DZD
Deutsches Zentrum
für Diabetesforschung

DZD Datenschutzkonzept:
DZD Forschungsdatenplattform und
DZD Biobank Data Integration System

München, 04.07.2024

Deutsches Zentrum für Diabetesforschung e.V. (DZD)
Geschäftsstelle am Helmholtz Zentrum München
Ingolstädter Landstr. 1
85764 Neuherberg

Vorstand: Prof. Dr. Dr. h.c. mult. Martin Hrabě de Angelis, Prof. Dr. Andreas Birkenfeld, Prof. Dr. Annette Schürmann
Geschäftsführung: Dr. Astrid Glaser
Registergericht: Amtsgericht Berlin VR 29195 B

Version vom 04.07.2024

Hinweis: Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers (m/w/d) verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

Dieses Dokument ersetzt ältere Versionen des DZD Datenschutzkonzepts.

1 Abkürzungsverzeichnis

AES	Advanced Encryption Standard
AMG	Arzneimittelgesetz
AnaDAT	Analysedaten
BDSG	Bundesdatenschutzgesetz
BLÄK	Bayerische Landesärztekammer
DIS	Data Integration System
DSFA	Datenschutzfolgeabschätzung
DSGVO	Datenschutz-Grundverordnung
DZD	Deutsches Zentrum für Diabetesforschung e. V.
DZD_CDS	DZD Core Dataset (DZD Basisdatensatz)
e.V.	Eingetragener Verein
eCRF	electronic Case Report Form
ETL	Extract, Transform, Load
EU-DSGVO	Europäische Datenschutzgrundverordnung
GCP-V	Good Clinical Practice-Verordnung
IDAT	Identifizierende Daten
LabID	Labor-Identifikator
MDAT	Medizinische Daten
MDR	EU-Medizinprodukte-Verordnung
MPG	Medizinproduktegesetz
OHDSI	Observational Health Data Sciences and Informatics program
OMOP	Observational Medical Outcomes Partnership
OrgDAT	Organisatorische und beschreibende Bioprobeninformationen
PDF	Portable Document Format
PID	Patienten-Identifikator
PSN	Pseudonym
SIC	Subject Identification Code (nach AMG für klinische Studien)
SOP	Standard Operating Procedures
SSL	Secure Sockets Layer
TMF	Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V.
TOM	Technische und organisatorische Maßnahmen
UAC	Use & Access Committee

2 Einleitung

Die Mitglieder des Deutsches Zentrums für Diabetesforschung e. V. (DZD) erheben in klinischen Studien medizinische Daten und Bioprobeninformationen für biomedizinische akademische Forschungsprojekte. Diese liefern neue Erkenntnisse, insbesondere zu metabolischen Erkrankungen wie Diabetes, und können zur Entwicklung von neuen, patientennahen Therapie- und Diagnoseverfahren beitragen. Aus ethischer Sicht sind solche Forschungsansätze mit menschlichen Biomaterialien (im Folgenden „Bioproben") sowie die Auswertung medizinischer Daten, mit dem Ziel den größtmöglichen Nutzen zu erzielen, absolut förderungswürdig.

Ziel des DZD ist es, als nationaler Verbund Experten auf dem Gebiet der Diabetesforschung zusammenzubringen und somit Grundlagenforschung, translationale Forschung, Epidemiologie und klinische Anwendung zu verzahnen und damit Prognose, Prävention, Diagnostik und Behandlung im Zusammenhang mit Diabetes für den Patienten zu verbessern.

Zu diesem Zweck stellt das DZD unter anderem eine Forschungsdatenplattform und eine Biobank bereit.

Empfänger von Gesundheitsdaten und Bioproben können Forschende des DZD sein oder Wissenschaftler an akademischen Forschungsinstitutionen innerhalb der EU bzw. in Ländern mit einem von der europäischen Kommission ausgewiesenen angemessenen Datenschutzniveau. Die Übermittlung erfolgt zum Zwecke medizinischer Forschung. Eine Übermittlung in datenschutzrechtlich unsichere Drittstaaten erfolgt nicht.

2.1 Zielsetzung des Datenschutzkonzepts

Besonderes Augenmerk legt das DZD auf den Schutz der Rechte und Interessen der Spender von Daten und Bioproben für die klinischen Studien des DZD bzw. für die DZD Biobank. Das vorliegende Dokument beschreibt die einzelnen Verfahren zur Datenerhebung und Datenverarbeitung und die entsprechenden Sicherheitsmaßnahmen zum Datenschutz.

Mit qualitätsgesicherten Prozessen und Datenschutzmaßnahmen gewährleistet das DZD, dass das Risiko eines Missbrauchs von Bioproben und medizinischen Daten in der Obhut des DZD minimiert wird.

2.2 Anwendungsbereich

Das vorliegende Datenschutzkonzept findet Anwendung für die DZD klinische Forschungsdatenplattform, die diese umfassenden Module und Prozesse und für das DZD Biobank-DIS.

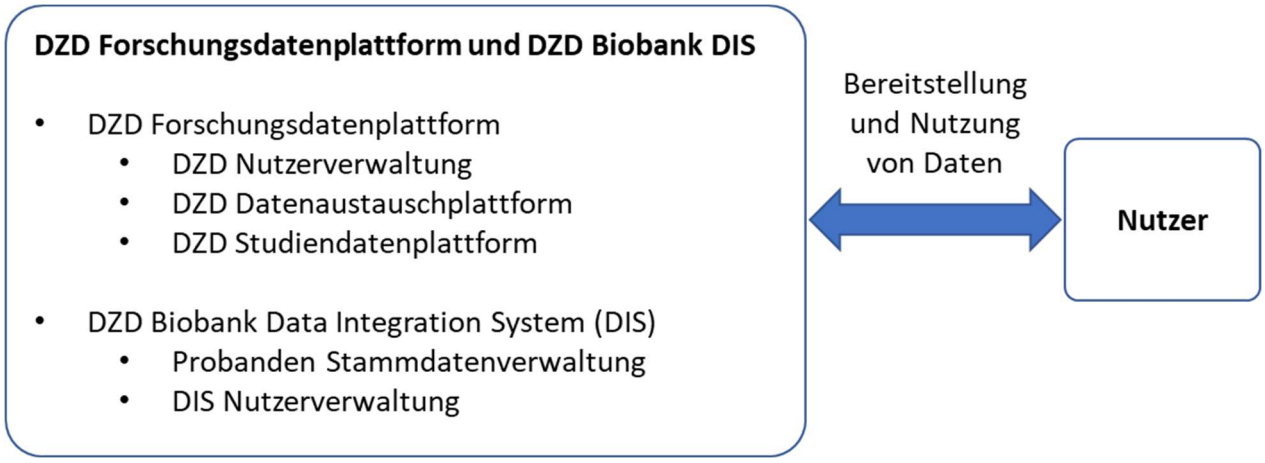

Abbildung 1: Anwendungsbereich des Datenschutzkonzepts.

Das Datenschutzkonzept umfasst diese Infrastruktur und die hierüber bereitgestellten Dienstleistungen.

Die DZD Forschungsdatenplattform wird vom DZD betrieben und enthält eine Nutzerverwaltung für alle Dienste, die über die Forschungsdatenplattform genutzt werden können. Zur Beschreibung der bereitgestellten Dienste werden diese in zwei Kategorien aufgeteilt: Dienste der Datenaustauschplattform und Dienste der Studiendatenplattform. Dienste der Datenaustauschplattform dienen der sicheren Kommunikation und insbesondere dem sicheren Datentransfer zwischen Nutzern *untereinander* sowie zwischen Nutzern und zentralen Ansprechpartnern. Außerdem werden Dienste zur Information der Nutzer bereitgestellt.

Die wesentliche Funktion der Studiendatenplattform und der DZD Biobank ist die Bereitstellung von medizinischen Daten (MDAT) und/oder Bioproben für medizinische Forschungszwecke für seine Mitglieder und akademischen Forschungspartner gemäß dem durch den DZD Use and Access Prozess freigegebenen bzw. durch einen DZD Nutzungsvertrag geregelten Umfang. Genaueres zur Anfrage und Nutzung von MDAT und Bioproben wird durch die *Nutzungsordnung des DZD e.V.* geregelt (siehe Anhang 2).

Für die Erfassung und Verwaltung aller an den Studienorten anfallenden Daten zu DZD Biobankproben nutzt die DZD Biobank eine zentrale IT-Infrastruktur, das DIS. DIS ist ein eigenständiges System und wird unabhängig von der DZD Forschungsdatenplattform von der Firma Bitcare GmbH betrieben.

2.3 Organisatorische Struktur

Organe des DZD sind die Mitgliederversammlung, der Vorstand, die Kommission der Zuwendungsgeber.

Die organisatorische Struktur sowie die Steuerungsmechanismen und -gremien des DZD sind in der *Leitlinie für die funktionale und strukturelle Organisation des Deutschen Zentrum für Diabetesforschung (DZD) e.V.* beschrieben (siehe Anhang 1).

Ein wesentliches Gremium für die Prüfung von Anträgen zur Nutzung medizinischer Daten ist das Use & Access Committee (UAC). Der Aufbau des UAC sowie der Prozess und die einzuhaltenden Regeln für die Nutzung von Daten und die Wahrnehmung der Betroffenenrechte ist in der *Nutzungsordnung des DZD e.V.* beschrieben (siehe Anhang 2).

2.4 Definitionen

Folgende Definitionen werden in Anlehnung an die Nutzungsordnung des DZD verwendet.

2.4.1 DZD Infrastruktur

DZD Forschungsdatenplattform

Zentrale Infrastruktur zur Speicherung, Verarbeitung und Bereitstellung von klinischen Forschungsdaten sowie zur Bereitstellung von Diensten zur Kommunikation, Information und für den Datenaustausch.

DZD Studiendatenplattform

MDAT, die in DZD-Studienfolgeprojekten oder DZD Biobankprojekten generiert werden, werden zentral in der DZD Studiendatenplattform gespeichert und können hierüber Forschenden zur Nutzung bereitgestellt werden. Für Biobankprojekte werden außerdem Bioprobendaten (OrgDat) gespeichert und bereitgestellt.

Datentransferdienst (Data Sharing Service)

Dienst für den sicheren Datenaustausch zwischen Forschenden

DZD Biobank

DZD-Studienstandorte bieten Probanden von DZD-Studien die Teilnahme an einem studienübergreifenden, zweckunabhängigen und prospektiven DZD Biobankprojekt an. Sie werden gebeten, ein definiertes Biobank-Set aus Proben und Daten an die DZD Biobank zu spenden. Die gesammelten Proben und Daten stehen für medizinische Forschungsfragen unter den in der *Nutzungsordnung des DZD e.V.* beschrieben beschriebenen Prozessen zur Verfügung (siehe Anhang 2).

2.4.2 Daten und Bioproben

Identifizierende Daten (IDAT)

IDAT sind Daten, die eine Person genau identifizieren können. Jeder Person, deren medizinischen Daten erfasst werden, wird ein eindeutiger Identifikator (PID oder PSN) zugeordnet. Die IDATs werden je nach klinischer Studie direkt in den Studienzentren vor Ort archiviert und pseudonymisiert mittels geeigneter Software, wie z.B. durch das DIS-System.

Bioprobendaten (OrgDAT, LabID)

OrgDAT und LabID sind Daten, die im Rahmen der Bioprobensammlung, -prozessierung, und -lagerung entstehen (z.B. Probenart, Probenqualität, Präanalytik, Angaben zur Gewinnung/Verarbeitung, Transport und Lagerung).

Medizinische Daten (MDAT)

Die abzufragenden und zu messenden medizinischen bzw. klinischen Daten werden je nach Studie definiert und bei allen Studienteilnehmenden der entsprechenden Studie erfragt bzw. gemessen. Für alle seit dem Jahr 2021 begonnenen DZD klinischen Studien ist der DZD Basisdatensatz in der zu Beginn der jeweiligen Studie aktuellen Version Teil der Datenerhebung.

MDAT sind Daten, die im Rahmen von DZD klinischen Studien an den jeweiligen Studienzentren erhoben werden. Sie umfassen eine breite Palette von Informationen, darunter:

- Studienspezifische Metawerte: Hierzu zählen Angaben zum Zeitplan und zu den Visiten, wie Zeitpunkt (Datum) und Ausfüllstatus der einzelnen Formulare. Dies umfasst die Angabe, wann und wie oft die Teilnehmemenden während der Studie untersucht oder befragt wurden.

- AnaDAT
- Krankheitsspezifische Messungen: Je nach Studienziel werden spezifische Daten zu den betreffenden Krankheitssymptomen oder -indikatoren erfasst.
- Fragebögen: Vom Probanden erfragte Angaben z. B. zu Vorerkrankungen, Lebensstil, Familiengeschichte und weiteren Faktoren.

Analysedaten (AnaDAT)

Alle Daten, die mit laboranalytischen Verfahren aus Bioproben ermittelt werden. Viele Laborwerte werden auch in der Diagnostik eingesetzt und sind de Facto auch Gesundheitsparameter und somit auch als MDAT zu bezeichnen. Vitalparameter: Aufzeichnungen von lebenswichtigen Funktionen wie Puls, Blutdruck, Atemfrequenz und Körpertemperatur.

DZD Basisdatensatz / DZD Core Dataset (DZD_CDS)

Standardisierter klinischer Basisdatensatz, der bei allen DZD-Studienteilnehmenden erhoben wird und der auch Projekten, die Proben aus der DZD Biobank nutzen, zur Verfügung steht. Veröffentlicht u.a. auf dem MDM-Portal https://www.medical-data-models.org/45923

2.4.3 Projekte

DZD-Studienfolgeprojekt

Werden Projekte nach der Erstpublikation im Rahmen einer klinischen Studie des DZD avisiert bzw. durchgeführt, spricht das DZD von DZD-Studienfolgeprojekten. Zu deren Durchführung bedarf es eines Studienfolgeantrags und nach positivem Bescheid des Abschlusses eines Nutzungsvertrags.

DZD Biobankprojekt

DZD Biobankprojekte sind studienunabhängige Projekte, die auf Proben und Daten der DZD Biobank oder zugehörigen Studiendaten der DZD-Forschungsdatenplattform zurückgreifen. Zur Durchführung eines DZD- Biobankprojektes bedarf es eines Biobankantrags und nach positivem Bescheid des Abschlusses eines Nutzungsvertrags.

2.4.4 Personen, Gremien und Organisationen

Studien-Probanden / Biobank-Probanden

Studien-Probanden sind Freiwillige, die an den Klinischen Studien des DZD teilnehmen. Studien-Probanden, die neben der Studien-Einwilligung zusätzlich ihre Einwilligung zur Teilnahme an der DZD Biobank geben, werden in diesem Zusammenhang als Biobank-Probanden bezeichnet.

Nutzer (User)

Nutzer sind alle gemäß Datenschutzbestimmungen und Nutzungsordnung des DZD für die Nutzung von Daten und Diensten einschließlich des DIS autorisierten Personen.

Für Dienste, die nicht der Nutzungsordnung des DZD unterliegen, beispielsweise Dienste aus dem Bereich Datentransfer, Kommunikation und Information, können ebenfalls Personen für die Nutzung autorisiert werden. Diese werden ebenfalls als Nutzer bezeichnet.

DZD Use and Access Committee (UAC)

Das UAC ist ein in der DZD-Nutzungsordnung definiertes Komitee aus DZD-Wissenschaftlern, welches eine wissenschaftliche Einschätzung zur Freigabe der Nutzung von Bioproben oder Daten erstellt.

Forschungspartner

Forschungspartner sind Wissenschaftler an akademischen Forschungsinstitutionen innerhalb der EU bzw. in Ländern mit einem von der europäischen Kommission ausgewiesenem angemessenen Datenschutzniveau (EU-DSGVO konform), die mit dem DZD kooperieren, indem sie Daten bereitstellen oder nutzen.

Studienzentren

In Studienzentren werden die Einwilligungen der Studien-Probanden / Biobank-Probanden erfasst und verwaltet, klinische Studien des DZD durchgeführt und DZD-Bioproben genommen. Die Studienzentren gehören organisatorisch und rechtlich DZD-Mitgliedern oder DZD Assoziierten Partnern. Details zu DZD-Mitgliedern und DZD Assoziierten Partnern sind in der *Leitlinie für die funktionale und strukturelle Organisation des Deutschen Zentrum für Diabetesforschung (DZD) e.V.* beschrieben (s. Anhang 1).

2.5 Rechtsgrundlagen

Die EU-DSGVO, ergänzt durch das Bundesdatenschutzgesetz BDSG, ist neu geltendes Recht seit dem 25.05.2018. Die Rechtsgrundlage zur Verarbeitung der den Studienteilnehmenden betreffenden personenbezogenen Daten bildet primär seine freiwillige schriftliche Einwilligung nach Art. 6 Abs. 1a DSGVO. Da es sich im Fall der Gesundheitsforschung um besondere Kategorien personenbezogener Daten handelt, gilt in diesem Fall die Legitimation der Verarbeitung personenbezogener Daten nach ausdrücklicher Einwilligung wie dargelegt in Art. 9 Abs. 2a DSGVO.

Da die Daten- und Bioprobensammlung des DZD zum Zweck der wissenschaftlichen Forschung in öffentlichem Interesse erfolgt, zählen dieses Dokument betreffende Daten zu den Ausnahmen von der Pflicht zur Speicherbegrenzung (Art. 5 Abs. 1 e DSGVO). Die Daten werden für die wissenschaftliche Gesundheitsforschung für definierte Zwecke (Art. 5 Abs. 1 b DSGVO) („Zweckbindung") genutzt.

Um dem Schutz der Rechte und Freiheiten betroffener Studienteilnehmenden gerecht zu werden und den größtmöglichen Schutz zu gewährleisten, wird in der einschlägigen Literatur das Konzept der informationellen Gewaltenteilung vorgeschlagen. Dies wird gefordert als Grundlage, um die in der DSGVO vorgesehenen Freiheiten der wissenschaftlichen Forschung nutzen zu dürfen, siehe Art. 89 Abs. 1 DSGVO§ 27 Abs. 3. BDSG].

Die zur Umsetzung der rechtlichen Rahmenbedingungen notwendigen TOM werden in dem vorliegenden Datenschutzkonzept festgehalten.

Neben den der Datenschutzgesetzgebung haben folgende weitere Gesetze und Richtlinien Einfluss auf dieses Datenschutzkonzept: AMG, MDR, MPG, GCP-V.

3 DZD Infrastruktur, Datenverarbeitung und -bereitstellung

Die wesentlichen in diesem Dokument beschriebenen Infrastrukturelemente, Datenflüsse und Daten sind in Abbildung 2 dargestellt.

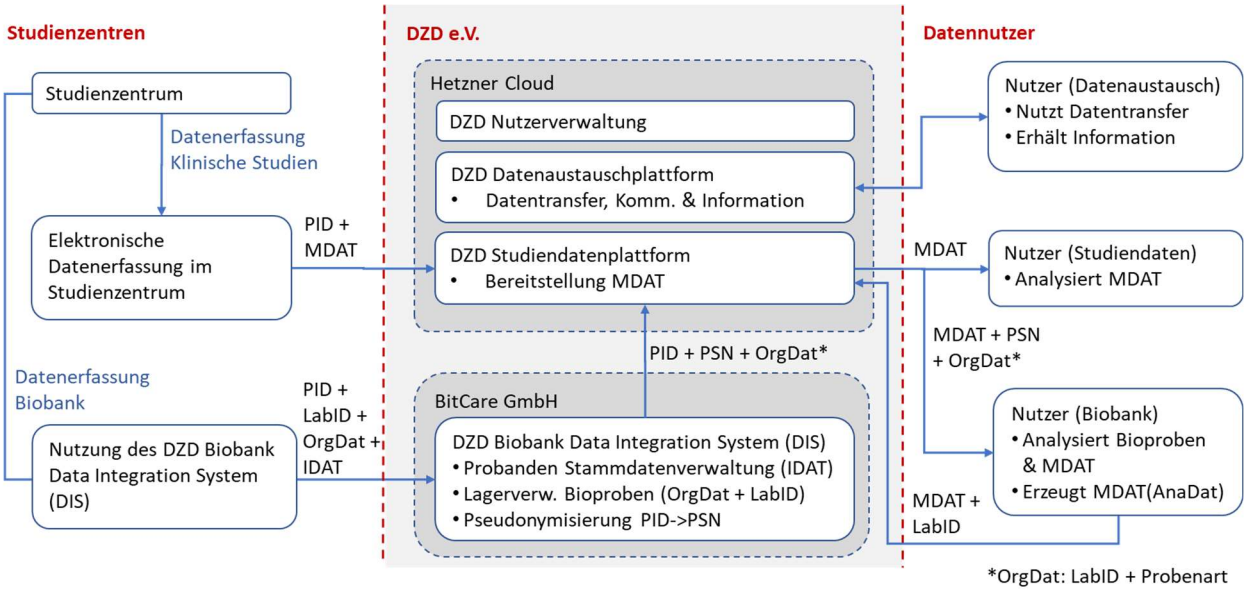

Abbildung 2: Wesentliche Infrastruktur-Komponenten und Datenflüsse des Datenschutzkonzepts.

In der Infrastruktur des DZD werden medizinische Daten, zugehörige Metadaten,wie beispielsweise beschreibende Information zu Studien, öffentlich verfügbare Daten und außerdem die von Nutzern für den Datenaustausch und für die Kommunikation erzeugten Daten gehalten.

In der Infrastruktur des DZD werden keine Daten gehalten, die eine genaue Identifizierung von Studien-Probanden / Biobank-Probanden erlauben (IDAT). Eine Ausnahme bilden IDAT, die Studienzentren in dem DZD Biobank Data Integration System (DIS) verwalten. Diese IDAT sind jedoch nur den Studienzentren zugänglich und werden vom DZD nicht verarbeitet.

In diesem Konzept werden drei Arten von Benutzerrollen für die folgenden Nutzungsszenarien unterschieden

1. Nutzung von Datenaustausch- und Kommunikationsdiensten. Für diese Dienste ist keine Freigabe durch das DZD UAC erforderlich. Abhängig von dem Dienst kann aber eine Zugriffsbeschränkung auf einzelne Nutzergruppen bestehen.
2. Nutzung von Studiendaten (MDAT) der DZD Studiendatenplattform. Berechtigte Personen erhalten Zugriff auf die zuvor durch einen Nutzungsantrag beschriebenen und vom DZD Use and Access Committee freigegebenen Daten. Die Nutzer verpflichten sich, die Regeln für die Nutzung von Daten und die Wahrnehmung der Betroffenenrechte gemäß *Nutzungsordnung des DZD e.V.* (siehe Anlage 2) einzuhalten.
3. Nutzung von Bioproben der DZD Biobank. Personen erhalten die zuvor durch einen Nutzungsantrag beschriebenen und vom DZD UAC freigegebenen Bioproben und zugehörige MDAT. Nutzer von Bioproben verpflichten sich zur Einhaltung eines individuellen Nutzungsvertrags und stellen die aus Bioproben gewonnenen Daten dem DZD zur Sekundärnutzung zur Verfügung. Die Nutzer verpflichten sich, die Regeln für die Nutzung von Daten und Bioproben sowie zur Wahrnehmung der Betroffenenrechte gemäß *Nutzungsordnung des DZD e.V.* (siehe Anlage 2) einzuhalten.

Die in der Infrastruktur des DZD gespeicherten medizinischen Daten werden somit von Studienzentren und den Nutzern der DZD Bioproben dem DZD bereitgestellt.

3.1 DZD Infrastruktur

3.1.1 DZD Forschungsdatenplattform

Die DZD Forschungsdatenplattform wird vom DZD betrieben. Die Hardwareplattform sowie die darin gehaltenen bzw. übertragenen Daten werden ausschließlich in Deutschland gehostet, aktuell bei dem Unternehmen Hetzner Online GmbH (Industriestr. 25, 91710 Gunzenhausen).

Die DZD Forschungsdatenplattform wurde auf Basis von Open Source Software entwickelt. Die Plattform ist modular aufgebaut, einzelne Dienste der Plattform werden in Software Containern konfiguriert und betrieben.

Die **DZD Nutzerverwaltung** ist ein zentraler Dienst für die Verwaltung aller Nutzer der Forschungsdatenplattform. Dieser Dienst forciert eine 2-Faktor Authentifizierung der Nutzer. Für eine einfache Trennung der grundlegenden Nutzungsszenarien wird die DZD Forschungsdatenplattform in zwei Dienste-Plattformen unterteilt:

- Die DZD Datenaustauschplattform dient der Kommunikation, Information und dem Datenaustausch von Forschenden untereinander.
- Die DZD Studiendatenplattform dient der Bereitstellung medizinischer Daten (MDAT) und ausgewählter DZD Biobankdaten (OrgDAT/LabID & PSN; Umsetzung in Planung) an Forschende (vgl.Abbildung 2).

Die **DZD Datenaustauschplattform (DZD Data Hub)** umfasst aktuell folgende Dienste

- Datentransferdienst (Data Sharing Service)
- Informationsdienst (Wiki)

Als zukünftiger Dienst ist außerdem ein Kommunikationsdienst (Chat) geplant.

Die **DZD Studiendatenplattform** umfasst aktuell folgende Dienste

- Datendienste für den Zugriff auf medizinische Daten (MDAT) und Bioprobendaten (OrgDAT)
- Wissensgraph (Knowledge Graph)

In Abschnitt 0 werden diese Dienste und die zugehörigen Technisch-Organisatorischen Maßnahmen genauer beschrieben.

3.1.2 DZD Biobank Data Integration System (DIS)

Für die Erfassung und Verwaltung von Bioproben im Rahmen der DZD Biobank wird an der DZD-Geschäftsstelle und an den beteiligten Studienorten die Software *Data Integration System (DIS)* der Firma Bitcare GmbH verwendet. Der Betrieb von DIS erfolgt vollkommen unabhängig von der o.g. DZD Forschungsdatenplattform.

Sowohl für den technischen Betrieb (Wartung, Sicherung) als auch die datenschutzgerechte Nutzung des DIS ist ausschließlich die Firma Bitcare (München, Corneliusstr. 1) verantwortlich. Die Hardwareplattform sowie die darin gehaltenen bzw. übertragenen Daten werden ausschließlich in Deutschland gehostet, aktuell an der Technischen Universität München (TUM).

Ausgewählte OrgDAT und LabID zu DZD Biobankproben in DIS werden zusammen mit Biobank-Probanden-Pseudonymen (PSN) in der DZD Studiendatenplattform mit MDAT aus Studien verknüpft und können so für die Recherche und Planung weiterer Studien genutzt werden.

In Abschnitt 5 werden das DIS und weitere Teilsysteme sowie die zugehörigen TOM genauer beschrieben.

3.2 Prozesse für die Nutzung der DZD Forschungsdatenplattform und Biobank

Das DZD hat einen einheitlichen Use & Access Prozess zur Bereitstellung von Daten aus DZD Studien sowie von Daten und Bioproben aus der DZD Biobank. Dieser Prozess ist durch die *Nutzungsordnung des DZD e.V.* (siehe Anhang 2) festgelegt.

Die Nutzung der DZD Datenaustauschplattform dient der Kommunikation, Information und dem Datenaustausch von Forschenden untereinander und steht Forschenden des DZD und auch Wissenschaftlern, die mit dem DZD zusammenabreiten, generell zur Verfügung. Nutzer dieser Dienste müssen sich zur Einhaltung der jeweiligen Nutzungsbedingungen bereiterklären und haben ggf. keinen Zugriff auf Informationsdienste, für die ein eingeschränkter Nutzerkreis festgelegt ist.

4 DZD Forschungsdatenplattform

Die DZD Forschungsdatenplattform verknüpft verschiedene Datenbanken und Services, die das DZD zentral für die Kooperation der Forschenden und für die Nutzung von klinischen Daten anbietet. Für die technische Plattform werden quelloffene Anwendungen genutzt, die vom DZD entsprechend der datenschutzrechtlichen Anforderungen konfiguriert und betrieben werden. Im Folgenden werden die einzelnen Komponenten der DZD Forschungsdatenplattform beschrieben und datenschutzrelevante Maßnahmen erläutert.

Alle für die Entwicklung der Anwendungen erforderlichen Konfigurationen werden in Konfigurationsdateien abgelegt. Der Betrieb erfolgt mit Anwendung der Container-Technologie Docker. Durch diese Kapselung können die Dienste isoliert voneinander betrieben und ggf. mit einem begrenzten Aufwand zu anderen Hosting-Optionen umgezogen werden.

Die Hardwareplattform sowie die darin gehaltenen bzw. übertragenen Daten werden ausschließlich in Deutschland gehostet, aktuell bei dem Unternehmen Hetzner Online GmbH (Industriestr. 25, 91710 Gunzenhausen).

4.1 DZD Nutzerverwaltung

Zu den Kernkomponenten der DZD Forschungsdatenplattform zählt die DZD Nutzerverwaltung, die identifizierende Daten der Nutzer speichert. Die Plattform verfügt über ein Protokoll-Tool, dass den Zugriff und die Manipulation der Daten durch die Nutzer erfasst.

Die DZD Nutzerverwaltung wird mit einer quelloffenen Software umgesetzt. Als zentraler Identity Provider erlaubt die Nutzerverwaltung ein vollkommen einheitliches Single Sign-on aller Nutzer der DZD Forschungsdatenplattform. Für die Einrichtung und Nutzung eines Kontos gelten die folgenden Regeln:

- Nur mit dem DZD verbundene Personen dürfen ein Konto erhalten und somit Nutzer werden. Dazu gehören Mitarbeiter der Mitglieder des DZD oder Personen, die für die Kooperation mit dem DZD ein Konto benötigen, beispielsweise im Rahmen eines genehmigten Nutzungsantrags auf Daten aus DZD Klinischen Studien oder auf Daten aus dem DZD Biobank DIS-System.
- Neue Nutzer registrieren sich mit ihrer geschäftlichen E-Mail-Adresse (soweit diese existiert) und müssen bei der Registrierung ein Zugangspasswort und eine 2-Faktor-Authentifizierung einrichten und fortan nutzen.
- Jedes neu angelegte Benutzerkonto ist zunächst deaktiviert und wird von der DZD-Geschäftsstelle geprüft, bevor es aktiviert wird.
- Dienste, die keinen besonderen Einschränkungen unterliegen, stehen allen aktivierten Nutzern zur Verfügung. Abhängig von der E-Mail-Domäne der Nutzer können weitere Dienste, die insbesondere allen Mitarbeitern einer Organisation zugänglich sein sollen, automatisch bereitgestellt werden.

In besonderen Fällen können Nutzer auch ohne eine aktiviertes DZD Konto DZD Dienste nutzen. Dazu gehört der Zugriff auf die öffentliche Information zum Einrichten eines DZD Kontos (aktuell https://help.apps.dzd-ev.org/en/public/create-dzd-account).

4.2 DZD Datenaustauschplattform

4.2.1 DZD Datentransferdienst (Data Sharing Service)

Der DZD Datentransferdienst erlaubt den DSGVO-konformen Transfer von Daten zwischen unterschiedlichen Endpunkten. Der Dienst basiert auf der Open Source Lösung Nextcloud mit einer für diesen Dienst speziellen Konfiguration.

Die Nextcloud ist eine im öffentlichen Sektor anerkannte Lösung für DSGVO-konforme Datenhaltung bzw. Datenaustausch und wurde beispielsweise vom ITZBund für die cloudbasierte Datenorganisation des Bundes gewählt.

Die spezielle Konfiguration stellt folgende Funktionalität sicher:

- Der Datentransfer ist nur zwischen registrierten DZD Nutzern möglich
- 2 Faktor-Login über die zentrale Nutzerverwaltung ist erforderlich
- Nutzer können in ihrem privaten Bereich Verzeichnisse anlegen und Dateien hochladen
- Verzeichnisse oder Dateien müssen anderen Nutzern individuell freigegeben werden
- Der Datenzugriff durch Nutzer wird protokolliert
- Der Dienst garantiert keine permanente Datenhaltung. Dateien werden nach 120 Tagen automatisch gelöscht

4.2.2 Private Bin

Dieser Dienst erlaubt es DZD Nutzern unter anderem, Texte (insbesondere Einmalpasswörter) für das *einmalige* Lesen (burn after reading) mit beliebigen Empfängern auszutauschen, beispielsweise online während einer Videokonferenz. Dadurch kann die Integrität der Information sichergestellt und unberechtigter Zugriff durch Dritte ausgeschlossen werden.

PrivateBin ist eine minimalistische Open Source Lösung (https://privatebin.info/), bei der der Server keinerlei Kenntnis der Inhalte hat. Die Daten werden im Browser mit 256 Bit AES ver- und entschlüsselt.

4.2.3 DZD Informationsdienste (Wiki)

Das DZD betreibt aktuell mehrere Wikis, die als jeweils isolierte Instanzen (in separaten Docker Containern) betrieben werden. Basis bildet die Open Source Lösung Wiki.js. Aktuell existieren Wikis zu

- DZD Klinischen Studien, Daten- und Bioprobennutzung und der DZD Biobank
- DZD Infrastruktur sowie technischen Anwendungen wie beispielsweise eCRF Systemen

Die Wikis halten keine MDAT. Dennoch können die Nutzergruppen individuell eingeschränkt sein. Die Verantwortung über die Inhalte obliegt den für den jeweiligen Inhalt verantwortlichen Mitarbeitern der DZD-Geschäftsstelle. Diese können Administratoren bzw. Editoren der Inhalte bestimmen.

4.3 DZD Studiendatenplattform

4.3.1 Datendienste für den lesenden Zugriff auf medizinische Daten (MDAT) und Bioprobendaten (OrgDAT)

Die DZD Studiendatenplattform wird gegenwärtig für die Bereitstellung von MDAT gemäß der DZD Use & Access Vorgaben genutzt.

Die technische Grundlage bildet die in Abschnitt 4.2.1 beschriebene Open Source-Lösung Nextcloud in einer zu dem DZD Datentransferdienst abweichenden Konfiguration. Dadurch wird folgende Funktionalität umgesetzt.

- Ausschließlich lesender Zugriff durch die gemäß Use & Access Prozess individuell autorisierten Nutzer
- Autorisierte Nutzer müssen bei dem ersten Datenzugriff explizit den Nutzungsbedingungen für den ordnungsgemäßen Umgang mit den Daten zustimmen
- Autorisierte Nutzer erhalten individuelle, ggf. mit einer individuellen Signatur versehene Dateien

Aktuell werden MDAT ausschließlich denjenigen Studienzentren zur Verfügung gestellt, die die zugrundeliegenden Daten bzw. Bioproben bereitgestellt und zugehörige IDs (Identifier bzw. Pseudonyme für Probanden oder Bioproben) für die Verknüpfung zu weiteren Daten erzeugt haben. Diese von den Studienzentren gelieferten IDs werden aktuell unverändert den Forschenden übermittelt. Das Record-Linkage zu begleitenden Patienten- bzw. Probandendaten der Studienzentren wird von den Forschenden in den jeweiligen Studienzentren eigenverantwortlich durchgeführt.

Für die zukünftige Datenbereitstellung sind folgende Funktionen in der Entwicklung:

- Semantisches Mapping von Studienparametern in das OHDSI OMOP Format
- Datentransformation (ETL) von Studiendaten in das OHDSI OMOP Format
- Pseudonymisierung sowie Randomisierung der aus Quellsystemen bereitgestellten PID / Proben ID
- Erstellung kombinierter Datensätze insbesondere aus Studiendaten im OMOP Format

Begleitend werden Funktionen zur Identifikation und Löschung von Daten aus den in obigen Schritten erstellten Datensätzen entwickelt, um Betroffenenrechte durchgängig und weitgehend automatisiert erfüllen zu können. Die dafür ggf. erforderliche Zuordnung von IDAT zu PID hat durch die jeweiligen Studienzentren zu erfolgen, da das DZD keinen Zugriff auf IDAT der Studienprobanden hat.

Für die zukünftige Nutzung von DZD Biobank Proben ist außerdem die Zusammenführung von OrgDAT aus DIS mit zugehörigen MDAT aus DZD Studien geplant (siehe auch Abschnitt 3.1.2).

Alle Datensätze werden gemäß *Nutzungsordnung des DZD e.V.* (siehe Anhang 2) bereitgestellt.

4.3.2 Wissensgraph (Knowledge Graph)

Am DZD wurde ein Wissensgraph („knowledge graph") DZDconnect entwickelt, der Daten aus der Grundlagenforschung und Metadaten aus klinischen Studien verknüpft. Die in dem Wissensgraph bereitgestellten Daten wurden aus öffentlich zugänglichen Quellen ermittelt und stellen keine vertraulichen Daten dar.

4.4 Technische und organisatorische Maßnahmen

Für den DSGVO konformen Betrieb der DZD Forschungsdatenplattform sind eine Reihe wesentlicher Regeln einzuhalten und Maßnahmen zu gewährleisten, die im Folgenden beschrieben werden.

4.4.1 Zugang zu der technischen Plattform und Administration der Systeme

Auf der DZD Forschungsdatenplattform werden personenbezogene Daten erfasst (z.B. Benutzerkonten einschließlich Zugriffsdaten sowie von Benutzern hochgeladene Dateien). Um die Vertraulichkeit dieser Daten zu gewährleisten, sind folgende Regeln einzuhalten.

Administratoren der Plattform haben prinzipiell Zugriff auf diese Daten und dürfen diesen Zugriff ausschließlich aus zwingenden Gründen zum Erfüllen ihrer Aufgaben nutzen. Alle Administratoren sind außerdem zur Verschwiegenheit verpflichtet und dürfen personenbezogene Daten nur unter Einhaltung der gesetzlichen Auflagen nutzen oder weitergeben. Für alle Konten einschl. lokale Admin-Konten sind zehnstellige Passwörter und eine 2-Faktor-Authentifizierung erforderlich.

Sollten externe Dienstleister mit Aufgaben zur Administration oder Entwicklung beauftragt werden, so ist ein DSGVO-konformer Vertrag zur Auftragsdatenverarbeitung zu schließen.

4.4.2 Datenschutz bei Speicherung und Transfer von Daten

Wenn möglich werden die abgelegten Daten auf den Servern mittels openssl_seal im RC4 Modus verschlüsselt. Die auf der DZD Studiendatenplattform bereitgestellten MDAT sind bei der Übertragung und der Lagerung mittels SSL AES-256-Standard verschlüsselt.

4.4.3 Mandantenfähige Dienstbereitstellung

Dienste der DZD Forschungsdatenplattform können nach Mandanten getrennt werden, indem sie als separate Anwendung (separate Container) für jeweils einzelne Mandanten bereitgestellt werden.

4.4.4 Backup

Backups werden in regelmäßigen Zeitabständen erstellt und an zwei unterschiedlichen physischen Orten aufbewahrt. Die Backup-Erstellung erfolgt nach dem "write-only"-Prinzip, d.h. Clients können auf die Backup-Speicherorte nur schreibend zugreifen und nicht lesen, löschen oder überschreiben.

4.4.5 Zugriff auf Dienste durch Nutzer & Monitoring

Jeder Nutzer hat bei der Registrierung den Nutzungsbedingungen für die DZD Forschungsdatenplattform zuzustimmen. Insbesondere stimmen Nutzer zu, dass Daten über ihre Nutzung auditiert werden (Zeit des Zugriffs, IP-Adresse usw.).

Die in der DZD Nutzerverwaltung eingesetzte Software hat ein sogenanntes Reputation Score System, welches für jedes Paar von Account und IP-Adressen Punkte gibt und ggf. den Zugang sperrt. So können fehlgeschlagene Anmeldungen von ungewöhnlichen Orten, z.B. aus dem Ausland, schneller zu Accountsperrungen führen.

Außerdem werden in einem Admin Dashboard der Nutzerverwaltung Statistiken über fehlgeschlagene Logins erhoben. Dies kann den Admins helfen, abnorme Vorgänge schneller zu erkennen bzw. dazu genutzt werden, automatisiert Warnungen per Mail an die Admins zu schicken.

5 DZD Biobank Data Intgration System (DIS)

5.1 Hintergrund und allgemeiner Aufbau

Neben den im Rahmen der klinischen Studien gewonnen Studienproben werden in der DZD Biobank zusätzlich auch langfristig zu lagernde Bioproben für spätere Forschungsprojekte gesammelt. Bioproben und Daten für die DZD Biobank werden bei Personen erhoben, die bereits an Klinischen Studien des DZD teilnehmen (im Folgenden „**Studien-Probanden**“) und die zusätzlich ihre Einwilligung zur Teilnahme an der DZD Biobank geben (im Folgenden „**Biobank-Probanden**“). Die mit DZD Biobank-Probandeneinwilligung an den DZD-Studienzentren gesammelten, aufbereiteten und temporär zwischengelagerten Bioproben werden bei Helmholtz Munich dauerhaft gelagert.

Für die Erfassung und Verwaltung aller an den Studienorten anfallenden Daten zur Verwaltung von DZD Biobankproben betreibt die DZD Biobank eine zentrale IT-Infrastruktur, das Data Integration System (DIS).

Abbildung 3 gibt einen Überblick über die Prozesse sowie den Daten- und Probenfluss der DZD Biobank.

Wissenschaftlich und organisatorisch relevante Daten zu Bioproben der DZD Biobank werden in der DZD Studiendatenplattform mit medizinischen Daten (MDAT) aus den Klinischen Studien assoziiert (Umsetzung in Planung). DZD Biobankproben sind somit nach wissenschaftlichen Aspekten recherchierbar und werden über einen standardisierten Use & Access Prozess für berechtigte Forschungsinteressen zur Verfügung gestellt (siehe *Nutzungsordnung des DZD e.V.*, Anhang 2).

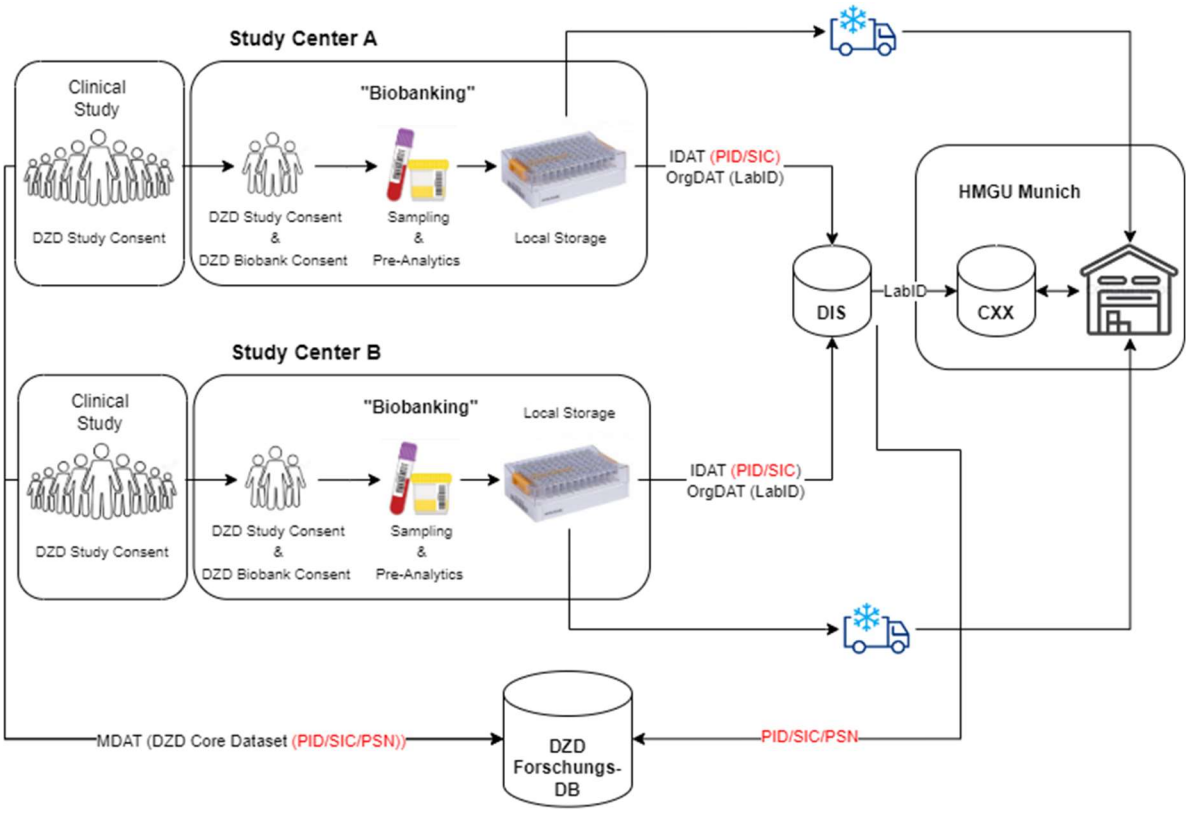

Abbildung 3: Allgemeiner Workflow DZD Biobank

5.2 Teilsysteme und verarbeitete Datenkategorien

Data Integration System (DIS): Alle im Rahmen des DZD Biobankings notwendigen Daten werden primär mit dem DIS (BitCare GmbH) erhoben und verwaltet. Grundlage für die System-Architektur des DIS ist die informationelle Gewaltenteilung, wie von der Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V. (TMF) beschrieben (siehe Abbildung 4). Das bedeutet, die Speicherung und Verwaltung der IDAT erfolgt in DIS organisatorisch und räumlich getrennt von anderen Daten-Kategorien (OrgDAT) und in separaten Datenbanksystemen.

Sämtliche Prozesse der Datenverarbeitung im DIS erfolgen ausschließlich mit doppelt pseudonymisierten Daten. Zugriff auf unverschlüsselte IDATs haben ausschließlich am jeweiligen Studienzentrum autorisierte, geschulte und zur Verschwiegenheit verpflichtete Benutzer.

Zu weiteren Details siehe *Datenschutzrahmenkonzept Data Integration System (DIS)*, aktuelle Version 2.3 vom 26.08.2020; überprüft am 21.03.2022 im Anhang 3.

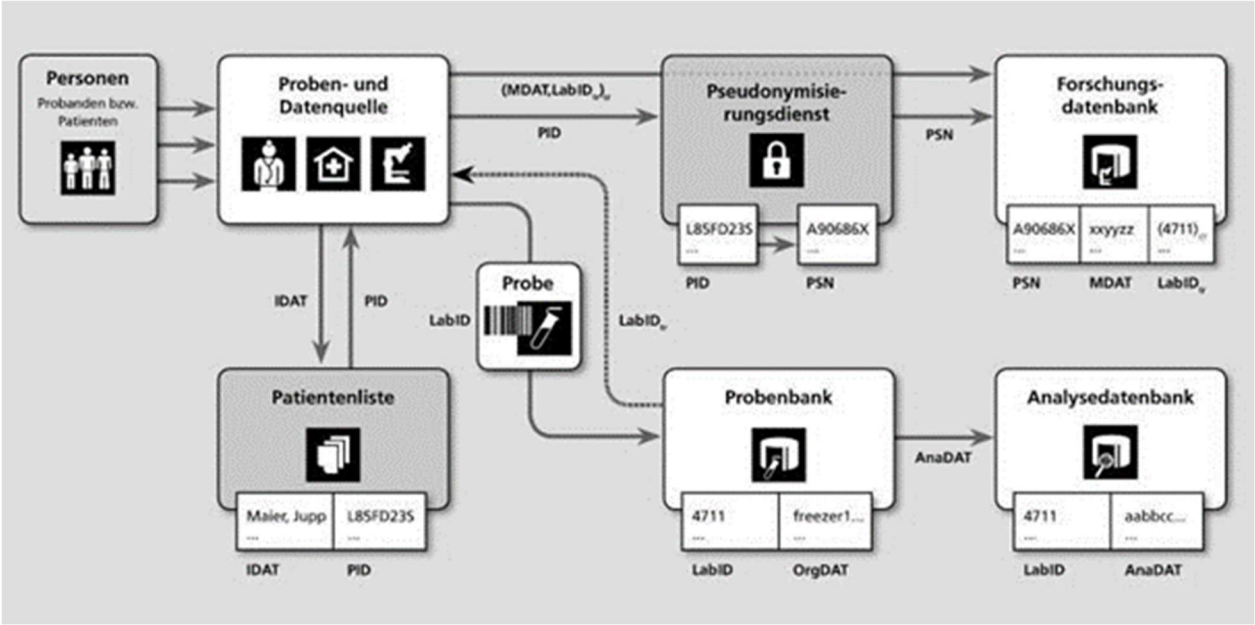

Abbildung 4: Architekturskizze und Informationsfluss im TMF-Maximalmodell [Pommerening K. Das Datenschutzkonzept der TMF für Biomaterialbanken. 2007, it – Inf. Technol.:49, 352.].

CentraXX (Kairos GmbH.): DZD Biobankproben und die dazugehörigen OrgDAT werden bei der Gewinnung der Biobankproben an den Studienzentren über das DIS erfasst. Zur langfristigen Lagerung werden DZD-Bioproben an Helmholtz Munich überführt, wobei auch für die Lagerung notwendige OrgDAT in das lokale IT-System importiert werden (aktuelle Software CentraXX). IDATs werden auch nach der Überführung von DZD-Bioproben weiterhin ausschließlich in DIS gespeichert und verwaltet. Für das Ethik- und Datenschutzkonzept der Biobank bei Helmholtz Munich liegt ein positives Votum der Ethikkommission der Bayerischen Landesärztekammer vor (Aktenzeichen 19091).

5.3 Verantwortlichkeiten

Alle Verantwortlichen, Benutzer und Auftragsverarbeiter der DZD Biobank stellen in gleichem Maße sicher, dass der Datenschutz sowie die Gesetze und Regeln eingehalten werden.

Verantwortlich für die Beauftragung des **Betriebs und der Wartung des zentralen IT-Systems** der DZD Biobank und die **Herausgabe von Proben** aus der zentralen Lagerung bei Helmholtz Munich und assoziierter medizinischer Daten aus der DZD Forschungsdatenplattform ist das Deutsche Zentrum für Diabetesforschung (DZD e.V.), Geschäftsstelle bei Helmholz Munich (Ingolstädter Landstraße 1, 85764 Neuherberg).

Verantwortlich für die **primäre Datenerfassung** im Rahmen der DZD Biobank im zentralen IT-System der DZD Biobank sind die beteiligten Studienzentren. Dies betrifft insbesondere folgende Aspekte: Akquise von Biobank-Probanden inkl. Aufklärung, Einholung und Dokumentation der Einwilligungen und Erfassung der Präanalytik und OrgDAT zu den gesammelten Bioproben.

Verantwortlich für die **Einrichtung und von (Be)Nutzern und ggfs. lokalen Fach-Administratoren** in DIS im Rahmen der DZD Biobank (= DZD Biobank-Accounts) ist die DZD-Geschäftsstelle in Absprache mit den lokalen Studienzentren. Die Erstellung bzw. Deaktivierung von Accounts erfolgt durch die DZD-Geschäftsstelle nach schriftlicher Beantragung durch lokale Studienzentren. Benutzer und Administratoren unterliegen der Verschwiegenheitspflicht. Die Studienzentren sind dabei alleinverantwortlich für Art, Umfang und Dauer von **Zugriffsberechtigungen** sowie für die entsprechende **Schulung** der betroffenen Mitarbeiter und die Überwachung der **Verschwiegenheitspflicht** am Studienzentrum.

Auftragsverarbeiter werden gemäß Art. 28 DSGVO ausgewählt und die Verarbeitung erfolgt nur auf Grundlage eines **Auftragsverarbeitungsvertrages**. Eine Verarbeitung erfolgt ausschließlich auf Weisung durch die DZD-Geschäftsstelle. Auftragsverarbeiter für das DIS als zentrales IT-Systems der DZD Biobank und die Fernwartung, ist die Firma Bitcare GmbH, (Corneliusstr. 30, 80469 München, mail@bitcare.de, 089 – 94301309).

Die Funktion des zuständigen **Datenschutzbeauftragten** für das Deutsche Zentrum für Diabetesforschung (DZD e.V.) übernimmt im Auftrag die Firma Bredex GmbH (Lindentwete 1, 38100 Braunschweig).

5.4 Zweck der Verarbeitung und rechtliche Grundlage

Primärer Zweck des zentralen IT-Systems der DZD Biobank ist die **Erfassung**, **Verwaltung** und **Sicherung** von Daten zu Bioproben der DZD Biobank zum Zweck der konsistenten und datenschutzgerechten Verarbeitung sowie der wissenschaftlichen Nutzung und der entsprechenden **Zugriffssteuerung** in allen Systembereichen. Grundlage für die Verarbeitung der Probendaten der DZD Biobank ist die freiwillige und informierte **Einwilligung** der Betroffenen (Biobank-Probanden) sowie das **Ethikvotum** der Bayerischen Landesärztekammer (BLÄK) vom 22.05.2024 mit der Nummer 20091.

Für die Durchführung der Datenverarbeitung in DIS müssen in beschränktem Maße personenbezogene Daten auch von **Benutzern in DIS** verwaltet werden. Diese Daten sind notwendig, um im Rahmen des Qualitätsmanagements die Verarbeitungskette von Probendaten vollständig nachvollziehen zu können.

Die Benutzer des DIS, Mitarbeiter der klinischen Studien, werden im Rahmen des Anlegens eines personifizierten Nutzer-Accounts in DIS im Vorfeld mit aktuellen Datenschutz-Hinweisen über die Speicherung ihrer personenbezogenen Daten in DIS und über ihre Rechte in Kenntnis gesetzt.

5.5 Datenerhebungsprozesse

Die Datenerhebungsprozesse der DZD Biobank werden durch Standard Operating Procedures (SOPs) verbindlich definiert. Im Rahmen der Akquise für die DZD Biobank werden an den beteiligten Studienzentren die für eine eindeutige Zuordnung von Proben zu Personen und zur Kontaktierung notwendigen personenidentifizierenden Daten (IDAT) direkt von den Biobank-Probanden erhoben.

Die Erfassung von Daten im Rahmen der Prä-Analytik (OrgDAT) erfolgt durch DIS-Benutzer am jeweiligen Studienzentren in DIS.

Ggfs. im Rahmen von Studienfolgeprojekten anfallende Analysedaten (AnaDAT) werden nach Studienabschluss in die DZD Forschungsdatenplattform importiert.

Im Rahmen der DZD Biobank-Prozesse findet keine zusätzliche Datenübernahme aus anderen Verfahren statt.

Sobald DZD Biobankproben in das zentrale Lager bei Helmholz Munich überführt wurden, werden die bis dahin erhobenen OrgDAT aus Sicht des ursprünglich erhebenden Studienzentrums „eingefroren". Das heißt, die Daten können nur durch berechtigte DIS-Benutzer der DZD Biobank editiert werden.

5.6 Datensicherheit DZD Biobank

Für den Zugriff auf DIS ist ein **DIS-Benutzerzugang** mit Namen und Passwort erforderlich (=> **DIS-Benutzer**). Je nach Funktion werden DIS-Benutzern bestimmte Zugriffsrechte zugewiesen. Rechte beschreiben hierbei die Lese-/Schreibberechtigung für einzelne Ansichten bzw. Formulare im System. Rollen beschreiben dagegen übergeordnete Muster von Lese- und Schreibrechten. Lese- und Zugriffsrechte auf bestimmte Ansichten bzw. Formulare und insbesondere auf Dateninhalte werden in DIS durch die Zugehörigkeit eines Benutzers zu einer bestimmten Organisationseinheit bzw. „Site" sowie durch die dem Benutzer zugewiesene und ggfs. individuell angepasste Rolle und durch die Zuordnung einer oder mehrerer Studien bzw. Projekte definiert (vgl. **Abschnitt 5.6.1**).

Jedem DIS-Benutzer ist genau eine Rolle zugeordnet.

5.6.1 DIS Technische und organisatorische Maßnahmen (TOM)

TOM nach Art. 32 der DSG-VO sind in Abschnitt 10 des **DIS-Datenschutzrahmenkonzepts** ausführlich beschrieben (siehe Anhang 3). Die wesentlichen Aspekte bzgl. TOM sind:

Serverräume: Die Teilsysteme sind in standardkonformen Serverräumen gemäß Bundesamt für Sicherheit in der Informationstechnik (BSI) IT-Grundschutz-Katalog untergebracht. Sie unterliegen unterschiedlicher Hoheit.

Endgeräte: Standard-Endgeräte der IT sind PCs, auf denen keine personenbezogenen Daten gespeichert werden. Die Software ist webbasiert, die Übertragung zum Server ist verschlüsselt (s.u.) und die Zwischenspeicherung (Cache) von Daten wird deaktiviert. Optional ist die Verwendung mobiler Endgeräte möglich, auf denen ebenso keine Datenspeicherung erfolgt. Die verwendeten Browser müssen festgelegten Vorgaben (System, Version, Sicherheitseinstellungen) entsprechen.

Pseudonymisierung: In DIS werden alle Daten und insbesondere IDATs zweistufig pseudonymisiert. Die verwendeten Pseudonyme sind eindeutig, bedeutungsfrei und zufällig generiert (unter Verwendung eines kryptographisch sicheren Zufallszahlengenerators).

Vertraulichkeit, Authentizität, Integrität: Die Speicherung der identifizierenden Daten und die Kommunikation zwischen allen Teilsystemen erfolgt verschlüsselt (AES bzw. https, konform mit

der technischen Richtlinie des BSI). Zwischen Servern werden Zertifikate eingesetzt, für die Clients erfolgt eine Einschränkung auf IP-Adressen oder -Adressbereiche (in Absprache mit den IT-Verantwortlichen an den Standorten).

Alle Dateneinträge und Änderungen werden in einem Audit Trail protokolliert. Es wird ein rollenbasiertes Zugriffsberechtigungssystem eingesetzt (s.u.). Eine Weitergabe von Daten und Proben erfolgt nur auf der Basis von Einwilligungserklärungen und Ethikvoten in pseudonymisierter Form (projektspezifische Pseudonyme). Dabei verpflichtet sich jede empfangende Stelle zur Einhaltung strenger Datenschutzmaßnahmen.

Rollenbasiertes Zugriffsberechtigungssystem: Alle Teilsysteme sind durch personengebundene Zugriffsberechtigungen gesichert, die entsprechend den jeweiligen Aufgaben rollenbasiert vergeben werden. Aufgabenbezogen sind damit nur eingeschränkte, speziell autorisierte und zur strikten Vertraulichkeit verpflichtete Benutzerkreise in der Lage, die zur Erfüllung ihrer Aufgabe notwendigen Maßnahmen im IT-System bzw. beim Handling von Proben durchzuführen (vgl. **Abschnitt 5.6.2**). Die Vergabe und Verwaltung von Zugriffsberechtigungen erfolgt durch die Administratoren der DZD-Geschäftsstelle.

Die in verschiedenen Teilsystemen getrennt gespeicherten Daten werden dabei ausschließlich auf dem Rechner des Benutzers zur Präsentation zusammengeführt.

Zur Nachvollziehbarkeit der Datenqualität ist in DIS ein **Audit Trail** implementiert, einmal angelegte Benutzer-Accounts werden nicht gelöscht. Zur Vermeidung von nicht berechtigten Zugriffen über ggfs. nicht mehr genutzte Accounts werden diese nach einer bestimmten Zeit automatisch auf "inaktiv" gestellt. Die Re-Aktivierung eines inaktiven Accounts funktioniert nur über ein Verfahren zum Zurücksetzen des Passworts über die im System zum jeweiligen Account registrierte E-Mail. Eine dauerhafte Stilllegung bzw. Deaktivierung eines Accounts kann nur durch Administratoren erfolgen. Deaktivierte Accounts können vom Nutzer nicht selbstständig wieder aktiviert werden.

Verfügbarkeit: Alle Daten werden regelmäßig gesichert und getrennt gelagert. Die Offsite-Backups innerhalb des Geländes des Klinikums rechts der Isar und ein entsprechender Wiederanlaufplan liegen vor.

Datenauswertung: Soweit vorhanden wird die Auswertung von MDAT und OrgDAT ausschließlich pseudonymisiert durch Berechtigte im Rahmen von durch die zuständige Ethikkommission genehmigten Projekten vorgenommen.

Löschung: Soweit gesetzliche Vorgaben nicht längere Archivierungspflichten vorsehen, werden im Falle eines Widerrufs der Einwilligung des Probanden oder Lebendspenders seine Daten gelöscht bzw. seine Biomaterialien vernichtet (vgl. **Abschnitt 6.1**).

5.6.2 Rollen und Rechtekonzept im DIS

Folgende Rollen sind in DIS für die DZD Biobank implementiert:

System-Administrator-Rolle (BitCare GmbH):

- Übergeordnete Rolle mit allen Rechten zur Systempflege und Systemwartung**. System-Anpassungen und Erweiterungen außerhalb der üblichen Wartung erfolgen in Absprache mit den Verantwortlichen der DZD Biobank bzw. in deren Auftrag.**
- Im Rahmen des Routinebetriebes ohne Zugriff auf Fachdaten (MDAT, OrgDAT) oder IDAT. Ist der Zugriff auf Fachdaten erforderlich, kann dieser in Absprache mit der DZD Biobank temporär gewährt werden.
- Anlegen zusätzlicher **System-Administratoren**
- **Diese Rolle ist im Rahmen der Auftragsdatenverarbeitung den zuständigen Mitarbeitern der Fa. BitCare vorbehalten.**

Lokale (Fach)Administrator-Rolle:

- Zugriff auf die Benutzerverwaltung für die eigene Site
- Anlegen lokaler Fach-Administratoren inkl. Liste mit Rechten, die an andere DIS-Benutzer der eigenen Site vergeben werden können.
- Beinhaltet automatisch auch die Rolle WUser (s.u.).

WUser:

- Lese- und Schreibrechte auf Patientendaten und Probendaten, sofern diese für ihn sichtbar sind (=> individuelle Rechte).

RUser:

- Nur Leserechte auf Patientendaten und Probendaten, sofern diese für ihn sichtbar sind (=> individuelle Rechte).

In DIS können je DIS-Benutzer mehrere Ansichten bzw. Formulare mit Lese-/Schreibrechten versehen werden. Das Recht zum Daten-Export wird aus Datenschutzgründen nur ausgewählten DIS-Benutzern zur Verfügung gestellt, die in den datenschutzkonformen Umgang mit den exportierten Daten eingewiesen sind.

5.6.3 Weitergabe von Proben und Daten

Die wissenschaftliche Nutzung von Bioproben und/oder Daten aus der DZD Biobank unterliegt der aktuell gültigen ***Nutzungsordnung des DZD e.V.,*** **in der auch der Probenversand** und die **Datenübergabe geregelt werden** (siehe Anhang 2).

6 Übergeordnete Maßnahmen zum Datenschutz

Allen Nutzern von MDAT aus der DZD Forschungsdatenplattform sowie von Bioproben und Daten der DZD Biobank ist es grundsätzlich untersagt, Maßnahmen zur Identifikation des Spenders zu ergreifen. Die Verbindung zwischen pseudonymisierten Daten und der identifizierenden Daten zu Studien-Probanden bzw. Biobank-Probanden kann nur durch autorisierte und zur Verschwiegenheit verpflichtete Personen, wie das Studienpersonal, hergestellt werden. IDATs unterstehen generell der ärztlichen Schweigepflicht.

Unbefugte Zugriffe werden durch geeignete Maßnahmen erschwert (z. B. Umsetzung der Password-Policy und Begrenzung der Zahl fehlgeschlagener Anmeldeversuche).

6.1 Datenlöschung nach gesetzlich vorgeschriebenen Fristen

Das DZD hat alle relevanten gesetzlichen Anforderungen in Bezug auf die Aufbewahrung personenbezogener Daten sorgfältig geprüft und dokumentiert. Das DZD stellt sicher, dass Daten nach Ablauf der gesetzlichen Aufbewahrungsfristen ordnungsgemäß und zeitnah gelöscht werden, sofern keine anderen rechtlichen Verpflichtungen bestehen, die einer Löschung entgegenstehen.

6.2 Datenschutzbeauftragter des DZD

Interne und externe Betroffenen können sich an den Datenschutzbeauftragten des DZD unter der folgenden E-Mail-Adresse wenden:

edsb@bredex.de

7 Wahrung der Betroffenenrechte

7.1 Betroffene

Betroffene Personen müssen stets über die Art, den Umfang und den Zweck der Datenerhebung und -verarbeitung auf ihre Anfrage informiert werden.

Betroffene im Sinne der DSGVO sind:

1. Studien-Probanden/Biobank-Probanden
2. Externe oder interne Nutzer, die für die Nutzung der DZD Infrastruktur (s.o.) bzw. für die Ausübung ihrer beruflichen Tätigkeit einen vom DZD zentral verwalteten Zugang/Account benötigen.

Betroffene haben jederzeit das Recht, sich an die Einrichtungen des DZD zu wenden, um ihre Betroffenenrechte gemäß DSGVO auszuüben. Studien-Probanden/Biobank-Probanden wenden sich dabei üblicherweise an die zuständigen lokalen Studienzentren, die für die Rekrutierung von DZD-Studien zuständig sind. Nutzer der zentralen DZD Infrastruktur wenden sich an hierbei an die DZD-Geschäftsstelle.

7.2 Transparenz und Informationspflicht (Art. 12 Abs. 1 DSGVO)

Studien-Probanden/Biobank-Probanden werden vor ihrer Einwilligung durch Mitarbeiter der jeweiligen Studienzentren umfassend und u.a. auch über ihre Betroffenenrechte aufgeklärt. Für die korrekte Durchführung und Dokumentation der Einwilligung sind die Studienzentren verantwortlich. Die Aufklärung beinhaltet unter anderem die im Folgenden beschriebenen Möglichkeiten zur Wahrung der Betroffenenrechte der Probanden. Sie bestätigen durch ihre Unterschrift auch, dass sie über ihre Betroffenenrechte informiert wurden und den Bedingungen zustimmen. Die studienspezifischen Vorlagen zur Einwilligung liegen dem DZD in der jeweils aktuellen Version vor.

Nutzer der DZD Infrastruktur werden durch entsprechende Datenschutzhinweise im Rahmen der Anmeldung bzw. Registrierung bei Diensten oder Softwareprodukten über Umfang und Nutzung personenbezogener Daten und ihre Betroffenenrechte informiert.

Sowohl die Aufklärung als auch die Datenschutzhinweise enthalten Angaben zu:

- Zweck, Art und Umfang der Datenverarbeitung
- Verantwortlichen Stellen und Ansprechpartnern für die Wahrnehmung ihrer Betroffenenrechte

Aufklärungen/Einwilligungen zu Studien erfordern in der Regel entsprechende Ethik-Voten vor Beginn der Studie und Akquise von Studien-Probanden/Biobank-Probanden.

Datenschutzhinweise sollen in möglichst verständlicher Form verfasst sein und jederzeit sowie leicht zugänglich sein. Anpassungen/Änderungen sollen möglichst schnell mitgeteilt werden.

7.3 Prozess zur Wahrnehmung von Betroffenenrechten

Betroffene können den Weg der Anfrage (E-Mail, Brief, Anruf, Persönlich) selbst wählen, ebenso die Form der Auskunftserteilung. Stellt die betroffene Person ihren Antrag elektronisch, kann die Auskunft per pdf-Dokument erfolgen.

Der wichtigste Schritt bei Anfragen und Umsetzung von Betroffenenrechten und insbesondere vor der Mitteilung an die Betroffenen ist die Prüfung der Identität und Rechtmäßigkeit der Anfrage.

Zu beachten ist, dass grundsätzlich alle Personen Auskunft darüber verlangen können, ob personenbezogene Daten über ihre Person verarbeitet werden. Ist dies nicht der Fall, erfolgt eine entsprechende **Negativauskunft**.

Folgende Betroffenenrechte können Studienteilnehmende oder Nutzer der DZD Infrastruktur formlos beim zuständigen Studienzentrum bzw. bei der DZD-Geschäftsstelle wahrnehmen:

- Auskunftsrecht (Art. 15 DSGVO)
- Recht auf Berichtigung (Art. 16 DSGVO)
- Widerruf der Einwilligung (Art. 7 DSGVO)
- Recht auf Löschung "Vergessenwerden" (Art. 17 DSGVO)
- Datenportabilität (Datenübertragbarkeit Art. 20 DSGVO)

Die zu ergreifenden Schritte sind abhängig von der Art des Antrags und des Betroffenenrechts sowie davon, ob lokale Studienzentren oder die DZD-Geschäftsstelle für die Umsetzung verantwortlich sind/ist.

Das Vorgehen bei Betroffenenanfragen muss aufgrund der Rechenschaftspflicht nachweisbar dokumentiert werden.

Nach Art. 12 Abs. 3 DSGVO müssen Betroffenenanfragen unverzüglich, jedoch spätestens innerhalb eines Monats nach Eingang des Auskunftsersuchens beantwortet werden. Eine Verlängerung um weitere zwei Monate ist nur Ausnahmefällen möglich. Für die Einhaltung der Frist ist je nach Art des Betroffenen (Studienteilnehmer, Nutzer) das jeweilige Studienzentrum bzw. die DZD-Geschäftsstelle verantwortlich.

Neben den o.g. Betroffenenrechten haben alle Betroffene gemäß Art. 77 DSGVO zusätzlich das Recht, sich insbesondere bei der für das DZD zuständigen Datenschutzaufsichtsbehörde zu beschweren, wenn die Auffassung besteht, dass personenbezogenen Daten nicht rechtmäßig verarbeitet wurden.

Die Anschrift der am Studienort zuständigen Aufsichtsbehörde wird in Rahmen der Aufklärung mitgeteilt.

Für Nutzer von zentralen DZD-Diensten ist der Berliner Beauftragte für Datenschutz und Informationsfreiheit, Alt-Moabit 59-61, 10555 Berlin zuständig.

8 Anhang

Zu diesem Datenschutzkonzept gehören die folgenden Anhänge

1. Leitlinie für die funktionale und strukturelle Organisation des Deutschen Zentrum für Diabetesforschung (DZD) e.V. (Stand 18.10.2023)
2. Nutzungsordnung des DZD e.V. (Version 2.0, 15.09.2023)
3. Datenschutzrahmenkonzept Data Integration System (DIS) (Version 2.3 vom 26.08.2020; überprüft am 21.03.2022)