TMF – Technologie- und Methodenplattform
für die vernetzte medizinische Forschung e.V.

Antony G, Bialke M, Pommerening K, Repp R:

Checkliste zur Erstellung eines Datenschutzkonzeptes

Version 1.0 vom 12. Dezember 2017

Die vorliegende Checkliste basiert auf langjährigen Erfahrungen der TMF AG Datenschutz. Sie wurde unter Nachnutzung ausgewählter Inhalte der *Mustervorlage zur Erstellung von Datenschutzkonzepten* des *Projekts MOSAIC* des Instituts für Community Medicine der Universitätsmedizin Greifswald (ICM)[i][1], dem *Leitfaden zur Erstellung von Datenschutzkonzepten im Gesundheitswesen* der AG Datenschutz der Deutschen Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie (*GMDS*)[ii], dem *Standard-Datenschutzmodell* (SDM) der 92. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder[iii] und den aktuellen Empfehlungen 2017 zu Datenschutz und Forschungsdaten des Rats für Informationsinfrastrukturen (RFII)[iv] erstellt. Zudem verweist diese Checkliste auf Anforderungen durch die jüngsten Änderungen des *Bundesdatenschutzgesetzes* (BDSG)[v] und der neuen *EU-Datenschutz-Grundverordnung* (EU-DS-GVO)[vi].

Die entstandene Checkliste soll in kurzer und übersichtlicher Form darüber informieren, welche Fragen Ersteller von Datenschutzkonzepten zu klären haben und welche Dokumente zu erstellen sind. Gleichzeitig soll sie als Wegweiser zu den für das Projekt relevanten Teilen des *Datenschutzleitfadens der TMF* dienen. Dieser ist in der TMF-Schriftenreihe erschienen:

> K. Pommerening | J. Drepper | K. Helbing | T. Ganslandt. **Leitfaden zum Datenschutz in medizinischen Forschungsprojekten.** Generische Lösungen der TMF 2.0. 2014. [ISBN 978-3-95466-123-7]

Er wird ergänzt durch das generische Datenschutzkonzept für Biobanken, das als Band 6 der TMF-Schriftenreihe angekündigt ist:

> Becker, R., Ihle, P., Pommerening, K., Harnischmacher, U. **Ein generisches Datenschutzkonzept für Biomaterialbanken** (Version 1.0). 2006. TMF. http://www.tmf-ev.de/produkte/P010021 (Abruf: 2017-11-01)

Diese Checkliste ist nicht notwendig als Gliederungsvorlage für ein Datenschutzkonzept vorgesehen, sondern dient in erster Linie zur Überprüfung, ob alle relevanten Gesichtspunkte bedacht wurden.

[1] Referenzen [i] bis [vi] am Ende des Dokuments

Inhalt

Was ist ein Datenschutzkonzept?

Medizinische Forschung greift fast zwangsläufig in grundgesetzlich garantierte Persönlichkeitsrechte der Betroffenen – Patienten oder Probanden – ein. Dieser Eingriff ist durch den gesellschaftlich akzeptierten Nutzen des medizinischen Fortschritts und durch die ebenfalls im Grundgesetz verankerte Wissenschaftsfreiheit *in gewissen Grenzen* gerechtfertigt und muss dann durch besonders sorgfältige Schutzmaßnahmen kompensiert werden.

Das Datenschutzkonzept eines medizinischen Forschungsprojekts begründet die *Erforderlichkeit und Angemessenheit* der Vorgehensweise und beschreibt alle Maßnahmen, die zum wirksamen Schutz der Persönlichkeitsrechte beitragen.

Zur **Begründung der Erforderlichkeit** ist möglichst konkret darzustellen, welches Forschungsziel erreicht werden soll und welche Daten- und Probensammlungen dazu benötigt werden.

Die **Beschreibung der Maßnahmen** stellt die Wirksamkeit des Schutzes von Persönlichkeitsrechten, insbesondere von personenbezogenen Daten dar, auch die Minimierung und Kontrolle des Re-Identifizierungsrisikos. Sie umfasst organisatorische Regelungen und technische Maßnahmen zur IT-Sicherheit.

Die **Beschreibung der Angemessenheit** umfasst die Begründung, warum das Forschungsziel auf diese Weise und nicht mit geringeren Eingriffen in Persönlichkeitsrechte erreicht werden kann, sowie eine Abwägung der Angemessenheit der Schutzmaßnahmen. Hierher gehört auch die Begründung, an welchen Stellen Daten personenbezogen vorliegen müssen, wo Pseudonymisierung angemessen ist und wo anonymisierte Daten ausreichen.

Um ein Datenschutzkonzept formulieren zu können, aber auch unabhängig davon zur Projektplanung im Allgemeinen, muss man sich klar sein über

- Projektziele und das zu ihrer Erreichung geplante Vorgehen, einschließlich der wissenschaftlichen Methodik,
- organisatorische Strukturen, Prozesse und Kommunikationswege des Forschungsprojekts oder -verbunds (einschließlich geplanter Biobanken oder Probenaufbewahrung),
- das IT-Konzept: geplante Anwendungsfälle mit Daten, Datenflüssen und Datenverwendung
- sowie dessen Umsetzung mit IT-Architektur und Datenspeichern.

Allgemeine, grundsätzliche und auch spezielle Fragen zu einem Datenschutzkonzept werden in den FAQ zum Datenschutz beantwortet:

> http://www.tmf-ev.de/Arbeitsgruppen_Foren/AGDS/FAQsDatenschutz.aspx
> (Abruf: 2017-11-01)

Erstellung eines Datenschutzkonzepts und Begutachtung

Grundlage zur Erstellung eines Datenschutzkonzepts für ein medizinisches Forschungsprojekt ist der ausführliche Leitfaden der TMF, der generische Datenschutzkonzepte für verschiedene Szenarien beschreibt.

Für ein Datenschutzkonzept, das gemäß dem Leitfaden erstellt wurde und die einzelnen Punkte dieser Checkliste abhandelt, kann die TMF-AG Datenschutz ein schriftliches Votum abgeben, das die Konformität mit dem Leitfaden bestätigt und

- bei der gesetzlich vorgeschriebenen Beratung und Prüfung durch die zuständigen behördlichen oder betrieblichen Datenschutzbeauftragten,
- bei der Durchführung einer Datenschutz-Folgenabschätzung[2] i.S.d. Europäischen Datenschutz-Grundverordnung (EU-DS-GVO),
- bei einer Prüfung durch die Datenschutzaufsichtsbehörde (z. B. bei der Prüfung der Beschreibung des Verfahrens in der Verarbeitungsübersicht[3]),
- bei der Prüfung des Ethikantrages

vorgelegt werden kann.

Die wesentlichen Schritte zur Erlangung eines solchen Votums sind in dem Dokument „Informationen zum Beratungsangebot“ beschrieben;
http://www.tmf-ev.de/Arbeitsgruppen_Foren/AGDS/Beratung.aspx (Abruf: 2017-11-01).

Ein Datenschutzkonzept umfasst eine Reihe von zusätzlichen Dokumenten, die, sofern sie zur Beurteilung des Konzepts wesentlich sind, der TMF-AG Datenschutz vorgelegt bzw. im Datenschutzkonzept hinsichtlich ihres Regelungsinhaltes näher dargelegt werden sollten.

- Information für Probanden und Formular zur Einwilligungserklärung,
- Kooperationsvereinbarungen und Verträge zwischen Projektpartnern,
- Verträge mit Auftragnehmern,
- Bedingungen und Auflagen bei Erhalt von Zuwendungen,
- Interne Richtlinien, Verpflichtungserklärungen, SOPs,
- IT-Sicherheitskonzept (mit ausführlicherer Beschreibung der Maßnahmen, die im eigentlichen Datenschutzkonzept in nicht-technischer Form kurz aufgeführt werden).

Es kann sich dabei um separate Dokumente oder Anhänge handeln. Die rechtliche Korrektheit dieser Dokumente wird von der TMF-AG Datenschutz nicht bewertet.

[2] vgl. Art. 35, 36 EU-DS-GVO i.V.m. § 67 BDSG (nF)

[3] vgl. Art. 30 EU-DS-GVO

I. Darstellung des Forschungsvorhabens

Das Forschungsvorhaben soll beschrieben und seine Erforderlichkeit begründet werden. Der Nutzen des Vorhabens, ggf. auch für die betroffenen Personen, soll dargestellt werden.

- Was ist das Ziel des Forschungsvorhabens, wie soll es erreicht werden?
- Welcher Fortschritt in der Wissenschaft wird angestrebt bzw. was ist der zu erwartende Nutzen?
- Wie grenzt sich dieses Forschungsvorhaben zu ähnlichen ab?
- Wie sind Behandlungs-und Forschungskontext im Rahmen des Fotschungsvorhabens abgegrenzt?
- Welche bereits formulierten oder künftig zu verfolgenden Forschungsfragen werden verfolgt?
- Welche Auswirkungen auf die Behandlungsqualität werden erhofft?
- Was rechtfertigt den Eingriff in das geschützte Grundrecht natürlicher Personen auf Schutz personenbezogener Daten?
- Gibt es abgrenzbare Phasen des Forschungsvorhabens, z. B. eine Pilotphase mit vereinfachten Maßnahmen für einen eng beschränkten Zeitraum?
- Ist ein stufenweiser Ausbau des Forschungsvorhabens vorgesehen, für dessen folgende Stufen die Konzeption erst später konkretisiert werden kann oder soll?
- Wie sieht das Design des Forschungsvorhabens aus (z. B. Studiendesign)?
- Ist das Ziel des Forschungsvorhabens erreichbar?
- Welche wissenschaftliche, speziell biomathematische Methodik, soll angewendet werden?
- Wie werden Methodiker/Biometriker/Informatiker eingebunden?
- Wie weit kann mit anonymisierten oder pseudonymisierten Daten gearbeitet werden bzw. bei welchen Verarbeitungsprozessen ist ein expliziter Personenbezug unvermeidbar?
- Wie lang ist die vorgesehe Laufzeit des Forschungsvorhabens?
- Ist eine Weiterführung des Vorschungsvorhabens auch nach Ablauf der aktuellen Projektfinanzierung geregelt?

II. Organisatorische Struktur

Die Personen und Organisationen, die am Projekt beteiligt sind oder sein sollen, ihre Beziehungen zueinander und ihre Verantwortungsbereiche sollen beschrieben werden.

A. Verantwortlicher Verarbeiter

- Wer ist für die personenbezogenen Daten bzw. Bioproben Verantwortlicher[4] i.S.d. EU-DS-GVO (z. B. Hochschule/Institut/Klinik, andere Organisation)?
- Wie ist dessen rechtliche Stellung (z. B. Anstalt oder Körperschaft des öffentlichen Rechts, öffentliche Stiftung, Gesellschaft privaten Rechts)?
- Welche Forschungsschwerpunkte hat der für die Verarbeitung Verantwortliche?

B. Beteiligte, Kooperationspartner, gemeinsam für die Verarbeitung Verantwortliche

- Welche anderen Organisationen, Partner und Institutionen sind beteiligt?
- Gibt es mehrere für die Verarbeitung Verantwortliche[5]? Wenn ja, welcher Verantwortliche erfüllt welche Verpflichtung gemäß der EU-DS-GVO? Wie ist deren rechtliche Stellung?
- Welche Gründe gibt es für eine Beteiligung von Kooperationspartnern oder Dienstleistern und welche Funktionen bzw. Aufgaben übernehmen sie im Rahmen des Forschungsvorhabens?
- Wie sind die Verantwortungsbereiche definiert? (Welche Partner und Stellen sind auf welche Weise beteiligt und unterliegen wessen Weisung?)
- Wodurch ist die Zusammenarbeit im Forschungsvorhaben geregelt (z. B. Geschäftsordnung, Satzung, Kooperationsverträge, Gesellschaftervertrag, je nach Rechtsform)?
- Welches Leitungsgremium und andere Entscheidungsträger sind vorgesehen (z. B. Vorstand, Mitgliederversammlung, Gesellschafterversammlung, Geschäftsführung)?
- In welcher Rolle und Funktion sind ggf. Fachgesellschaften und Patientenorganisationen eingebunden?

C. Organisatorische Abhängigkeiten

- Welche Instanzen des Forschungsvorhabens in einem Forschungsverbund sind selbständige Partner?
- Wer ist Auftragnehmer bzw. Dienstleister (z. B. Hosting)?
- Welche möglichen Interessenkonflikte bestehen?

[4] vgl. Art. 4 As. 7 EU-DS-GVO

[5] vgl. Art. 26 EU-DS-GVO

- Welche Treuhänderdienste (Datentreuhänder, Vertrauensstelle) sollen eingebunden werden (z. B. MI-Institut, interne Datenschutzbeauftragte, externe Firma, Notar)? Begründung der Eignung?
- Wie ist die informationelle Gewaltenteilung konkret geregelt? (Z. B. Datenverteilungsmatrix aus der hervorgeht, welcher Partner welche Informationen einsehen kann.)

D. Internationale Aspekte

- Welche ausländischen Projektpartner sind beteiligt?
- Werden Aufträge ins Ausland vergeben (z. B. für Laboruntersuchungen)? Falls ja, auf welcher Rechtsgrundlage?
- Ist die Nutzung von personenbezogenen Daten und/oder Bioproben durch ausländische Interessenten vorgesehen? Falls ja, auf welcher Rechtsgrundlage sollen personenbezogene Daten und/oder Biomaterialproben in das Ausland übermittelt werden, (z. B. EU-Raum, Angemessenheitsbeschluss der Europäischen Kommission[6], geeignete Garantien[7] ggf. mit Genehmigung der zuständigen Aufsichtsbehörde für den Datenschutz)?

E. Finanzierung des Forschungsvorhabens

- Wer fördert das Forschungsvorhaben wie lange (z. B. Grundfinanzierung, befristete Projektfinanzierung, Auftragsforschung)?
- Welche Art der Weiterführung ist nach Auslauf der gegenwärtigen Finanzierung geplant?
- In welche Trägerschaft sollen personenbezogene Daten und Bioproben langfristig übergehen bzw. wie wird mit personenbezogenen Daten und/oder Bioproben nach Ablauf der Förderdauer oder des Forschungsvorhabens umgegangen?

III. Datenschutzrelevante Rahmenbedingungen

Die grundsätzlich zur Durchführung des Projekts vorgesehenen Prozesse mit ihren organisatorischen und rechtlichen Rahmenbedingungen sollen vorgestellt werden.

[6] vgl. Art. 45 EU-DS-GVO
[7] vgl. Art. 46 EU-DS-GVO

A. Anwendungsfälle

Arbeitsablauf	Erläuterung
Einholung Einwilligung	…
Erhebung von Daten bzw. Bioproben	…
Rekrutierung von Teilnehmern	…
Übermittlung von Daten bzw. Bioproben	…
Speicherung bzw. Lagerung von Daten bzw. Bioproben	…
Bereitstellung von Daten bzw. Bioproben	…
Durchführung von Follow-Ups	…
Widerruf von Einwilligungen	…

Beispielhafte Übersicht von Arbeitsabläufen

B. Grundlegende Rahmenbedingungen

- Welchem allgemeinen Datenschutzrecht unterliegt die für die Verarbeitung verantwortliche Stelle neben der EU-DS-GVO (Bundesdatenschutzgesetz, Landesdatenschutzgesetz)?
- Unterliegt das Forschungsvorhaben einschlägigen Spezialgesetzen (wie z. B. Krebsregistergesetze, Arzneimittelgesetz, Sozialgesetzbücher, Bundesmeldegesetz)?
- Sollen personenbezogene Daten aus anderen Quellen mit speziellen gesetzlichen Rahmenbedingungen verwendet werden (z. B. Sekundärnutzung von Routinedaten, Meldedaten)?
- Sind bundeslandspezifische Regelungen bei Sekundärnutzung von Behandlungsdaten zu beachten (z. B. Landeskrankenhausgesetze)?
- Sollen personenbezogene Daten und/oder Bioproben aus der Behandlungsdokumentation für das Forschungsvorhaben genutzt werden oder aus dem Forschungsvorhaben in eine Behandlungsdokumentation zugeführt werden (Schweigepflichtsentbindung, Übermittlungserlaubnis)?
- Ist eine direkte Rückwirkung auf die Behandlung einzelner Patienten bzw. Probanden zu erwarten oder denkbar?

C. Umfang der Verarbeitung von Daten und Ab- bzw. Entnahme von Bioproben für das geplante Forschungsvorhaben

- Welche Personen/Personengruppen sind von der geplanten Datenverarbeitung betroffen (Patienten und Probanden, Angehörige, Beschäftigte beteiligter Institutionen, Beschäftigte nicht beteiligter Institutionen wie z. B.behandelnde Ärzte, …)?
- Betrifft das Forschungsvorhaben Kinder[8] i.S.d. EU-DS-GVO?
- Betrifft das Forschungsvorhaben vulnerable Personen oder Personengruppen (z. B. nicht einwilligungsfähige Personen)?

[8] vgl. Art. 8 EU-DS-GVO

- Wie sind Ein- und Ausschlusskriterien für Probanden definiert?
- Welche personenbezogenen identifizierenden Daten sollen verarbeitet werden?
- Welche personenbezogenen medizinischen Daten sollen verarbeitet werden?
- Sollen Biomaterialien entnommen und ggf. gelagert werden?
- Welche Biomaterialproben werden benötigt?
- Welche besonderen Kategorien personenbezogener Daten[9] i.S.d. EU-DS-GVO sollen verarbeitet werden?
- Sollen personenbezogene identifizierende bzw. medizinische Daten und/oder Bioproben aus anderen eigenen Forschungsvorhaben genutzt oder von anderen Einrichtungen zur Verfügung gestellt werden (z. B. Biobank)? Wenn ja, von welcher Einrichtung und auf welcher Rechtsgrundlage (z. B. Einwilligungserklärung, Zweckänderung, Datennutzungvertrag, Material Transfer Agreement)? Wie werden die Informationspflichten[10] gemäß der EU-DS-GVO nachweisbar erfüllt?
- Sollen oder müssen Zulieferer von personenbezogenen Daten und/oder Bioproben Zugriff auf die Daten behalten bzw. sollen oder müssen personenbezogene Daten diesen Zulieferern mitgeteilt werden (z. B. Zufallsfunde oder andere Analyseergebnisse innerhalb des Forschungsvorhabens)? Falls ja, auf welcher Rechtsgrundlage?
- Welcher Einzugsbereich und welche Fallzahlen sind für das Forschungsvorhaben vorgesehen?

D. Erhebung von personenbezogenen Daten und/oder Bioproben

Die geplante Erhebung personenbezogener Daten und/oder Bioproben soll beschrieben werden.

- Wie erfolgt die Erhebung personenbezogener Daten und/oder Bioproben im Detail?
- Wer ist verantwortlich für die Aufklärung von Probanden und die Einholung einer Einwilligungserklärung?
- Wer führt die Erhebung personenbezogener Daten und/oder Bioproben durch? Sind ggf. Partner an der Erhebung personenbezogener Daten und/oder Bioproben beteiligt?
- Wie werden die personenbezogenen Daten bei der Erhebung qualitätsgesichert (z. B.Prüfung auf Plausibilität und Vollständigkeit)?
- Wie groß ist das geschätzte Datenvolumen?
- Wie oft werden personenbezogene Daten einer einzelnen Person erhoben (Follow-ups)?

E. Datenintegration und Speicherung personenbezogener Daten

Die Speicherung personenbezogener Daten soll beschrieben werden.

- Wie erfolgt die Speicherung personenbezogener Daten im Detail?
- An welchem Ort werden welche personenbezogenen Daten gespeichert?

[9] vgl. Art. 9 i.V.m. Art. 3 Abs. 13 ff. EU-DS-GVO
[10] vgl. Art. 14 EU-DS-GVO

- Wie werden die personenbezogenen Daten gespeichert (z. B. zentral, dezentral, Papier-basiert, Datei-basiert, Datenbank, Datawarehouse)?
- Werden die personenbezogenen Daten vor oder bei der Speicherung anonymisiert bzw. pseudonymisiert? (Zu den technischen Verfahren siehe VII H)
- Wie erfolgt ggf. die Zusammenführung der multizentrisch erhobenen personenbezogenen Daten?
- Wie erfolgt ggf. die Zusammenführung heterogener personenbezogener Daten?
- Werden die personenbezogenen Daten versioniert oder mit Hilfe eines Audit Trail Verfahrens dokumentiert (historisiert)?

F. Lagerung der Bioproben

- An welchem Ort / welchen Orten werden die Bioproben wie lange gelagert?
- Wie werden die Bioproben aufbewahrt (zentrale oder verteilte Biobank)?
- Soll ggf. eine eigene Biobank aufgebaut oder genutzt werden?

G. Nutzung der personenbezogenen Daten und/oder Bioproben

- Wofür sollen die personenbezogenen Daten und/oder Bioproben primär und/oder sekundär genutzt werden (z. B. für Beobachtungsstudien, Hypothesengenerierung/Data Mining, Rekrutierung für künftige klinische oder epidemiologische Studien, translationale Forschung, medizinische Qualitätskontrolle)?
- Wie weit kann die künftige sekundäre Nutzung schon eingegrenzt werden, wie weit soll sie offen bleiben?
- Wer soll personenbezogene Daten und/oder Bioproben nutzen dürfen?
- Ist eine Weitergabe von personenbezogenen Daten und/oder Bioproben an andere interne und/oder externe Forschungsvorhaben vorgesehen?
- In welcher Form werden personenbezogene Daten und/oder Bioproben Dritten bereitgestellt?
- Gibt es ein standardisiertes Antragsverfahren, um personenbezogene Daten und/oder Bioproben intern nachzunutzen bzw. extern zu nutzen? Wer entscheidet über diese Anträge?
- Welche Schritte (z. B. Reidentifizierung /Anonymisierung) sind für die Übermittlung der personenbezogenen Daten und/oder Bioproben an Dritte notwendig?
- Ist eine Rückmeldung von Analyseergebnissen an die Bioproben-Herausgeber oder eine Rückgabe von Bioproben erforderlich?

H. Anonymisierung und Löschung von personenbezogenen Daten und/oder Vernichtung von Bioproben

- Werden personenbezogene Daten nach dem Tod von Probanden gelöscht oder anonymisiert?

- Gibt es Regelfristen zur Löschung der personenbezogenen Daten?
- Werden Bioproben nach dem Tod von Probanden vernichtet?
- Gibt es Regelfristen zur Vernichtung der Bioproben?
- Werden Vergleichsproben zu Bioproben archiviert, die für wissenschaftliche Publikationen verwendet wurden? Wenn ja, wo und wie?
- Wie werden personenbezogene Daten archiviert, die für wissenschaftliche Publikationen verwendet wurden?

IV. Grundlagen zum Schutz der Rechte und Freiheiten der betroffenen Personen

Die grundsätzlichen Überlegungen zum Datenschutz in der Terminologie der Datenschutzgesetzgebung sollen vorgestellt werden.

A. Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz[11]

- Ist eine schriftliche Einwilligungserklärung von Probanden erforderlich oder erfolgt die Verarbeitung der personenbezogenen Daten und/oder Bioproben auf der Grundlage einer gesetzlichen Regelung? Wenn ja, auf welcher gesetzlichen Grundlage?
- Wie wird mit eingeschränkter Einwilligungsfähigkeit oder Nichteinwilligungsfähigkeit von natürlichen Personen verfahren (z. B. bei Kindern)?
- Gibt es Anforderungen von Patientenorganisationen oder Ethikkommissionen hinsichtlich der Aufklärung von Probanden und an die Einwilligungserklärung?
- Inwiefern ist eine separate Entbindung von einer gesetzlichen Schweigepflicht erforderlich?
- Ist die pseudonyme Verarbeitung personenbezogener Daten und/oder Bioproben durch die Einwilligungserklärung abgedeckt?
- Ist ein Anonymisieren der personenbezogenen Daten durch die Einwilligungserklärung abgedeckt?
- Welche zusätzlichen Maßnahmen zur Transparenz werden für das Forschungsvorhaben eingerichtet (z. B. Öffentlichkeitsarbeit, Webpräsenz, Publikationsregeln)?

B. Zweckbindung[12]

- Wie breit ist die Einwilligungserklärung formuliert? Handelt es sich um eine breiter angelegte Einwilligungserklärung oder wird eine detaillierte, zweckgebundene Einwilligungserklärung eingesetzt?
- Sind Abstufungen oder eindeutige Wahlmöglichkeiten für die Einwilligungserklärung vorgesehen?

[11] vgl. Art. 5 Abs. 1 lit. a EU-DS-GVO

[12] vgl. Art. 5 Abs. 1 lit. b EU-DS-GVO

- Ist die Rekontaktierung von Probanden durch die Einwilligungserklärung abgedeckt (z. B. bei Zufallsfunden oder Follow-Ups)?

C. Richtigkeit[13]

- Wird die Einwilligungserklärung auf Vollständigkeit und ggf. Teilstreichungen kontrolliert? Wann liegt eine gültige Einwilligung des Betroffenen vor?
- Wie wird sichergestellt, dass die personenbezogenen Daten richtig erhoben werden und zu einem späteren Zeitpukt korrigiert oder ggf. gelöscht werden können?

D. Speicherbegrenzung[14]

- Wie wird sichergestellt, dass ausschließlich für den Forschungszweck relevante und notwendige personenbezogene Daten und/oder Bioproben verarbeitet werden?
- Werden nicht mehr benötigte personenidentifizierende Daten gelöscht, wenn diese nicht mehr zwingend erforderlich sind?

E. Integrität und Vertraulichkeit[15]

- Wie wird sichergestellt, dass personenbezogene Daten und/oder Bioproben vor unbefugter oder unrechtmäßiger Verarbeitung geschützt werden?
- Wie werden personenbezogene Daten und/oder Bioproben gegen Verlust, Zerstörung oder Schädigung geschützt?

F. Abschätzung der Risiken für die Rechte und Freiheiten natürlicher Personen:

- Sollen Prozesse zur Durchführung einer Datenschutz-Folgenabschätzung[16] eingerichtet oder genutzt werden und wer ist daran beteiligt?
- Wurde der betriebliche bzw. behördliche Datenschutzbeauftragte bei der Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen und Angemessenheits-prüfung der vorgesehenen technischen und organisatorischen Maßnahmen eingebunden?
- Wurde die geplante Verarbeitung personenbezogener Daten und/oder Bioproben systematisch beschrieben? Wird die geplante Verarbeitung mit den Zwecken und dem verfolgten Interesse des für die Verarbeitung Verantwortlichen gut begründet?
- Liegt eine detaillierte Bewertung der Notwendigkeit und Verhältnismäßigkeit der geplanten Verarbeitung für das Forschungsvorhaben vor?
- Wurden etwaige Risiken für die Rechte und Freiheiten der betroffenen Personen aufgrund der Form der geplanten Verarbeitung personenbezogener Daten und/oder Bioproben für das Forschungsvorhaben festgestellt? Wurde die Eintrittswahrscheinlichkeit der festgestellten Risiken bewertet?

[13] vgl. Art. 5 Abs. 1 lit. d EU-DS-GVO

[14] vgl. Art. 5 Abs. 1 lit. e EU-DS-GVO

[15] vgl. Art. 5 Abs. 1 lit. f EU-DS-GVO

[16] vgl. Art. 35 EU-DS-GVO

- Konnten geeignete und nachweisbar wirksame organisatorische und/oder technische Maßnahmen identifiziert werden, die die identifizierten hohen Risiken für die Rechte und Freiheiten der betroffenen Personen ausreichend eindämmen?
- Wurden gegebenfalls die Standpunkte der betroffenen Personen oder ihrer Vertreter (z. B. Patientenorganisationen) eingeholt?
- Wurden geeignete Prozesse eingerichtet, um Änderungen der mit der Verarbeitung personenbezogener Daten und/oder Bioproben verbundenen Risiken zu überwachen bzw. auf Ihre Wirksamkeit zu überprüfen?

V. Rechte der betroffenen Personen

- Wer ist Ansprechpartner der Probanden zur Wahrnehmung ihrer Betroffenenrechte?
- Wie und wo werden die Kontaktdaten zum Ansprechpartner für Betroffenenrechte veröffentlicht bzw. mitgeteilt?

A. Transparenz

- Wie wird sichergestellt, dass personenbezogene Daten und/oder Bioproben auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbare Weise verarbeitet werden?

B. Informationspflicht, wenn die Erhebung personenbezogener Daten und/oder Biomaterialproben bei der betroffenen Person erfolgt

- Erfolgt eine Information gemäß Art. 13 EU-DS-GVO i.V.m § 32 BDSG-neu rechtzeitig und vollständig? Liegen begründete Ausnahmen von den Informationspflichten vor?
- Wie werden die Informationspflichten[17] gemäß der EU-DS-GVO nachweisbar erfüllt?

C. Informationspflicht, wenn die Erhebung personenbezogener Daten und/oder Biomaterialproben nicht bei der betroffenen Person erfolgt

- Erfolgt eine Information gemäß Art. 14 EU-DS-GVO i.V.m. § 33 BDSG-neu rechtzeitig und vollständig? Liegen begründete Ausnahmen von den Informationspflichten vor?

D. Auskunft

- Wie können betroffene Personen Auskunft über verarbeitete personenbezogenen Daten und/oder Bioproben erhalten, die sie selbst betreffen?
- Wie können betroffene Personen eine Kopie der verarbeiteten personenbezogenen Daten erhalten, die sie selbst betreffen?
- Erfolgt eine Information gemäß Art. 15 EU-DS-GVO i.V.m. § 34 BDSG-neu vollständig? Liegen begründete Ausnahmen von den Informationspflichten vor?

[17] vgl. Art. 13 EU-DS-GVO

- Welche Prozesse greifen bei Auskunftsbegehren von betroffenen Personen? Wer ist daran beteiligt?

E. Löschung und Recht auf Vergessen werden

- Wie können betroffene Personen Ihr Recht auf Löschung von personenbezogenen Daten und/oder Vernichtung von Bioproben wahrnehmen, die sie selbst betreffen?
- Wie erfolgt die Löschung von personenbezogenen Daten bzw. Vernichtung von Bioproben im Einzelnen? Liegen begründete Ausnahmen von der Verpflichtung zur Löschung vor?
- Werden personenbezogene Daten nach dem Tod von Probanden gelöscht?
- Gibt es Regelfristen zur Löschung der personenbezogenen Daten?
- Wie werden personenbezogene Daten archiviert, die für wissenschaftliche Publikationen verwendet wurden?
- Wie wird das Recht auf Löschung durchgesetzt, wenn personenbzogene Daten öffentlich gemacht wurden?[18]

F. Einschränkung der Verarbeitung[19]

- Wie können betroffene Personen ihr Recht auf Einschränkung der Verarbeitung personenbezogener Daten und/oder Bioproben wahrnehmen, die sie selbst betreffen?
- Wie erfolgt die Einschränkung der Verarbeitung personenbezogener Daten und/oder Bioprobe im Einzelnen? Liegen begründete Ausnahmen von der Verpflichung zu Einschränkung der Verarbeitung vor?
- Wie wird die betroffene Person über die Aufhebung der Einschränkung der Verarbeitung personenbezogener Daten und/oder Bioproben unterrichtet?

G. Datenübertragbarkeit[20]

- Wie können betroffene Personen ihr Recht auf Datenübertragbarkeit personenbezogener Daten und/oder Bioproben wahrnehmen, die sie selbst betreffen?

H. Widerspruch der Verarbeitung[21] und Widerruf der Einwilligungserklärung[22]

- Wie können betroffene Personen ihr Recht auf Widerspruch gegen die Verarbeitung personenbezogener Daten und/oder Bioproben wahrnehmen, die sie selbst betreffen?
- Wie erfolgt ein Widerspruch gegen die Verarbeitung personenbezogener Daten und/oder Bioproben im Einzelnen? Liegen begründete Ausnahmen von der Verpflichtung zur Durchführung eines Widerspruchs vor?

[18] vgl. Art. 17 Abs. 2 EU-DS-GVO

[19] vgl. Art. 18 EU-DS-GVO

[20] vgl. Art. 20 EU-DS-GVO

[21] vgl. Art. 21, insb. Abs. 6 EU-DS-GVO

[22] vgl. Art. 7 Abs. 3 EU-DS-GVO

- Wie können betroffenen Personen ihrer Einwilligungserklärung widerrufen (Mail, Telefon, Fax, persönlich, Komplettwiderruf, Teilwiderruf)?
- Wer bearbeitet Erklärungen zum Widerspruch gegen die Verarbeitung personenbezogener Daten und/oder Bioproben und zum Widerruf einer Einwilligungserklärung?
- Wo werden Erklärungen zum Widerspruch gegen die Verarbeitung personenbezogener Daten und/oder Bioproben und zum Widerruf einer Einwilligungserklärung dokumentiert, protokolliert und aufbewahrt?
- Auf welche Weise werden Erklärungen zum Widerspruch gegen die Verarbeitung personenbezogener Daten und/oder Bioproben und zum Widerruf einer Einwilligungserklärung gegenüber Dritten durchgesetzt?
- Welche Auswirkungen haben Erklärungen zum Widerspruch gegen die Verarbeitung personenbezogener Daten und/oder Bioproben und zum Widerruf einer Einwilligungserklärung (Löschung, Vernichtung, Sperrung, Anonymisierung, Nutzungseinschränkung)?
- Können Widerspruch und Widerruf zurück genommen werden? Was geschieht ggf. in einem solchen Fall?

VI. Organisatorische Maßnahmen

Die organisatorischen Maßnahmen (Verantwortlichkeiten, Verpflichtungen und datenschutzrelevante Prozesse) im Projekt sollen beschrieben werden.

A. Gremien und Funktionen

- Wer bildet das Leitungsgremium (Mitglieder als Rolle oder Person)? Welches sind seine Aufgaben?
- Wer nimmt die Funktionen des Ausschusses Datenschutz (z. B. als Use and Access Committee) wahr (Mitglieder als Rolle oder Person)? Welches sind seine Aufgaben?
- Wer gehört welchem Beirat an?
- Wurde ein betrieblicher bzw. behördlicher Datenschutzbeauftragter bestellt und sind dessen Kontaktdaten für die betroffenen Personen einsehbar?
- Wurde ein Beauftragter für die IT-Sicherheit bestellt?

B. Interne Regelungen

- Wird in Satzungen oder Gesellschafterverträgen etwas für das Forschungsvorhaben Relevantes geregelt?
- Welche Richtlinien (Policies), Dienstanweisungen (SOPs) gelten für Beschäftigte am Forschungsvorhaben?

C. Zugriffsregelungen

- Welche Rollen können Beschäftigte am Forschungsvorhaben einnehmen?
- Welche Rechte gehören zu den jeweiligen Rollen? Wer kann welche personenbezogenen Daten sehen, eingeben, verändern oder löschen? Wer hat welchen Zugriff zu Bioproben?
- Welche Rollenkonflikte können auftreten und wie werden sie aufgelöst?
- Wie werden die Zugriffsrechte überwacht bzw. ihre Einhaltung erzwungen?

D. Datentreuhänderschaft

- Wie ist die Unabhängigkeit eines Datentreuhänderdienstes gewährleistet?
- Wie ist die Funktionsübertragung der Datentreuhänderschaft geregelt?
- An welche Regelungen ist der Datentreuhänderdienst gebunden?

E. Nutzung von personenbezogenen Daten und Bioproben

- Wird die Einwilligungserklärung in Papierform oder in elektronischer Form eingeholt?
- Wie lange ist eine Einwilligungserklärung gültig? Läuft diese ggf automatisch aus?
- Wird die Einwilligungserklärung erneut eingeholt? (z. B. bei Follow-Ups)
- Wie und wo und wie lange werden Einwilligungserklärungen aufbewahrt?
- Wer ist für die Verwaltung der Einwilligungserklärungen zuständig?
- Welche Prozesse greifen bei einem Widerspruch gegen die Verarbeitung personenbezogener Daten und/oder Bioproben von betroffenen Personen? Wer ist daran beteiligt?
- Wer ist für die Durchführung der einzelnen Prozesse der Pseudonymisierung, Anonymisierung, Einschränkung der Verarbeitung und Löschung von personenbezogenen Daten und/oder Bioproben zuständig?
- Welche Prozesse greifen bei einem Begehren auf Einschränkung der Verarbeitung von betroffenen Personen? Wer ist daran beteiligt?
- Welche Prozesse greifen bei einem Löschbegehren von betroffenen Personen? Wer ist daran beteiligt?
- Ist nach Durchführung dieser Verfahren ggf. eine Information an Probanden erforderlich? Wer ist dafür zuständig?
- Wie ist die Nutzung von personenbezogenen Daten und/oder Bioproben grundsätzlich geregelt (z. B. nur interne Nutzung, anonymisierter Export, Zugang mit Auflagen, Datenauswertung nur vor Ort mit Herausgabe von Ergebnissen)?
- Wer entscheidet über die Nutzung von personenbezogenen Daten und/oder Bioproben im Einzelfall und auf Antrag?

- Welche Auflagen sind mit der Nutzung von personenbezogenen Daten und/oder Bioproben verbunden? Wo werden diese Auflagen geregelt und vereinbart (z. B. Anerkennen von Nutzungsordnungen, Datennutzungsvertrag, Material Tranfer Agreement)?
- Gibt es vertragliche Regelungen (z. B. Datennutzungsvertrag) mit dem Datenempfänger, die eine erneute Weitergabe personenbezogener Daten, die Speicherdauer und Versuche zur Re-Identifikation von Probanden regeln?
- Gibt es vertragliche Regelungen (z. B. Material Transfer Agreement) zwischen bereitstellender Einrichtung und den Empfängern von Bioproben, die eine erneute Weitergabe der Bioproben, die Aufbewahrung und Verbote von Versuchen zur Re-Identifizierung von Probanden regeln?
- Wer ist am Prozess der Bereitstellung von personenbezogenen Daten und/oder Bioproben zuständig bzw. daran beteiligt?
- Welche Prozesse greifen bei einem Begehren auf Datenübertragung personenbezogener Daten und/oder Bioproben von betroffenen Personen? Wer ist daran beteiligt?
- Wie erfolgt die Datenübertragung personenbezogener Daten und/oder Bioproben im Einzelnen?

F. Monitoring-Verfahren

- Gibt es ein Monitoring-Verfahren und wie sieht es aus (z.B. Monitoring Manual)?
- Wer ist als Monitor vorgesehen?
- Wie läuft ein Monitoring ab?
- Welche Daten sieht der Monitor und welche Bearbeitungsrechte (z.B. Sperren, Löschen) hat er?

G. Datenqualitätssicherung

- In welcher Form werden qualitätssichernde Maßnahmen in den einzelnen Arbeitsmaßnahmen integriert und wirksam nachgehalten?
- Welche Datenqualitätssicherungsverfahren werden für das Forschungsvorhaben vorgesehen?
- Wird ein Datenqualitätsmanager für das Forschungsvorhaben vorgesehen? Wenn ja, welche personenbezogenen Daten kann er einsehen?
- Welche gesonderten Anforderungen an den Datenschutz ergeben sich sich aus dem Datenqualitätssicherungsverfahren in Bezug auf die Re-Identifikation von Probanden, die Rückmeldung an Probanden und die Datenerhebung?

H. Internes Audit-Verfahren

- Gibt es ein internes Auditverfahren und wie sieht es aus (Beschreibung)?
- Wer kontrolliert die Einhaltung der technischen und organisatorischen Sicherheitsmaßnahmen?

- Wer ist für die Konfiguration der Audit Trail-Mechanismen zuständig?
- Wo werden erforderliche Verfahren und Prozesse dokumentiert?
- Was wird jeweils konkret erfasst?
- Wer hat Zugriff auf diese Auditierungs-Protokolle?
- Welche Befugnisse hat ein Auditor?
- Werden Sicherheitsüberprüfungen anlassbezogen oder regelmäßig (wie oft konkret) durchgeführt?
- Werden Überprüfungen stichprobenartig oder vollständig durchgeführt? Wie läuft das Verfahren dazu ab?
- Inwiefern werden Zugriffe sowohl auf die personenbezogene Daten als auch auf die datenspeichernden Systeme protokolliert?
- Wird zu diesem Zweck eine spezifische Software eingesetzt? Wenn ja, welche genau und aus welchem Grund?
- Wie lange werden Protokolldateien gespeichert?[23]

I. Auswertung von personenbezogenen Daten

- Wer ist für die Auswertung der Daten verantwortlich?
- Auf welche Weise werden die Daten ausgewertet?
- Werden die Daten zur Auswertung pseudonymisiert bzw. anonymisiert?

J. Räumliche Maßnahmen

- Welche räumlichen Maßnahmen sind aus Datenschutzsicht erforderlich?
- Wie werden die Räumlichkeiten geschützt?
- Wer hat Zugang zu den Räumlichkeiten?
- Wer vergibt Zugangsberechtigungen?

K. Personelle Maßnahmen

- Werden die am Forschungsvorhaben beteiligten Beschäftigten auf das Datengeheimnis verpflichtet und unterwiesen?
- Welche personellen Maßnahmen sind aus Datenschutzsicht erforderlich?
- Wie ordnen sich diese Maßnahmen in die Hierarchie der oder des für die Verarbeitung Verantworlichen ein?
- Haben die am Forschungsvorhaben beteiligten Beschäftigten eine Datenschutzschulung absolviert? Sind ggf. gesonderte Schulungen im Rahmen des Forschungsvorhabens notwendig (z. B. auf SOPs)?

[23] gem. Empfehlung des BSI (IT-Grundschutzkatalog)[vii]

- Wie wird die Einhaltung von SOPs nachhaltig überwacht? Was passiert bei Verstößen?

L. Verletzungen des Schutzes personenbezogener Daten

- Welche Maßnahmen zur Feststellung von Verletzungen des Schutzes personenbezogener Daten sollen eingerichtet bzw. genutzt werden?
- Wie soll sichergestellt werden, dass eine Meldung dieser Verletzung innerhalb der gesetzlichen Frist von möglichst 72 Stunden an die zuständige Aufsichtsbehörde für den Datenschutz erfolgen kann?
- Welche Prozesse zur Mitteilung über eine Verletzung des Schutzes personenbezogener Daten an die betroffenen Personen wurden eingerichtet und wer ist daran wie beteiligt?
- Wurde ein Notfallplan entwickelt, der alle Aspekte dieser Meldungen berücksichtigt?

VII. Technische Maßnahmen

Es soll beschrieben werden, wie die für die Einhaltung der Datenschutzanforderungen notwendigen Maßnahmen aus Sicht der informationstechnischen Implementierung gestaltet werden sollen.

A. Systemkomponenten

- Welche Module des TMF-Konzepts sind relevant?
- Welche Register, Biobanken einschließlich Biomaterialverwaltung, Studiendatenbanken, Bilddatenbanken, Forschungsdatenbanken und Analysedatenbanken sind geplant?
- Wurde im Falle eines Registers entschieden, ob es im Klinischen Modul oder im Forschungsmodul angesiedelt werden soll? (Als Entscheidungshilfe werden in der folgenden Tabelle Gemeinsamkeiten und Unterschiede dieser beiden Module aufgeführt.) Anmerkung: Ein großes Verbundprojekt kann mehrere Register, auch unterschiedlicher Art umfassen.
- Wurde im Falle einer Biobank entschieden, ob für die Aufbewahrung der Annotationsdaten (siehe Glossar) eine Klinische Datenbank oder eine Forschungsdatenbank besser geeignet ist? (Auch hierfür dient die folgende Tabelle als Entscheidungshilfe.)
- Wurde im Falle einer Bilddatenbank entschieden, ob sie Teil des Klinischen Moduls oder des Forschungsmoduls sein soll oder ob der Aufbau eines separaten Bilddatenmoduls erforderlich ist? (Auch hierfür dient die folgende Tabelle als Entscheidungshilfe.)

Klinisches Modul	Forschungsmodul
Allgemeine Datenschutz- und Schweigepflichtsregelung	Allgemeine Datenschutzregelung, evtl. Spezialgesetze (Krebsregister)
Langfristige Datenaufbewahrung	Langfristige Datenaufbewahrung
Offener Forschungsansatz	Offener Forschungsansatz
Forschung und Behandlung verzahnt	Forschung und Behandlung deutlich getrennt
Dateneingabe/-übernahme aus Behandlungszusammenhang	Kein Online-Zugang aus Behandlungszusammenhang, oft zusätzliche Datenerhebung, z. B. „soziodemographische“ Daten

B. Systemmodell

Daten (-kategorien), Prozesse, Datenflüsse und -speicher sollen so weit beschrieben werden, dass die IT-Architektur in dem Umfang deutlich wird, wie sie für die Identifizierung der nötigen Datenschutz- und IT-Sicherheitsmaßnahmen notwendig ist.

- Liegt eine Beschreibung bzw. Kategorisierung der zu erhebenden Daten vor?
- Welche Datenkategorien, -formate und -typen sollen genutzt werden?
- Gibt es heterogene, homogene und/oder unstrukturierte Datentypen?
- Sind die Prozesse mit den nötigen Details beschrieben, um die IT-Architektur zu begründen und notwendige Datenschutz- und IT-Sicherheitsmaßnahmen zu identifizieren?
- Wie sollen die personenbezogenen Daten unter dem Gesichtspunkt der informationellen Gewaltenteilung verteilt werden? Wie läuft der Datenfluss zwischen verschiedenen Modulen und Komponenten ab?
- Welche zentralen/verbindenden Komponenten werden benötigt (z. B. Rechtemanagement, Datenqualitätssicherung, Probandenmanagement, Kontaktmanagement, Identitäts-management, Pseudonymmanagement, Einwilligungsmanagement)?
- Wo sollen Systemkomponenten logisch und physisch angesiedelt werden? Unter welcher Verantwortung?
- Welche Rolle spielen diese Komponenten in den Prozessen des Forschungsvorhabens? (Hier wäre eine tabellarische Darstellung der Komponenten und Prozesse hilfreich, z. B. Pseudonymisierung, Re-Pseudonymisierung, Schweigepflicht, Datenqualitätssicherung, Widerruf, Löschung.)
- Wie kann eine grafische Darstellung der gesamten Datenflüsse im Detail aussehen?

C. Technische Infrastruktur

- Welche Software soll eingesetzt werden (z. B. Datenbank, EDC-System, Probenverwaltung, Pseudonymverwaltung, Einwilligungsverwaltung, Personenverwaltung)?
- Welche Server sollen betrieben werden? An welchen Standorten?
- Welche externen Dienste sollen in Anspruch genommen werden? (Wie sieht es mit der Mandantenfähigkeit dieser Dienste aus?)

D. Authentifizierung und Berechtigungen

Die eingesetzten technischen Verfahren sollen dargestellt und ihre Umsetzung beschrieben werden.

- Welches Authentifizierungsverfahren[24] wird eingesetzt?
- Wurde das Verfahren zur Autorisierung beschrieben (Rollen- und Rechtesteuerung)?
- Für welche Bereiche ist das Rechte-Rollenkonzept gültig?
- Welche Rollen gibt es und welche Rechte haben sie jeweils (ggf. tabellarische Übersicht)?
- Wer ist für die Zuweisung der Rollen und Rechte zuständig?
- Wie werden Zugriffe gesteuert?
- Welche Maßnahmen werden vorgesehen, um nachträglich überprüfen und feststellen zu können, ob und von wem personenbezogene Daten eingesehen, eingegeben, verändert oder gelöscht wurden (z. B. durch Protokolle)?
- Wie wird mit den Protokollen umgegangen?

E. Absicherung des Netzwerks (IT-Sicherheit)

Im Datenschutzkonzept sollen die prinzipiellen Maßnahmen nur kurz dargestellt werden. Technische Details sollten im IT-Sicherheitskonzept beschrieben werden.

- Wie wird die Netzkommunikation geschützt?
- Wie ist der Schutz des Netzwerkes auf physischer, logischer und Anwendungsebene geregelt (z. B. räumliche Trennung von Serverinfrastrukturen, Firewalls, Routing, IP-Filter, Authentifizierung)?
- Wer hat Zugriff auf das Projektnetzwerk?
- Wie werden Server gegen Angriffe von außen / unberechtigte Zugriffe geschützt (insb. Serverhärtung[25])?
- Wie wird für die Sicherheit bei Endnutzern gesorgt (insb. notwendige lokale Sicherheitsmaßnahmen für Client-Rechner und andere Endgeräte) bzw. welche Voraussetzungen müssen zum Aufbau einer Netzwerkverbindung zu den Projektdatenbanken erfüllt sein?

[24] Empfehlung: Nach Möglichkeit bessere Authentifizierungsverfahren als bloßen Passwortschutz vorsehen.

[25] Fachbegriff, der beschreibt, wie weit Server gegen Angriffe aus dem Netz immun sind.

- Wie werden Zertifikate verteilt und genutzt?
- Werden Virtualisierungstechniken eingesetzt?
- Werden relevante Teile der IT-Grundschutzkataloge des BSI berücksichtigt (z.B. Zugangskontrollen, Datenträgerkontrollen)?

F. Backup-Strategie

- Wie und wie oft werden Daten gesichert?
- Wie werden gesicherte Daten geschützt?
- Werden die Datensicherungen verschlüsselt? Wenn ja, wer hat die Zugangsdaten? Wer hat eine Kopie der Zugangsdaten? Wo werden die Zugangsdaten für den Ernstfall hinterlegt? Wer ist für die Verschlüsselung verantwortlich? Wie wird im Detail verschlüsselt? Wie beeinflusst die Verschlüsselung die automatische Datensicherung?
- Wie werden die Daten vor unerlaubtem Zugriff geschützt?
- Wie werden die Daten vor versehentlicher / vorsätzlicher Änderung / Löschung geschützt?
- Wer hat Zugriff auf die Datensicherungen?
- Wie werden Daten im Bedarfsfall aus den Backup-Beständen gelöscht?
- Gibt es redundante Systeme im Falle eines Systemausfalls?

G. Eingesetzte Verschlüsselungstechnik

Die eingesetzten Verschlüsselungsverfahren und ihre Einbindung sollen dargestellt werden.

- Welche Verschlüsselungstechnik wird für die Sicherung der Kommunikationsverbindungen eingesetzt?
- Welche Verschlüsselungstechnik wird für die Sicherung der Datenspeicher eingesetzt?
- Welche Verschlüsselungstechnik wird für Pseudonymisierungsverfahren eingesetzt?

H. Pseudonymisierung

Die technischen Umsetzungsaspekte der Pseudonymisierungsverfahren sollen dargestellt werden.

- Werden Probanden jeweils eindeutige Kennungen in Form von Pseudonymen zugeordnet?
- Wenn ja, welche technischen Verfahren liegen dieser Zuordnung zugrunde?
- Wie erfolgt eine Depseudonymisierung (Auflösung eines Pseudonyms)?
- Falls in verschiedenen Modulen verschiedene Pseudonyme verwendet werden: Wie erfolgt die Zuordnung?
- Ist der Einsatz von Record-Linkage-Verfahren geplant?
- Falls das Pseudonymisierungsverfahren geändert werden muss: Wie erfolgt die Umpseudonymisierung?

I. Ausfallschutz

- Welche Auswirkungen kann ein Ausfall der Systeme auf den Projektbetrieb haben?
- Welche Maßnahmen können dagegen getroffen werden?

J. Die „Gebote“ der Datenschutzgesetze zur IT-Sicherheit

- Wurden die Gebote der Datenschutzgesetze zur IT-Sicherheit ausreichend berücksichtigt? Anmerkung: Die Sicherheit der Verarbeitung personenbezogener Daten unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten betroffener Personen, ist ein Kernelement der EU-DS-GVO[26]. Demnach sind geeignete technische und organisatorische Maßnahmen vorzusehen, die ein dem Risiko angemessenes Schutzniveau gewährleisten sollen, um personenbezogene Daten zu pseudonymisieren und zu verschlüsseln, die Fähigkeit, Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit von Systemen und Diensten im Zusammenhang der Verarbeitung auf Dauer sicherzustellen sowie die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen.

VIII. Vergleich mit dem TMF-Datenschutzleitfaden

Abweichungen vom Datenschutzleitfaden sollen zusammengefasst und begründet werden. Dies dient zur erleichterten Beurteilung durch die TMF und durch Datenschutzbeauftragte.

- In welchen Punkten sind Abweichungen vom Leitfaden notwendig?
- Welche Verhältnismäßigkeitsabwägungen[27] liegen den Abweichungen zugrunde?

[26] vgl. Art. 32 EU-DS-GVO

[27] Einige oft vorkommende vereinfachte Architekturvarianten werden im Anhang des generischen Datenschutzkonzepts für Biomaterialbanken (siehe Präambel) definiert.

Glossar

Grundlage dieses Glossars sind Begriffsdefinitionen aus dem Leitfaden der TMF zur Erstellung eines Datenschutzkonzepts für ein medizinisches Forschungsprojekt.

Annotation (-sdaten)

Medizinische Daten (MDAT), die die zu einer Probe gehörigen diagnostischen und therapeutischen Informationen enthalten. Sie sind zu unterscheiden von reinen Verwaltungsdaten, die nicht-personenbezogene technische und organisatorische Informationen zu einer Probe darstellen.

Anonymisierung

Anonymisierung ist die Aufhebung der Personenbezogenheit von Daten zu einer Person. „Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können“.

Archivierung

Dauerhafte Aufbewahrung von Daten auf geeigneten Datenträgern

Audit

Als Audit werden allgemein Untersuchungsverfahren bezeichnet, die dazu dienen, Prozessabläufe hinsichtlich der Erfüllung von Anforderungen und Richtlinien zu bewerten.

Aufklärung

Siehe *Patienteninformation*

BDSG

Bundesdatenschutzgesetz

Biobank (Biomaterialbank, Probenbank, Gewebebank, Genbank, Probensammlung)

Eine Biobank ist eine Einrichtung, die Proben menschlicher Körpersubstanzen sammelt, ggf. aufbereitet, durch demographische und krankheits- bzw. fragestellungsbezogene („medizinische“) Daten des Probanden ergänzt und Proben und Daten in geeigneter Form für Forschungszwecke zur Verfügung stellt.

Biomaterial

Siehe *Probe*

Datentreuhänder

Siehe *Treuhänder*

Depseudonymisierung

Befugte Wiederherstellung des Personenbezugs von pseudonymisierten Daten und Proben

Einwilligungserklärung (informed consent, Einwilligung nach Aufklärung, Einverständniserklärung)

Die vom Datenschutzrecht geforderte Voraussetzung zur Verarbeitung personenbezogener Daten des Betroffenen, sofern diese nicht aufgrund eines Gesetzes erlaubt ist.

EU-DS-GVO

Europäische Datenschutz-Grundverordnung

IDAT = Personenbezogene oder identifizierende Daten

Personenbezogene Daten „sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.“[28]

MDAT = Forschungsdaten oder medizinische Daten

MDAT ist die übergreifende Bezeichnung für Daten, die zum Zwecke der Forschung in der zentralen Datenbank eines medizinischen Forschungsverbundes gespeichert werden. MDAT umfassen in der Regel klinische Sachverhalte wie Befunde und Diagnosen sowie soziodemographische Daten, die eine entsprechende Klassifikation des Patienten oder Probanden zu wissenschaftlichen Zwecken erlauben.

Monitor (Klinischer Monitor)

Der Klinische Monitor überwacht Klinische Prüfungen, insbesondere nach dem Arzneimittelgesetz.

Patient

siehe *Proband*

Patienteninformation

Mitteilung an den Teilnehmer eines Forschungsvorhabens, was mit seinen Daten und ggf. Proben passieren wird.

Proband

Patient und Proband sind die Personen, die dem Forschungsverbund Daten zu ihrer Gesundheit und Materialien ihres Körpers zu Zwecken der biomedizinischen Forschung zur Verfügung stellen. Erfolgt die Datengewinnung oder Probenentnahme im Behandlungszusammenhang, ist der Spender „Patient“. Erfolgt die Datengewinnung oder Probenentnahme im Forschungszusammenhang, ist der Spender „Proband“. Der Begriff „Proband“ wird auch als Oberbegriff für „Patient und/oder Proband“ verwendet, insbesondere, wenn eine Kontrollgruppe in die Studie involviert ist.

[28] vgl. Art. 3 Nr. 1 EU-DS-GVO

Probe

Dem menschlichen Körper zu diagnostischen oder wissenschaftlichen Zwecken entnommene Substanz

Pseudonymisierung

Pseudonymisierung „ ist die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.“[29]

PSN = Pseudonym

Das PSN ist ein nichtsprechender Identifikator eines Patienten oder Probanden (Buchstaben oder Zahlen, die nicht auf die personenidentifizierenden Daten rückschließen lassen).

Reidentifizierung

Im Wege der Reidentifizierung wird der Personenbezug von anonymisierten oder pseudonymisierten Daten und Proben unbefugt wieder hergestellt.

Schweigepflicht

Die ärztliche Schweigepflicht ist die ethische und rechtliche Pflicht des Arztes, Verschwiegenheit über alles zu wahren, was ihm bei der Ausübung seines Berufes über einen Patienten bekannt wird (Wahrung des Patientengeheimnisses).

TMF

Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V.

Treuhänder

Der Datentreuhänder ist eine rechtlich, räumlich und personell selbstständige und unabhängige Stelle, die idealerweise einer besonderen Geheimhaltungspflicht unterliegt, z. B. ein Notar oder ein externer Arzt.

Widerruf

Unter dem Widerruf der Daten- oder Probenverwendung versteht man die teilweise oder vollständige Rücknahme der Einwilligungserklärung (siehe dort) mit der Folge, dass Daten (Datenkategorien) und Proben vom Forschungsverbund nicht bzw. nur noch in eingeschränktem Maße für eigene oder fremde Forschungsvorhaben verwendet werden dürfen. Aus der Vereinbarung mit dem Patienten oder Probanden kann sich nach dem Widerruf der Einwilligungserklärung auch die Pflicht ergeben, Daten zu löschen oder zu anonymisieren bzw. die Probe an den Probanden herauszugeben, sie zu vernichten oder zumindest zu anonymisieren. Es sind auch Fälle denkbar, in denen ein Widerruf der Einwilligungserklärung ausgeschlossen ist.

[29] vgl. Art. 3 Nr. 5 EU-DS-GVO

Referenzen*

* [alle Abruf: 2017-11-12]

[i] MOSAIC (Projekt „Open Source Werkzeuge für zentrales Datenmanagement in der epidemiologischen Forschung“ der Universität Greifswald), Vorlage Datenschutzkonzept:
https://mosaic-greifswald.de/werkzeuge-und-vorlagen/datenschutzkonzept.html

[ii] Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie (GMDS e.V.), AG "Datenschutz und IT-Sicherheit im Gesundheitswesen" (DIG), Leitfaden zur Erstellung eines Datenschutzkonzepts:
https://www.gesundheitsdatenschutz.org/doku.php/gmds-dgi-empfehlungen

[iii] 92. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, Standard-Datenschutzmodell (SDM)
https://www.datenschutzzentrum.de/uploads/SDM-Methode_V_1_0.pdf

[iv] Rat für Informationsinfrastrukturen (RFII), Datenschutz und Forschungsdaten, Aktuelle Empfehlungen März 2017
http://www.rfii.de/de/category/dokumente/

[v] Bundesdatenschutzgesetz (BDSG):
https://www.gesetze-im-internet.de/bdsg_1990/index.html#BJNR029550990BJNE001902301

[vi] Europäische Datenschutz-Grundverordnung (EU-DS-GVO)
http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679&from=DE

[vii] Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutz-Kataloge
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html