UNIVERSITÄT BIELEFELD
Medizinische Fakultät OWL

Handlungsleitfaden zur Erstellung eines Datenschutzkonzeptes für Forschungsprojekte

Stand: 07.11.2023
Version: 1.0
Bearbeiter*in: Isabell Jungnitz

Inhalt

1. Zweck des Dokumentes

Diese Handreichung bietet Leitfragen für die Erstellung eines Konzepts zur Gewährleistung datenschutzrechtlicher Anforderungen in medizinischen Forschungsprojekten (Datenschutzkonzept). Ein Datenschutzkonzept konkretisiert die gesetzlichen Vorgaben und erleichtert den Nachweis über deren Einhaltung. Insbesondere Informationen für betroffene Personen wie z.B. Probanden, Verträge mit Kooperationspartnern und Anträge an Ethikkommissionen lassen sich auf Basis eines Datenschutzkonzepts einfacher erstellen.

Die Leitfragen dieser Handreichung orientieren sich an den Empfehlungen der Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V. (TMF) AG Datenschutz.
Es sollten **zu allen nummerierten Gliederungspunkt** Angaben gemacht werden, wobei nicht jede Einzelfrage obligatorisch ist. Die Beantwortung der Leifragen zielt auf eine nachvollziehbare Begründung, warum die Verarbeitung personenbezogener Daten im konkreten Forschungsvorhaben erforderlich und gegenüber den betroffenen Personen angemessen ist.

Zwingende erforderlich für die Erstellung eines Datenschutzkonzepts ist eine strukturierte Vorplanung mit folgenden Inhalten:

- Projektziele und das zu ihrer Erreichung geplante Vorgehen, einschließlich der wissenschaftlichen Methodik,
- Projektbeteiligte (interne/externe), organisatorische Strukturen, Verantwortungs- und Aufgabenzuweisung, Prozesse und Kommunikationswege innerhalb des Forschungsprojekts oder -verbunds,
- ein technisches Konzept hinsichtlich geplanter Datenerfassung, Speicherung, Übermittlung und weiteren Verwendung bis zur Löschung,
- sowie dessen Umsetzung mit IT-Architektur, Datenspeichern (einschließlich etwaiger Biomaterialaufbewahrung) und Zugriffsrechten.

2. Darstellung des Forschungsvorhabens

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

- Was ist das Ziel des Forschungsvorhabens? Wie soll es erreicht werden?
- Welche Fragestellungen, Anforderungen oder Herausforderungen sollen durch die Umsetzung des Vorhabens gelöst werden?
- Wie grenzt sich dieses Forschungsvorhaben zu ähnlichen ab?
- Wie sind Behandlungs-und Forschungskontext im Rahmen des Forschungsvorhabens abgegrenzt?
- Welche wissenschaftliche Methodik, soll angewendet werden?
- Wie weit kann mit anonymisierten oder pseudonymisierten Daten gearbeitet werden bzw. warum ist ein Personenbezug unvermeidbar?
- Wie lang ist die vorgesehen Laufzeit des Forschungsvorhabens?
- Ist eine Weiterführung des Forschungsvorhabens auch nach Ablauf der aktuellen Projektfinanzierung geregelt?
- Welche (Kooperations-) Partner sind an dem Vorhaben beteiligt?
- Welche Infrastruktur (bezogen auf personenbezogene Daten) soll genutzt werden? Durch wen wird diese betrieben?
- Hat eine Beratung durch die Ethikkommission stattgefunden, bzw. wurde ein Antrag gestellt oder durch wen wird dies zukünftig erfolgen?

3. Organisatorische Struktur

3.1. Verantwortlicher Verarbeiter

- Welche Organisationseinheit ist für die Forschung mit personenbezogenen Daten Verantwortlicher i.S.d. DSGVO (z. B. Universität/Institut/Klinik, andere Organisation)?
- Welche Forschungsschwerpunkte werden hier verfolgt?
- Sind verantwortliche Entscheidungsträger, Administratoren sowie die jeweiligen Anwender zur Vertraulichkeit verpflichtet, hinsichtlich der geplanten Datenverarbeitung eingewiesen, sowie speziell zu Datenschutz und IT-Sicherheit geschult?
- Wurde ein Datenschutzbeauftragter für den / die Verantwortlichen bestellt und wie lauten die jeweiligen Kontaktdaten? Gibt es weitere Ansprechpersonen, die bei der Umsetzung des Datenschutzes unterstützen (DISM)?

3.2. Beteiligte, Kooperationspartner, gemeinsam für die Verarbeitung Verantwortliche

- Welche anderen Organisationen, Partner und Institutionen sind beteiligt?
- Gibt es mehrere für die Verarbeitung Verantwortliche?
- Wodurch werden die Verantwortungsbereiche definiert?
- Welcher Verantwortliche wird welche datenschutzrechtlichen Verpflichtungen wahrnehmen?
- Gibt es Gründe für eine Beteiligung von Kooperationspartnern oder Dienstleistern und wenn ja, welche?
- Welche Funktionen bzw. Aufgaben übernehmen welche Partner und Stellen im Rahmen des Forschungsvorhabens?
- Wodurch wird die Zusammenarbeit im Forschungsvorhaben geregelt (werden), z. B. Kooperations- oder Konsortialvertrag, Geschäftsordnung, Satzung?
- Werden Treuhänderdienste (Datentreuhänder, Vertrauensstelle) eingebunden und falls ja wie?
- Gibt es vertragliche Regelungen über die Weitergabe von Bioproben (z. B. Material Transfer Agreement)?
- Welche organisatorischen Abhängigkeiten könnten Interessenkonflikte bei Durchführung des Forschungsprojekts auslösen, z.B. Auftragsforschung?

3.3. Finanzierung durch Dritte

- Wer fördert das Forschungsvorhaben wie lange (z. B. Grundfinanzierung, befristete Projektfinanzierung, Auftragsforschung)?
- Handelt es sich um ein drittmittelgefördertes Projekt? Ist das Referat Forschung und Karriereentwicklung beteiligt?
- Welche 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?

3.4. Internationale Aspekte

- Welche ausländischen Projektpartner sind beteiligt?
- 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, insbesondere Standardvertragsklauseln oder geeignete Garantien)?
- Welche Vereinbarungen oder Verträge mit ausländischen Partnern wurden getroffen?

4. Studiendesign

Bei Forschung im medizinischen Kontext werden regelmäßig sensible Datenkategorien gemäß Art. 9 DSGVO verarbeitet, z.B. Gesundheitsdaten oder genetische Daten. Bitte beschreiben Sie das Vorhaben in seinem regulatorischen Rahmen und das Vorgehen entlang des gesamten Data-LifeCycle, d.h. von der ursprünglichen Erhebung bis zur Löschung.

4.1. Gesetzliche Rahmenbedingungen

- Handelt es sich um eine klinische Studie, eine interventionelle (= experimentelle) oder nicht interventionelle (= beobachtende) Studie, sowie um eine prospektive oder retrospektive Studie?
- Erfolgt die Datenerhebung im Sinne einer Querschnittstudie oder Längsschnittstudie?
- Handelt es sich um eine klinische Prüfung (CTR / MDR)?
- Unterliegt das Forschungsvorhaben anderen Spezialgesetzen (wie z. B. Krebsregistergesetze, Sozialgesetzbücher, Bundesmeldegesetz)?
- Sollen personenbezogene Daten aus anderen Quellen mit speziellen gesetzlichen Rahmenbedingungen verwendet werden (z. B. Sekundärnutzung von Routinedaten, Meldedaten, Versicherungsdaten)?
- Sind bundeslandspezifische Regelungen bei Sekundärnutzung von Behandlungsdaten zu beachten (z. B. Gesundheitsdatenschutzgesetz NRW, andere Landeskrankenhausgesetze)?
- Sollen personenbezogene Daten und/oder Bioproben aus der Behandlungsdokumentation für das Forschungsvorhaben genutzt werden oder aus dem Forschungsvorhaben in eine Behandlungsdokumentation zugeführt werden (Schweigepflichtentbindung, Übermittlungserlaubnis)?
- Ist eine direkte Rückwirkung auf die Behandlung einzelner Patienten bzw. Probanden zu erwarten oder denkbar?

4.2. Umfang der Verarbeitung von Daten bzw. Bioproben für das geplante Forschungsvorhaben

- Welche Personen/Personengruppen sind von der geplanten Datenverarbeitung betroffen (z.B. Patienten, Angehörige, Beschäftigte beteiligter Institutionen, Beschäftigte nicht beteiligter Institutionen, externe behandelnde Ärzte, …)?
- Betrifft das Forschungsvorhaben Kinder oder vulnerable Personen (z. B. nicht einwilligungsfähige Personen, abhängig Beschäftigte)?
- Wie sind Ein- und Ausschlusskriterien für Probanden definiert?
- Welche personenbezogenen identifizierenden Daten von welchen Personen/Personengruppen sollen verarbeitet werden (z.B. Unterscheidung von Patienten-Anamnese-Daten und Diagnostik-Daten; sowie bei Beschäftigtendaten z. B. Personalverwaltungsdaten, Gehaltsdaten, Dienstplanung etc.)?
- Welche personenbezogenen medizinischen Daten von welchen Personen/Personengruppen sollen verarbeitet werden?
- Sollen Biomaterialien entnommen und ggf. gelagert werden?

- Sollen andere besondere Kategorien personenbezogener Daten i.S.d. Artikel 9 DSGVO verarbeitet werden und falls ja, welche?
- 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, Datennutzungsvertrag, Material Transfer Agreement)?
- Wenn die Daten nicht bei der betroffenen Person direkt erhoben werden: Wie wird die Information der betroffenen Person gemäß Art. 14 DSGVO sichergestellt?
- 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?

4.3. Beschreibung Art der Datenerhebung

- Wie erfolgt die Erhebung personenbezogener Daten (z.B. Befragung, Probenentnahme, Auswertung vorhandener Daten, Dokumentation durch Studienpersonal etc.) konkret?
- Wer ist verantwortlich für die Information der Probanden und ggf. die Einholung der Einwilligungserklärung nach Aufklärung? Wie und wie lange werden Einwilligungserklärungen aufbewahrt?
- Wer führt die Erhebung personenbezogener Daten und/oder Bioproben durch? Sind ggf. Partner an der Erhebung personenbezogener Daten und/oder Bioproben beteiligt?
- Wie und durch wen werden die personenbezogenen Daten bei der Erhebung qualitätsgesichert (z.B. Prüfung auf Plausibilität und Vollständigkeit)?
- Wie oft werden personenbezogene Daten einer einzelnen Person erhoben (Follow-ups)?

4.4. Speicherung personenbezogener Daten

- Wie erfolgt die Speicherung personenbezogener Daten technisch (z.B. Papierform, eCRF etc.)?
- In welchem IT-System werden welche personenbezogenen Daten gespeichert und wer betreibt die zugehörigen Server?
- Werden die personenbezogenen Daten vor oder bei der Speicherung anonymisiert bzw. pseudonymisiert?
- Werden Daten übermittelt? Falls ja, zu welchem Zweck, an wen/von wem werden Daten übermittelt? Wurde ggf. eine vertragliche Vereinbarung über die Übermittlung geschlossen?
- 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)?
- 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?

4.5. Ziele und Zweckbestimmung der weiteren Verarbeitung

- Welche Auswertungen sollen von wem aus welchem Grund wann vorgenommen werden?
- Warum / zu welchem Zweck sind personenbezogene (ggf. pseudonyme) Daten zwingend erforderlich? Liegt eine detaillierte Bewertung der Notwendigkeit und Verhältnismäßigkeit der geplanten Verarbeitung für das Forschungsvorhaben vor?
- 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 offenbleiben?
- 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? Falls ja, wie wird das Zugangsverfahren und die Übermittlung geregelt sein?
- Welche Schritte (z. B. Re-Identifizierung /Anonymisierung) sind für die Übermittlung der personenbezogenen Daten an Dritte notwendig?
- Ist eine Rückmeldung von Analyseergebnissen an die Bioproben-Herausgeber oder eine Rückgabe von Bioproben erforderlich? Falls ja, wie wurde diese vertraglich festgelegt?
- Wurde die geplante Verarbeitung personenbezogener Daten und/oder Bioproben insgesamt betrachtet systematisch beschrieben? Wird die geplante Verarbeitung mit den Zwecken und dem verfolgten Interesse des für die Verarbeitung Verantwortlichen gut begründet?

- Fallen personenbezogene Meta-Daten während der Verarbeitung und/oder in den genutzten IT-Systemen an?
- Wie wird sichergestellt, dass ausschließlich für den Forschungszweck relevante und notwendige personenbezogene Daten und/oder Bioproben verarbeitet werden?

4.6. Speicherbegrenzung

- Werden nicht mehr benötigte identifizierende Daten gelöscht, wenn diese nicht mehr zwingend erforderlich sind? Nach welcher Frist und welcher Löschroutine?
- Lässt sich der Data-LifeCycle nachvollziehbar darstellen (ggfs. in einem Daten-Flussdiagramm)?

4.7. Pseudonymisierung

- Werden Probanden jeweils eindeutige Kennungen in Form von Pseudonymen zugeordnet? Wenn ja, welche Methodik und welche technischen Verfahren liegen dieser Zuordnung zugrunde?
- Unter welchen Bedingungen erfolgt eine Re-Identifikation?
- Wer hat Zugriff auf Zuordnungsschlüssel? Ist sichergestellt, dass die Anwender/Nutzer der pseudonymisierten Daten keinen Zugriff auf den Zuordnungsschlüssel erhalten und dass ein Abgleich der pseudonymisierten Daten mit den Daten der Echtumgebung (zum Beispiel aus Patientendatenverwaltungssystemen) ausgeschlossen ist? Welches der beiden Organisationsmodelle ist hier eher zutreffend: Zentrale Pseudonymverwaltung bei der Studienzentrale (bei einer Vertrauensstelle) vs. Dezentrale Pseudonymverwaltung (z.B. bei Prüfstellen anstatt in der Studienzentrale)?
- Wie wird gewährleistet, dass die Einhaltung der Bedingungen für eine Re-Identifikation in jedem Einzelfall durch den oder die Verantwortlichen geprüft und das Ergebnis dokumentiert wird?
- Falls 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?
- Ist sichergestellt, dass die Zuordnungsschlüssel nach Beendigung des Verfahrens vernichtet werden?
- Ist gewährleistet, dass das Pseudonymisierungsverfahren alle identifizierenden Daten erfasst, ggf. auch Freitextfelder, Kommentarfelder, Anlagen usw.?
- Unter welchen Bedingungen könnte aus den pseudonymisierten Daten die Identität der betroffenen Personen auch ohne den Zuordnungsschlüssel ermittelt werden? Wie hoch ist der Aufwand?

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

- Welche Aufbewahrungsfristen existieren für welche Daten(arten) und/ oder gibt es Regelfristen zur Löschung der personenbezogenen Daten?
- Ist eine Anonymisierung der Daten für die Aufbewahrung möglich?
- Ist ein Anonymisieren der personenbezogenen Daten durch die Einwilligungserklärung abgedeckt oder liegt eine gesetzliche Erlaubnis hierfür vor (ggf. bitte benennen)?
- Existiert ein Anonymisierungskonzept und ist die Methodik der Anonymisierung dokumentiert? Erfolgt die Anonymisierung automatisiert und falls ja, wie und durch wen?
- Der Aufwand bei der Erlangung der originalen Information aus einem anonymisierten Datenbestand muss für jedermann unverhältnismäßig hoch sein. Ist dies gewährleistet? Ist gewährleistet, dass das Anonymisierungsverfahren auch Freitextfelder, Kommentarfelder, Anlagen usw. im Hinblick auf die Ersetzung identifizierenden Daten berücksichtigt?
- Gibt es Regelfristen zur Vernichtung der Bioproben?
- Werden Vergleichsproben zu Bioproben archiviert, die für wissenschaftliche Publikationen verwendet wurden? Wenn ja, wo und wie?
- Werden Bioproben nach dem Tod von Probanden vernichtet?
- Werden personenbezogene Daten nach dem Tod von Probanden gelöscht oder anonymisiert?
- Wie werden personenbezogene Daten archiviert, die für wissenschaftliche Publikationen verwendet wurden?

5. Rechtsgrundlage der Datenverarbeitung (Auswahl und Begründung)

5.1. Wirksame schriftliche Einwilligung des Betroffenen

- Wird die betroffene Person hinreichend aufgeklärt?
- Besteht Gelegenheit zu Rückfragen?
- Wird ein Mustertext genutzt und falls ja, welcher?

5.2. Erlaubnis durch ein Gesetz

- Auf welche gesetzliche Erlaubnis soll die geplante Datenverarbeitung gestützt werden: Allgemeine Forschung: Art. 6 Abs. 1 S. 1 lit. e) DSGVO i.V.m. Art. 89 Abs. 1 DSGVO und § 17 Abs. 2-5 DSG NRW oder Art. 9 Abs. 2 lit. j) DSGVO i.V.m. Art. 89 Abs. 1 DSGVO und § 6 Abs. 2 GDSG NRW i.V.m. § 3 Abs. 1 DSG NRW?
- Bestehen andere Erlaubnisnormen, z.B. für andere beteiligte Stellen?

5.3. Transparenzanforderungen

- Wird ein Mustertext verwendet und falls ja, welcher?
- Gibt es Anforderungen von Patientenorganisationen oder Ethikkommissionen hinsichtlich der Aufklärung von Probanden und an die Einwilligungserklärung und wie werden diese ggf. erfüllt?
- Ist eine separate Entbindung von einer gesetzlichen Schweigepflicht erforderlich?
- Sind alle geplanten Datenverarbeitungen beschrieben?
- Welche zusätzlichen Maßnahmen zur Transparenz werden für das Forschungsvorhaben eingerichtet (z. B. Öffentlichkeitsarbeit, Webpräsenz, Publikationsregeln)?
- Wie breit ist die Einwilligungserklärung formuliert? Handelt es sich um eine breiter angelegte Einwilligungserklärung, bei der ggf. nachinformiert wird, oder wird eine detaillierte, zweckgebundene Einwilligungserklärung eingesetzt?
- Sind Abstufungen oder eindeutige Wahlmöglichkeiten für die Einwilligungserklärung vorgesehen?
- Ist die Kontaktierung von Probanden durch die Einwilligungserklärung abgedeckt (z. B. bei Zufallsfunden oder Follow-Ups)?

6. 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?
- Wie erfolgt die Identitätsfeststellung einer anfragenden Person?
- Wie können betroffenen Personen ihrer Einwilligungserklärung widerrufen (Mail, Telefon, Fax, persönlich, Komplettwiderruf, Teilwiderruf)?
- Wie sind die Ablaufprozesse gestaltet, wenn betroffene Personen ihr Recht auf Widerruf eine Einwilligung, Widerspruch gegen die Verarbeitung personenbezogener Daten und/oder Bioproben, Auskunft, Berichtigung oder Löschung ausübt?
- Welche Auswirkungen haben der Widerruf einer Einwilligungserklärung oder Erklärungen zum Widerspruch gegen die Verarbeitung personenbezogener Daten und/oder Bioproben, (z.B. Löschung, Vernichtung, Sperrung, Anonymisierung, Nutzungseinschränkung)?
- Wie können betroffene Personen Ihr Recht auf Löschung von personenbezogenen Daten und/oder Vernichtung von Bioproben wahrnehmen, die sie selbst betreffen? Wie können betroffene Personen Auskunft und ggf. eine Kopie der über sie verarbeiteten personenbezogenen Daten und/oder Bioproben erhalten?
- Wie können betroffene Personen ihr Recht auf Einschränkung der Verarbeitung personenbezogener Daten und/oder Bioproben wahrnehmen?
- Wie erfolgt die Einschränkung der Verarbeitung personenbezogener Daten und/oder Bioprobe im Einzelnen? Liegen begründete Ausnahmen von der Verpflichtung zu Einschränkung der Verarbeitung vor?
- Wie wird die betroffene Person über die Aufhebung der Einschränkung der Verarbeitung personenbezogener Daten und/oder Bioproben unterrichtet?
- Wie können betroffene Personen ihr Recht auf Datenübertragbarkeit personenbezogener Daten und/oder Bioproben wahrnehmen, die sie selbst betreffen?

7. Festlegung des Schutzbedarfs der Daten

- Welches Schutzniveau benötigen die verwendeten Daten? Welche Schäden/Beeinträchtigungen drohen den betroffenen Personen, wenn die Daten z. B. bekannt/verändert/vernichtet würden?
- Vgl. Informationsklassifizierung nach BSI-Standard 200-2
- Genügen die bestehenden Schutzmaßnahmen für die geplanten Abläufe und die genutzten IT-Systeme diesem Schutzbedarf oder sind Zusatzmaßnahmen zu treffen? Bitte auf das jeweilige Schutzkonzept Bezug nehmen und zusätzliche Maßnahmen ergänzend angeben.

8. Risikobestimmung, Schwellwertanalyse und Datenschutz-Folgenabschätzung

- Wurden etwaige Risiken für die Rechte und Freiheiten der betroffenen Personen aufgrund der Form der geplanten Datenerarbeitung im Forschungsvorhaben festgestellt (Risiko = Eintrittswahrscheinlichkeit x Schadenshöhe)?
- 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? Falls nein: Wurde gemäß Art. 35 DSGVO eine Datenschutz-Folgenabschätzung durchgeführt?
- Wurden ggf. 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?

9. Technische und organisatorische Maßnahmen zur Sicherheit

- Liegt ein Sicherheitskonzept betreffend die genutzten Datenverwaltungssysteme vor? Ggf. als erforderlich erkannte Ergänzungen beschreiben.
- Wurde ein projektspezifisches Rollen- und Berechtigungskonzept erstellt? Wird dessen Einhaltung protokolliert und stichprobenartig überprüft?
- Besteht ein ausreichendes Back-up / Recovery-Konzept?

10. Datenverarbeitung zur Qualitätssicherung

- Gibt es ein Monitoring-Verfahren? Welche Daten sieht der Monitor und welche Bearbeitungsrechte (z.B. Sperren, Löschen) hat er (z.B. gemäß Monitoring Manual)?
- Welche Datenqualitätssicherungsverfahren werden für das Forschungsvorhaben vorgesehen? In welcher Form werden qualitätssichernde Maßnahmen in den einzelnen Arbeitsmaßnahmen integriert und wirksam nachgehalten?
- Gibt es ein internes Auditverfahren und wie sieht es aus (Beschreibung)? Wer kontrolliert die Einhaltung der technischen und organisatorischen Sicherheitsmaßnahmen?

11. Anlagen

Einige zur Darstellung der Einhaltung des Datenschutzes bzw. zur Erfüllung datenschutzrechtlicher Anforderungen werden ggf. in externen Dokumenten dargestellt. Bitte benennen Sie hier alle Dokumente, aus denen sich ggf. ergänzend zu diesem Datenschutzkonzept datenschutzrechtliche Anforderungen ergeben. Bitte geben Sie ggf. an, ob Sie Muster der der Medizinischen Fakultät OWL verwenden werden, oder ob ein anderer Beteiligter diese stellt.

Beispielsweise:

- Daten-Management-Plan
- Datenflussdiagramm
- Berechtigungskonzepte für zentrale Datenverwaltungssysteme
- Dokumente zur Patienteninformation, Aufklärung, Einwilligung
- Antrag an die Ethikkommission / Ethik-Votum
- Verträge (insb. Kooperationsvertrag, Prüfzentrumsvertrag, Material Transfer Agreement, Gemeinsame Verantwortung, Auftragsverarbeitungsvertrag)
- Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DSGVO beteiligter Stellen