen hinzugezogen. Die Zentrale Ethikkommission der Bundesärztekammer hat beispielsweise bis zu 16 Mitgliedern, unter denen sich folgende 12 Mitglieder befinden sollten: „fünf Vertreter der Medizin, zwei Vertreter der Philosophie oder Theologie, zwei Vertreter der Naturwissenschaften, ein Vertreter der Sozialwissenschaften, zwei Vertreter der Rechtswissenschaften“.

Für einige besondere [3]Formen von klinischen Studien wurden rechtliche Rahmenbedingungen geschaffen:

- Bei Arzneimittelstudien darf die klinische Prüfung am Menschen gemäß § 40 Abs. 1 AMG erst begonnen werden, wenn die zuständige Ethik-Kommission diese nach Maßgabe des § 42 Abs. 1 AMG zustimmend bewertet und die zuständige Bundesoberbehörde diese nach Maßgabe des § 42 Abs. 2 AMG genehmigt hat[4].
- Gleiches gilt für Medizinprodukte: § 20 Abs. 1 MPG schreibt vor, dass klinische Prüfungen erst beginnen dürfen, wenn die zuständige Ethik-Kommission diese nach Maßgabe des § 22 MPG zustimmend bewertet und die zuständige Bundesoberbehörde diese nach Maßgabe des § 22a MPG genehmigt hat[5].
- Auch Studien mit ionisierender Strahlung bedürfen entsprechend § 31 StrlSchG einer behördlichen Genehmigung, welche nur erteilt werden darf, wenn insbesondere die Voraussetzungen von § 31 Abs. 4 StrlSchG erfüllt sind[6].

[1] HKG – Kammergesetz für die Heilberufe. [Online, zitiert am 2019-09-17]; Verfügbar unter https://www.ms.niedersachsen.de/startseite/gesundheit_pflege/gesundheit/13054.html

[2] Heilberufe-Kammergesetz. [Online, zitiert am 2019-09-17]; Verfügbar unter https://www.aerztekammer-bw.de/10aerzte/40merkblaetter/20recht/10gesetze/hbkg.pdf

[3] Statut der Zentralen Kommission zur Wahrung ethischer Grundsätze in der Medizin und ihren Grenzgebieten (Zentrale Ethikkommission). [Online, zitiert am 2019-09-17]; Verfügbar unter https://www.zentrale-ethikkommission.de/fileadmin//user_upload/downloads/pdf-Ordner/Zeko/Statut20120420.pdf

[4] Gesetz über den Verkehr mit Arzneimitteln (Arzneimittelgesetz, AMG). [Online, zitiert am 2019-09-17]; Verfügbar unter https://www.gesetze-im-internet.de/amg_1976/

[5] Gesetz über Medizinprodukte (Medizinproduktegesetz, MPG). [Online, zitiert am 2019-09-17]; Verfügbar unter https://www.gesetze-im-internet.de/mpg/index.html#BJNR196300994BJNE002904377

[6] Gesetz zum Schutz vor der schädlichen Wirkung ionisierender Strahlung (Strahlenschutzgesetz, StrlSchG). [Online, zitiert am 2019-09-17]; Verfügbar unter https://www.gesetze-im-internet.de/strlschg/

2.1 Arten von klinischen Studien

Klinische Studien können nach verschiedenen Kriterien eingeteilt werden.

Einerseits können interventionelle (= experimentelle) und nicht interventionelle (= beobachtende) Studien unterschieden werden:

- Beobachtungsstudien: Beobachtungsstudien sind nichtexperimentelle Studien, bei welchen die Patienten bzw. die Probanden über eine im Studiendesign definierte Zeitspanne hinweg unter natürlichen Bedingungen hinsichtlich eines oder mehrerer interessierenden/r Merkmals/e, beobachtet werden. Dies kann prospektiv bzw. retrospektiv erfolgen. Beobachtungsstudien sind meist als rein explorative Studien angelegt, die zum Generieren von Hypothesen oder zum Abschätzen der Gültigkeit von Hypothesen eingesetzt werden.
- Interventionsstudien: Interventionsstudien untersuchen gezielt die Einführung einer Behandlung (= Intervention) auf ein Erkrankungsrisiko. Interventionsstudien werden i.d.R. dann durchgeführt, wenn aufgrund von Beobachtungsstudien ein Zusammenhang zwischen einem Einflussfaktor und der Erkrankung wahrscheinlich ist. Bei den Interventionsstudien werden randomisierte kontrollierte Studien und nichtrandomisierte kontrollierte Studien unterschieden.
    - Bei randomisierten kontrollierten Studien werden Versuchspersonen nach dem Zufallsprinzip (randomisiert) in zwei oder mehrere Gruppen aufgeteilt. Die Personen der einen Gruppe erfahren die Intervention (z.B. erhalten das zu untersuchende Medikament), während die Angehörigen der anderen Gruppe(n) eine konventionelle Therapie, eine Vergleichstherapie, ein Placebo oder nichts erhalten. Wissen weder der Proband bzw. der Patient noch der Forscher, wer welche Therapie erhält, handelt es sich um eine Doppelblindstudie. Ist der Forscher, aber nicht die Versuchsperson informiert, spricht man von einer Blindstudie.
    - Nichtrandomisierte kontrollierte Studien weisen den Unterschied auf, dass Versuchspersonen nicht nach dem Zufallsprinzip den Gruppen zugeordnet werden.

  Weiterhin können interventionelle Studien in fünf Phasen eingeteilt werden:
    - Phase-0-Versuche (ca. 10 bis 15 Personen) sind Therapiestudien, welche mit subtherapeutischen Dosen der Behandlung durchgeführt werden, bei Medikamenten spricht man von „Microdosing“-Studien. Es handelt sich um die ersten Versuche an gesunden Menschen („First-In-Man“-Studien - kurz „FIM“ - oder auch „First-In-Human“-Studien - kurz „FIH“). Dabei stehen im Bereich einer Arzneimittelstudie die Erforschung von Pharmakokinetik und Pharmakodynamik im Vordergrund. Das Prüfpräparat wird als „Investigational Medicinal Product“ oder kurz „IMP“ bezeichnet.
    - Phase I-Studien sind kleinere Studien mit ca. 20 bis 80 Personen, in welchen eine neue Behandlung an gesunden Freiwilligen (Probanden) getestet wird; es erfolgt keine Gabe (Applikation) an Patienten. In diesem Stadium werden grundlegende Eigenschaften wie Verträglichkeit und Sicherheit einer neuen Behandlung überprüft, um zu sehen, ob es sich für einen Einsatz beim Menschen eignet und mit welchen Nebenwirkungen zu rechnen sind.
    - Phase II-Studien sind etwas größer angelegt als Phase I-Studien und umfassen i.d.R. zwischen 50 und 200 Patientinnen und Patienten, die an jener Erkrankung leiden, für welche die Behandlung konzipiert wurde. In diesen Studien sollen erste Daten zur Wirksamkeit ermittelt werden. Auch soll die optimale Dosierung herausgefunden

werden, bei welcher die beste Wirkung mit den geringsten Nebenwirkungen erzielt wird.

- Phase III-Studien sind große Studien mit bis zu 10.000 Personen und geben recht präzise Auskunft über Wirksamkeit und Verträglichkeit der untersuchten Behandlung. Phase III-Studien sind meistens Vergleichsstudien in denen die Wirkungen und Nebenwirkungen der Behandlung auf Patientinnen und Patienten im Vergleich zu einer Kontrollgruppe, die eine andere Behandlung erhält, ermittelt werden.
- Phase IV-Studien finden statt, wenn eine Behandlung bereits auf dem Markt ist. Diese Studien können aus verschiedenen Gründen erfolgen. Phase IV-Studien werden z.B. von den Zulassungsorganisationen zur Identifikation seltener Nebenwirkungen gefordert, nicht selten aber auch zu Zwecken des Marketings eingesetzt. Hierzu zählt z. B. auch die Meldung von "unerwünschten Arzneimittelreaktionen" (sog. "UAWs").

Weiterhin werden Studien nach dem zeitlichen Verlauf unterschieden:

- Querschnittstudie: Hier erfolgt bei jedem Studienteilnehmer nur zu einem Zeitpunkt eine Messung.
- Längsschnittstudie: Bei diesen Studien erfolgen bei jedem Studienteilnehmer Messungen zu mindestens zwei Zeitpunkten.
- Prospektive Studie: Das zu untersuchende Ereignis wie beispielsweise eine Erkrankung oder die Einwirkung eines Medikamentes auf einen Erkrankungsverlauf liegt bei Studienbeginn in der Zukunft.
- Retrospektive Studie: Das zu untersuchende Ereignis wie beispielsweise eine Erkrankung oder die Einwirkung eines Medikamentes auf einen Erkrankungsverlauf liegt bei Studienbeginn in der Vergangenheit.

Studien werden entweder mit Patienten oder mit gesunden Probanden durchgeführt. Evidenzbasierte Studien sind wissenschaftlich abgesicherte Studien; jede Studie kann – entsprechendes Vorgehen vorausgesetzt, eine evidenzbasierte Studie darstellen.

2.2 Sonderformen klinischer Studien

Es gibt einige Sonderformen klinischer Studien. Die bekanntesten sind:

1) Basket-Studie: Dabei handelt es sich um klinische Studien, welche den Einfluss eines Arzneistoffs auf eine Mutation erforschen, die bei (verschiedenen) Krebsformen auftritt.
2) Health Technology Assessment: Bei einem Health Technology Assessments (HTA) werden bereits eingeführte diagnostische, therapeutische oder präventive Verfahren und Technologien hinsichtlich ihrer Auswirkung auf die gesundheitliche Versorgung der Bevölkerung untersucht.
3) Meta-Analysen fassen mehrere Studien zur gleichen Fragestellung zusammen. Häufig werden dabei die Ergebnisse der Einzelstudien zusammengefasst und neu bewertet, wodurch i.d.R. die Aussagekraft wesentlich gesteigert werden kann.
4) Multi-Center-Studie: Dies sind klinische Studien, welche in mehreren klinischen Zentren (z.B. in verschiedenen Krankenhäusern) von unterschiedlichen Untersuchern durchgeführt werden.
5) Umbrella-Studie: Hierbei handelt es sich um klinische Studien, in welchen der Einfluss mehrerer Arzneistoffe auf verschiedene Mutationen einer Krebsform untersucht wird.

2.3 Klinische Studien und Datenschutz

Bei jeder klinischen Studie werden personenbezogene Daten von menschlichen Patienten oder Probanden verarbeitet, seien die Daten direkt einer Person zuordenbar oder pseudonymisiert. Selbst wenn Studien mit anonymisierten Daten arbeiten, müssen zunächst personenbezogene Daten erfasst und anschließend anonymisiert werden. Daher sind in jeder klinischen Studie datenschutzrechtliche Rahmenbedingungen zu beachten.

Bei klinischen Studien werden grundsätzlich die in Art. 9 Abs. 1 DS-GVO beschriebenen besonderen Kategorien von Daten verarbeitet, insbesondere Gesundheitsdaten oder auch genetische Daten. ErwGr. 51 DS-GVO hebt hervor, dass diese Daten hinsichtlich der Grundrechte und Grundfreiheiten besonders sensibel sind und daher einen besonderen Schutz verdienen. Die Verarbeitung dieser Daten beinhaltet grundsätzlich erhebliche Risiken für die Grundrechte und Grundfreiheiten der betroffenen Personen. Daher ist die Verarbeitung grundsätzlich verboten, d.h. für die Verarbeitung derartiger Daten muss ein Erlaubnistatbestand vorliegen, welcher entsprechend ErwGr. 52 DS-GVO angemessene Garantien zum Schutz der personenbezogenen Daten und anderer Grundrechte aufweisen muss. Im Rahmen von klinischen Studien stellt i.d.R. die Einwilligung der betroffenen Personen die Rechtsgrundlage für die Verarbeitung dar, jedoch bedingen die Vorgaben der DS-GVO, dass für eine rechtlich gültige Einwilligung gemäß den Anforderungen von ErwGr. 51 DS-GVO auch entsprechend angemessene Schutzmaßnahmen zur Verarbeitung dieser sensiblen Daten vorhanden sind.

ErwGr. 53 DS-GVO betont, dass besondere Kategorien personenbezogener Daten, die ja eines höheren Schutzes bedürfen, nur dann für gesundheitsbezogene Zwecke verarbeitet werden sollen, wenn die Verarbeitung für das Erreichen dieser Zwecke im Interesse einzelner natürlicher Personen und der Gesellschaft insgesamt erforderlich ist. D.h.: Bei jeder klinischen Studie muss entsprechend den Vorgaben von Art. 5 DS-GVO nachgewiesen werden, dass

a) die Studie im Interesse einzelner natürlicher Personen erforderlich ist, oder
b) die Studie im Interesse der Gesellschaft insgesamt erforderlich ist.

Daneben existieren noch diverse andere Vorgaben, die zu beachten sind. Festzuhalten ist daher, dass die Umsetzung datenschutzrechtlicher Vorgaben zu jeder Studie gehört.

3 Datenschutzrechtliche Vorgaben bei verschiedenen klinischer Studien: Eine erste Einordnung

Im Folgenden werden einleitend einige Vorgaben der DS-GVO erläutert, woraufhin in den folgenden Kapiteln diese Anforderungen präzisiert werden. Die Anforderungen der DS-GVO gelten für alle Studientypen gleichermaßen, dennoch gibt es bei einigen Studienkategorien Besonderheiten, die in aller Kürze dargestellt werden.

3.1 Für jede Studie gilt

3.1.1 Verbot mit Erlaubnisvorbehalt

Art. 9 Abs. 1 DS-GVO verbietet kategorisch alle Verarbeitungen besonderer Kategorien personenbezogener Daten. Unter diese Kategorien fallen:

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

Damit fällt auch jegliche Verarbeitung von Patientendaten unter dieses „Verbot mit Erlaubnisvorbehalt“. Art. 9 Abs. 2 DS-GVO schränkt dieses Verbot ein: Liegt ein gesetzlich normierter Erlaubnistatbestand zur Verarbeitung vor, ist die Verarbeitung nur für diesen Zweck statthaft.

3.1.2 Bei jeder Verarbeitung zu Beachten: Die Grundsätze für die Verarbeitung personenbezogener Daten

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

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

2. Was genau der Verordnungsgeber unter der Regelung einer „Verarbeitung nach Treu und Glauben“ versteht, wird an keiner Stelle in der DS-GVO präzisiert. Jedoch findet sich in ErwGr. 38 RL 95/46[7] hierzu Folgendes:

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

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

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

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

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

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

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

3.2 Retrospektiv Studien

Bei einer retrospektiven Studie fand die Datenerhebung vor Beginn der Studie statt. Im Falle retrospektiver klinischer Studien werden ausschließlich Patientendaten aus in der Vergangenheit stattgefundenen Behandlungen genutzt.

Als Rechtsgrundlage könnte eine Einwilligung dienen. Die Schwierigkeit besteht darin, dass die Patienten als Ansprechpartner nur indirekt über postalische Wege erreichbar sind. Erfahrungsgemäß werden Rücklaufquoten von 8 % bei Anfragen bzgl. Einwilligung in eine Studie bereits als gut gewertet. Umfragen ergaben, dass Patienten i.d.R. keine Einwände gegen die Nutzung der Daten für klinische Studien haben, ihnen aber der Aufwand des Zurücksendens der Einwilligung zu groß ist, selbst wenn ein ausgefüllter und frankierter Rückumschlag beiliegt; insbesondere das Lesen der Informationen zur Studie erfordert ihnen zu viel Zeit. Daher ist eine Einwilligung hier weniger geeignet, denn 8 % (oder häufig weniger) ist für eine statistische Aussage nicht immer ausreichend.

Der Gesetzgeber hat im medizinischen Umfeld die „Eigenforschung“ privilegiert. Eigenforschung bedeutet, dass die Forschung mit Daten von Patienten erfolgt, welche der Forscher selbst behandelt oder mitbehandelt hat. Hier erfolgt keine Offenbarung i. S. d. § 203 StGB, die Verarbeitung beinhaltet

für den Patienten nur minimal höhere Risiken, da kein Unbefugter die Daten verarbeitet. Die Eigenforschung wird dabei in aller Regel auf alle Patienten der eigenen Abteilung wie beispielsweise Neurochirurgie oder Kardiologie eines Krankenhauses ausgedehnt, da jede Ärztin und jeder Arzt die Patienten der Abteilung ja mit behandelten, zumindest bei gemeinsamen Besprechungen im Rahmen von Fallkonferenzen oder Visiten.

Im Rahmen einer Eigenforschung können die Daten aber nicht Dritten zur Verfügung gestellt werden. D.h. eine Single-Center-Studie ist möglich, aber im Falle multizentrischer Studien muss eine Rechtsgrundlage die Weitergabe an Forscher, die nicht in die Behandlung involviert waren, erlauben.

3.3 Prospektiv klinische Studien

Bei einer prospektiven klinischen Studie wird vor Beginn der Studie (und insbesondere damit auch vor Beginn der Erhebung der Daten) festgelegt, welche Fragestellung über die Wirksamkeit einer Behandlungsmethode geprüft werden soll. Da die Daten erst ab dem Zeitpunkt des Studienbeginns gesammelt und ausgewertet werden, können Patienten noch während des Behandlungsaufenthaltes bzgl. einer Einwilligung zur Nutzung seiner Daten an einer Studie gebeten werden. Insbesondere im Falle von multizentrischen Studien ist oftmals eine Einwilligung erforderlich, da die Privilegierung der Eigenforschung eine Weitergabe der Daten an nicht in die Behandlung integrierter Personen nicht beinhaltet.

3.4 Single-center Studien

Eine Single-Center-Studie ist eine klinische Studie, welche nur einem klinischen Zentrum wie beispielsweise einem Krankenhaus durchgeführt wird. Hier besteht der Vorteil, dass i. d. R. der Vorteil der Eigenforschung die Nutzung von Patientendaten ermöglicht.

Allerdings sind im Falle von Krankenhäusern die jeweiligen Landeskrankenhausgesetze zu beachten (siehe Abschnitt 5.3.2).

3.5 Multicenter Studien

Eine Multi-Center-Studie ist eine klinische Studie, welche in mehreren klinischen Zentren (i.d.R. in verschiedenen Krankenhäusern) durchgeführt wird. Insbesondere sind an jedem beteiligten Zentrum Forscher aktiv in die Studie eingebunden. Durch die Zusammenarbeit von mehreren Forschern an verschieden Zentren und der damit i. d. R. verbundenen höheren Fallzahl, weisen Multi-Center-Studien bei der Bewertung von Therapieverfahren meist i. d. R. eine höhere wissenschaftliche Aussagekraft als eine Single-Center-Studie auf.

Datenschutzrechtlich ist hier die Privilegierung der Eigenforschung als Erlaubnistatbestand der Daten unzureichend. Da selbst pseudonyme Daten noch personenbezogene Daten i. S. d. DS-GVO darstellen, ist selbst die Weitergabe pseudonymisierter Patientendaten nicht von dieser Privilegierung abgedeckt, sodass i. d. R. immer eine Einwilligung der Patienten bzgl. Nutzung ihrer Daten für die Multi-Center-Studie erforderlich ist.

4 Zusammenarbeit mit dem Datenschutzbeauftragten

4.1 Information des und Prüfung durch den Datenschutzbeauftragten

Gemäß Art. 38 Abs. 1 DS-GVO muss ein Datenschutzbeauftragte „ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden“ werden. Dies beinhaltet natürlich auch Forschungsprojekte mit personenbezogenen Daten, insbesondere auch klinische Studien.

D. h. der Datenschutzbeauftragte muss vor Beginn einer klinischen Studie über das Vorhaben informiert werden. Entsprechend Art. 39 Abs. 1 lit. a DS-GVO ist der Datenschutzbeauftragte zur Überwachung der Einhaltung der Vorgaben aller datenschutzrechtlichen Bestimmungen verpflichtet. Der Datenschutzbeauftragte muss daher nicht nur informiert werden, sondern es müssen alle Informationen bereitgestellt werden, damit der Datenschutzbeauftragte seinen Prüfpflichten genügen kann. Dies gilt sowohl für den Vorgang der Studienplanung als auch der Studiendurchführung.

4.2 Gutachten für die Ethikkommission

Der Arbeitskreis Medizinischer Ethik-Kommissionen in der Bundesrepublik Deutschland e.V. veröffentlichte im Juni 2018 eine Formulierungsempfehlung bzgl. datenschutzrechtlicher Bewertung durch Ethikkommissionen[8], darin heißt es:

> „Datenschutzrechtliche Aspekte von Forschungsvorhaben werden durch die Ethikkommission grundsätzlich nur kursorisch geprüft. Dieses Votum / diese Bewertung ersetzt mithin nicht die Konsultation des zuständigen betrieblichen oder behördlichen Datenschutzbeauftragten.“

Seitdem kommt es vor, dass Ethik-Kommissionen für die Beratung bzw. Bewertung von Studien bei der Einreichung eine datenschutzrechtliche Bewertung des zuständigen Datenschutzbeauftragten erhalten wollen. Da der Datenschutzbeauftragte zur Überprüfung der Einhaltung des Datenschutzrechts gesetzlich verpflichtet ist, liegt der Mehraufwand lediglich im Schreiben des Gutachtens für die Ethik-Kommission.

Beachtet werden sollte allerdings der Schreibaufwand für das Gutachten: Kurzfristig ist dies nicht immer zu gewährleisten, daher sollte an die möglichst frühzeitige Einbindung des Datenschutzbeauftragten in die klinische Studie gedacht werden und dabei auch zugleich auf das benötigte Gutachten hingewiesen werden.

[8] Der Arbeitskreis Medizinischer Ethik-Kommissionen in der Bundesrepublik Deutschland e.V. (2018) Wirksamwerden der DSGVO – Handreichung für Ethik-Kommissionen für die Beratung bzw. Bewertung von Studien (Stand 2018) [Online, zitiert am 2019-11-06]; Verfügbar unter https://www.ak-med-ethik-komm.de/docs/intern-2018/DSGVO_Empfehlungen.pdf

5 Erlaubnistatbestand zur Datenverarbeitung in klinischen Studien

Grundsätzlich benötigt jede Verarbeitung personenbezogener Daten einen Erlaubnistatbestand, dies gilt selbstverständlich auch für klinische Studien.

Forschung mit Daten von Patienten, die vom Forscher behandelt wurden, ist i.d.R. durch die jeweiligen landesrechtlichen Regelungen für Krankenhäuser bzw. durch die entsprechenden bundesrechtlichen Regelungen für niedergelassene Ärzte erlaubt, dies gilt in diesen Fällen natürlich auch für klinische Studien. In den meisten landesrechtlichen Regelungen findet sich jedoch keine Erlaubnis der beliebigen Zusammenführung von Daten aus unterschiedlichen Institutionen (siehe Abschnitt 5.3.2).

Außerhalb der Sekundärnutzung von Daten aus der Patientenversorgung finden sich keine gesetzlichen Erlaubnistatbestände außerhalb der Einwilligung, sodass für klinische Studien, insbesondere für prospektive klinische Studien, eine Einwilligung der betroffenen Probanden resp. Patienten erforderlich ist.

5.1 Einwilligung

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

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

Für eine wirksame Einwilligung müssen die Vorgaben der DS-GVO eingehalten werden. Näheres zur rechtskonformen Einwilligung findet sich z. B. in der Ausarbeitung „EU DS-GVO: Anforderungen an eine Einwilligung“ der GMDS[9].

5.2 Broad Consent

Auf Grund der zentralen Rolle, welche der Forschung in der Europäischen Union innewohnt[10], wird in ErwGr. 33 DS-GVO vorgeschlagen, dass es betroffenen Personen erlaubt sein sollte, „ihre Einwilligung für bestimmte Bereiche wissenschaftlicher Forschung zu geben, wenn dies unter Einhaltung der anerkannten ethischen Standards der wissenschaftlichen Forschung geschieht“.

Daher kann eine Einwilligung zur Nutzung personenbezogener Gesundheitsdaten wie auch genetischer Daten im Sinne von Art. 4 Ziff. 13 und 15 DS-GVO zu wissenschaftlicher Forschung, welche unter Einhaltung der anerkannten ethischen Standards der wissenschaftlichen Forschung durchgeführt wird, erfolgen, auch wenn der Zweck zum Zeitpunkt der Erhebung der personenbezogenen Daten nicht vollständig angegeben werden kann (sogenannte „breite Einwilligung“ („broad consent“[11]).

[9] GMDS (2016): EU DS-GVO: Anforderungen an eine Einwilligung. [Online, zitiert am 2019-09-17]; Verfügbar unter https://www.gesundheitsdatenschutz.org/ (Download als pdf-Datei)

[10] 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 […]“

[11] Zu „broad consent“ siehe auch Bundesministerium für Wirtschaft und Energie (BMWi): Orientierungshilfe zum Gesundheitsdatenschutz, Abschnitt 2.1.1 „Einwilligung, Broad Consent“ auf Seite 74. [Online, zitiert am 2019-09-17]; Verfügbar unter https://www.bmwi.de/Redaktion/DE/Downloads/M-O/orientierungshilfe-gesundheitsdatenschutz.pdf?__blob=publicationFile&v=16

Dabei muss, soweit es das konkrete Design des Forschungsvorhabens ermöglicht, die Verwendung der erhobenen Daten für die betroffene Person nachvollziehbar eingegrenzt werden. Dies kann insbesondere erreicht werden durch:

a. Verwendung einer für den Einwilligenden zugänglichen Nutzungsordnung oder eines einsehbaren Forschungsplanes, der die geplanten Arbeitsmethoden und die Fragen, die Gegenstand der Forschung sein sollen, beleuchtet sowie
b. Einrichten einer Internetpräsenz, durch die die Studienteilnehmer über laufende und künftige Studien informiert werden

Betroffenen Personen muss es entsprechend den Vorgaben von ErwGr. 33 DS-GVO hierbei möglich sein, ihre Einwilligung nur für bestimme Forschungsbereiche oder Teile von Forschungsprojekten in dem vom verfolgten Zweck zu erteilen.

Eine Verarbeitung auf Grundlage einer solcherart erteilten Einwilligung stellt erhöhte Anforderungen an die technischen und organisatorischen Maßnahmen, um Rechte und Freiheiten natürlicher Personen auch bei unvollständiger Angabe des Zweckes der Verarbeitung zu gewährleisten. Zu diesen die technischen und organisatorischen Maßnahmen zählen insbesondere[12]:

1. Die Verarbeitung der personenbezogenen Daten erfolgt im Inland, oder in einem anderen Mitgliedstaat der Europäischen Union. In einem Drittstaat oder in einer internationalen Organisation darf eine Verarbeitung dieser Daten nur erfolgen, wenn ein Angemessenheitsbeschluss gemäß Art. 45 DS-GVO vorliegt.
2. Es existieren gesonderte Zusagen zur Einhaltung der in Art. 5 DS-GVO genannten Grundsätze für die Verarbeitung personenbezogener Daten, insbesondere zu r Umsetzung der Anforderungen hinsichtlich Datenminimierung, Richtigkeit der Daten, der Speicherbegrenzung sowie der Gewährleistung von Integrität und Vertraulichkeit.
3. Es existieren Vorgaben zum Einsatz von Verschlüsselung, sowie zum Transport als auch zur Speicherung der Daten.
4. Die Daten sind zu anonymisieren, sobald dies nach dem Forschungszweck möglich ist, es sei denn, berechtigte Interessen der betroffenen Person stehen dem entgegen. Bis dahin sind die Merkmale, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person zugeordnet werden können, im Sinne von Art. 4 Ziffer 5 DS-GVO gesondert zu speichern.
5. In einem Berechtigungskonzept existieren spezifische Vorschriften für die Begrenzung des Zugriffs auf die erhobenen Daten sowie eine Beschreibung, wie die Durchsetzung der Zugriffsbeschränkungen gewährleistet wird.

5.3 Sekundärnutzung

Klinische Studien verlaufen häufig prospektiv, die Daten werden speziell für die Studie erhoben. Aber des Öfteren werden diese Daten mit bereits vorhandenen Daten „angereichert“. Häufig geschieht dies mit personenbezogenen Daten aus der Patientenversorgung. Auch bei retrospektiven Studien werden oftmals personenbezogenen Daten aus der Patientenversorgung genutzt. In all diesen Fällen spricht man von „Sekundärnutzung“ der Daten; der primäre Zweck der Datenverarbeitung war ja die Patientenversorgung.

[12] Beschluss der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zu Auslegung des Begriffs „bestimmte Bereiche wissenschaftlicher Forschung“ im Erwägungsgrund 33 der DS-GVO vom 3. April 2019. [Online, zitiert am 2019-09-17]; Verfügbar unter https://www.datenschutzkonferenz-online.de/media/dskb/20190405_auslegung_bestimmte_bereiche_wiss_forschung.pdf

Art. 5 Abs. 1 lit. b DS-GVO beinhaltet die Regelung, dass „eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke 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 können der „alte" und der „neue" Zweck miteinander vereinbar sein. Art. 5 Abs. 1 lit. b DS-GVO beinhaltet jedoch nicht, dass dies immer der Fall ist; vielmehr muss im Einzelfall nachgewiesen werden, dass der Forschungszweck vereinbar mit dem ursprünglichen Zweck (i.d.R. Patientenversorgung) ist[13]. Dieser Nachweis der Vereinbarkeit ist entsprechend den Vorgaben von Art. 6 Abs. 4 DS-GVO zu führen. Dazu muss der Forscher unter anderem folgende Kriterien berücksichtigen:

a) „Jede Verbindung zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung"
   Beispielsweise ist der Patient an Prostatakrebs erkrankt und die klinische Studie dient der Verbesserung dieser Behandlung, was man als starken Hinweis für einen kompatiblen Zweck ansehen könnte. Hingegen wäre eine Forschung bzgl. nächtlichen Harndrangs trotz des gemeinsamen urologischen Fachgebietes nicht so ein offensichtlicher Hinweis.
b) „Den Zusammenhang, in dem die personenbezogenen Daten erhoben wurden, insbesondere hinsichtlich des Verhältnisses zwischen den betroffenen Personen und dem Verantwortlichen"
   Werden die Daten zur Forschung von denselben Menschen genutzt, die auch in die Behandlung involviert waren, so besteht einerseits ein starkes Vertrauensverhältnis resultierend aus der Arzt-Patienten-Beziehung, zudem werden die Daten keinen weiteren Personen offenbart. Dies ist bei Nutzung der Daten durch Personen, die nicht an der Behandlung beteiligt waren, nicht der Fall.
c) „Die Art der personenbezogenen Daten, insbesondere ob besondere Kategorien personenbezogener Daten gemäß Artikel 9 verarbeitet"
   Gesundheits- und genetische Daten haben einen besonders hohen Schutzbedarf, daher muss die Kompatibilität zwischen den neuen (Forschungs-) Zweck und dem primären Zweck entsprechend deutlich ausgeprägt sein.
d) „Die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen"
   Hier sind insbesondere zu betrachten, welche Bedeutung eine weitergehende Offenbarung der aus der Erkrankung resultierenden Daten für den Patienten haben können, wie z.B. Stigmatisierung, Verlust von Ehepartner, Freunden oder auch den Job usw.
e) „Das Vorhandensein geeigneter Garantien, wozu Verschlüsselung oder Pseudonymisierung gehören kann"
   Je sensibler die Daten und je höher der Schutzbedarf der Daten, desto besser müssen die technisch-organisatorischen Maßnahmen zum Schutz dieser Daten sein.

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

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

ursprünglichen Erlaubnistatbestand legitimiert wurde, wird ggf. ein neuer Erlaubnistatbestand benötigt

5.3.1 Zweckkompatibel, aber trotzdem Zweckänderung

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

5.3.2 Landesspezifische Regelungen für Krankenhäuser

Die meisten Landesgesetze enthalten Regelungen zur Nutzung Daten von im Krankenhaus angefallenen Patientendaten zu Forschungszwecken. Im Nachfolgenden werden die wichtigsten Inhalte kurz dargestellt, jedoch muss man sich vor Beginn einer klinischen Studie jeweils den genauen und vollständigen Wortlaut ansehen, da insbesondere zur Weitergabe oder Nutzung an Dritte spezielle Regelungen existieren, desgleichen besondere Anforderungen an die technischen und organisatorischen Maßnahmen in einzelnen Landesgesetzen existieren.

- Baden-Württemberg: § 46 Abs. 1 Ziff. 2a LKHG
  Entsprechend § 46 Abs. 1 Ziff. 2a LKHG dürfen Patientendaten an Personen und Stellen außerhalb des Krankenhauses übermittelt werden, soweit dies zur Durchführung medizinischer Forschungsvorhaben des Krankenhauses erforderlich ist. D. h. es ist immer erforderlich, dass es sich um ein Forschungsvorhaben des Krankenhauses handelt.
- Bayern: Art. 27 Abs. 4 BayKrG
  Entsprechend Art. 27 Abs. 4 S. 1 BayKrG dürfen Krankenhausärzte Patientendaten nutzen, soweit dies zu Forschungszwecken im Krankenhaus oder im Forschungsinteresse des Krankenhauses erforderlich ist. Entsprechend Art. 27 Abs. 4 S. 2 2.HS BayKrG dürfen Krankenhausärzte zu Zwecken der Forschung auch anderen Personen die Nutzung von Patientendaten gestatten, wenn dies zur Durchführung des Forschungsvorhabens nach Satz1 erforderlich ist und die Patientendaten im Gewahrsam des Krankenhauses verbleiben.
  Auch in Bayern muss es sich immer um die Forschung eines im Krankenhaus ärztlichen Beschäftigten oder um das Forschungsinteresse des Krankenhauses handeln.
- Berlin: § 25 LKG
  Nach § 25 Abs. 1 LKG Berlin ist grundsätzlich eine Aufklärung der Patienten in das Forschungsvorhaben sowie die Erteilung einer Einwilligung erforderlich. § 25 Abs. 1 S.2 LKG Berlin kennt vier Ausnahmen von der Erfordernis der Erteilung einer Einwilligung:
  1. Ärztinnen und Ärzte verarbeiten Patientendaten für eigene wissenschaftliche Forschungsvorhaben und schutzwürdige Belange der Patientin oder des Patienten stehen der Verarbeitung nicht entgegenstehen; eine gewerbliche Nutzung der Daten muss ausgeschlossen sein.
  2. Es ist nicht zumutbar, die Einwilligung einzuholen und schutzwürdige Belange der Patientin oder des Patienten nicht beeinträchtigt werden.
  3. Das berechtigte Interesse der Allgemeinheit an der Durchführung des Forschungsvorhabens überwiegt das Geheimhaltungsinteresse der Patientin oder des Patienten erheblich.
  4. Im Rahmen der Krankenhausbehandlung erhobene und gespeicherte Patientendaten werden vor ihrer weiteren Verarbeitung zur Forschung anonymisiert.

- Brandenburg: § 31 BbgKHEG
  § 31 BbgKHEG verlangt, dass eine Offenlegung von Patientendaten an andere Stellen oder Personen für Forschungszwecke ohne Einwilligung der betroffenen Person nur erfolgen darf, wenn zuvor die Bestätigung der zuständigen Rechtsaufsichtsbehörde vorliegt.
  Weiterhin gilt entsprechend § 31 S. 3 BbgKHEG § 25 BbgDSG „unbeschränkt", d. h. für ein bestimmtes Forschungsvorhaben können Stellen wie ein Krankenhaus Patientendaten auch ohne Einwilligung verarbeiten, wenn schutzwürdige Belange der Patienten nicht beeinträchtigt werden oder das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Belange der Patienten überwiegt und der Zweck der Forschung nicht auf andere Weise erreicht werden kann.
- Bremen: § 7 BremKHDSG
  § 7 Abs. 1 BremKHDSG verlangt die Einwilligung des Patienten in die Nutzung seiner Daten zu Forschungszwecken, jedoch beinhaltet § 7 Abs. 2 BremKHDSG hiervon eine Ausnahme: Der Einwilligung bedarf es nicht, soweit schutzwürdige Belange der betroffenen Patienten nicht beeinträchtigt werden oder wenn das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Belange des Patienten oder der Patientin erheblich überwiegt und der Zweck der Forschung nicht auf andere Weise oder nur mit unverhältnismäßigem Aufwand erreicht werden.
- Hamburg: § 12 HmbKHG
  Entsprechend § 12 Abs. 1 HmbKHG darf ein Krankenhaus oder eine Krankenhausgruppe die eigenen Patientendaten ohne Einwilligung für eigene wissenschaftliche Forschung verarbeiten.
  Darüber hinaus darf ein Krankenhaus besondere Kategorien personenbezogener Daten ohne Einwilligung für Forschungszwecke verarbeiten, wenn die Verarbeitung zu diesem Zweck erforderlich ist und das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schützenswerten Interessen der betroffenen Person überwiegt. D.h. grundsätzlich dürfen zu den eigenen Patientendaten noch weitergehenden Daten zu Forschungszwecken verarbeitet werden.
- Hessen: § 12 Abs. 3 HKHG 2011 i.V.m. § 24 HDSIG
  Gemäß § 12 Abs. 3 HKHG 2011 gilt § 24 HDSIG für Krankenhäusern. § 24 Abs. 1 HDSIG gestattet die Verarbeitung von Patientendaten für Forschungszwecke ohne Einwilligung, wenn die Verarbeitung zu diesen Zwecken erforderlich ist und die Interessen des Verantwortlichen an der Verarbeitung die Interessen der betroffenen Person an einem Ausschluss der Verarbeitung überwiegen.
- Mecklenburg-Vorpommern: § 37 LKHG M-V
  Entsprechend § 37 Abs. 1 LKHG M-V ist für die Nutzung von Patientendaten zu Forschungszwecken grundsätzlich eine Einwilligung der Patienten erforderlich, ausgenommen
  1. schutzwürdige Belange der Patientinnen und Patienten wegen der Art der Daten, ihrer Offenkundigkeit oder der Art ihrer Nutzung werden nicht beeinträchtigt oder
  2. das für die Aufsicht für das Krankenhaus zuständige Ministerium stellte fest, dass das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Belange der Patientinnen und Patienten erheblich überwiegt und der Zweck des Forschungsvorhabens auf andere Weise, insbesondere mit anonymisierten Daten, nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

- Nordrhein-Westfalen: § 6 GDSG NW
  Grundsätzlich ist eine Einwilligung zur Nutzung von Patientendaten zu Forschungszwecken erforderlich. Entsprechend § 6 Abs. 2 GDSG NW darf wissenschaftliches Personal Patientendaten, auf die es im Rahmen seiner Versorgungstätigkeit nach § 2 Abs. 1 GDSG NW ohnehin Zugriff hat, zu Forschungszwecken auch ohne Einwilligung der jeweiligen Patienten nutzen.
  Der Einwilligung des Patienten bedarf es ferner nicht, wenn
  1. der Zweck eines Forschungsvorhabens nicht auf andere Weise erreicht werden kann,
  2. das berechtigte Interesse der Allgemeinheit an der Durchführung des Forschungsvorhabens das Geheimhaltungsinteresse des Patienten erheblich überwiegt und
  3. es entweder nicht möglich ist oder dem Patienten aufgrund seines derzeitigen Gesundheitszustandes nicht zugemutet werden kann, ihn um seine Einwilligung zu bitten.
- Rheinland-Pfalz: § 37 LKG
  Entsprechend § 37 Abs. 1 S. 2 LKG bedarf es zur Nutzung von Patientendaten keiner Einwilligung durch die Patienten, wenn
  1. es nicht zumutbar ist, die Einwilligung einzuholen und schutzwürdige Belange der Patientin oder des Patienten nicht beeinträchtigt werden,
  2. das berechtigte Interesse der Allgemeinheit an der Durchführung des Forschungsvorhabens das Geheimhaltungsinteresse der Patientin oder des Patienten erheblich überwiegt oder
  3. im Rahmen der Krankenhausbehandlung erhobene und gespeicherte Patientendaten vor ihrer weiteren Verarbeitung anonymisiert werden.

  Ansonsten ist die Nutzung von Patientendaten nur mit Einwilligung der jeweiligen Patienten statthaft.
- Saarland: § 14 SKHG
  Entsprechend § 14 Abs. 1 SKHG dürfen Krankenhausärztinnen und Krankenhausärzte die innerhalb ihrer Fachabteilung zu Behandlungszwecken aufgezeichneten Patientendaten für eigene medizinische wissenschaftliche Forschung nutzen, wenn der Zweck der Forschung auf andere Weise nicht erreicht werden kann und
  1. die Patientin oder der Patient nach Unterrichtung über Art, Umfang und Zweck des Forschungsvorhabens nicht widersprochen hat oder
  2. schutzwürdige Belange nicht beeinträchtigt werden und nachträglich die Möglichkeit zum Widerspruch nicht oder nur mit unverhältnismäßigem Aufwand eingeräumt werden kann.
- Sachsen: § 34 SächsKHG
  Entsprechend § 34 Abs. 1 SächsKHG dürfen Ärzte Patientendaten, die innerhalb ihrer Fachabteilung oder bei Hochschulen innerhalb ihrer medizinischen Einrichtungen, in den Universitätsklinika oder in sonstigen medizinischen Einrichtungen gespeichert sind, für eigene wissenschaftliche Forschungsvorhaben verarbeiten,
  Ansonsten ist eine Nutzung von Patientendaten nur mit Einwilligung zulässig. Gemäß § 34 Abs. 3 SächsKHG bedarf es keiner Einwilligung, wenn der Zweck eines bestimmten Forschungsvorhabens nicht auf andere Weise erfüllt werden kann und

1. das berechtigte Interesse der Allgemeinheit an der Durchführung des Forschungsvorhabens das Geheimhaltungsinteresse des Patienten erheblich überwiegt oder
2. es nicht zumutbar ist, die Einwilligung einzuholen und schutzwürdige Belange des Patienten nicht beeinträchtigt werden.

- Sachsen-Anhalt: § 17 KHG LSA
  Eine Verarbeitung von Patientendaten zu Forschungszwecken ist nach § 17 Abs. 1 KHG LSA mit Einwilligung zulässig. § 17 Abs. 1 S. 2 KHG LSA erlaubt eine Verarbeitung ohne Einwilligung, wenn
  1. im Rahmen der Krankenhausbehandlung erhobene und gespeicherte Patientendaten vor ihrer weiteren Verarbeitung anonymisiert werden,
  2. die Einholung der Einwilligung des Patienten unzumutbar ist, der Forschungszweck auf andere Weise nicht erreicht werden kann und schutzwürdige Interessen des Patienten nicht betroffen sind oder
  3. das berechtigte Interesse der Allgemeinheit an der Durchführung des Forschungsvorhabens das Geheimhaltungsinteresse des Patienten erheblich überwiegt.
- Thüringen: § 27 Abs. 4 ThürKHG, § 27a ThürKHG
  Krankenhausärzte dürfen Patientendaten zu Forschungszwecken im Krankenhaus oder im Forschungsinteresse des Krankenhauses verarbeiten, wenn die Verarbeitung dieser Daten zur Erreichung des Forschungszweckes erforderlich ist.

Außer Niedersachsen und Schleswig- Holstein [14] existieren somit in jedem Land spezialgesetzliche Regelungen zur Nutzung von Patientendaten zu Forschungszwecken. I.d.R. legitimieren die Regelungen aber nur „Eigenforschung“, d.h. man darf nur die Daten von Patienten, an deren Behandlung die Institution beteiligt war, zu Forschungszwecken der eigenen Institution nutzen, aber nicht weitergeben zu Forschungszwecken anderer. Was als „Institution“ anzusehen ist, unterscheidet sich dabei von Bundesland zu Bundesland: in einem Bundesland ist darunter das Krankenhaus zu verstehen, im anderen Bundesland hingegen nur die jeweilige versorgende Fachabteilung des Krankenhauses. Somit müssen die Regelungen im jeweiligen Bundesland bzgl. der Nutzung von Patientendaten für klinische Studien geprüft werden.

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

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

6 Rechte der betroffenen Patienten

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

- Informationspflicht bei Erhebung bzw. Zweckänderung von personenbezogenen Daten, unterschieden nach:
  - Erhebung bei der betroffenen Person
  - Erhebung nicht bei der betroffenen Person („Dritterhebung“)
- Projekt- bzw. Studienbezogene Informationen:
  - Inhalt und Zweck der Studie
  - Betroffener Personenkreis
  - Beteiligte, Verantwortlicher im Sinne der Datenschutzgesetze
  - Erhobene Daten und Proben sowie deren Erforderlichkeit
  - Analyseergebnisse der Proben
  - Rechtsgrundlage, Einwilligungserklärung, Patienteninformation
  - Datenflüsse, Speicherorte
  - Lagerung und Weitergabe von Proben
  - Verfahren zur Pseudonymisierung und Anonymisierung inklusive Risikoabschätzung
  - Datenlöschung, Vernichtung von Proben, Nutzung von Daten und Proben noch Studienende
  - Workflow, Beschreibung typischer Abläufe
  - Qualitätssicherung, Monitoring
  - Technische Ausgestaltung
  - Technisch-organisatorische Sicherheitsmaßnahmen noch §64 Abs. 3BDSG
  - Beurteilung des eigenen Datenschutzbeauftragten
  - Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO
- 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.

Hinweis: Oftmals werden die Verantwortlichen bei klinischen Studien nur pseudonymisierte Daten erhalten. Auch hier gelten die Vorgaben der DS-GVO hinsichtlich der Betroffenenrechte, nur hat der Verantwortliche keinen Kontakt zu den betroffenen Personen. Hier empfiehlt sich, dass die Ärztinnen und Ärzte in den versorgenden Einrichtungen, in welchen die für die Studien benötigten klinischen Daten erhoben bzw. zur Studie zur Verfügung gestellt werden, als ausführende Organe des bzw. der Verantwortlichen agieren, d.h., einerseits die Informationspflichten erfüllen, aber auch als Ansprechpartner der Patienten bzgl. der Wahrnehmung der Betroffenenrechte wie bspw. Auskunftsrecht oder Berichtigung der Daten fungiert.

6.1 Informationspflichten

Bei Aufnahme in eine klinische Studie muss den aus Artt. 13 und 14 DS-GVO resultierenden Informationspflichten genügt werden.
Idealerweise erhält jeder Proband resp. Patient bei Aufnahme in die Studie eine Informationsbroschüre, in welcher die notwendigen Angaben entsprechend Art. 13 resp. Art. 14 DS-GVO enthalten sind. In dieser Broschüre sollte sich dann auch ein Link auf die Internetseite der Studie befindet, in welcher die Angaben zu den Auftragsverarbeiter gelistet sind:

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

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

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

6.2 Auskunftsrecht

Jeder Proband bzw. Patient hat das Recht auf Auskunft bzgl. der in der klinischen Studie verarbeiteten bzw. gespeicherten Daten. Dies sollte ihm im Rahmen der im Abschnitt 6.1 genannten Information mitgeteilt werden. Idealerweise wird in dieser Information weiterhin eine Telefonnummer als auch eine spezielle nicht-personalisierte E-Mailadresse, die somit auch bei einem Wechsel des zuständigen Sachbearbeiters erhalten bleibt, genannt.

Nach Art. 15 Abs. 3 DS-GVO muss der Verantwortliche betroffenen Personen auch eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung stellen. Dementsprechend sollte es im Rahmen klinischer Studien möglich sein, dass alle zu einem Probanden resp. Patienten gehörenden Daten in eine pdf-Datei exportiert werden können, welche der anfragenden betroffenen Person übergeben werden kann.

6.3 Recht auf Korrektur

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

Allerdings hat nach Art. 16 DS-GVO jeder Proband resp. Patient auch das Recht unvollständige Daten vervollständigt werden, ggf. auch mittels einer ergänzenden Erklärung. Hier kann es zu unterschiedlichen Interpretationen seitens datenverarbeitender Stelle und betroffener Person kommen, was „unvollständig“ bedeutet. Der europäische Gesetzgeber verlangt daher, dass dieses Recht „unter Berücksichtigung der Zwecke der Verarbeitung“ zu erfolgen hat. D.h. die Beurteilung

bzgl. Unvollständigkeit muss aus Sicht des Verarbeitungszweckes erfolgen. Entsprechend dem aus Art. 5 Abs. 1 lit. c DS-GVO resultierendem Gebot der Datenminimierung dürfen hier also nur für den Verarbeitungszweck erforderliche Daten ergänzt werden. Das diese Daten ergänzt werden, liegt aber wiederum im Interesse der datenverarbeitenden Stelle und wird daher jederzeit möglich sein.

Jeder Proband resp. Patient muss darauf hingewiesen werden, dass für ihn diese Rechte bestehen. Dies erfolgt idealerweise in dem in Abschnitt 6.1 erwähntem Informationsschreiben.

6.4 Recht auf Einschränkung der Verarbeitung („Sperrung“)

Gemäß Art. 18 DS-GVO hat jeder Proband resp. Patient das Recht, unter den Voraussetzungen von Art. 18 Abs. 1 DS-GVO von dem Verantwortlichen die Einschränkung der Verarbeitung (= „Sperrung“) zu verlangen. Durch die in Abschnitt 6.1 beschriebene Informationsbroschüre sollte jeder Proband resp. Patient darauf hingewiesen werden, dass er ein Recht auf die Einschränkung der Verarbeitung seiner Daten hat. Zugleich sollte er darauf hingewiesen werden, dass dieses Recht ggf. durch gesetzliche Bestimmungen eingeschränkt wird.

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

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

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

6.5 Recht auf Löschung

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

Durch die in Abschnitt 6.1 beschriebene Informationsbroschüre sollte jeder Patient darauf hingewiesen werden, dass er ein Recht auf Löschung seiner Daten hat. Zugleich sollte er darauf hingewiesen werden, dass dieses Recht ggf. durch gesetzliche Bestimmungen wie z. B. durch die Vorgabe gesetzlicher Aufbewahrungsfristen eingeschränkt wird.

6.6 Widerspruchsrecht

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

Jeder Proband resp. Patient sollte daher in dem in Abschnitt 6.1 erwähnten Informationsschreiben auf sein Recht zum Widerspruch gegen eine Datenverarbeitung hingewiesen werden. Dabei ist zu berücksichtigen, dass der Proband bzw. Patient auch darauf hingewiesen wird, dass ein Widerspruchsrecht ggf. durch gesetzliche Regelungen eingeschränkt wird, z. B. eine Speicherung aufgrund gesetzlicher Bestimmungen trotz seines Widerspruchs erfolgen muss.

6.7 Recht auf Datenübertragbarkeit

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

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

sowie

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

Jeder Patient sollte in der in Abschnitt 6.1 genannten Informationsbroschüre auf diese Rechte hingewiesen werden. Es sollte dabei aber auch darauf hingewiesen werden, dass kein Empfänger dieser Daten gesetzlich dazu verpflichtet ist, diese Daten überhaupt oder auch in dem vom Verantwortlichen bereitgestellten Format anzunehmen.

7 Datenverarbeitung

7.1 Datenqualität

Art. 5 Abs. 1 lit. d DS-GVO verlangt, dass Daten „sachlich richtig und erforderlichenfalls auf dem neuesten Stand“ sind: „es sind alle *angemessenen* Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden.“

Die „Leitlinie zur Guten Klinischen Praxis“ (GCP, Good Clinical Practice[15]) fordert unter 2.13, dass Systeme mit Maßnahmen eingeführt werden, welche die Qualität jedes Aspektes der klinischen Prüfung gewährleisten. Dokumente müssen die Bewertung der Durchführung einer klinischen Prüfung sowie der Qualität der erhobenen Daten zulassen (Begriffsbestimmung 1.23 „Essential Documents“). Diesen essentiellen Dokumenten ist das gesamte Kapitel 8 der GCP gewidmet, denn anhand dieser Unterlagen lässt sich sowohl die Einhaltung der GCP als auch von allen geltenden gesetzlichen Bestimmungen belegen.

In klinischen Studien müssen daher grundsätzlich nachvollziehbare Mechanismen existieren, welche die Qualität der Daten gewährleisten. Art. 32 DS-GVO fordert weiterhin, dass

- die Verfügbarkeit der Daten sowie der Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden sowie
- eine Ausfallsicherheit („Belastbarkeit“ existiert.

7.2 Sicherheit der Verarbeitung

7.2.1 Privacy by Design/Default

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

7.2.1.1 Privacy by Design: 7 grundlegende Prinzipien

Privacy by Design wird i.d.R. mit der Umsetzung der „7 grundlegenden Prinzipien“, aufgestellt von Ann Cavoukian[17,18], gleichgesetzt:

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

[15] ICH GCP: Leitlinie Zur Guten Klinischen Praxis. [Online, zitiert am 2019-10-01]; Verfügbar unter https://ichgcp.net/de/

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

[17] Ann Cavoukian: Privacy by Design - The 7 Foundational Principles. [Online, zitiert am 2017-12-07]; Verfügbar unter https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf

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

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

7.2.1.2 Umsetzung von Privacy by Design

Die kanadische Datenschutzbeauftragte Ann Cavoukian, die „Privacy by Design“ ins Leben rief, empfahl 2011 Unternehmen[19]:

1) Ein Unternehmen muss einen Privacy by Design Leiter und/oder ein Team einrichten, indem es die geeigneten Personen identifiziert.
2) Proaktive Prozesse und Praktiken zum Datenschutz durch Design einführen, umsetzen und einhalten:
    a) Anwendung auf das Design und die Architektur von Infrastruktur, IT-Systemen und Geschäftspraktiken, die mit personenbezogenen Daten interagieren oder deren Verwendung beinhalten;
    b) Beschreiben Sie jeden der Kernzwecke und Hauptfunktionen, die von diesen Infrastrukturen, Systemen und Praktiken erfüllt werden, einschließlich, aber nicht beschränkt, auf die Gewährleistung der Sicherheit und den Schutz der Privatsphäre bei personenbezogenen Daten;
    c) Datenminimierung einbeziehen und den höchstmöglichen Grad an Datenschutz für personenbezogene Daten bieten, während dies gleichzeitig den anderen Kernzwecken dienen und die anderen Hauptfunktionen erfüllen;
    d) Bereitstellung dieses Grades an Datenschutz durch den Einsatz der maximal möglichen Mittel, die erforderlich sind, um die Sicherheit, Vertraulichkeit und Integrität personenbezogener Daten während des gesamten Lebenszyklus der Daten zu gewährleisten, von der ursprünglichen Erhebung über die Verwendung, Speicherung, Verbreitung bis zur sicheren Vernichtung am Ende des Lebenszyklus;
    e) Wann immer dies angemessen ist, sehen Sie diesen Datenschutz automatisch vor, sodass keine Maßnahmen für einzelne Benutzer oder Kunden erforderlich sind, um die Privatsphäre ihrer personenbezogenen Daten zu schützen;
    f) Sicherstellen, dass Infrastruktur, IT-Systeme und Geschäftspraktiken, die mit personenbezogenen Daten interagieren oder deren Verwendung beinhalten, angemessen transparent bleiben und einer unabhängigen Überprüfung durch alle relevanten Interessengruppen, einschließlich Kunden, Nutzer und Kunden sowie Partnerorganisationen, unterliegen; und
    g) Förderung der Gestaltung und Aufrechterhaltung benutzerzentrierter Systeme und Praktiken, einschließlich starker Datenschutzvorgaben, angemessener Datenschutzhinweise und andere benutzerfreundliche Funktionen.

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

    (1) Angemessene Schulungen zum Thema Datenschutz und Sicherheit für seine Mitarbeiter durchführen;
    (2) Ein System zur Überwachung aller Projekte, die regelmäßig personenbezogene Daten verarbeiten, einführen;

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

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

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

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

- Richtlinien/Policy zum Datenschutz festlegen, also etwas in der Richtung
    - Das Unternehmen sollte den Datenschutz im gesamten Unternehmen und in jeder Phase der Entwicklung seiner Produkte und Dienstleistungen fördern.
    - Der Schutz der Privatsphäre sollte zu Beginn des Planungsprozesses in die Geschäftspraktiken einbezogen werden.
    - Umfassende Datenschutzmanagementverfahren sollten während des gesamten Lebenszyklus von Produkten und Dienstleistungen aufrechterhalten werden.
- Verantwortlichkeiten definieren, z.B.
    - Datenverarbeitung Büro
    - -Geschäftsprozessverantwortliche
    - -Produktentwickler
    - -Technische Lösungsentwickler / Manager
    - -Datenschutzbeauftragter
    - -…
- Weiterbildung für die an der Verarbeitung beteiligten Personen anbieten/ermöglichen
    - Integration mit Datenschutzschulungen und Sensibilisierungsprogrammen
    - Rollen- und aufgabenspezifische Inhalte für alle Beteiligten
    - Interdisziplinäres Publikum beachten: Geschäftsprozessverantwortliche, Softwareentwickler, Projektmanager, Vertriebsmitarbeiter...
- Verantwortlichkeiten definieren, z.B.
    - Datenverarbeitung Büro
    - Geschäftsprozessverantwortliche
    - Produktentwickler
    - Technische Lösungsentwickler / Manager
    - Datenschutzbeauftragter
    - …
- Rahmenwerk für ein Datenschutzmanagement implementieren, welches u.a. beinhaltet
    - Verwaltungsstruktur festlegen und im Verarbeitungszeitraum beibehalten
    - Bestandsaufnahme, welche personenbezogener Daten verarbeitet werden und welche Datenübertragungsmechanismen erfolgen, durchführen und den bestand pflegen
    - Interne Datenschutzrichtlinien einhalten und die Einhaltung entsprechend festgelegten Vorgaben prüfen
    - Durchführung von Schulungen und Sensibilisierungsprogrammen bei den an der Verarbeitung beteiligten Personen
    - Management von Informationssicherheitsrisiken
    - Drittrisiko-Management
    - Umgang mit Hinweisen/Meldungen festlegen (z.B., Whistleblower)
    - Umgang und Reaktion von Anfragen und Beschwerden von Personen festlegen und die Einhaltung überprüfen
    - Monitoring für neue betriebliche Praktiken festlegen und die Umsetzung prüfen

    - Verfahren zur Verwaltung von Datenschutzverletzungen festlegen und die Einhaltung prüfen
    - Monitoring der Datenverarbeitung
    - Externe Kriterien (z.B. Gesetzesänderungen) verfolgen
- Überprüfungen bzgl. Umsetzung Policy, Wahrnehmung Verantwortlichkeiten, Weiterbildung usw. durchführen
- Und natürlich: Dokumentation.

Speziell für den Einsatz von Oracle®-Datenbanken wurde 2013 eine Empfehlung für den Umgang mit Privacy by Design veröffentlicht[20]; da diese Datenbank im Gesundheitswesen oft eingesetzt wird, ist diese Empfehlung vermutlich auch von Interesse. Und grundsätzlich sind die Empfehlungen auf den Einsatz von anderen Enterprise-Strukturen sehr gut übertragbar.

7.2.1.3 PbD: der Europäischen Agentur für Netz-und Informationssicherheit (ENISA)

Es gibt Empfehlungen der Europäischen Agentur für Netz-und Informationssicherheit (ENISA) zum Thema[21]:

- Vier eher technische Empfehlungen
    - Datenminimierung (Minimizern): Beschränken Sie die Verarbeitung personenbezogener Daten so weit wie möglich.
    - Datentrennung (Separate): Die Verarbeitung personenbezogener Daten so weit wie möglich zu trennen.
    - Pseudonymisierung (Abstract): Beschränken Sie so weit wie möglich die Details, in denen personenbezogene Daten verarbeitet werden.
    - Verbergen (Hide): Personenbezogene Daten schützen oder nicht verlinkbar oder nicht beobachtbar machen. Stellen Sie sicher, dass es nicht öffentlich oder bekannt wird.
- Vier eher organisatorische Anforderungen
    - Informieren (Inform): die betroffenen Personen rechtzeitig und angemessen über die Verarbeitung ihrer personenbezogenen Daten zu informieren.
    - Kontrolle (Control): Den betroffenen Personen eine angemessene Kontrolle über die Verarbeitung ihrer personenbezogenen Daten zu geben.
    - Durchsetzen (Enforce): Sich verpflichten, personenbezogene Daten datenschutzgerecht zu verarbeiten und dies angemessen durchzusetzen.
    - Demonstrieren (Demonstrate): Zeigen Sie, dass Sie personenbezogene Daten datenschutzgerecht verarbeiten.

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

7.2.2 Datenschutzfolgenabschätzung

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

Dabei beschreibt Art. 35 DS-GVO verschiedene Fälle, in denen eine DSFA erfolgen muss. Weiterhin *dürfen* nationale Datenschutz-Aufsichtsbehörden Listen veröffentlichen, wann eine DSFA nicht

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

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

erforderlich ist (sog. „Whitelist“), und sie *müssen* Listen veröffentlichen, wann eine DSFA erforderlich ist. Alle Listen müssen, sofern die Verarbeitungstätigkeiten umfasst, welche mit dem Angebot von Waren oder Dienstleistungen in mehreren Mitgliedstaaten im Zusammenhang stehen, dem Kohärenzverfahren nach Art. 63 DS-GVO unterworfen werden, d.h. dem europäischen Datenschutz-Ausschuss vorgelegt werden. Die Entscheidung zur deutschen Liste findet sich auf der EDSA-Homepage[22], die Liste selbst ist auf der Homepage der Datenschutzkonferenz verfügbar[23].

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

Die Verbände bvitg, DKG und GMDS veröffentlichten eine Praxishilfe[24], in welcher der Umfang wie auch die Durchführung einer DSFA ausführlich beschrieben wird. Daher finden sich hier nur Hinweise, die speziell für klinische Studien zu beachten sind.

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

1) Verarbeitung von biometrischen Daten (siehe Art. 4 Ziff. 14 DS-GVO), wenn zugleich mindestens eines der nachfolgenden Kriterien erfüllt wird:
   - Daten zu schutzbedürftigen Betroffenen wie Patienten,
   - Innovative Nutzung oder Anwendung neuer technologischer organisatorischer Lösungen wie z.B. im Bereich der medizinischen Forschung,
   - Bewerten oder Einstufen (Scoring) wie beispielsweise, wer für eine Studie geeignet ist oder wer in welche Studiengruppe gruppiert wird,
   - Abgleichen oder Zusammenführen von Datensätzen wie z.B. Zusammenführen von Datensätzen aus mehreren Forschungszentren,
   - Betroffene werden an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags gehindert, wie beispielsweise dem Recht auf Löschung, da die Daten aus Forschungsinteresse vorerst nicht gelöscht werden sollten.

   Auch wenn daktyloskopische Daten ebenso wie Gesichtsbilder im Bereich der klinischen Studien eher selten zur Absicherung der Verarbeitung (z.B. zur Zugangsbeschränkung zu Serverräumlichkeiten genutzt werden, so definiert Art. 4 Ziff. 14 DS-GVO biometrische Daten dahingehend, dass entsprechende Daten eine Identifizierung *ermöglichen* können. Je nachdem, welche Daten in klinischen Studien verwendet werden, muss daher hier eine Prüfung erfolgen.
2) Verarbeitung von genetischen Daten, wenn zugleich mindestens eines der in Nr. 1 genannten Kriterien erfüllt wird. Da in klinischen Studien genetische Daten i.d.R. von Patienten stammen

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

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

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

und häufig auch noch von verschiedenen Institutionen zusammengeführt werden, wird bei der Verarbeitung genetischer Daten regelhaft von der Notwendigkeit einer DSFA auszugehen sein.

10) Zusammenführung von personenbezogenen Daten aus verschiedenen Quellen und der Verarbeitung der so zusammengeführten Daten, sofern
    - die Zusammenführung oder Verarbeitung in großem Umfang vorgenommen werden,
    - für Zwecke erfolgen, für welche nicht alle der zu verarbeitenden Daten direkt bei den betroffenen Personen erhoben wurden,
    - die Anwendung von Algorithmen einschließen, die für die betroffenen Personen nicht nachvollziehbar sind, und
    - der Entdeckung vorher unbekannter Zusammenhänge zwischen den Daten für nicht im Vorhinein bestimmte Zwecke dienen

    Dies kann beispielsweise zutreffen, wenn eine KI-Anwendung erprobt wird und hierzu im Rahmen der Sekundärnutzung Daten von Patienten aus verschiedenen Versorgungseinrichtungen genutzt werden.
11) Einsatz von künstlicher Intelligenz zur Verarbeitung personenbezogener Daten zur Steuerung der Interaktion mit den Betroffenen oder zur Bewertung persönlicher Aspekte der betroffenen Person.
    Dies kann beispielsweise zutreffen, wenn eine KI-Anwendung zur medizinischen Diagnostik erprobt wird, denn letztlich ist eine Diagnose eine Bewertung von persönlichen Aspekten einer betroffenen Person.
15) Anonymisierung von besonderen personenbezogenen Daten nach Artikel 9 DS-GVO nicht nur in Einzelfällen (in Bezug auf die Zahl der betroffenen Personen und die Angaben je betroffener Person) zum Zweck der Übermittlung an Dritte.
    Letztlich führt dies dazu, dass bei der Anonymisierung von aus der Versorgung stammenden Patientendaten zu Forschungszwecken regelhaft eine DSFA erforderlich ist.
16) Verarbeitung von personenbezogenen Daten gemäß Art. 9 Abs. 1 und Art. 10 DS-GVO – auch wenn sie nicht als „umfangreich“ im Sinne des Art 35 Abs. 3 lit. b) anzusehen ist - sofern eine nicht einmalige Datenerhebung mittels der innovativen Nutzung von Sensoren oder mobilen Anwendungen stattfindet und diese Daten von einer zentralen Stelle empfangen und aufbereitet werden.
    Klinische Studien, welche mit einem Telemonitoring arbeiten, fallen beispielsweise regelhaft unter diese Regelung.

7.2.3 IT-Sicherheit

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

Art. 32 DS-GVO schreibt vor, dass unter Berücksichtigung
- des Stands der Technik,
- der Implementierungskosten,
- der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie

- der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die persönlichen Rechte und Freiheiten

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

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

- Vertraulichkeit,
- Integrität,
- Verfügbarkeit und
- Belastbarkeit

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

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

Eine ausführliche Darstellung der Thematik findet sich in der Praxishilfe[25] von bvitg und GMDS.

7.3 Archivierung / Speicherdauer

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

Für während der Forschung anfallende Daten gelten je nach rechtlicher Grundlage der Forschung die entsprechenden gesetzlichen Aufbewahrungszeiträume. Einige werden im Folgenden kurz vorgestellt.

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

7.3.1 Arzneimittelstudien[26]

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[27], 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-Zertifikat.
- 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.

[26] Dieser Text entstammt Kapitel 9.2.1 „Gesetzliche Aufbewahrungspflichten“ der Praxishilfe „Datenschutzrechtliche Anforderungen an die medizinische Forschung unter Berücksichtigung der EU Datenschutz-Grundverordnung (DS-GVO“ von GDD und GMDS. [Online, zitiert am 2019-10-01]; Verfügbar unter https://ds-gvo.gesundheitsdatenschutz.org/html/forschung.php

[27] Richtlinie 2001/83/EG des Europäischen Parlaments und des Rates vom 6. November 2001 zur Schaffung eines Gemeinschaftskodexes für Humanarzneimittel. [Online, zitiert am 2019-11-17]; Verfügbar unter http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=uriserv:OJ.L_.2001.311.01.0067.01.DEU

8 Verzeichnis der Verarbeitungstätigkeiten

Das „Verzeichnis der Verarbeitungstätigkeiten“, nachfolgend Verzeichnis genannt, hat die nach Bundesdatenschutzgesetzt (BDSG) bzw. länderspezifische Datenschutzgesetzen bekannte Dokumentation „Verfahrensverzeichnis“ abgelöst. Jedoch umfasst ein Verzeichnis jede einzelne Verarbeitungstätigkeit eines Verantwortlichen, dass frühere Verfahrensverzeichnis jedoch nur meldepflichtige automatisierte Verarbeitungen.

Zum Thema „Verzeichnis der Verarbeitungstätigkeiten“ wird bzgl. der Interpretation der Regelungen auf die Praxishilfe der GMDS[28] verwiesen. Nachfolgend werden grundlegende Anforderungen an ein Verzeichnis durch die DS-GVO dargestellt, eventuelle Vorgaben durch Spezialgesetze werden nicht betrachtet.

8.1 Allgemein

Verantwortliche, Auftragsverarbeiter sowie deren Vertreter werden nach Artikel 30 DS-GVO verpflichtet ein Verzeichnis zu führen, soweit die Verarbeitung ihrer Verantwortung unterliegt.

Entsprechend Erwägungsgrund 82 dient ein Verzeichnis zum Nachweis der Einhaltung der DS-GVO. Ein Verzeichnis stellt somit eine besondere Form der Zusammenstellung vorhandener Informationen dar und bildet eine prozessorientierte Übersicht der Verarbeitung personenbezogener Daten.

Die DS-GVO beschreibt in ihrem Art. 30 Abs. 5 verschiedene Kriterien, wann ein Verzeichnis zu führen ist und definiert ebenso konkrete Ausnahmen von dieser Verpflichtung. Spezielle Regelungen bzgl. eines Verzeichnisses zur Datenverarbeitung für Studien- oder Forschungszwecke werden in der DS-GVO nicht getroffen. Die Verarbeitung von Daten, die einer „besondere Kategorie“ gem. Art 9 Abs. 1 DS-GVO angehören, verpflichten zwingend zur Führung eines Verzeichnis. Gesundheitsdaten wie auch genetische Daten gehören u.a. zu dieser besonderen Kategorie. Im Rahmen der „Klinischen Studien“ wird die Verarbeitung von Gesundheitsdaten einen Regelfall darstellen. Für Forschungen im Gesundheitsreich besteht bei der Verarbeitung von personenbezogenen Daten eine dokumentationspflichtige Verarbeitungstätigkeit und ist damit in das Verzeichnis des Verantwortlichen aufzunehmen.

8.2 Zweck eines Verzeichnis der Verarbeitungstätigkeiten

Der Zweck zur Anlage und Führung eines Verzeichnisses, besteht grundsätzlich in der Umsetzung der Verpflichtung nach Art. 30.

Für den Verantwortlichen bietet dieser Überblick aller Verarbeitungsvorgänge aber auch weitere Möglichkeiten. U.a. kann der Nachweis zur Erfüllung diverser Rechte und Pflichten auf Grundlage des Verzeichnisses geführt werden. Dies bezieht sich auch auf die Verarbeitungstätigkeiten innerhalb Forschung und Studien.

Ein Verzeichnis kann z.B. als ein Baustein für folgende weitere Zwecke genutzt werden:

- Nachweis der Rechtmäßigkeit der Verarbeitung gem. Art. 5 Abs. 1 lit. a DS-GVO
- Erfüllung der Rechenschafts- und Dokumentationspflicht gem. Art. 5 Abs. 2 DS-GVO, Art. 24 DS-GVO

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

- Nachweis bzgl. der Erfüllung der Rechte betroffener Personen gem. Art. 12 Abs. 1 DS-GVO (Transparenz, Auskunftsrecht, Recht auf Datenübertragbarkeit, Recht auf Löschung, Informationspflicht)
- Risikobewertung, Darstellung geeigneter technischer und organisatorische Maßnahmen gem. Art. 24 Abs. 1 sowie Art. 32 DS-GVO
- Dokumentation einer erfolgten Prüfung bzgl. der Notwendigkeit der Durchführung einer Datenschutzfolgenabschätzung nach Art. 35 DS-GVO.

Nach Art. 30 Abs. 4 DS-GVO stellen Verantwortliche, Auftragsverarbeiter sowie ggfs. deren Vertreter, der Aufsichtsbehörde auf Anfrage das Verzeichnis zur Verfügung. Die Zusammenarbeit mit der Aufsichtsbehörde gem. Art. 31 DS-GVO wird durch das Führen eines Verzeichnisses ebenfalls unterstützt.

8.3 Merkmale Verarbeitungstätigkeit

Für jede einzelne Verarbeitungstätigkeit ist eine Beschreibung gem. Art. 30 DS-GVO anzufertigen. Der Begriff „Verarbeitungstätigkeit“ ist nicht eindeutig definiert und wird i.d.R. als „prozessorientierte Verarbeitung“ ausgelegt[29].

Die Datenschutzkonferenz hat in ihrer Ausarbeitung „Hinweise zum Verzeichnis von Verarbeitungstätigkeiten, Art. 30 DS-GVO“, eine Trennung einzelner Verarbeitungstätigkeiten an dem konkreten Zweck der Datenverarbeitung angelehnt:

> „Es ist ein strenger Maßstab anzulegen, sodass jeder neue Zweck der Verarbeitung eine eigene Verarbeitungstätigkeit darstellt. Bei einer nur geringen Zweckänderung muss geprüft werden, ob eine bereits bestehende Beschreibung einer Verarbeitungstätigkeit angepasst werden muss oder ob eine vollständig neue Beschreibung anzufertigen ist."[30]

Hierbei wird grundsätzlich der konkrete Verarbeitungszweck als eine Verarbeitungstätigkeit verstanden.

Im Rahmen von klinischen Studien grenzen sich einzelne Studien zu unterschiedlichen Zwecken voneinander ab und stellen damit eine einzelne Verarbeitungstätigkeit dar.

8.4 Rechtsvorschriften zum Führen eines Verzeichnis der Verarbeitungstätigkeiten

Die für einen Verantwortlichen geltenden datenschutzrechtlichen Regelungen, seien sie europäische oder nationale Vorgaben, finden auch im Rahmen der Forschung und daher natürlich auch bei klinischen Studien Anwendung.

---

[29] So z.B.

- GDD-Praxishilfe DS-GVO V: Verzeichnis von Verarbeitungstätigkeiten, Abschnitt 1.2 „Inhalte“. [Online, zitiert am 2019-11-16]; Verfügbar unter https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_5.pdf
- Evangelische Kirche Deutschland: Verzeichnis von Verarbeitungstätigkeiten, Abschnitt „Was muss das Verzeichnis konkret enthalten?“. [Online, zitiert am 2019-11-16]; Verfügbar unter https://datenschutz.ekd.de/wp-content/uploads/2018/04/01-Kurzpapier-Verzeichnis-von-Verfahrenst%C3%A4tigkeiten.pdf

[30] Datenschutzkonferenz: Hinweise zum Verzeichnis von Verarbeitungstätigkeiten, Art. 30 DS-GVO [Online, zitiert am 2019-11-16]; Verfügbar unter https://www.datenschutzkonferenz-online.de/media/ah/201802_ah_verzeichnis_verarbeitungstaetigkeiten.pdf

Da Art. 30 DS-GVO eine abschließende Regelung darstellt, kann der nationale Gesetzgeber diese Regelungen nicht ändern. Gleichwohl können nationale Gesetzgeber weitergehende Auflagen bzgl. der Dokumentation einführen, z.B. könnte ein nationaler Gesetzgeber die Dokumentation der Rechtsgrundlage aufnehmen. Art. 30 Abs. 1 S. 2 DS-GVO ist jedoch eine abschließende Aufzählung, d.h. alle weiteren Angaben können zwar technisch bei einem Verzeichnis der Verarbeitungstätigkeiten angesiedelt sein, sind aber kein „offizieller" Bestandteil des Verzeichnisses.

8.5 Sanktionen bei einem Verstoß bzgl. Verzeichnis der Verarbeitungstätigkeiten

Ein Verstoß gegen datenschutzrechtliche Vorschriften kann die zuständige Aufsichtsbehörde mit einer Geldbuße ahnden. Die Höhe des Bußgeldes wird im Einzelfall bestimmt und kann bis zu 20.000.000 Euro bzw. im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs betragen (vgl. Art. 83 DS-GVO).

8.6 Inhalt

Die wesentlichen Inhalte sowie geforderte Pflichtangaben eines Verzeichnisses werden im Folgenden aufgeführt.

Die DS-GVO beschreibt im Art. 30 Abs. 1 die Mindestinhalte eines Verzeichnisses:

a) Name und Kontaktdaten des Verantwortlichen, gegebenenfalls des gemeinsam mit ihm Verantwortlichen, Vertreter des Verantwortlichen und eines etwaigen Datenschutzbeauftragten:
   Die zweifelsfreie Identifikation des Verantwortlichen sowie eines Ansprechpartners wie auch des Datenschutzbeauftragten dient der Transparenz der Verarbeitung.
b) Zweck der Verarbeitung
   Die Zweckbestimmung ermöglicht i.d.R. einen Rückschluss auf die Rechtsgrundlage, ohne diese konkret in ein Verzeichnis aufzunehmen.
c) Beschreibung der Kategorien betroffener Personen sowie personenbezogener Daten
   Gruppen von Personen, z.B. Mitarbeiter, Patienten, Datengruppen wie z.B. Stammdaten (Name, Adresse, Krankenkasse)
d) Kategorien von Empfängern, denen die pbD offengelegt wurden bzw. werden, einschließlich Empfänger in Drittländern oder internationale Organisationen
   Empfänger ist entsprechend Art. 4 Ziff. 9 DS-GVO „jede 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". Insbesondere gilt dies natürlich auch für interne oder externe Empfängergruppen, z.B. SV-Träger, Banken, Universitäten
e) Übermittlungen von pbD an ein Drittland oder an eine internationale Organisation, einschließlich Angabe des betreffenden Drittlands oder betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien.
   Länder und Organisationen außerhalb der EU bzw. des EWR, Zweck ist u.a. die Beurteilung des Datenschutzniveaus für eine Risikobewertung
f) Wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien

Angabe der Löschfristen so konkret wie möglich, die Angabe einer allgemeinen Aufbewahrungsfrist oder sogar eine Angabe zu unterlassen, wird als nicht ausreichend angesehen.

g) Wenn möglich eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 1.
z.B. Verweis auf ein allgemeines Sicherheitskonzept und/oder TOMs, hier lediglich Abweichungen dokumentieren

Die Rechtmäßigkeit der Verarbeitung sowie Anforderungen durch Spezialgesetze werden im Verzeichnis nicht dokumentiert. Der Verantwortliche kann aber weitere Informationen zu einer Verarbeitungstätigkeit in diesem Verzeichnis pflegen, wie z.B. den Nachweis der Rechtsgrundlage. Bei der Aufforderung das Verfahrensverzeichnis zu übergeben, sind jedoch nur die in Art. 30 Abs. 1 DS-GVO für Verantwortliche bzw. Art. 30 Abs. 2 DS-GVO für Auftragsverarbeiter genannten Angaben den Aufsichtsbehörden zur Verfügung zu stellen, da Art. 30 DS-GVO sowohl in Abs. 1 als auch in Abs. 2 abschließende Aufzählungen enthält. Grundsätzlich darf man den Aufsichtsbehörden aber auch die ergänzenden Angaben mit zur Verfügung stellen. Da Aufsichtsbehörden grundsätzlich alle zur Beurteilung des jeweiligen Vorgangs benötigten Angaben zur Verfügung gestellt werden müssen, kann durch die Bereitstellung der zusätzlichen Informationen der Bearbeitungsprozess eventuell sogar beschleunigt werden. Im Zweifelsfall empfiehlt sich die Rücksprache mit der zuständigen Aufsichtsbehörde.

8.7 Form

Grundsätzlich ist ein Verzeichnis schriftlich zu führen, wobei ein elektronisches Format ebenfalls möglich ist. Verzeichniseinträge müssen zur Vorlage bei der zuständigen Aufsichtsbehörde in Papier- oder elektronische Form (Textformat) exportierbar sein.

Ein Verzeichnis ist regelmäßig in deutscher Sprache zu führen.

Die konkrete Form wird von dem Verantwortlichen bestimmt und er stellt i.d.R. eine Vorlage zur Verfügung. Verschiedene Aufsichtsbehörden, Organisationen, Verbände etc. bieten Mustervorlagen für ein Verzeichnis an. Folgende Aufsichtsbehörden stellen z.B. unter den Internet-Links Muster zur Verfügung:

- Datenschutzkonferenz
  - Muster: https://www.datenschutzkonferenz-online.de/media/ah/201802_ah_muster_verantwortliche.pdf
  - Hinweise zum Verzeichnis: https://www.datenschutzkonferenz-online.de/media/ah/201802_ah_verzeichnis_verarbeitungstaetigkeiten.pdf
- Baden-Württemberg: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/02/Muster-Verarbeitungsverzeichnis-Verantwortlicher.pdf
- Sachen-Anhalt: https://www.datenschutz.sachsen-anhalt.de/fileadmin/Bibliothek/Landesaemter/LfD/PDF/binary/Informationen/Internationales/Datenschutz/Grundverordnung/Verzeichnis_der_Verarbeitungstaetigkeiten/Muster_Verarbeitungsverzeichnis_Verantwortlicher.pdf

- Nordrhein-Westfalen:
  https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Verzeichnis-Verarbeitungstaetigkeiten/Inhalt/Verarbeitungstaetigkeiten/Muster-Verarbeitungsverzeichnis-Verantwortlicher.pdf
- Hessen:
  https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/content-downloads/Muster%20Verarbeitungsverzeichnis%20Verantwortlicher.docx

9 Zusammenarbeit

Bei der Durchführung klinischer Studien arbeiten in der Regel mehrere juristische Personen zusammen. Die Form der Zusammenarbeit bestimmt dabei das datenschutzrechtliche Vertragsverhältnis. Darf der Auftragsverarbeiter die personenbezogenen Daten nur in Übereinstimmung mit der Weisung des Verantwortlichen verarbeiten, liegt eine Auftragsverarbeitung vor. Handelt es sich hingegen um gleichberechtigte Partner, besteht eine Gemeinsame Verantwortlichkeit. Die nachstehende Tabelle verdeutlicht zunächst in einer knappen Übersicht die grundlegenden Unterschiede zwischen einer Auftragsverarbeitung und einer Gemeinsamen Verantwortlichkeit, die daraufhin in den beiden Unterkapiteln 8.1 und 8.2 konkretisiert werden.

Kriterium	Auftragsverarbeitung	Gemeinsame Verantwortlichkeit
Grundsatz	Weisungsgebundene Verarbeitung von Daten durch Auftragnehmer	(Gleichberechtigte) Partnerschaft mit gemeinsamer Verantwortung
Erlaubnistatbestand	Verantwortlicher verfügt über einen Erlaubnistatbestand	Die gemeinsam an der Verarbeitung Beteiligten haben einen (gemeinsamen) Erlaubnistatbestand
Voraussetzung für Verarbeitung	Vertrag oder anderes Rechtsinstrument gemäß Art. 28 Abs. 3 DS-GVO	Aufteilung der Pflichten gemäß Art. 26 Abs. 1 DSG-VO (und entsprechende vertragliche Regelung / Vereinbarung)

9.1 Auftragsverarbeitung

Laut der Artikel-29-Datenschutzgruppe muss eine Organisation für eine Einstufung als Auftragsverarbeiter zwei grundlegende Bedingungen erfüllen: Sie muss in Bezug auf den für die Verarbeitung Verantwortlichen rechtlich eigenständig sein und sie muss personenbezogene Daten im Auftrag des Verantwortlichen verarbeiten[31].

Dass die Verarbeitung im Auftrag und auf Weisung des Verantwortlichen erfolgt, soll sicherstellen, dass der Verantwortliche „Herr" der Verarbeitung bleibt. Dem wird vor allem dadurch Rechnung getragen, dass der Auftragnehmer gegenüber dem Verantwortlichen weisungsgebunden ist. Die Daten befinden sich zwar im Machtbereich des Auftragsverarbeiters, sie dürfen jedoch nur in Übereinstimmung mit den Weisungen des Verantwortlichen verarbeitet werden. Eigene Entscheidungsbefugnisse stehen ihm im Hinblick auf die personenbezogenen Daten nur soweit zu, wie sie im Auftragsverhältnis vereinbart sind.

Im Rahmen der Auftragsverarbeitung erlaubt ist es allerdings, dass der Verantwortliche die Entscheidung über die technischen und organisatorischen Mittel an den Auftragsverarbeiter delegiert, z. B. welche Hard- oder Software für die Datenverarbeitung eingesetzt wird.

Sobald der Auftragsverarbeiter Daten zu eigenen Zwecken verarbeitet, handelt es sich um keine Auftragsverarbeitung. Denn in diesem Fall werden sowohl die Mittel als auch die Zwecke vom Auftragsverarbeiter bestimmt, er agiert somit als eigenständiger Verantwortlicher. Damit es sich um

[31] Artikel-29-Datenschutzgruppe, WP 169, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter". [Online, zitiert am 2019-11-17]; Verfügbar unter http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_de.pdf, Stand: 16.02.2010, S. 30

eine Auftragsverarbeitung handelt, ist die Verarbeitung ausschließlich den Weisungen des Verantwortlichen entsprechend durchzuführen[32] .

Für eine Auftragsverarbeitung sprechen daher insbesondere ausführliche Weisungen durch den für die Verarbeitung Verantwortlichen.

Die angesprochene Weisungsgebundenheit und einige andere Vereinbarungen, die in Art. 28 DS-GVO beschrieben sind, müssen bei Vorliegen einer Verarbeitung personenbezogener Daten im Auftrag in Form eines Vertrages verbindlich festgelegt werden. Zur Erstellung dieses Vertrages gibt es eine Praxishilfe[33], auf die an dieser Stelle verwiesen wird.

Die Auftragsverarbeitung, sprich die Weitergabe von Daten an einen Dienstleister, gilt als „privilegierte“ Form der Verarbeitung. Grundsätzlich muss im Falle einer Weitergabe von personenbezogenen Daten an eine externe Stelle eine gesonderte Rechtsgrundlage vorliegen. Das kann neben einer entsprechenden gesetzlichen Regelung insbesondere die Einwilligung der betroffenen Person sein. „Privilegiert“ ist die Auftragsverarbeitung dahingehend, dass sie eben keiner weiteren Rechtfertigung i.S.v. Art. 6 bis 10 DS-GVO bedarf als diejenige, auf die der Verantwortliche selbst die Verarbeitung stützt. Durch einen Vertrag zwischen Verantwortlichem und Auftragsverarbeiter, der die gesetzlichen Anforderungen nach Art. 28 DS-GVO erfüllt, wird eine rechtlich ausreichende Basis für die Weitergabe der Daten an einen Dienstleister geschaffen. Der Auftragnehmer ist datenschutzrechtlich kein Dritter i. S. v Art. 4 Nr. 10 DS-GVO, sondern wird datenschutzrechtlich wie Personal des Verantwortlichen angesehen[34].

Beispiel für eine Auftragsverarbeitung:

1) Biometrische Auswertung im Rahmen einer Studie
   Ein Biometriker führt im Rahmen einer Studie eine statistische Untersuchung durch. Sowohl die Fragestellung als auch die Daten, die ihm für die Auswertung zur Verfügung stehen, sind von anderen vorgegeben. Da dem Biometriker hinsichtlich der Verarbeitung klare Vorgaben aufgegeben wurden und er insbesondere nicht über die Mittel und Zwecke der Verarbeitung entscheidet, liegt eine Auftragsverarbeitung vor[35].
2) Klinische Studie (Arzneimittel, Medizinprodukt)
   Prüfer (i.S.v. § 4 Nr. 25 AMG, § 3 Nr. 24 MPG) arbeiten in der Regel auf Weisung, das heißt der Sponsor gibt ihnen die Zwecke der Verarbeitung vor, sie können jedoch nicht frei darüber bestimmen. Insofern liegt in der Regel bei diesen eine Auftragsverarbeitung vor[35].

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

---

[32] Spoerr W.: Art. 28, Rn. 19 in: Wolff/Brink (Hrsg.) BeckOK Datenschutzrecht, 30. Ed. Stand: 01.11.2019

[33] BvD, bvitg, DKG, GDD, GMDS: Mustervertrag zur Auftragsverarbeitung (2018). [Online, zitiert am 2019-11-17]; Verfügbar unter https://ds-gvo.gesundheitsdatenschutz.org/html/adv-vertrag.php

[34] So zu finden bei:

- Müller S, Stief M. (2019) Auftragsverarbeitung Orientierungshilfe, S.7. [Online, zitiert am 2019-11-17]; Verfügbar unter https://www.datenschutz-bayern.de/technik/ orient/oh_ auftragsverarbeitung.pdf
- Spoerr W.: Art. 28, Rn. 1 in: Wolff/Brink (Hrsg.) BeckOK Datenschutzrecht, 30. Ed. Stand: 01.11.2019

[35] Schütze/Spyra, gmds, Art. 26 DS-GVO: Gemeinsam Verantwortliche. [Online, zitiert am 2019-11-17]; Verfügbar unter https://ds-gvo.gesundheitsdatenschutz.org/download/Art.26-Gemeinsam_Verantwortliche .pdf, Stand: 17.06.2018, S. 7

9.2 Gemeinsame Verantwortlichkeit

Keine Auftragsverarbeitung liegt ferner vor, wenn Gemeinsame Verantwortlichkeit gemäß Art. 26 DS-GVO gegeben ist, das heißt wenn mehrere Verantwortliche gemeinsam über die Zwecke und Mittel der Verarbeitung entscheiden. Diese Rechtsfigur wird auch als „Joint Controllership" bezeichnet. Hierunter können je nach Gestaltung eine Reihe von Verarbeitungen fallen, darunter auch klinische Arzneimittelstudien, wenn mehrere Mitwirkende (Sponsoren, Studienzentren, Ärzte) jeweils in Teilbereichen Entscheidungen über die Verarbeitung treffen[36].

Gemäß der Interpretation der Artikel -29-Datenschutzgruppe muss der Begriff „gemeinsam" „im Sinne von ‚zusammen mit' oder ‚nicht alleine' in unterschiedlichen Spielarten und Konstellationen ausgelegt werden"[37]. Wie der EuGH in seinem Facebook-Urteil feststellte, muss nicht jeder der Verantwortlichen gleich viel Verantwortung haben und über alle Daten verfügen, damit von einer gemeinsamen Verantwortung gesprochen werden kann[38].

Liegt eine gemeinsame Verantwortlichkeit vor, verpflichtet Art. 26 Abs. 1 DS-GVO die Verarbeitenden zum Abschluss einer Vereinbarung. In erster Linie müssen sie hierin ihre Pflichten aus der DS-GVO untereinander aufteilen, insbesondere was die Wahrnehmung der Betroffenenrechte angeht, und wer welchen Informationspflichten nach den Art. 13 und 14 DS-GVO nachkommt. Die weiteren Anforderungen an die Vereinbarung über die Gemeinsame Verantwortlichkeit und deren Mindestinhalt schreibt Art. 26 Abs. 1 DS-GVO fest. Ein Verstoß gegen Art. 26 DS-GVO ist nach Art. 83 Abs. 4 lit. a DS-GVO bußgeldbewehrt. Unterlassen es zwei Verantwortliche, eine Vereinbarung zur Gemeinsamen Verantwortlichkeit abzuschließen, liegt somit ein Ordnungswidrigkeitentatbestand vor[39].

In der Praxishilfe „Art. 26 DS-GVO: Gemeinsam Verantwortliche" der Deutschen Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie (gmds) finden sich sowohl eine ausführliche Interpretation der Regelungen als auch einige Hinweise zur Vertragsgestaltung[40].

Bei der Beurteilung der Tatsache, ob die Parteien gemeinsam über Zwecke und Mittel bestimmen können, kommt es allerdings weniger auf die vertragliche Ausgestaltung an, ausschlaggebend ist vielmehr, dass eine solche Entscheidungsbefugnis in der Realität auch tatsächlich gegeben ist. Damit

---

[36] DSK, Kurzpapier Nr. 13: Auftragsverarbeitung, Art. 28 DS-GVO. [Online, zitiert am 2019-11-17]; Verfügbar unter https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_13.pdf, Stand: 17.12.2018, S. 4f.

[37] Artikel-29-Datenschutzgruppe. (2010) WP 169 Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", Abschnitt III.1.d) Zweites Element: „allein oder gemeinsam mit anderen", S. 22. [Online, zitiert am 2019-11-17]; Verfügbar unter http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_de.pdf

[38] Europäischer Gerichtshof (EuGH). Urt. V. 05. Juni 2018, AZ: C-210/16. Rn. 38. [Online, zitiert am 2019-11-17]; Verfügbar unter http://curia.europa.eu/juris/document/document.jsf?text=&docid=202543&pageIndex=0&doclang=d &mode=lst&dir=&occ=first&part=1&cid=568857

[39] Auler, Die Gemeinsame Verantwortlichkeit nach Art. 26 DS-GVO. [Online, zitiert am 2019-11-17]; Verfügbar unter https://www.telemedicus.info/article/3407-Die-Gemeinsame-Verantwortlichkeit-nach-Art.-26-DSGVO.html, Stand: 02.04.2019

[40] Schütze/Spyra, gmds, Art. 26 DS-GVO: Gemeinsam Verantwortliche. [Online, zitiert am 2019-11-17]; Verfügbar unter https://gesundheitsdatenschutz.org/download/Art.26-Gemeinsam_Verantwortliche.pdf, Stand: 17.06.2018

kommt es hinsichtlich der Beurteilung also maßgeblich auf die Betrachtung und Bewertung anhand der tatsächlichen Gegebenheiten an[41].

Die wohl wichtigste Konsequenz der Gemeinsamen Verantwortlichkeit für jeden der Verantwortlichen folgt aus Art. 26 Abs. 3 DS-GVO: Kein Verantwortlicher kann sich der Pflicht entziehen, für die Ansprüche des jeweils von der Datenverarbeitung Betroffenen zuständig zu sein.

Wie die Verantwortlichen intern ihre Pflichten verteilt haben, spielt also nur im Innenverhältnis eine Rolle. Der Betroffene kann seine Rechte jedoch gegenüber jedem einzelnen der Beteiligten geltend machen[42].

Im Gegensatz zur Auftragsverarbeitung besteht bei der Gemeinsamen Verantwortlichkeit keine „Privilegierungswirkung". Verantwortlichkeit ist keine Befugnis zur Datenverarbeitung. Sie stellt nur klar, wer welche Aufgaben aus der DS-GVO zu erfüllen hat. Bei Art. 26 handelt es sich daher weder um eine Rechtsgrundlage für eine Verarbeitung durch mehrere Verantwortliche, noch bedarf es einer Rechtsgrundlage dafür, dass sich mehrere Verantwortliche zusammenschließen. Die Übermittlung personenbezogener Daten unter gemeinsam Verantwortlichen hingegen ist ein eigener Verarbeitungsvorgang im Sinne von Art. 4 Nr. 2 DS-GVO und bedarf als solcher einer Rechtsgrundlage. Soweit der jeweilige Verantwortliche im Rahmen der Gemeinsamen Verantwortlichkeit personenbezogene Daten verarbeitet, benötigt er für diese Verarbeitung dementsprechend eine eigene Rechtsgrundlage nach Art. 6 Abs. 1 DS-GVO und soweit besondere Kategorien personenbezogener Daten verarbeitet werden nach Art. 9 Abs. 2 DS-GVO[43].

Beispiele für eine gemeinsame Verantwortlichkeit:

1) Biometrische Auswertung im Rahmen einer Studie
   Ein Biometriker arbeitet gemeinsam mit anderen Forschern an einem Projekt. Vor Beginn der Studie legen sie gemeinsam die in der Studie zu beantwortenden / zu behandelnden Fragestellungen fest. Der Biometriker entscheidet, welche Daten im Rahmen der Forschung erhoben werden müssen, damit er eine qualifizierte Auswertung durchführen kann. Die Daten werden daraufhin von den anderen Forschern erhoben, dem Biometriker zur Auswertung übergeben und die Ergebnisse anschließend an die anderen Forscher weitergegeben. Hier findet eine gemeinsame Verarbeitung statt, der Biometriker als auch seine Forscherkollegen sind bzgl. der Entscheidung hinsichtlich der Zwecke und Mittel des Forschungsvorhabens gemeinsam-verantwortlich[44].
2) Klinische Studie (Arzneimittel, Medizinprodukt)
   Der Sponsor als die für die Veranlassung, Organisation und Finanzierung einer klinischen Prüfung verantwortliche natürliche oder juristische Person einer klinischen Studie (vgl. § 4 Ziff.

[41] Hartung J. Art. 26 Rn. 14 in Kühling/Buchner (Hrsg.) DS-GVO Datenschutz-Grundverordnung Kommentar. C.H.Beck Verlag, 2. Auflage 2018. ISBN 978-3-406-719325
[42] Auler, Die Gemeinsame Verantwortlichkeit nach Art. 26 DS-GVO. [Online, zitiert am 2019-11-17]; Verfügbar unter https://www.telemedicus.info/article/3407-Die-Gemeinsame-Verantwortlichkeit-nach-Art.-26-DSGVO.html, Stand: 02.04.2019
[43] DSK, Kurzpapier Nr. 16: Gemeinsam für die Verarbeitung Verantwortliche, Art. 26 DS-GVO. [Online, zitiert am 2019-11-17]; Verfügbar unter https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_16.pdf. Stand: 19.03.2018, S. 1
[44] Schütze/Spyra, gmds, Art. 26 DS-GVO: Gemeinsam Verantwortliche. [Online, zitiert am 2019-11-17]; Verfügbar unter https://gesundheitsdatenschutz.org/download/Art.26-Gemeinsam_Verantwortliche.pdf, Stand: 17.06.2018, S. 6

24 AMG, § 3 Ziff. 23 MPG) ist datenschutzrechtlich immer ein Verantwortlicher. Daraus folgt, dass immer, wenn mehr als ein Sponsor an einem Studienvorhaben beteiligt sind, diese datenschutzrechtlich i.d.R. als gemeinsame Verantwortliche zu betrachten sind[45], z. B.:
Ein Pharmaunternehmen gibt mehrere Arzneimittelstudien in Auftrag und wählt die sich bewerbenden Studienzentren anhand der jeweiligen Eignung und Spezialgebiete aus; es entwirft das Studienprotokoll, erteilt den Zentren die erforderlichen Weisungen hinsichtlich der Datenverarbeitung und überprüft, ob die Zentren das Protokoll und die jeweiligen internen Verfahren einhalten.
Obwohl der Auftraggeber keine Daten direkt erhebt, erhält er die von den Studienzentren erhobenen Patientendaten und verarbeitet diese Daten auf verschiedene Weise (Bewertung der in den medizinischen Unterlagen enthalten Informationen; Empfang der Daten über Nebenwirkungen; Erfassung dieser Daten in der entsprechenden Datenbank; Durchführung statistischer Analysen zur Erstellung der Studienergebnisse). Das Studienzentrum führt die Studie autonom durch – wenn auch unter Einhaltung der Weisungen des Auftraggebers; es überreicht den Patienten die Informationsunterlagen und holt ihre Zustimmung zur Verarbeitung der sie betreffenden Daten ein; es gewährt den Mitarbeitenden des Auftraggebers zu Überwachungszwecken Zugang zu den Original-Patientenunterlagen; und es sorgt für die sichere Aufbewahrung dieser Unterlagen. Daher scheint es, als ob die Verantwortung bei den einzelnen Akteuren liegt.
In diesem Fall treffen jedoch sowohl die Studienzentren als auch der Auftraggeber wichtige Entscheidungen darüber, wie personenbezogene Daten im Zusammenhang mit den klinischen Studien verarbeitet werden, insbesondere entscheiden beide über Mittel und Zwecke der Verarbeitung. Infolgedessen können sie als Gemeinsam Verantwortliche i. S. d. Art. 26 DS-GVO angesehen werden. In den Fällen, in denen der Auftraggeber über die Zwecke und die wesentlichen Elemente der Mittel entscheidet und die Forscher nur einen sehr engen Handlungsspielraum haben, könnte die Beziehung zwischen dem Auftraggeber und den Studienzentren hingegen anders ausgelegt werden[46].

[45] Schütze/Spyra, gmds, Art. 26 DS-GVO: Gemeinsam Verantwortliche. [Online, zitiert am 2019-11-17]; Verfügbar unter https://ds-gvo.gesundheitsdatenschutz.org/download/Art.26-Gemeinsam_Verantwortliche.pdf, Stand: 17.06.2018, S. 7

[46] Artikel-29-Datenschutzgruppe, WP 169, [Online, zitiert am 2019-11-17]; Verfügbar unter https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_de.pdf, Stand: 16.02.2010, S. 36f

10 Datenpannen und Meldepflicht[47]

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

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

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

10.1 Verzeichnis der Datenpannen

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

Grundsätzlich müssen in diesem Verzeichnis alle Datenpannen dokumentiert werden.

10.2 Meldepflicht bei Datenpannen: Aufsichtsbehörde

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

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

1. eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe
   - der Kategorien der Daten (z. B. Bankdaten, Gewerkschaftsdaten oder Gesundheitsdaten) und
   - der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien der Personen (z. B. Patienten oder Beschäftigte) und
   - der ungefähren Zahl der betroffenen personenbezogenen Datensätze
2. den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen

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

3. eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten
4. eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

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

Bei der EU-Vorgabe von 72 Stunden ist zu beachten, dass die EU-Verordnung 1182/71[48] Regeln für die Fristen, Daten und Termine beinhaltet, die bei allen europäischen Regelungen, die selbst keine abweichenden Vorgaben beinhalten, anzuwenden sind. Da die DS-GVO keine eigenen Regelungen hinsichtlich des Umgangs mit Fristen, Daten und Termine beinhaltet, gelten somit die Vorgaben der Verordnung 1182/71. Hierbei sind bei der Vorgabe von den in Art. 33 DS-GVO vorgegebenen 72 Stunden insbesondere zu beachten:

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

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

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

Auftragsverarbeiter gelten als der „verlängerte“ Arm des Verantwortlichen, d.h. hat der Auftragsverarbeiter Kenntnis von der Verletzung, gilt dies als Kenntnisnahme des Verantwortlichen und die Zeitspanne, in welcher eine Meldung zu erfolgen hat, beginnt. Grundsätzlich ist der Auftragsverarbeiter durch Art. 33 Abs. 2 DS-GVO gesetzlich verpflichtet, eine Verletzung unverzüglich dem Verantwortlichen zu melden. Je nach vertraglicher Gestaltung können bei einer „unverzüglichen“ (= ohne schuldhaftes Verzögern) Meldung aber 2-3 Tage vergehen, man denke nur an Freitagnachmittag und anschließendes Wochenende. Bekommt der Verantwortliche die Meldung

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

aber ggf. mit 48 Stunden Verzögerung, bleibt kaum noch Zeit zur Bearbeitung des Vorfalls durch den Verantwortlichen. Daher sollten vertragliche Regelungen eine entsprechend schnelle Meldung des Auftragsverarbeiters an den Verantwortlichen beinhalten, wobei der Verantwortliche in diesen Fällen natürlich auch die Bearbeitung des Vorfalls an Wochenenden und Feiertagen gewährleisten muss.

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

10.3 Meldepflicht bei Datenpannen: Betroffene Personen

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

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

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

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

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

1. Der Verantwortliche hat geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen, dass die betroffenen personenbezogenen Daten für alle unbefugten/unberechtigten Personen unzugänglich sind. Dies kann z.B. durch den Einsatz von dem Stand der Technik entsprechender Verschlüsselung gewährleistet sein.
2. Der Verantwortliche stellte durch nachfolgende Maßnahmen sicher, so dass für die betroffenen Personen durch die Verletzung aller Wahrscheinlichkeit nach kein hohes Risiko mehr besteht. Dies kann z.B. dadurch geschehen, wenn beim Diebstahl eines mobilen Datenträgers unmittelbar nach dem Diebstahl ein „Remote Wipe[49]“ erfolgte.

[49] Remote Wipe ist ein Sicherheitsfeature, welches erlaubt, aus der Ferne Daten auf einem Computer, Smartphone oder Tablet zu löschen. Allerdings funktioniert Remote Wipe nur mit existierender Verbindung zu

3. Die Meldung ist mit einem unverhältnismäßigen Aufwand verbunden. In diesem Fall hat stattdessen eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden. In diesen Fällen kann beispielsweise eine Veröffentlichung des Vorfalles in regionalen oder überregionalen (je nach Gruppe betroffener Personen) Tageszeitungen erfolgen. Ein bloßes Bekanntgeben auf der eigenen Homepage alleine wird i.d.R. nicht ausreichen, da man nicht davon ausgehen kann, dass die betroffenen Personen zeitnah die Homepage aufsuchen. Eine Darstellung auf der eigenen Homepage kann nur eine ergänzende Maßnahme darstellen, z.B. um ergänzend zum Zeitungsartikel weitere Informationen bereitzustellen.

10.4 Umgang mit Datenpannen: Was ist zu tun?

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

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

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

- Welche Vorfälle werden zu welchen Zeitpunkten durch wen an wen gemeldet?
- Wer hat welche Zuständigkeiten?
  - Wie erfolgt durch wen bis wann eine Risikobewertung?
  - Wer darf der Aufsichtsbehörde melden?
  - Wer meldet an die betroffenen Personen? Oder führt eine entsprechende öffentliche Bekanntgabe durch?
  - Wenn kein Datenschutzbeauftragter benannt wurde: Wer ist Ansprechpartner für die zuständige Aufsichtsbehörde?
- Wie sind die Regelungen bzgl. Auftragsverarbeiter?
  - Wer ist Anlaufstelle für Auftragsverarbeiter?

---

einem Netzwerk (Internet oder Mobilfunknetz, je nach eingesetzter IT-Lösung). Daher kann man von einem erfolgreichen Löschen der Daten erst dann ausgehen, wenn das Gerät den Erhalt des Löschbefehls sowie die durchgeführte Löschung bestätigte. Die Abgabe des Remote Wipe Löschbefehles alleine reicht nicht aus um davon ausgehen zu können, dass das Risiko aller Wahrscheinlichkeit nach nicht mehr besteht.

- Wann muss/kann ein Auftragsverarbeiter melden?
- Welche Zuarbeit muss ein Auftragsverarbeiter in welchem Zeitraum leisten? Nur innerhalb der vereinbarten Servicezeiten oder ggf. auch außerhalb? Letzteres kann mit zusätzlichen Kosten verbunden sein.

- Wer führt das gesetzlich geforderte Verzeichnis?

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

11 Ethik-Kommission

Fortschritte lassen sich in der Medizin ohne angemessene Forschung kaum verwirklichen. Dies erfordert auch eine Forschung am Menschen, wie zum Beispiel durch die Erprobung neuer Medizinprodukte oder medizinischer Verfahren. Aufgrund vielzähliger gesetzlicher Beschränkungen unterliegen Forschungsprojekte am Menschen strengsten ethischen und rechtlichen Kriterien zur Durchführung. Die Überwachung der Einhaltung dieser Kriterien unterliegt der Aufgabe der Ethikkommissionen. Eine Ethikkommission darf also niemals medizinisch unvertretbare Versuche erlauben.

Durch die Datenschutzgesetze ergeben sich weitere Voraussetzungen für eine ordnungsgemäße Durchführung von klinischen Forschungsprojekten.

11.1 Aufgaben einer Ethikkommission

In Deutschland versteht man unter Ethikkommissionen die gesetzlich etablierten Einrichtungen der Gesamtheit der Ärztinnen und Ärzte in Deutschland zur Beurteilung von Forschungsvorhaben am Menschen[50]. Ihre Aufgabe ist es, medizinische Forschungsvorhaben an menschlichen Personen zu beurteilen und forschende Ärzte zu beraten[51]. Ethikkommissionen haben einerseits Fürsorge für den Patienten, andererseits allerdings auch Fürsorge gegenüber dem medizinischen Fortschritt zu tragen[52]. Außerdem hat die Ethikkommission auch den Forscher zu schützen. Dieser soll davor bewahrt werden, die Grenzen des ethisch Zulässigen zu überschreiten[53].

Ethikkommissionen sind in erster Linie zur Bewahrung von Patienten und Probanden vor gefährlicher oder überraschender Forschung zuständig. Daher muss die Kommission einzelfallbezogen prüfen, ob der Forschungsplan in Ordnung ist, ob die Aufklärung der Patienten und Probanden gesichert ist, sowie dass die Belastung der Probanden auf das vertretbare Minimum beschränkt bleibt und dass gefährliche Versuche nicht bzw. nur unter außergewöhnlichen Sicherheitsvorkehrungen durchgeführt werden. Außerdem muss darauf geachtet werden, dass ein Abbruch möglich ist und individuelle Einfluss- und Ausschlusskriterien angegeben werden. Auch auf die Möglichkeit des Ausscheidens aus der Studie ohne Nachteile für die Probanden ist hinzuwiesen. Nicht zuletzt muss eine Probandenversicherung gewährleistet werden[54].

Die Ethikkommission hat außerdem die Aufgabe, anhand der vorgelegten Unterlagen sowie aufgrund eigener wissenschaftlicher Erkenntnisse zu prüfen, ob die grundlegenden Anforderungen an die Rechtmäßigkeit der Durchführung einer klinischen Studie vorliegen. Dazu gehören unter anderem der Prüfplan, das Design der Studie sowie das Prüfprodukt und die angewandten Patientenauswahlkriterien. Konkret ergeben sich sie Prüfungspunkte aus dem Prüfkatalog des § 5 Abs. 4 MPKPV (Verordnung über klinische Prüfungen von Medizinprodukten)[55].

[50] Kern: Standortbestimmung: Ethikkommissionen - auf welchen Gebieten werden sie tätig?, in: MedR (2008) 26: 631-636 (631).
[51] Gödicke: Berufsrechtliche Grundlagen für die Tätigkeit von Ethik-Kommissionen – überflüssige Zwangsberatung von Ärzten?, in: MedR (2008) 26: 636-640 (636).
[52] Gödicke: Berufsrechtliche Grundlagen für die Tätigkeit von Ethik-Kommissionen – überflüssige Zwangsberatung von Ärzten?, in: MedR (2008) 26: 636-640 (636).
[53] Deutsch: Entstehung und Funktion der Ethikkommissionen in Europa, in: MedR (2008) 26: 650-654 (654).
[54] Deutsch: Entstehung und Funktion der Ethikkommissionen in Europa, in: MedR (2008) 26: 650-654 (653).
[55] Rehmann/Wagner/Rehmann, 3. Aufl. 2018, MPG § 22 Rn. 2.

11.2 Rechtliche Rahmenbedingungen[56]

Neuartige Arzneimittel oder Medizinprodukte dürfen erst an Menschen erprobt werden, nachdem ein Verwaltungsverfahren durchlaufen wurde, an dem eine Ethikkommission sowie eine Bundesoberbehörde beteiligt ist – in der Regel ist dies das Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM)[57].

Im deutschen Recht sind derzeit gesetzliche Regelungen über Ethikkommissionen insbesondere in den folgenden sieben Gesetzen zu finden[58].

Alle folgenden Gesetze – mit Ausnahme des Transfusionsgesetzes – verlangen, dass eine Ethikkommission einzuschalten ist, bevor ein Forschungsvorhaben eingeleitet werden darf. Neben diesen bundesrechtlichen Regelungen finden sich solche auch im jeweiligen Landesrecht, welche unter anderem die Zusammensetzung von Ethikkommissionen regeln.

- Arzneimittelgesetz (§ § 40-42 AMG),
- Transfusionsgesetz (§ § 8, 9 TFG),
- Medizinproduktegesetz (§ § 20, 22 MPG),
- Stammzellgesetz (§ § 6, 8, 9 StzG),
- Strahlenschutzgesetz (§ 26 StrlSchG),
- Strahlenschutzverordnung § 92 StrlSchV)
- Durchführungsverordnung des Bundesministeriums zum AMG (GCP-V)
- Musterberufsordnung für Ärzte (§ 15 MBO-Ä)

Das AMG und das MPG legen den Fokus auf das Gefahrenabwehrrecht für spezielle und wichtige Bereiche der öffentlichen Gesundheitssorge[59].

Die zentrale Ethikkommission (ZEKO) ist bei der Bundesärztekammer angesiedelt, jedoch gibt es 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 Berlin

[56] Dieser Text entstammt zum überwiegenden Teil dem Kapitel 9.1.1 „Rechtliche Grundlagen“ der Praxishilfe „Datenschutzrechtliche Anforderungen an die medizinische Forschung unter Berücksichtigung der EU Datenschutz-Grundverordnung (DS-GVO“ von GDD und GMDS. [Online, zitiert am 2019-10-01]; Verfügbar unter https://ds-gvo.gesundheitsdatenschutz.org/html/forschung.php

[57] Gödicke: Berufsrechtliche Grundlagen für die Tätigkeit von Ethik-Kommissionen – überflüssige Zwangsberatung von Ärzten?, in: MedR (2008) 26: 636-640 (636).

[58] Kern: Standortbestimmung: Ethikkommissionen - auf welchen Gebieten werden sie tätig?, in: MedR (2008) 26: 631-636 (631).

[59] Gödicke: Berufsrechtliche Grundlagen für die Tätigkeit von Ethik-Kommissionen – überflüssige Zwangsberatung von Ärzten?, in: MedR (2008) 26: 636-640 (636).

- Brandenburg
    - § 7 Heilberufsgesetz
    - Satzung der Ethik-Kommission der Landesärztekammer Brandenburg
- 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
    - § 6 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

11.3 Struktur der Ethikkommissionen

Die Verfahrensabläufe werden normiert und innerstaatlichen Verwaltungsvorschriften angepasst. Die entscheidende Beurteilung eines Forschungsprojektes erfolgt durch ehrenamtliche Mitglieder, ausgewählt durch ausgewiesene Qualifikation in ihren Berufsfeldern und nach Interesse für eine Mitarbeit.

11.4 Abwägung Risiko – Nutzen

Für die ordnungsgemäße Durchführung einer klinischen Prüfung muss eine positive Risiko-Nutzen-Abwägung vorliegen. Diese wird durch die Ethikkommission geprüft. In einer solchen Prüfung werden Risiken und Nachteile des Forschungsvorhabens gegenüber dem Nutzen für die Person, bei welcher die Studie durchgeführt werden soll, sowie für die allgemeine Medizin, miteinander abgewogen. Die Abwägung ist positiv, wenn sie im Ergebnis ärztlich vertretbar ist[60].

Im Falle von gesunden Versuchspersonen dürfen nur vorübergehende, erträgliche Belastungen zugelassen werden. Bei erkrankten Personen muss die Schwere der Erkrankung in die Abwägung miteinbezogen werden[61].

11.5 Patienten- und Probandenschutz[62]

In erster Linie besteht die Pflicht einer Ethik-Kommission darin, Patienten bzw. Probanden vor gefährlicher oder überraschender Forschung zu bewahren[63]. Zu diesem Zweck muss sie prüfen, ob die Aufklärung der Patienten und Probanden in verständlicher und umfassender Form erfolgt. Des Weiteren trägt die Kommission dafür Sorge, dass bei den 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[64].

Bei klinischen Studien zur Prüfung der Wirksamkeit und/oder Unbedenklichkeit von Arzneimitteln am Menschen – sogenannte klinische Prüfungen – nehmen Ethikkommissionen neben ihrer beratenden Funktion auch eine gesetzliche Gutachter- und Überwachungsfunktion wahr[65].

11.6 Rechtsverbindlichkeit von Entscheidungen einer Ethik-Kommission[66]

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 [67]. Daher wird

---

[60] Pramann/Albrecht, Forschung im Krankenhaus, Düsseldorf 2014, S. 87.
[61] Deutsch, in: Deutsch/Lippert, AMG, § 40 Rn. 8.
[62] Dieser Text entstammt Kapitel 9.1.2 „Eine Pflicht der Ethikkommission: Patienten- und Probandenschutz“ der Praxishilfe „Datenschutzrechtliche Anforderungen an die medizinische Forschung unter Berücksichtigung der EU Datenschutz-Grundverordnung (DS-GVO“ von GDD und GMDS. [Online, zitiert am 2019-10-01]; Verfügbar unter https://ds-gvo.gesundheitsdatenschutz.org/html/forschung.php
[63] Deutsch, Erwin: Der Beitrag des Rechts zur klinischen Forschung in der Medizin, in: NJW (1995): 3019-3024 (3023).
[64] Rehmann, in: Rehmann, AMG, 4. Aufl. München 2014, vor § § 40-42b, Rn. 2.
[65] Rehmann/Wagner/Rehmann, 3. Aufl. München 2018, MPG § 22 Rn. 1.
[66] Dieser Text entstammt Kapitel 9.1.3 „Rechtsverbindlichkeit von Entscheidungen einer Ethik-Kommission“ der Praxishilfe „Datenschutzrechtliche Anforderungen an die medizinische Forschung unter Berücksichtigung der EU Datenschutz-Grundverordnung (DS-GVO“ von GDD und GMDS. [Online, zitiert am 2019-10-01]; Verfügbar unter https://ds-gvo.gesundheitsdatenschutz.org/html/forschung.php
[67] 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

bereits seit 1981 gefordert, dass neben der zustimmenden Kenntnisnahme durch die Ethik-Kommission auch ein juristisch begründetes Gutachten eingeholt wird[67,68]. 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[67]. 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.

11.7 Einsichtnahme in Patienten- bzw. Probandendaten[69]

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.

11.8 Datenschutzrechtliche Anforderungen an die Einwilligung für die klinische Prüfung von Arzneimitteln

Nach § 40 Abs. 1 Nr. 3a AMG dürfen grundsätzlich nur volljährige, einwilligungsfähige Personen in eine klinische Prüfung eingebunden werden, wenn sie über das Vorhaben ausreichend aufgeklärt werden, die Informationen schriftlich erhalten und schriftlich eingewilligt haben. Die Einwilligungserklärung ist gemäß § 3 Abs. 2 lit. b GCP-V (Anwendung der Guten Klinischen Praxis bei der Durchführung von klinischen Prüfungen mit Arzneimitteln zur Anwendung am Menschen) zu datieren und vom Teilnehmer zu unterschreiben. Zudem muss über Wesen, Bedeutung, Risiken und Tragweite der klinischen Prüfung aufgeklärt werden[70].

Die Versuchsperson wird darüber aufgeklärt, dass sie die Teilnahme an dem Forschungsvorhaben jederzeit formlos beenden sowie die Zustimmung zur Teilnahme widerrufen kann, ohne einen Nachteil zu erlangen. Nur in Ausnahmefällen kann von der schriftlichen Einwilligung abgewichen werden, etwa in Fällen eines nicht schreibfähigen Probanden.

In der Geschäftsfähigkeit beschränkte und geschäftsunfähige Personen können mithilfe einer Einwilligung ihres gesetzlichen Vertreters an einem Forschungsvorhaben teilnehmen. Die

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

[69] Dieser Text entstammt Kapitel 9.1.4 „Einsichtnahme in Patienten- bzw. Probandendaten“ der Praxishilfe „Datenschutzrechtliche Anforderungen an die medizinische Forschung unter Berücksichtigung der EU Datenschutz-Grundverordnung (DS-GVO“ von GDD und GMDS. [Online, zitiert am 2019-10-01]; Verfügbar unter https://ds-gvo.gesundheitsdatenschutz.org/html/forschung.php

[70] Pramann/Albrecht, Forschung im Krankenhaus, Düsseldorf 2014, S. 32.

Ethikkommission hat in diesem Fall zu prüfen, ob der Patientenschutz gewährleistet ist und prüft, auf welchem Weg die Einwilligung der Geschäftsunfähigen bzw. beschränkt Geschäftsfähigen eingeholt wurde[71].

Die Aufklärungs- und Einwilligungsunterlagen sind der Ethikkommission vorzulegen[72].

[71] Pramann/Albrecht, Forschung im Krankenhaus, Düsseldorf 2014, S. 37.
[72] Pramann/Albrecht, Forschung im Krankenhaus, Düsseldorf 2014, S. 32.

12 Publikationen und Veröffentlichungen von Studienergebnissen

Gemäß § 27 Abs. 4 BDSG darf ein Verantwortliche personenbezogene Daten nur veröffentlichen, wenn die betroffene Person eingewilligt hat oder dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist. Dabei ist „veröffentlichen" weit zu verstehen: es handelt sich nicht nur um die Darstellung von Ergebnissen in Fachzeitschriften, sondern darum, dass personenbezogene Daten der Öffentlichkeit zugänglich gemacht werden. Einige Fachzeitschriften verlangen bei Veröffentlichungen beispielsweise die Herausgabe der Rohdaten, damit jeder die Forschungsergebnisse überprüfen kann. D.h., die Rohdaten werden der gesamten Fach-Öffentlichkeit zur Verfügung gestellt. Sind in diesen Rohdaten personenbezogene Daten enthalten – was beispielsweise bei genetischen Daten ja immer der Fall ist -, so ist dies nur unter den Voraussetzungen von § 27 Abs. 4 BDSG zulässig.

Dabei muss bedacht werden, dass gemäß Art. 44 Abs. 1 DS-GVO eine Einwilligung nur eingeschränkt für die Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen genutzt werden kann: nur ausnahmsweise kann eine Einwilligung dies legitimieren. Bei der oben angesprochenen Weitergabe von Rohdaten ist aber kein Ausnahmetatbestand gegeben, d.h. die Einwilligung kann die Verarbeitung in einem Drittstaat nicht legitimieren. D.h., wenn Daten von Forschern zur Verarbeitung (was die Überprüfung der eigenen Forschungsergebnisse einschließt) in einem Drittstaat weitergegeben werden, muss einer der in Artt. 44ff DS-GVO beschriebenen Erlaubnistatbestände vorhanden sein.

Werden Ergebnisse von klinischen Studien veröffentlicht, sollte das Statement der WHO[73] beachtet werden. Darin schreibt die WHO: „Der Nutzen des Austauschs von Forschungsdaten und die Erleichterung der Forschung durch einen besseren Zugang zu primären Datensätzen ist ein Prinzip, das die WHO für wichtig hält. Diese Erklärung zielt nicht darauf ab, die Primärdaten zu teilen." D.h. die WHO erkennt an, dass für den Fortschritt in der Medizin ein Datenaustausch zwingend erforderlich ist, was aber nicht die ggf. personenbezogenen bzw. personenbeziehbaren Primärdaten einschließen muss.

§ 42b AMG fordert, dass die „Berichte über alle Ergebnisse konfirmatorischer klinischer Prüfungen zum Nachweis der Wirksamkeit und Unbedenklichkeit der zuständigen Bundesoberbehörde zur Eingabe in die Datenbank nach § 67a Abs. 2" AMG zur Verfügung gestellt werden müssen. Desgleichen müssen Ergebnisse von klinischen Studien, die mit einem bereits zugelassenen oder für das Inverkehrbringen genehmigten Arzneimittel durchgeführt wurden, der Behörde (= BfArM) zur Verfügung gestellt werden.

Auch die ab Mai 2020 in Wirkung tretende europäische Verordnung 2017/745 über Medizinprodukte[74] verlangt eine „Veröffentlichung von Ergebnissen im Einklang mit den rechtlichen Anforderungen und den ethischen Grundsätzen gemäß Kapitel I Abschnitt 1".

[73] World Health Organization (WHO): WHO Statementon Public Disclosure of Clinical Trial Results. [Online, zitiert am 2019-10-01]; Verfügbar unter https://www.who.int/ictrp/results/WHO_Statement_results_reporting_clinical_trials.pdf?ua=1

[74] Verordnung (EU) 2017/745 des Europäischen Parlaments und des Rates vom 5. April 2017 über Medizinprodukte, zur Änderung der Richtlinie 2001/83/EG, der Verordnung (EG) Nr. 178/2002 und der Verordnung (EG) Nr. 1223/2009 und zur Aufhebung der Richtlinien 90/385/EWG und 93/42/EWG des Rates. [Online, zitiert am 2019-10-01]; Verfügbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32017R0745

Festzuhalten ist, dass keine gesetzlichen Regelungen existieren, welche eine Veröffentlichung personenbezogener Daten fordert. Lediglich die Forschungsergebnisse selbst sollen oder – je nach Rechtslage - müssen veröffentlicht werden.

13 Spezielle Fragestellungen

13.1 EU Verordnung 536/2014 über klinische Prüfungen mit Humanarzneimitteln und das Verhältnis zur DS-GVO

Die europäische Verordnung Nr. 536/2014 des Europäischen Parlaments und des Rates v. 16. 4. 2014 über klinische Prüfungen mit Humanarzneimitteln und zur Aufhebung der RL 2001/20/EG[75], welche sechs Monate nach der Veröffentlichung der Funktionsfähigkeit des gemäß Art. 82 Abs. 3 einzurichtenden EU-Portals sowie der EU-Datenbank in Wirkung tritt (was wahrscheinlich 2020 geschieht[76]), enthält in Kapitel V Regelungen zum Schutz von Prüfungsteilnehmern sowie zur Einwilligung. Artikel 29 enthält Anforderungen bzgl. der Informationen, welche zwingend gegeben werden müssen und ist daher ergänzend zu Art. 7 DS-GVO zu betrachten. Zu beachten ist, dass EU VO 536/2014 noch eine schriftliche Information vorsieht.

Allerdings sieht Art. 29 die Möglichkeit vor, dass Mitgliedsstaaten für Prüfungen, die nur in ihrem Land durchgeführt werden, vereinfachte Verfahren zur Einwilligung vorsehen. Von dieser Möglichkeit machte die deutsche Regierung im „Vierten Gesetz zur Änderung arzneimittelrechtlicher und anderer Vorschriften[77]“ gebrauch, die entsprechenden Regelungen finden sich in § 40 Abs. 2a AMG.

EDSA veröffentlichte 2019 eine Stellungnahme bzgl. des Zusammenspiels von DS-GVO und der Verordnung 536/2014[78]. Darin hält EDSA fest, dass die DS-GVO und die Verordnung 536/2014 in keinem hierarchischen Verhältnis zueinander stehen, sondern parallel Anwendung finden. In ihrer Stellungnahme geht EDSA davon aus, dass während einer klinischen Studie nicht alle Verarbeitungstätigkeiten den gleichen Zwecken dienen und dementsprechend nicht alle auf den gleichen Erlaubnistatbestand gestützt werden. EDSA unterscheidet zwischen

- Verarbeitungsvorgänge zu Zwecken der Zuverlässigkeit und Sicherheit (Kap. 2.1 der Stellungnahme) und
- Ausschließlich Forschungstätigkeiten dienende Verarbeitungsvorgänge (Kapitel 2.2 der Stellungnahme).

Bei allen ausschließlich Forschungstätigkeiten dienende Verarbeitungsvorgänge empfiehlt EDSA in ihren Schlussfolgerungen drei alternative Rechtsgrundlagen erwägen:

- Wahrnehmung einer Aufgabe im öffentlichen
  oder

[75] Verordnung (EU) Nr. 536/2014 des Europäischen Parlaments und des Rates vom 16. April 2014 über klinische Prüfungen mit Humanarzneimitteln und zur Aufhebung der Richtlinie 2001/20/EG Text von Bedeutung für den EWR. [Online, zitiert am 2019-10-01]; Verfügbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32014R0536

[76] Clinical trials - Regulation EU No 536/2014 - EU Clinical Trial Portal and Database. [Online, zitiert am 2019-10-01]; Verfügbar unter https://ec.europa.eu/health/human-use/clinical-trials/regulation_en bzw. auch Clinical Trial Regulation – Implementation. [Online, zitiert am 2019-10-01]; Verfügbar unter https://www.ema.europa.eu/en/human-regulatory/research-development/clinical-trials/clinical-trial-regulation#implementation-section

[77] Viertes Gesetz zur Änderung arzneimittelrechtlicher und anderer Vorschriften. [Online, zitiert am 2019-10-01]; Verfügbar unter http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl116s3048.pdf

[78] Europäische Datenschutzausschuss (EDSA): Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR). [Online, zitiert am 2019-10-01]; Verfügbar unter https://edpb.europa.eu/our-work-tools/our-documents/avis-art-70/opinion-32019-concerning-questions-and-answers-interplay_en bzw. Direktlink zur dt. pdf-Datei https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinionctrq_a_final_de.pdf

- Wahrung der berechtigten Interessen des Verantwortlichen
  oder
- ausdrücklicher Einwilligung der betroffenen Person.

Der Regelfall bei klinischen Studien dürfte die ausdrückliche Einwilligung darstellen.

13.2 Studienzentren[79]

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, sodass Personal des Studienzentrums personenbeziehbare Daten verarbeitet. Hier kann es - je nach Konstellation - notwendig sein, dass z. B.

- 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).

[79] Dieser Text entstammt Kapitel 9.6 „Studienzentren“ der Praxishilfe „Datenschutzrechtliche Anforderungen an die medizinische Forschung unter Berücksichtigung der EU Datenschutz-Grundverordnung (DS-GVO“ von GDD und GMDS. [Online, zitiert am 2019-10-01]; Verfügbar unter https://ds-gvo.gesundheitsdatenschutz.org/html/forschung.php

14 Abkürzungen

Abs	Absatz
Art	Artikel
Artt	Artikel (Mehrzahl)
BDSG	Bundesdatenschutzgesetz
BfArM	Bundesinstitut für Arzneimittel und Medizinprodukte
BvD	Berufsverband der Datenschutzbeauftragten Deutschlands e. V.
bvitg	Bundesverband Gesundheits-IT e. V.
BVerfG	Bundesverfassungsgericht
DKG	Deutsche Krankenhausgesellschaft e. V.
DSFA	Datenschutz-Folgenabschätzung
DSG	Datenschutzgesetz
DSK	Datenschutzkonferenz
DS-GVO	Datenschutz-Grundverordnung
EDPB	European Data Protection BOARD (=EDSA)
EDSA	Europäischer Datenschutz-Ausschuss (= EDPB)
EDV	Elektronische Datenverarbeitung
ENISA	Europäische Agentur für Netz-und Informationssicherheit (European Union Agency for Cybersecurity)
ErwGr	Erwägungsgrund/Erwägungsgründe
EU	Europäische Union
GDD	Gesellschaft für Datenschutz und Datensicherheit e. V.
GG	Grundgesetz
GMDS	Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V.
IT	Informationstechnik, informationstechnisches…
Kap	Kapitel
LDSG	Landesdatenschutzgesetz
LKG	Landeskrankenhausgesetz
lit	littera (lat. „Buchstabe“)
pbD	Personenbezogene Daten
LKHG	Landeskrankenhausgesetz
ZEKO	Zentrale Ethikkommission
Ziff	Ziffer

15 Ergänzende Literatur

15.1 Fachzeitschriften

1) Bischoff C. (2019) Datenschutz im Rahmen klinischer Prüfungen – das Zusammenspiel der Verordnung über klinische Prüfungen und der Datenschutz-Grundverordnung. PharmR: 265-272
2) Bischoff C, Wiencke J. (2019) Datenschutzrechtliche Voraussetzungen klinischer Prüfungen. Das Verhältnis von AMG und DS-GVO. ZD: 8-13
3) Buchner B, Hase F, Borchers D, Pigeot I. (2019) Aufgaben, Regularien und Arbeitsweise von Ethikkommissionen. Bundesgesundheitsbl 62:690–696
4) Deutsch E. (2008) Entstehung und Funktion der Ethikkommissionen in Europa. MedR 26: 650−654
5) Dienemann S, Wachenhausen H. (2014) Alles neu, macht die EU – Die Verordnung über klinische Prüfungen und ihre Auswirkungen auf das deutsche Recht. PharmR: 452-459
6) Doppelfeld E. (2008) Mögliche neue Tätigkeitsfelder für Ethik-Kommissionen. MedR 26: 645−650
7) Doppelfeld E, Hasford J. (2019) Medizinische Ethikkommissionen in der Bundesrepublik Deutschland: Entstehung und Einbindung in die medizinische Forschung. Bundesgesundheitsbl 62:682–689
8) Eagleson et al. (2017) Implementation of clinical research trials using web-based and mobile devices: challenges and solutions. BMC Medical Research Methodology: 17:43
9) Geminn C. (2019) Wissenschaftliche Forschung und Datenschutz. Neuerungen durch die Datenschutz-Grundverordnung. DuD: 640-646
10) Geminn C. (2019) Die Forschungstätigkeit des Arztes im Spannungsfeld zur Schweigepflicht. RDV:116-122
11) Gödicke P. (2008) Berufsrechtliche Grundlagen für die Tätigkeit von Ethik-Kommissionen – überflüssige Zwangsberatung von Ärzten? MedR 26: 636−640
12) Graf von Kielmansegg S, Benda, N, Grass G, Sudhop T. (2019) Die Rolle von Ethikkommissionen bei der Bewertung klinischer Arzneimittelprüfungen. Bundesgesundheitsbl 62:706–712
13) Hasford J. (2017) Die EU-Verordnung 536/2014 und ihr Einfluss auf die Aufgaben und Arbeitsweisen der Ethikkommissionen in Deutschland. Bundesgesundheitsbl 60:830–835
14) Herbst T. (2009) Die Widerruflichkeit der Einwilligung in die Datenverarbeitung bei medizinischer Forschung. MedR 27: 149−152
15) Hüppe A, Dziubek K, Raspe H. (2014) Zum Verbesserungspotenzial schriftlicher Aufklärungsmaterialien zu (bio)medizinischen Forschungsvorhaben – Empirische Analyse von Antragsunterlagen einer Forschungsethikkommission. Ethik Med 26:211–224
16) Just H. (2008) Die Professionalisierung der Ethik-Kommissionen, einer Einrichtung der Selbstkontrolle der Wissenschaft. MedR 26: 640−645
17) Kern BR. (2006) Der postmortale Geheimnisschutz. MedR: 205-208
18) Kern BR (2008) Standortbestimmung: Ethikkommissionen – auf welchen Gebieten werden sie tätig? MedR 26: 631−636
19) Lanzerath D. (2019) Europäische Ethikkommissionen im Wandel: Herausforderungen durch neue Rahmenbedingungen. Bundesgesundheitsbl 62:697–705
20) Lippert HD. (2013) Das Patientenrechtegesetz und die biomedizinische Forschung – wird die Forschung etwa stiefmütterlich behandelt? MedR 31: 714–718
21) Miller JD. (2010) Sharing clinical research data in the United States under the health insurance portability and accountability act and the privacy rule. Trials 11:112

22) Pigeot et al. (2019) Ethische Bewertung von Studien am Menschen außerhalb des regulatorischen Rahmens: nicht bindend, aber von großer Wichtigkeit. Bundesgesundheitsbl 62:722–728
23) Rauch et al. (2019) Aktuelle Herausforderungen bei der Bewertung von Ethikanträgen – Aspekte der Digitalisierung und Personalisierung im Gesundheitswesen. Bundesgesundheitsbl 62:758–764
24) Richter G, Buyx A. (2016) Breite Einwilligung (broad consent) zur Biobank-Forschung – die ethische Debatte. Ethik Med 28:311–325
25) Ritter C. (2007) Aufgaben der öffentlich-rechtlichen Ethikkommissionen in der Bundesrepublik Deutschland. Rechtsmedizin 17:225–233
26) Röcken et al. (2013) Beteiligung und Unterstützung klinischer Studien und anderer wissenschaftlicher Untersuchungen - Stellungnahme der Deutschen Gesellschaft für Pathologie e. V. Pathologe 34:466–475
27) Rösler F. (2019) Ethikvoten in der psychologischen Forschung. Bundesgesundheitsbl 62:729–737
28) Röhrig B, du Prel JB, Wachtlin D, Blettner M. (2009) Studientypen in der medizinischen Forschung. Dtsch Arztebl 106(15): 262-268
29) Rossnagel A. (2019) Datenschutz in der Forschung. Die neuen Datenschutzregelungen in der Forschungspraxis von Hochschulen. ZD: 157-164
30) Rütsche B. (2014) Das Recht der biomedizinischen Forschung am Menschen: Nationales Recht im Spiegel internationaler Prinzipien. MedR 32: 725–732
31) Schaar K. (2017) Anpassung von Einwilligungserklärungen für wissenschaftliche Forschungsprojekte. Die informierte Einwilligung nach der DS-GVO und den Ethikrichtlinien. ZD: 213-220
32) Schütz H, Heinrichs B, Fuchs M, Bauer A. (2016) Informierte Einwilligung in der Demenzforschung. Eine qualitative Studie zum Informationsverständnis von Probanden. Ethik Med 28:91–106
33) Spranger TM, Schulz, T. (2017) Auswirkungen der Datenschutz-Grundverordnung auf die pharmazeutische Forschung. PharmR: 128-131
34) Swart E, Stallmann C, Powietzka J, March S. (2014) Datenlinkage von Primär- und Sekundärdaten. Bundesgesundheitsbl 57:180–187
35) Taupitz J. (2012) Medizinische Forschung an jungen und alten Patienten. MedR 30: 583–588
36) Thüsing G, Rombey S. (2019) Forschung im Gesundheitswesen: Anforderungen an einen passgenauen Datenschutz. NZS: 201-205
37) Tucker et al. (2016) Protecting patient privacy when sharing patient-level data from clinical trials. BMC Medical Research Methodology 16(Suppl 1):77
38) Vonthein R. (2019) Besonderheiten von Medizinproduktstudien bei der Bewertung und Beratung durch Ethikkommissionen. Bundesgesundheitsbl 62:713–721
39) Werkmeister C, Schwaab M. (2019) Auswirkungen und Reichweite des datenschutzrechtlichen Forschungsprivilegs. CR: 85-90
40) Weisser R, Bauer A. (2005) Datenschutz bei internationalen klinischen Studien1. MedR: 339-346
41) Winkler et al. (2013) Personalisierte Medizin und Informed Consent: Klinische und ethische Erwägungen im Rahmen der Entwicklung einer Best Practice Leitlinie für die biobankbasierte Ganzgenomforschung in der Onkologie. Ethik Med 25:195–203
42) Woellert K. (2019) Das Klinische Ethikkomitee: Ziele, Strukturen und Aufgaben Klinischer Ethik. Bundesgesundheitsbl 62:738–743

15.2 Bücher

1) Bohnet-Joschko S, Zippel C, Krummenauer F. Sichtbarwerdung klinischer Studien von und mit Medizinprodukten: Entwicklung im Spiegel des Deutschen Registers für Klinische Studien. Springer Fachmedien Wiesbaden, 1. Auflage 2018. ISBN 978-3-658-15986-3
2) Ceylan R, Sajak CP (Hrsg.) Freiheit der Forschung und Lehre? Das wissenschaftsorganisatorische Verhältnis der Theologie zu den Religionsgemeinschaften. Springer Fachmedien Wiesbaden, 1. Auflage 2017. ISBN 978-3-658-14897-3
3) Deutsch et al. Hrsg.) Die Implementierung der GCP-Richtlinie und ihre Ausstrahlungswirkungen. Springer-Verlag Berlin Heidelberg, 1. Auflage 2011. ISBN 978-3-642-13176-9
4) Kandler HC. Rechtliche Rahmenbedingungen biomedizinischer Forschung am Menschen. Das Zusatzprotokoll zum Übereinkommen über Menschenrechte und Biomedizin über biomedizinische Forschung. Springer-Verlag Berlin Heidelberg, 1. Auflage 2008. ISBN 978-3-540-75515-9
5) Karaalp RM. Der Schutz von Patientendaten für die medizinische Forschung in Krankenhäusern. Eine rechtsvergleichende Untersuchung der Regelungen in Deutschland und Frankreich. Springer Fachmedien Wiesbaden GmbH, 1. Auflage 2017. ISBN 978-3-658-16184-2
6) Lenk C, Duttge G, Fangerau H. (Hrsg.) Handbuch Ethik und Recht der Forschung am Menschen. Springer-Verlag Berlin Heidelberg, 1. Auflage 2014. ISBN 978-3-642-35098-6
7) Listl S. Die zivilrechtliche Haftung für Fehler von Ethikkommissionen. Springer-Verlag Berlin Heidelberg, 1. Auflage 2012. ISBN 978-3-642-21240-6
8) Pramann O. Publikationsklauseln in Forschungsvertragen und Forschungsprotokollen klinischer Studien. Springer-Verlag Berlin Heidelberg, 1. Auflage 2007. ISBN 978-3-540-69569-1
9) Reimer F. Die Forschungsverfügung. Eine Untersuchung zu antizipierten Verfügungen in der Humanforschung unter besonderer Berücksichtigung der Arzneimittelforschung mit Demenz- und Notfallpatienten. Springer-Verlag Berlin Heidelberg, 1. Auflage 2017. ISBN 978-3-662-53261-4
10) Schumacher M, Schulgen G. Methodik klinischer Studien. Methodische Grundlagen der Planung, Durchführung und Auswertung. Springer-Verlag Berlin Heidelberg, 2. Auflage 2007. ISBN-10 3-540-36989-9
11) Sprecher F. Medizinische Forschung mit Kindern und Jugendlichen nach schweizerischem, deutschem, europäischem und internationalem Recht. Springer-Verlag Berlin Heidelberg, 1. Auflage 2007. ISBN 978-3-540-73757-5
12) Vogeler M. Ethik-Kommissionen – Grundlagen, Haftung und Standards. Springer-Verlag Berlin Heidelberg, 1. Auflage 2011. ISBN 978-3-642-17949-5
13) von Freier, F. Recht und Pflicht in der medizinischen Humanforschung. Zu den rechtlichen Grenzen der kontrollierten Studie. Springer-Verlag Berlin Heidelberg, 1. Auflage 2009. ISBN 978-3-540-95876-5
14) Weigel J. Das Biobankgeheimnis. Tectum Baden-Baden, 1. Auflage 2018. ISBN 978-3-8288-3990-8

Anhang 1. Begriffsbestimmungen

Anhang 1.1 Personenbezogene Daten[80]

Entsprechend Art. 4 Ziff. 1 DS-GVO sind personenbezogene Daten „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen“. Damit fallen nicht nur Informationen darunter, welche direkt eine Person identifizieren, sondern auch alle Informationen, welche über Zwischenschritte eine Person identifizieren. D. h. soweit und solange die Informationen aus sich heraus Rückschluss auf eine einzelne Person zulassen, handelt es sich um Daten einer bestimmten Person.

Der Begriff „identifizierbar“ muss daher im Sinne von „als Einzelperson wahrnehmbar“ bzw. einer „Einzelperson zuordenbar“ verstanden werden.

Die Identifizierbarkeit ist damit Dreh- und Angelpunkt hinsichtlich der Beurteilung, ob Daten als anonym oder pseudonym angesehen werden können.

Anhang 1.2 Gesundheitsdaten[81]

Gesundheitsdaten werden nach der Verordnung als personenbezogene Daten definiert, „*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*“. Die Verordnung verwendet mithin eine ziemlich weite Definition der Gesundheitsdaten.

Diesbezüglich empfiehlt es sich, ergänzend auch den Erwägungsgrund 35 einzubeziehen. Dieser führt weitere Bereiche auf, in denen Gesundheitsdaten verarbeitet werden. So gilt gemäß dieses Erwägungsgrunds „*zu den personenbezogenen Gesundheitsdaten sollten alle Daten zählen, die sich auf den Gesundheitszustand einer betroffenen Person beziehen und aus denen Informationen über den früheren, gegenwärtigen und künftigen körperlichen oder geistigen Gesundheitszustand der betroffenen Person hervorgehen. Dazu gehören auch Informationen über die natürliche Person, die im Zuge der Anmeldung für sowie der Erbringung von Gesundheitsdienstleistungen im Sinne der Richtlinie 2011/24/EU des Europäischen Parlaments und des Rates für die natürliche Person erhoben werden, Nummern, Symbole oder Kennzeichen, die einer natürlichen Person zugeteilt wurden, um diese natürliche Person für gesundheitliche Zwecke eindeutig zu identifizieren, Informationen, die von der Prüfung oder Untersuchung eines Körperteils oder einer körpereigenen Substanz, auch aus genetischen Daten und biologischen Proben, abgeleitet wurden, und Informationen etwa über Krankheiten, Behinderungen, Krankheitsrisiken, Vorerkrankungen, klinische Behandlungen oder den physiologischen oder biomedizinischen Zustand der betroffenen Person unabhängig von der Herkunft der Daten, ob sie nun von einem Arzt oder sonstigem Angehörigen eines Gesundheitsberufes, einem Krankenhaus, einem Medizinprodukt oder einem In-vitro-Diagnostikum stammen.*“

[80] Zitiert aus: GMDS, GDD „Arbeitshilfe zur Pseudonymisierung/Anonymisierung“ (Stand 29. Juni 2018) [Online, zitiert am 2019-11-05]; Verfügbar unter https://gesundheitsdatenschutz.org/html/pseudonymisierung_anonymisierung.php

[81] Zitiert aus: bvitg, GMDS „Gemeinsame Empfehlung bzgl. des Umgangs mit der EU Datenschutz-Grundverordnung (DS-GVO) im Gesundheitswesen“ (Stand 01.07.2016) [Online, zitiert am 2019-11-05]; Verfügbar unter https://gesundheitsdatenschutz.org/html/umsetzungshilfe.php

Zusammenfassend lässt sich deshalb feststellen, dass der Definition der DS-GVO folgend, sehr viele Daten, denen man unmittelbar keinen Gesundheitsbezug ansehen würde, aufgrund der Möglichkeit der Kombination mit anderen Daten, schnell einen Gesundheitsbezug „erben“ können.

Anhang 1.3 Genetische Daten[81]

Art. 4 Abs. 13 führt aus: genetische Daten sind „personenbezogene Daten

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

D. h. unter genetische Daten werden alle Arten von Informationsträgern erfasst, die ererbte oder erworbene genetische Informationen zu einer natürlichen Person enthalten und aus denen Informationen bzgl. Physiologie und/oder Gesundheit gewonnen werden können.

Damit umfasst der Begriff der genetischen Daten natürlich neben den „klassischen“ Proben einer Biomaterialbank auch andere Materialien, die innerhalb der Gesundheitsversorgung von einem Patienten gewonnen werden wie beispielsweise Blutproben.

Die Artikel-29-Datenschutzgruppe äußerte sich zu diesem Thema bereits 2004 in WP 91[82] und bezog bei der Interpretation auch die Definition der UNESCO[83] mit ein. Zu den aus dem Material gewinnbaren Informationen, die bei der Beurteilung „genetisches Datum ja/nein“, berücksichtigt werden müssen, zählen demnach insbesondere

- Biologische Abstammung
- Krankheitsdispositionen
- Informationen über gewisse Besonderheiten /Fähigkeiten
- Informationen über Lebensumstände.

Diese Art von Informationen behalten zudem über lange Zeiträume ihre Gültigkeit und ermöglichen sogar Aussagen über zukünftige Entwicklungen. Weiterhin können die darin implizit enthaltenen Informationen eine Bedeutung von erheblicher Tragweite für das Leben des Betroffenen sowie naher Anverwandter beinhalten. Eine Speicherung und spätere Auswertung genetischer Daten kann sogar heute noch ungeborene Personen berühren. Z. B. wenn aufgrund der heute gewonnenen genetischen Daten einer Person in 60 Jahren bei einem Enkel der Person eine (heute evtl. noch unbekannte) Erkrankung offenbart wird, die zur Stigmatisierung und Ausgrenzung führt. Daher beinhalten genetische Daten oftmals nicht nur Informationen zu einer Person und es stellt sich immer die Frage, in wieweit eine Person bei einer Einwilligung bzgl. der Verarbeitung genetischer Daten auch für andere betroffene Personen (Eltern, Kinder, Geschwister, ...) einwilligen kann.

[82] Artikel-29-Datenschutzgruppe (2004) Arbeitspapier über genetische Daten. [Online, zitiert am 2019-11-17]; Verfügbar unter http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp91_de.pdf

[83] United Nations Educational, Scientific and Cultural Organization (2003) International Declaration on Human Genetic Data. [Online, zitiert am 2019-11-17]; Verfügbar unter http://unesdoc.unesco.org/images/0013/001331/133171e.pdf#page=45

Anhang 1.4 Verantwortlicher[81]

Der „Verantwortliche“ wird von der Verordnung definiert als „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“.

Die Bestimmung der Verantwortlichkeit ist maßgeblich für die nach der DS-GVO zu erfüllenden Pflichten. Aus diesem Grund ist es erforderlich, gerade bei Sachverhalten, in denen viele Beteiligte eine gewisse Rolle bei der Datenverarbeitung spielen, zu entscheiden, wer eigentlich für welche Datenverarbeitung die Verantwortung trägt.

Dazu ist es entscheidend, abzugrenzen, wer von den jeweils Beteiligten im jeweiligen Einzelsachverhalt über die Mittel und Zwecke der Datenverarbeitung entscheidet. Gerade bei Datenverarbeitungen, die ausgelagert (z. B. in einer „Cloud“ eines externen Anbieters) erfolgen, ist dies nicht immer trivial, aber dennoch zwingend erforderlich.

Grundsätzlich macht es dem Gesetzeswortlaut der Verordnung nach zunächst keinen Unterschied, ob es sich um einen öffentlichen oder privaten Verantwortlichen handelt. Für beide gilt prinzipiell gleiches Recht und deshalb müssen sie grundsätzlich auch die gleichen Pflichten / Anforderungen erfüllen.

Der Arbeitskreis Medizinischer Ethik-Kommissionen in der Bundesrepublik Deutschland e.V. schreibt in seiner Handreichung bzgl. DS-GVO zum Verantwortlichen[8] dazu:

> „‘Verantwortlicher‘ ist primär der Sponsor oder die studienleitende Einrichtung. Bei multizentrischen Studien ist das teilnehmende Zentrum grundsätzlich ebenfalls ein Verantwortlicher. Damit liegt ein Fall gemeinsamer oder komplementärer Verantwortung gem. Art. 26 DSGVO vor. In den Fällen, in denen die Forscher nur einen sehr engen Handlungsspielraum haben, könnte die Beziehung zwischen dem Auftraggeber und den Studienzentren auch als schlichte Auftragsverarbeitung auszugestalten sein (vgl. WP 169 der Artikel-29-Datenschutzgruppe) – mit entsprechender Auswirkung auf den Drittmittelvertrag. Bei Arzneimittelprüfungen wird dies jedoch eine seltene Ausnahme sein.“

Anhang 1.5 Auftragsverarbeiter

Um einen „Auftragsverarbeiter“ handelt es sich laut der Legaldefinition des Art. 4 Nr. 8 DS-GVO, wenn eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

Anhang 1.6 Verarbeitung

Die DS-GVO definiert im Art. 4 Nr. 2 den Begriff der Verarbeitung. Grundsätzlich besitzt die Verarbeitung personenbezogener Daten folgende Merkmale:

- sie erfolgt ganz, teilweise oder nicht-automatisiert
- sind bereits in einem Dateisystem gespeichert bzw. sollen zukünftig gespeichert werden

Der Begriff der „Verarbeitung“ erfasst als Oberbegriff alle Arten des „Datenumgangs“. So erfasst er:

- *das Erheben,*
- *das Erfassen,*
- *die Organisation,*
- *das Ordnen,*
- *die Speicherung,*

- *die Anpassung oder Veränderung,*
- *das Auslesen,*
- *das Abfragen,*
- *die Verwendung,*
- *die Offenlegung durch Übermittlung,*
- *die Verbreitung oder eine andere Form der Bereitstellung,*
- *den Abgleich oder die Verknüpfung,*
- *die Einschränkung* (in Deutschland auch bekannt als „Sperrung"),
- *das Löschen oder etwa die Vernichtung*.

Anhang 1.7 Profiling

Im Art. 4 Nr. 4 DS-GVO wird der Begriff Profiling definiert. Profiling stellt eine besondere Art der Verarbeitung dar. Dabei werden personenbezogene Daten automatisiert verarbeitet und für die Bewertung, Analyse oder Vorhersage bestimmter persönlicher Aspekte verwendet. Diese Aspekte werden nicht abschließend aufgeführt, Beispiele sind u.a. Gesundheit, persönliche Vorlieben, Verhalten oder Arbeitsleistung.

Anhang 1.8 Gemeinsam Verantwortliche[84]

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

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

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

Um den Vorgaben von Art. 26 DS-GVO zu genügen, ist es daher unabdingbar, dass die jeweiligen an der gemeinsamen Verarbeitung beteiligten Parteien auch tatsächlich über die Zwecke und Mittel entscheiden bzw. entscheiden können; eine weisungsgebundene Tätigkeit wird somit nicht adressiert. Nicht zu dieser Regelung hingegen zählen Vorgänge, bei denen mehrere Verarbeitungen mit jeweils selbstständigen Verantwortlichkeiten nebeneinander vorliegen.

Der Arbeitskreis Medizinischer Ethik-Kommissionen in der Bundesrepublik Deutschland e.V. schreibt in seiner Handreichung bzgl. DS-GVO zum Verantwortlichen[8] dazu:

[84] Zitiert aus: GMDS „Art. 26 DS-GVO: Gemeinsam Verantwortliche" (Stand 17. Juni 2018) [Online, zitiert am 2019-11-05]; Verfügbar unter https://gesundheitsdatenschutz.org/html/gemeinsam_verantwortlich.php

„‘Verantwortlicher‘ ist primär der Sponsor oder die studienleitende Einrichtung. Bei multizentrischen Studien ist das teilnehmende Zentrum grundsätzlich ebenfalls ein Verantwortlicher. **Damit liegt ein Fall gemeinsamer oder komplementärer Verantwortung gem. Art. 26 DSGVO vor. In den Fällen, in denen die Forscher nur einen sehr engen Handlungsspielraum haben, könnte die Beziehung zwischen dem Auftraggeber und den Studienzentren auch als schlichte Auftragsverarbeitung auszugestalten sein** (vgl. WP 169 der Artikel-29-Datenschutzgruppe) – mit entsprechender Auswirkung auf den Drittmittelvertrag. Bei Arzneimittelprüfungen wird dies jedoch eine seltene Ausnahme sein.“

Anhang 1.9 „Forschung“ aus Sicht der DS-GVO[85]

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.“

Anhang 1.10 „Wissenschaftliche Forschung“ aus Sicht der DS-GVO[85]

Die wissenschaftliche Forschung ist ein spezieller Bereich der Forschung. Im „Hochschul-Urteil[86]“ 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:

---

[85] Zitiert aus: GMDS, GDD „Datenschutzrechtliche Anforderungen an die medizinische Forschung unter Berücksichtigung der EU Datenschutz-Grundverordnung (DS-GVO)“ (Stand 15.05.2017) [Online, zitiert am 2019-11-05]; Verfügbar unter https://gesundheitsdatenschutz.org/html/forschung.php

[86] BVerfG, Urteil vom 29.05.1973, AZ.: 1 BvR 424/71 bzw 1 BvR 325/72 (Hochschul-Urteil). [Online, zitiert am 2019-09-17]; 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

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

Anhang 1.11 Klinische Studie

Laut Art. 2 Ziff. 2 EU Verordnung 536/2014[87] ist unter einer „klinischen Studie“

„jede am Menschen durchgeführte Untersuchung, die dazu bestimmt ist,

a) die klinischen, pharmakologischen oder sonstigen pharmakodynamischen Wirkungen eines oder mehrerer Arzneimittel zu erforschen oder zu bestätigen,
b) jegliche Nebenwirkungen eines oder mehrerer Arzneimittel festzustellen oder
c) die Absorption, die Verteilung, den Stoffwechsel oder die Ausscheidung eines oder mehrerer Arzneimittel zu untersuchen,

mit dem Ziel, die Sicherheit und/oder Wirksamkeit dieser Arzneimittel festzustellen“,

zu verstehen. Im klinischen Alltag wird der Begriff weiter ausgelegt und nicht nur auf Medikamente, sondern auch andere Behandlungsformen, medizinische Interventionen oder auch Medizinprodukte angewendet.

Im Rahmen dieser Ausarbeitung ist unter „klinischer Studie daher zu verstehen:

Jede am Patienten durchgeführte oder unter Zuhilfenahme von Patientendaten durchgeführte wissenschaftliche Untersuchung, die dazu bestimmt ist,

a) die klinischen, pharmakologischen oder sonstigen Wirkungen einer oder mehrerer medizinischer Behandlungsformen zu erforschen oder zu bestätigen sowie
b) jegliche Nebenwirkungen einer oder mehrerer Behandlungsformen festzustellen

mit dem Ziel, die Sicherheit und/oder Wirksamkeit dieser Behandlungsform festzustellen. Zu den Behandlungsformen zählen alle von der Schulmedizin anerkannten Behandlungsformen wie medikamentöse Therapien, medizinische Interventionen oder auch alle Methoden unter dem Einsatz von Medizinprodukten.

Anhang 1.12 Öffentliches Interesse[85]

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[88] kann man von einem öffentlichen Interesse ausgehen, wenn

a) das Vorhaben ein gegenwärtiges Anliegen der Allgemeinheit beinhaltet oder
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

[87] Verordnung (EU) Nr. 536/2014 des Europäischen Parlaments und des Rates vom 16. April 2014 über klinische Prüfungen mit Humanarzneimitteln und zur Aufhebung der Richtlinie 2001/20/EG Text von Bedeutung für den EWR. [Online, zitiert am 2019-09-17]; Verfügbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32014R0536

[88] Richtlinien für das Strafverfahren und das Bußgeldverfahren. Abschnitt 86 – Allgemeines. [Online, zitiert am 2019-09-17]; Verfügbar unter Verfügbar unter https://www.jurion.de/

Spendenaufkommen bei der Deutschen Krebshilfe[89] (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[90]).

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[91]. 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[91].

Anhang 1.13 Öffentliches Interesse i. V. m. öffentlicher Gesundheit[85]

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) 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:

---

[89] deutsche Krebshilfe: Geschäftsbericht. [Online, zitiert am 2019-09-17]; Verfügbar unter https://www.krebshilfe.de/

[90] Vgl. z.B. BVerwG, Urteil vom 24.09.1998, AZ.: 4 CN 2.98. [Online, zitiert am 2019-09-17]; 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/

[91] Metschke R, Wellbrock R. (2002) Datenschutz in Wissenschaft und Forschung. [Online, zitiert am 2019-09-17]; Verfügbar unter https://datenschutz-berlin.de/

„[...] 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".

Anhang 1.14 Erforderlichkeit, Notwendigkeit[85]

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?

Anhang 1.15 Interessenabwägung[85]

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)[92]. 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.

[92] Bundesgerichtshof Urt. v. 17.12.1985, Az.: VI ZR 244/84 [Online, zitiert am 2019-09-17]; Verfügbar unter http://dejure.org/

„Dabei sind Art, Inhalt und Aussagekraft der beanstandeten Daten an den Aufgaben und Zwecken zu messen, denen ihre Speicherung dient[93].

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“[94]. 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[94].

Bei der Darstellung der Betroffeneninteressen kann die Sphärentheorie[95,96] 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.

Anhang 1.16 Pseudonymisierung[80]

Der Begriff der Pseudonymisierung wird in Art. 4 Ziff. 5 DS-GVO definiert. Dort heißt es:

> „"Pseudonymisierung" 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“.

Dieser Definition folgend charakterisiert eine Pseudonymisierung daher Nachfolgendes:

- Die Pseudonymisierung ist eine Verarbeitung personenbezogener Daten.
- Pseudonyme Daten sind Daten, die ohne weitere Informationen einer spezifischen Person nicht zuordenbar sind.
- Die zur Zuordenbarkeit benötigten Informationen stehen dem Verantwortlichen nicht zur Verfügung, sondern
  - werden gesondert aufbewahrt und
  - sind durch technische und organisatorische Maßnahmen vor dem Zugriff durch den Verantwortlichen geschützt.

[93] Bundesgerichtshof Urt. v. 17.12.1985, Az.: VI ZR 244/84, Rn. 13 [Online, zitiert am 2019-09-17]; Verfügbar unter https://www.jurion.de/
[94] BeckOK DatenSR/von Lewinski BDSG § 10 Rn. 23-29
[95] BeckOK DatenSR/Wolff BDSG § 28 Rn. 64-70
[96] BVerfG Urteil vom 31.01.1973, AZ.: 2 BvR 454/71 [Online, zitiert am 2019-09-17]; Verfügbar unter http://dejure.org/ Az.: IV ZR 129/09 Online, zitiert am 2016-12-04; Verfügbar unter https://dejure.org/

→ Für den Verantwortlichen besteht bei der Verarbeitung pseudonymisierter Daten keine Möglichkeit der Identifizierung der betroffenen Person.

Hinweis: ErwGr. 26 führt aus, dass zur Feststellung, ob eine natürliche Person identifizierbar ist, alle Mittel berücksichtigt werden sollten, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren.
Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind.

Anhang 1.17 Pseudonyme Daten[80]

Entsprechend der in der DS-GVO enthaltenen Definition von Pseudonymisierung sind demnach pseudonyme Daten solche Daten, welche der oder die Verantwortlichen keiner spezifischen Person zuordnen können, jedoch für andere durch die Einbeziehung weitergehender Informationen („Zuordnungsregeln“) die grundsätzliche Möglichkeit der Zuordnung besteht. Dafür ist es nicht erforderlich, dass die betroffene Person durch die „Re-Identifizierung“ mit bürgerlichem Namen zu identifizieren ist[97]. Ausreichend ist vielmehr, wenn durch das Datum bzw. die Daten die betroffene Person individualisiert wird und Aussagen über deren sachliche und persönliche Verhältnisse möglich sind; ein Name muss nicht vorhanden sein[98].

Anhang 1.18 Anonyme Daten[80]

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

Daraus ergibt sich im Umkehrschluss, dass anonyme Daten weder direkt personenbezogene Daten noch pseudonymisierte Daten sein können. D. h., anonyme Daten sind Daten, bei denen keine Zuordnungsmöglichkeit zu einer spezifischen betroffenen Person existiert[99].

Hinweis: Anders als im BDSG a.F. bedeutet „anonym“ unter der DS-GVO, dass keine Möglichkeit zur Re-Identifikation besteht; eine Abwägung wie in § 3 Ziff. 6 BDSG a.F. „[…] oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft […]“ ist unter der DS-GVO nicht vorgesehen. Daher gilt, dass wenn eine Möglichkeit der Zuordnung der Daten zu einer spezifischen betroffenen Person existiert, die Daten keine anonymen Daten sind.

[97] Karg M. (2015) Anonymität, Pseudonyme und Personenbezug revisited. DuD: 520-526

[98] Artikel-29-Datenschutzgruppe. WP 136 „Stellungnahme 4/2007 zum Begriff 'personenbezogene Daten'“, S. 16: […] ein Name zur Identifizierung einer Person jedoch keineswegs immer notwendig ist“. [Online, zitiert am 2018-04-24]; Verfügbar unter http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf

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

Anhang 1.19 Anonymisierung[80]

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

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

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

Anhang 2. Internetadressen der Landeskrankenhausgesetze

- Landeskrankenhausgesetz Baden-Württemberg
  http://www.landesrecht-bw.de/jportal/?quelle=jlink&query=KHG+BW&psml=bsbawueprod.psml&max=true
- Bayerisches Krankenhausgesetz
  http://www.gesetze-bayern.de/Content/Document/BayKrG
- Landeskrankenhausgesetz Berlin
  http://gesetze.berlin.de/jportal/?quelle=jlink&query=KHG+BE&psml=bsbeprod.psml&max=true
- Gesetz zur Entwicklung der Krankenhäuser im Land Brandenburg
  http://bravors.brandenburg.de/de/gesetze-212704
- Brandenburgisches Datenschutzgesetz
  https://bravors.brandenburg.de/gesetze/bbgdsg
- Bremisches Krankenhausdatenschutzgesetz
  http://transparenz.bremen.de/sixcms/detail.php?gsid=bremen2014_tp.c.68007.de&asl=bremen203_tpgesetz.c.55340.de&template=20_gp_ifg_meta_detail_d
- Hamburgisches Krankenhausgesetz
  http://www.landesrecht-hamburg.de/jportal/portal/page/bshaprod.psml?showdoccase=1&st=lr&doc.id=jlr-KHGHArahmen
- Zweites Gesetz zur Weiterentwicklung des Krankenhauswesens in Hessen
  https://www.rv.hessenrecht.hessen.de/bshe/document/jlr-KHGHE2011V8IVZ
- Hessisches Datenschutz- und Informationsfreiheitsgesetz (HDSIG)
  https://www.rv.hessenrecht.hessen.de/bshe/document/jlr-DSIFGHEV1IVZ
- Krankenhausgesetz für das Land Mecklenburg-Vorpommern
  http://www.landesrecht-mv.de/jportal/portal/page/bsmvprod.psml?showdoccase=1&doc.id=jlr-LKHGMV2011rahmen
- Niedersächsisches Datenschutzgesetz
  http://www.voris.niedersachsen.de/jportal/?quelle=jlink&query=DSG+ND&psml=bsvorisprod.psml&max=true
- Gesetz zum Schutz personenbezogener Daten im Gesundheitswesen Nordrhein-Westfalen
  https://recht.nrw.de/lmi/owa/br_text_anzeigen?v_id=10000000000000000495
- Landeskrankenhausgesetz Rheinland-Pfalz
  http://landesrecht.rlp.de/jportal/portal/t/15bc/page/bsrlpprod.psml?doc.hl=1&doc.id=jlr-KHGRPrahmen&documentnumber=3&numberofresults=52&doctyp=Norm&showdoccase=1&doc.part=R&paramfromHL=true#focuspoint
- Saarländisches Krankenhausgesetzes
  http://sl.juris.de/cgi-bin/landesrecht.py?d=http://sl.juris.de/sl/KHG_SL_2015_rahmen.htm
- Sächsisches Krankenhausgesetz
  http://www.revosax.sachsen.de/vorschrift/1051-Saechsisches-Krankenhausgesetz
- Krankenhausgesetz Sachsen-Anhalt
  http://www.landesrecht.sachsen-anhalt.de/jportal/?quelle=jlink&query=KHG+ST&psml=bssahprod.psml&max=true
- Thüringer Krankenhausgesetz
  http://landesrecht.thueringen.de/jportal/?quelle=jlink&query=KHG+TH&psml=bsthueprod.psml&max=true

Anhang 3. DS-GVO Checkliste

	Verantwortliche/r (Erläuterung: s. u.)	Ja	Nein	Nachweis vorhanden und überprüfbar
(Verarbeitungs-) Zweck der Klinischen Studie beschrieben?	PV			
Lässt sich die Erforderlichkeit aller verarbeiteten Daten aus dem Zweck ableiten und wurde dies dokumentiert?	PV			
Ist die Rechtsgrundlage für die Verarbeitung geklärt und dokumentiert?	PV+JU			
Wird „Broad Consent“ genutzt? Wenn ja: Sind alle Voraussetzungen erfüllt und insbesondere entsprechende technische und organisatorische Maßnahmen vorhanden?	PV+DB			
Ist eine Sekundärnutzung von Daten gegeben? Wenn ja: Erfolgte eine Information der betroffenen Personen?	PV+DB			
Sind alle Betroffenenrechte berücksichtigt worden?	PV+DB			
Existiert ein Informationsschreiben, welches alle gesetzlich geforderten Informationen enthält und ist ein Prozess etabliert und dokumentiert, welcher gewährleistet, dass jede Person dieses Schreiben erhält?	PV+DB			
Ist ein Prozess etabliert und dokumentiert, welcher den Umgang mit Auskunftsanfragen regelt?	PV+DB			
Ist ein Prozess etabliert und dokumentiert, welcher den Umgang mit Anfragen bzgl. Korrektur der Daten regelt?	PV+DB			
Ist ein Prozess etabliert und dokumentiert, welcher den Umgang mit einem Widerspruch bzgl. der Verarbeitung personenbezogener Daten regelt?	PV+DB			
Ist ein Prozess etabliert und dokumentiert, welcher den Umgang mit Aufforderungen zur Einschränkung der Verarbeitung („Sperrung“) regelt?	PV+DB			
Ist ein Prozess etabliert und dokumentiert, welcher den Umgang mit Löschanfragen regelt?	PV+DB			
Ist ein Prozess etabliert und dokumentiert, welcher den Umgang mit Anfragen bzgl. der Wahrnehmung des Rechts auf Datenübertragbarkeit regelt?	PV+DB			
Existiert ein Verzeichnis der Verarbeitungstätigkeiten?	PV+DB			
Sind alle Auftragsverarbeiter gelistet und existieren die erforderlichen Verträge?	PV+DB			
Sind alle Auftragsverarbeiter ggf. vertraglich	PV+DB			

	Verantwortliche/r (Erläuterung: s. u.)	Ja	Nein	Nachweis vorhanden und überprüfbar
verpflichtet, die berufliche Schweigepflicht und das strafrechtliche Offenbarungsverbot einzuhalten?				
Sind die Anforderungen bzgl. der Sicherheit der Verarbeitung erfüllt?	PV+IT +DB			
Ist Pivacy by Design für die klinische Studie berücksichtigt und kann nachgewiesen werden?	PV+IT +DB			
Ist Pivacy by Default für die klinische Studie berücksichtigt und kann nachgewiesen werden?	PV+IT +DB			
Wurde die Notwendigkeit bzgl. einer DSFA geprüft und das Ergebnis festgehalten? Wurde bei positivem Ergebnis eine DSFA durchgeführt?	PV+IT +DB			
Wurde der Lebenszyklus der Daten beschrieben? Inklusive Löschzeitpunkt?	PV+DB			
Existiert ein Datenschutzkonzept? Wenn nein: Wurde nachvollziehbar dargelegt und dokumentiert, warum dies nicht erforderlich ist?	PV+DB			
Existiert ein Berechtigungskonzept für den Zugriff auf die Daten? Wenn nein: Wurde nachvollziehbar dargelegt und dokumentiert, warum dies nicht erforderlich ist?	PV+IT +DB			
Existiert ein Archivierungskonzept? Wenn nein: Wurde nachvollziehbar dargelegt und dokumentiert, warum dies nicht erforderlich ist?	PV+IT +DB			
Existiert ein Löschkonzept? Wenn nein: Wurde nachvollziehbar dargelegt und dokumentiert, warum dies nicht erforderlich ist?	PV+IT +DB			
Existiert ein IT-Sicherheitskonzept? Wenn nein: Wurde nachvollziehbar dargelegt und dokumentiert, warum dies nicht erforderlich ist?	PV+IT +DB			
Existiert ein Backupkonzept? Wenn nein: Wurde nachvollziehbar dargelegt und dokumentiert, warum dies nicht erforderlich ist?	PV+IT +DB			
Existiert ein Protokollierungskonzept? Wenn nein: Wurde nachvollziehbar dargelegt und dokumentiert, warum dies nicht erforderlich ist?	PV+IT +DB			
Sind interne Audits zur Überprüfung der	PV+DB			

	Verantwortliche/r (Erläuterung: s. u.)	Ja	Nein	Nachweis vorhanden und überprüfbar
Einhaltung der Vorgaben der DS-GVO vorgesehen? Existiert ein Zeitplan und werden die Audis dokumentiert?				
Sind externe Audits zur Überprüfung der Einhaltung der Vorgaben der DS-GVO vorgesehen? Existiert ein Zeitplan und werden die Audis dokumentiert?	PV+ Dritte			
Erfolgt eine Verarbeitung in einem Drittstaat?	PV			
Existiert für die Verarbeitung im Drittstaat eine Grundlage aus Kap. V der DS-GVO?	PV+JU od: DB			
Ist dies dokumentiert?	PV			
Ist der Umgang mit Datenpannen geregelt?	PV+DB			
Werden alle Datenpannen dokumentiert?	PV+DB			
Ist der Prozess bzgl. Meldung an die Aufsichtsbehörden etabliert und dokumentiert?	PV+DB			
Ist der Prozess bzgl. Meldung an die betroffene Person etabliert und dokumentiert?	PV+DB			
Ist bei Publikationen und Veröffentlichungen von Studienergebnissen gewährleistet, dass keine personenbezogenen Daten i.S.v. Art. 4 Abs. 1 DS-GVO enthalten sind?	PV+DB od: JU			

Legende:

Datenschutzbeauftragter:	DB
IT-Verantwortlicher:	IT
Juristischer Berater:	JU
Projektverantwortlicher:	PV

Anhang 4. Checkliste zur Information des Datenschutzbeauftragte sowie für dessen Prüfung

Bezeichnung des Forschungsprojekts:			
Kurzbeschreibung:			
Voraussichtlicher Beginn des Forschungsprojekts:		**Voraussichtliches Ende des Forschungsprojekts:**	

	Rechtsgrundlage	**Ja**	**Nein**	**Anmerkungen**
1. Grundrechtsprüfung				
Keine unangemessene Beeinträchtigung des Patienten durch Bedarf an Patientendaten?	Art. 2 Abs. 1 GG	☐	☐	

	Rechtsgrundlage	**Ja**	**Nein**	**Anmerkungen**
2. Zweckbindung				
Für Zwecke der wissenschaftlichen Forschung	Art. 5 Abs. 1 lit. b DSGVO i.V.m. EG 50 zur DSGVO	☐	☐	
Falls zutreffend: Voraussetzungen „klinische Prüfung“ der spezialgesetzliche Forschungsklausel (§ 40 AMG, 20 MPG etc.) positiv geprüft und festgestellt?	§ 40 AMG, § 20 MPG	☐	☐	
Zustimmende Bewertung Ethik-Kommission liegt vor?	§ 40 Abs. 1 AMG § 20 Abs. 1 MPG	☐	☐	
Voraussetzungen § 40 Abs. 1 Nr. 1-9 AMG, § 20 Abs. 1 Nr. 1-9 MPG erfüllt?	§ 40 Abs. 1 Nr. 1-9 AMG § 20 Abs. 1 Nr. 1-9 MPG	☐	☐	
☐ Vorhandensein eines Sponsors oder Vertreters des Sponsors mit Sitz in der EU (bzw. Europäischer Wirtschaftsraum)? ☐ Sind die vorhersehbaren Risiken und Nachteile gegenüber dem Nutzen für die betroffene Person und der voraussichtlichen Bedeutung des Forschungszwecks ärztlich vertretbar? ☐ Im Falle von gentechnisch veränderten Organismen: sind unvertretbare schädliche				

	Rechtsgrundlage	Ja	Nein	Anmerkungen
2. Zweckbindung				
Auswirkungen auf die Gesundheit Dritter und die Umwelt nicht zu erwarten? ☐ Wird die Prüfung in einer geeigneten Einrichtung unter Aufsicht eines qualifizierten Prüfers durchgeführt? (Prüfer benötigt mindestens zweijährige Erfahrung in der klinischen Prüfung von Arzneimitteln) ☐ (Falls im Projekt einschlägig): Wurde eine pharmakologisch-toxikologische Prüfung des Arzneimittels im Vorfeld durchgeführt? ☐ (Falls im Projekt einschlägig): Wurde jeder Prüfer durch einen für die pharmakologisch-toxikologische Prüfung verantwortlichen Wissenschaftler über die Ergebnisse und die voraussichtlichen Risiken informiert? ☐ Wurde eine Versicherung abgeschlossen? ☐ Ist für die medizinische Versorgung der betroffenen Person ein Arzt (bzw. Zahnarzt) verantwortlich?				
Können Minderjährigen-Besonderheiten bei der Projektumsetzung beachtet werden? *Z.B.: Einwilligung durch gesetzlichen Vertreter; Aufklärung des Minderjährigen sowie der ges. Vertreter; geringer Belastungsgrad sowie niedrige Risikoschwelle im Prüfplan eigens definiert und vom Prüfer ständig überprüft?; Vorteilsgewährung maximal im Rahmen einer angemessenen Aufwandsentschädigung*	§ 40 Abs. 4 AMG, § 20 Abs. 4 MPG	☐	☐	
Kann eine umfassende Aufklärung und Einwilligung betroffener Patienten erfolgen?	§ 40 Abs. 2, 2a AMG § 20 Abs. 2 MPG	☐	☐	
Ergebnis: a. und/oder b. mit JA erfüllt? → Weiter mit 3. **Sonst: Forschungsvorhaben kann nicht durchgeführt werden!**				

	Rechtsgrundlage	Ja	Nein	Anmerkungen
3. Datenerhebung/Datenzugang				
a. Werden konkrete Patientendaten für das Forschungsprojekt benötigt?	Art. 5 Abs. 1 lit. b i.V.m. Art. 89 Abs. 1 DSGVO sowie § 27 BDSG	☐	☐	
b. Kann das Projekt mit anonymisierten Daten verwirklicht werden?	§ 27 Abs. 3 BDSG	☐	☐	Nach der Anonymisierung darf kein Patientenbezug mehr möglich sein.
c. Datenanonymisierung in der Klinik möglich?	§ 27 Abs. 3 BDSG	☐	☐	
Wenn a. – c. mit JA erfüllt → Prüfung positiv beendet, Projekt startbereit! **Sonst: weiter mit d.**				
d. Kann das Projekt mit pseudonymisierten Daten realisiert werden?	§ 27 Abs. 3 BDSG Art. 4 Nr. 5 DSGVO, Art. 32 Abs. 1 lit. a DSGVO	☐	☐	Personenbezug ist mit eindeutigem ID-Kennzeichen möglich
e. Patienten-Versichertennummer ist NICHT das Pseudonymisierungsmerkmal?	§ 27 Abs. 3 BDSG Art. 4 Nr. 5 DSGVO, Art. 32 Abs. 1 lit. a DSGVO	☐	☐	Patienten-Versichertennummer darf nicht verwendet werden, da Dritte den Personenbezug herstellen können
f. Inhaltsdaten zu Patienten mit sonstigem Zusatzwissen Dritter NICHT wieder herstellbar?	§ 27 Abs. 3 BDSG Art. 4 Nr. 5 DSGVO	☐	☐	
Wenn d. – f. mit JA erfüllt → weiter mit 4, wenn f. mit NEIN beantwortet, weiter mit g. **Sonst: weiter mit g.**				
g. Ist die Pseudonymisierung der Patientendaten in eigener Einrichtung mit eigenem Personal realisierbar?	§ 27 Abs. 3 BDSG Art. 32 Abs. 1 lit. a DSGVO	☐	☐	
Weiter mit 4.				

	Rechtsgrundlage	Ja	Nein	Anmerkungen
4. Einwilligungen				
a. Werden von den Patienten Einwilligungen zur Verarbeitung ihrer Daten eingeholt?	Art. 9 Abs. 2 lit. a; Art. 7 Abs. 1 DSGVO		-	

	Rechtsgrundlage	Ja	Nein	Anmerkungen
4. Einwilligungen				
(1) Handelt es sich um ansprechbare Patienten?	Art. 9 Abs. 2 lit. a DSGVO	☐	☐	
(2) Sind die betroffenen Patienten erreichbar (ggf. Adressermittlung?)	Art. 9 Abs. 2 lit. a DSGVO	☐	☐	
(3) Können Einwilligen aufgrund der Anzahl der Fälle aus Organisationsgründen eingeholt werden?	Art. 9 Abs. 2 lit. a DSGVO	☐	☐	
b. Aufklärung über Forschungsinhalt und Patientendatenverwendung kann nachweisbar erfolgen?	§ 27 Abs. 3 BDSG n.F.	☐	☐	
c. Patient kann über Betroffenenrechte nachweisbar belehrt werden?	Art. 15 ff. DSGVO Art. 27 Abs. 2 DSGVO	☐	☐	
Wenn a. - c. mit JA erfüllt → weiter mit 5. **Sonst: weiter mit c.**				
c. Mangels Einwilligung: Wissenschaftliche (Forschungs-) Privilegien vorhanden? ***Im Falle von § 27 Abs. 1 BDSG n.F. i.V.m. Art. 9 Abs. 1 DSGVO:*** *Verarbeitung ist für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke zulässig, wenn die Verarbeitung erforderlich ist und die Interessen im Vergleich zu dem Interesse am Ausschluss der Verarbeitung deutlich überwiegt*	insbesondere § 27 Abs. 1 BDSG n.F. i.V.m. Art. 9 Abs. 1 DSGVO	☐	☐	
Angabe der gesetzlichen Grundlage:		Begründung:		
Steht die Forschungsklausel im angemessenen Verhältnis zu dem verfolgten	Art. 9 Abs. 2 lit. j DSGVO § 22 Abs. 2 S. 2 BDSG n.F.	☐	☐	

	Rechtsgrundlage	Ja	Nein	Anmerkungen
4. Einwilligungen				
Zweck? *z.B. Nachweis des Erfordernisses der erhobenen Daten zur Erreichung des Forschungszwecks; die Grundrechte und Interessen der betroffenen Person werden gewahrt*				
Wird der Wesensgehalt des Rechts auf Datenschutz gewahrt? *Wesensgehalt des Datenschutzes: Recht der informationellen Selbstbestimmung. Die Verarbeitung darf nicht außer Verhältnis zu den Interessen der betroffenen Person stehen.*	Art. 9 Abs. 2 lit. j DSGVO § 22 Abs. 2 S. 2 BDSG n.F. § 27 Abs. 3 BDSG n.F.	☐	☐	
Werden angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person gewahrt? *z.B. Einsatz von Pseudonymisierung, Verschlüsselung; frühestmögliche Anonymisierung/Löschung der Daten*	Art. 9 Abs. 2 lit. j DSGVO § 22 Abs. 2 S. 2 BDSG n.F.	☐	☐	
Werden die Patienten über die Zweckänderung bei der Verwendung der Daten informiert	Art. 13 Abs. 3 DS-GVO Art 14 Abs. 4 DS-GVO			
Wenn nicht: Ist eine Ausnahmeregelung erfüllt, nach welcher auf die Information bzgl. Zweckänderung verzichtet werden kann?	Art. 13 Abs. 4 DS-GVO Art. 14 Abs. 5 DS-GVO			
Wenn mit JA erfüllt → weiter mit 5. **Sonst: Forschungsvorhaben kann nicht durchgeführt werden!**				

	Rechtsgrundlage	Ja	Nein	Anmerkungen
5. Zusammenarbeit mit externen Partnern				
a. Sind alle am Projekt beteiligten Personen auf das Datengeheimnis verpflichtet (z. B. im Rahmen der Aufnahme des Arbeitsverhältnisses)?	§ 27 Abs. 1 BDSG n.F. i.V.m. § 22 Abs. 1 Nr. 1 lit. b, c BDSG n.F. § 203 Abs. 1 StGB	☐	☐	
b. Unterliegen alle am Projekt beteiligten Personen der Schweigepflicht gemäß § 203 StGB oder wurde darauf verpflichtet?				
c. Wird KEIN Zusatzvertrag zur Auftragsverarbeitung nach Art. 28 DSGVO benötigt?	vgl. Art. 28 Abs. 1 DSGVO	☐	☐	
Wenn mit c. JA erfüllt → weiter mit e. Wenn NEIN, weiter mit d.				
d. Zusatzvertrag zur Auftragsverarbeitung abgeschlossen und Vertrag liegt unterschrieben vor? (Vertragsprüfung durch Datenschutzbeauftragten möglich!)	Art. 28 Abs. 1 DSGVO	☐	☐	
e. Wird KEIN Zusatzvertrag zur gemeinsamen Verarbeitung nach Art. 26 DSGVO benötigt?	vgl. Art. 26 Abs. 1 DSGVO	☐	☐	
Wenn mit e. JA erfüllt → weiter mit g. Wenn NEIN, weiter mit f.				
f. Zusatzvertrag zur gemeinsamen Verarbeitung abgeschlossen und Vertrag liegt unterschrieben vor? (Vertragsprüfung durch Datenschutzbeauftragten möglich!)	Art. 26 Abs. 1 DSGVO	☐	☐	
Wenn mit f. JA erfüllt → weiter mit g.				
g. Können Externe (Mitarbeiter, die nicht zur Klinik gehören) auf Daten mit Personenbezug zugreifen?		☐	☐	
Handelt es sich um elektronische Daten?		☐	☐	
Wenn JA, wurde die IT eingebunden und hat angepasste Zugriffsrechte eingerichtet?	Art. 32 Abs. 1 DSGVO	☐	☐	

		Rechtsgrundlage	Ja	Nein	Anmerkungen
5. Zusammenarbeit mit externen Partnern					
Wenn NEIN, wurden organisatorische Regelungen getroffen, damit nur auf die notwendigen nicht elektronischen Daten (z.B. Mikrofiche, Papierakten) zugegriffen werden kann? **Wenn mit JA erfüllt → weiter mit e.**		Art. 32 Abs. 1 DSGVO	☐	☐	
h. Archivierungszeitraum definiert?	Art. 5 Abs. 1 lit. e DSGVO	☐ bis zum Studienende ☐ Jahre nach Studienende ☐	☐	☐	
i. Liegen dem Patienten Informationen des Forschungsprojekts und der damit verbundenen Datenverarbeitung vor inkl. der Belehrung über die Betroffenenrechte ins. Bzgl. Widerspruch zur Verarbeitung seiner Daten vor?		Kapitel III DSGVO	☐	☐	
Wenn mit JA erfüllt → weiter mit 6. **Forschungsvorhaben ohne Veröffentlichungsaspekt umsetzbar!**					

	Rechtsgrundlage	Ja	Nein	Anmerkungen
6. Veröffentlichung von Forschungsergebnissen				
a. Ist eine Veröffentlichung geplant?	§ 27 Abs. 4 BDSG n.F.	☐	☐	

	Rechtsgrundlage	Ja	Nein	Anmerkungen
6. Veröffentlichung von Forschungsergebnissen				
b. Sollen Patientendaten mit veröffentlicht werden?	§ 27 Abs. 4 BDSG n.F.	☐	☐	
(1) Liegt eine Einwilligung separat vor?	§ 27 Abs. 4 BDSG i.V.m. Art 9. Abs. 2 lit. a, Art. 7 Abs. 1 DSGVO i.V.m. EG 42 zur DSGVO	☐	☐	
(2) Ist eine Einwilligung hierfür in der Forschungseinwilligung enthalten?	§ 27 Abs. 4 BDSG i.V.m. Art 9. Abs. 2 lit. a, Art. 7 Abs. 1 DSGVO i.V.m. EG 42 zur DSGVO	☐	☐	
(3) Veröffentlichung inkl. Angabe der personenbezogenen Daten ist für die Darstellung der Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich	§ 27 Abs. 4 BDSG			
Wenn a. und eine Alternative von b. mit JA erfüllt → Veröffentlichung mit Patientenbezug möglich **Wenn b nicht erfüllt → Veröffentlichung nur ohne Patientennamen möglich**				

Beurteilung:

☐	Forschungsprojekt uneingeschränkt durchführbar
☐	Forschungsprojekt eingeschränkt durchführbar (ohne Veröffentlich der Forschungsergebnisse)
☐	Forschungsprojekt nicht durchführbar

Anhang 5. Checkliste für die Einholung eines Datenschutzgutachtens beim Datenschutzbeauftragten zur Vorlage bei der Ethik-Kommission

	Ja	Nein
Sind Fragestellungen und Ziele der geplanten Studie („Zweck“) so dokumentiert, dass durch den Datenschutzbeauftragten eine Begutachtung erfolgen kann?		
Wurde die Relevanz der Studie für die medizinische Versorgung von Patienten ausreichend dargestellt?		
Werden Unterlagen bereitgestellt, aus denen ersichtlich ist, welche personenbezogenen oder personenbeziehbaren (pseudonymen) Daten im Rahmen der Studie verarbeitet werden sollen?		
Lässt sich die Erforderlichkeit für die Verarbeitung der in der Studie angegebenen Datenarten/Datenkategorien aus der Formulierung der Forschungshypothesen bzw. der bereitgestellten Dokumentation ableiten?		
Werden Unterlagen bereitgestellt, welche die Rechtsgrundlage für die Verarbeitung darlegen?		
Wenn die Rechtsgrundlage eine Einwilligung darstellt: Liegt den Unterlagen eine Muster-Einwilligungserklärung bei?		
Wenn eine Erweiterung der Fragestellung im Verlauf der Studie erforderlich wird: Ist dargestellt, wie dies mit der Rechtsgrundlage für die Studie vereinbar ist?		
Wurde dargestellt, wie die Auswahl der Studienteilnehmer und deren Integration (Ansprache) in die Studie erfolgt?		
Wurde die Anzahl der benötigten Patienten/Probanden dargestellt und begründet?		
Wurden die Erhebungsverfahren unter Berücksichtigung der datenschutzrechtlichen Risiken für Probanden/Patienten dargestellt?		
Werden Unterlagen bereitgestellt, die belegen, dass Probanden/Patienten über Ziele und Ablauf der Studie ausreichend informiert werden?		
Wurden die statistischen Methoden sowie die aus der Auswertung evtl. resultierenden Folgen für die betroffenen Personen beschrieben?		
Wurden Unterlagen bereitgestellt, die darlegen, wie die Betroffenenrechte im Rahmen der Studie gewährleistet werden?		
Wurde dargestellt, wie die Sicherheit der Verarbeitung und insbesondere die Vertraulichkeit der Gesundheitsdaten im Rahmen der Studie gewahrt wird?		
Wurden Unterlagen bereitgestellt, die darlegen, wie die im Rahmen der Studie mit Datenpannen umgegangen wird?		
Ist dargestellt, ob und wenn ja wie Daten an andere Wissenschaftler/Kooperationspartner weitergegeben werden sollen?		
Bei Kooperationen: Ist eine Verarbeitung in einem Drittstaat (= Staat außerhalb EU/EWR) geplant? Wenn ja: Ist dargestellt, auf welchen Mechanismen (Artt. 44-50 DS-GVO) die Rechtsgrundlage zur Verarbeitung im Drittstaat beruht?		
Ist dargestellt, welche Daten in wissenschaftlichen Publikationen verwendet werden sollen, sodass beurteilt werden kann, welche Auswirkungen geplante Publikationen für betroffene Personen haben?		
Wenn Ergebnisse der Studie Relevanz für den Probanden/Patienten haben könnten: Ist dargestellt, wie eine Kommunikation der Ergebnisse mit Probanden/Patienten oder auch mit deren Hausärzten erfolgt?		