Nationales Register für Seltene Erkrankungen
NARSE

Datenschutzkonzept mit Datenschutz-Folgenabschätzung[1]

Projekt NARSE (Nationales Register für Seltene Erkrankungen)

Autor/innen Dr. Jessica Vasseur, Jens Göbel
Institut für Medizininformatik
Johann Wolfgang Goethe-Universität Frankfurt am Main

Dr. Franziska Krause
Eva Luise und Horst Köhler Stiftung für Menschen mit Seltenen Erkrankungen
BIH at Charité | Charité – Universitätsmedizin Berlin

Dr. Josef Schepers
Core Facility Digitale Medizin und Interoperabilität
BIH at Charité | Charité – Universitätsmedizin Berlin
Mitglied der TMF AG Datenschutz

Betreiber[2] Berlin Institute of Health at Charité (BIH)
Charité – Universitätsmedizin Berlin
Anna-Louisa-Karsch-Str. 2
10178 Berlin

[1] Dieses Datenschutzkonzept basiert auf einer Schablone für OSSE-Datenschutzkonzepte von M. Muscholl, M. Lablans, A. Borg, F. Ückert und TOF Wagner, überarbeitet von J. Vasseur, K. Schüler und J. Göbel (v2.0, Juni 2022). Es wurden in Abschnitt 1 „Einleitung“ und im Anhang in Abschnitt 8 „Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten“ ergänzende Elemente einer rudimentären Datenschutz-Folgenabschätzung (DSFA) gemäß Art. 35 Abs. 7 DSGVO eingefügt.

[2] Verantwortlicher im Sinne des Art. 4 DSGVO

Änderungshistorie[3]

Versionen DSK/DSFA[4]	Was	Wer	Wann
v0.1	Entwurf basierend auf Schablone für OSSE-Datenschutzkonzepte	JV, JG, FK	01.08.2022
v0.9/v0.9a	Entwurf mit Ergänzung um tabellarische DSFA	JS	04.11.2022
v0.96/v0.96a	Finalisierung für Votum in TMF AG Datenschutz	JS, JV, JG	21.03.2023
v0.99/v0.99a	Nachbesserungen für Votum in TMF AG Datenschutz	JS, JV, JG	06.06.2023
v1.0/v1.0a	Nachbesserungen nach Hinweisen der bDSB Charité	JS, JV, JG	30.06.2023
v1.1/ v1.1a	Redaktionelle Anpassungen, Einfügen von 2.1. Rollen und Berechtigungen, Löschen von vorübergehenden Anhängen	FK	17.10.2023
v1.2/v1.2a	Anpassungen an Nutzungsordnung und Aktualisierung Grafiken	JS, FK, StS	15.01.2024
v1.2/v1.2b	Anpassungen nach Rückmeldung aus TMF AG Datenschutz	JS, JV	15.04.2024
v2.0/v2.0a	umfassende Überarbeitung mit redaktionellen Anpassungen und Korrektur von Verweisen / Versionsnummern • Anpassung an aktualisierte Nutzungsordnung (v1.2 vom 19.12.2024) und Einwilligungsdokumente (v1.4 vom 03.12.2024) • Aktualisierung und Ergänzung Grafiken (Abb. 1 „Registerorganisation“, Abb. 3 „Datenflüsse“) • Beschreibung der Zielsetzung des NARSE analog zur Nutzungsordnung (Abschnitt 1.2) • Vereinheitlichung Begriffe (insb. Organisationsstruktur, Abschnitt 2) und Formatierung (Anpassung an andere Dokumente) • Angaben zu verantwortlichen Stellen für Betrieb der Komponenten verschoben in Abschnitt 3.1.2 • Beschreibung digitales Einwilligungsmanagement (Abschnitt 3.3) und der datenverarbeitenden Prozesse (Abschnitt 4.1) • Beschreibung Prozess Datenimport (Abschnitt 4.2 / 4.3.2) • Beschreibung Datenexport / Datennutzungsformen entsprechend der Nutzungsordnung ohne Use Files, inklusive Zugriff durch Administrierende (Abschnitt 4.4, Abschnitt 5.3) • Beschreibung Verschlüsselung mit Verweis auf Vorgaben des BSI ohne weitere Ausführungen (Abschnitt 5.3.2) • Beschreibung der modularen Einwilligungsoptionen (Abschnitt 6.1) • Überarbeitung Rollen & Berechtigungen (Anhang 7.3) • Redaktionelle Anpassungen in tabellarischer DSFA (Anhang 8)	JV, CH, FK	30.01.2025

[3] Interne Zwischenversionen im Rahmen der Erstellung und Überarbeitung des Dokuments werden in der Änderungshistorie nicht berücksichtigt

[4] Die DSFA-Tabelle wird mit fortlaufendem Versions-Suffix (a, b, c; …) in Anhang 8 gepflegt. Änderungen des Datenschutzkonzepts führen immer zu einer neuen Versionsnummer von Datenschutzkonzept (1.0, 1.1, 2.0) und DSFA (1.0a, 1.1a, 2.0a). Änderungen der DSFA kommen ohne und mit Änderungen des Datenschutzkonzepts infrage (1.0a, 1.0b, 1.0c, 1.1d) und berühren nicht die Gültigkeit des Datenschutzkonzepts.

Inhalt

1. EINLEITUNG

1.1 Zielsetzung des vorliegenden Dokuments

Das Nationale Register für Seltene Erkrankungen (NARSE) soll durch die Verarbeitung von personenbezogenen Daten von Betroffenen einer Seltenen Erkrankung einen relevanten Beitrag zum medizinischen Fortschritt leisten. Dabei sind sowohl die Rechte und Freiheiten der betroffenen Personen als auch die Verarbeitung ihrer personenbezogenen Daten in besonderem Maße zu schützen, insbesondere da es sich um Daten einer besonderen Kategorie personenbezogener Daten im Sinne von Art. 9 Abs. 1 Datenschutzgrundverordnung (DSGVO) handelt, die besonders sensibel sind und der ärztlichen Schweigepflicht nach § 203 StGB unterliegen können.

Das vorliegende Dokument umfasst als kontinuierlich zu pflegendes „lebendes Dokument" ein klassisches Datenschutzkonzept und eine gemäß Art. 35 DSGVO notwendige Datenschutz-Folgenabschätzung (DSFA) in tabellarischer Form. Die in Art. 35 Abs. 7 DSGVO geforderten Komponenten einer DSFA sind vorhanden und werden im stetigen Datenschutz-Assessment-Prozess in nachfolgenden Fassungen angepasst:

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

Das vorliegende Dokument folgt der Vorstellung im Kurzpapier Nr. 5 der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz), wonach die DSFA als *„ein spezielles Instrument zur Beschreibung, Bewertung und Eindämmung von Risiken für die Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten*" zu verstehen ist[5]. Ferner wird der Deklaration der Datenschutzkonferenz gefolgt, wonach eine DSFA kein einmaliger Vorgang ist[6].

In diesem Sinne befasst sich das vorliegende Datenschutzkonzept mit den Datenverarbeitungsstrukturen und -prozessen des NARSE. Als Grundlage der technischen Infrastruktur für das Register dient die OSSE-Software (Open Source Registersystem für Seltene Erkrankungen)[7], die auch für andere Register, insbesondere im Bereich der Seltenen Erkrankungen, eingesetzt wird. Neben der manuellen Datenerfassung über die web-basierte OSSE-Benutzerschnittstelle (OSSE EDC) sollen Dateneinspielungen aus anderen Datenbeständen, z.B. aus angeschlossenen Registern oder Betroffenendokumentationen so-

[5] https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_5.pdf Das vorliegende Dokument beachtet die sieben Gewährleistungsziele des Standarddatenschutzmodells der Datenschutzkonferenz des Bundes und Länder und die darin abgebildeten zentralen Datenschutzanforderungen der DSGVO. Die sieben angestrebten Gewährleistungsziele sind: Datenminimierung, Verfügbarkeit, Integrität, Vertraulichkeit, Nichtverkettung, Transparenz, Intervenierbarkeit.

[6] Überprüfung und Wiederholung des DSFA bei Änderungen fordert Art. 35 Abs. 11 DSGVO

[7] https://www.osse-register.de/

wie den Datenintegrationszentren der Universitätsklinika, ermöglicht werden. Der Datenschutz-Assessment-Prozess wird kontinuierlich fortgeführt und das Datenschutzkonzept inklusive DSFA, falls notwendig, entsprechend an technische Änderungen und neue Rahmenbedingungen angepasst, zum Beispiel durch genaue Beschreibung der ergänzenden Verarbeitungstätigkeiten, der damit verbundenen Risiken und der als notwendig erachteten Schutzmaßnahmen. Das vorliegende Datenschutzkonzept stellt eine zusammenfassende Dokumentation aller datenschutzrechtlichen Aspekte und Maßnahmen zur Einhaltung und Sicherung des Datenschutzes im NARSE dar.

1.2 Zielsetzung und Zweck der Datenverarbeitung im NARSE

In Europa gilt eine Erkrankung als „selten“, wenn weniger als fünf von von 10.000 Personen (Prävalenz 1:2.000) davon betroffen sind. In Deutschland sind schätzungsweise vier bis fünf Millionen Menschen von einer der 6.000 bis 10.000 bekannten verschiedenen Seltenen Erkrankungen betroffen. Bisher gibt es zu den Betroffenenzahlen in Deutschland jedoch keine verlässlichen Daten, auch nicht aus der Sekundärnutzung von Routinedaten. Forschung und Versorgung sind „im Blindflug“ unterwegs, was die Entwicklung von evidenzbasierten Behandlungen und neuen Therapien enorm erschwert.

Gerade bei Seltenen Erkrankungen, bei denen die Fallzahlen gering und die Erkenntnisse der Behandelnden durch eigene Beobachtungen limitiert sind, sind Register wichtige Instrumente der Epidemiologie und der Versorgungsforschung. Die in Deutschland bestehenden Register befassen sich im Regelfall mit spezifischen Seltenen Erkrankungen und unterscheiden sich erheblich in ihrer Qualität, Trägerschaft und erhobenen Daten. Nur wenige Register konnten so aufgesetzt und kontinuierlich gepflegt werden, dass tatsächlich ein Großteil der Betroffenen einer Seltenen Erkrankung in Deutschland erfasst ist und die Registerdaten eine nutzbare Ressource für die Forschung darstellen. In Deutschland existiert kein Register, das im Bereich der Seltenen Erkrankungen die Translation neuer Verfahren einrichtungs- und krankheitsübergreifend unterstützt. Das NARSE soll diese Lücke schließen und erstmals einen Überblick über die in Deutschland lebenden Betroffenen ermöglichen.

Das NARSE wurde im Mai 2021 vom Think Tank der Eva Luise und Horst Köhler Stiftung für Menschen mit Seltenen Erkrankungen (ELHKS) initiiert. Als institutionenübergreifende „Denkfabrik“ identifiziert das informelle Gremium besonders dringliche Vorhaben im Bereich der Seltenen Erkrankungen und treibt diese aktiv voran. Als eine prioritäre Aufgabe sah der Think Tank den Aufbau und die Entwicklung einer Struktur an, die die Auffindbarkeit, Zugänglichkeit, Interoperabilität und Nutzbarkeit der Gesundheitsdaten von Menschen mit Seltenen Erkrankungen gemäß der FAIR-Prinzipien (Auffindbarkeit, Zugänglichkeit, Interoperabilität und Wiederverwendbarkeit) verbessert. Vor diesem Hintergrund wurde, zunächst zivilgesellschaftlich finanziert, das NARSE vom Berlin Institute of Health in der Charité – Universitätsmedizin Berlin gemeinsam mit dem Institut für Medizininformatik der Goethe-Universität Frankfurt aufgesetzt.

Im NARSE werden die Daten von Betroffenen mit einer Seltenen Erkrankung mit Hilfe eines an europäischen Standards orientierten Minimaldatensatzes erfasst. Primäres Ziel des NARSE ist es, grundlegende Daten über in Deutschland Betroffene von Seltenen Erkrankungen zu erheben, um epidemiologische Aussagen über diese Erkrankungen für Deutschland treffen zu können. Mit dem NARSE soll eine Grundlage für effektive Forschung und die Entwicklung neuer evidenzbasierter Behandlungsmethoden geschaffen werden. Gerade Betroffenen mit Ultraseltenen Erkrankungen (Prävalenz < 1:50.000) eröffnet das NARSE die Chance für Vernetzung und schafft die Möglichkeit, über aktuelle Studien oder neue Therapien informiert zu werden.

1.3 Rechtsgrundlage

Die informierte Einwilligung der zu registrierenden Person (siehe Abschnitt 6.1 „Aufklärung und Einwilligung“) bildet die Rechtsgrundlage der Datenverarbeitung gemäß Art. 6 Abs. 1 lit. a i.V.m. Art. 9 Abs. 2 lit. a DSGVO. Sie nennt explizit die Institutionen und Personengruppen, die festgelegte Datenarten erheben, verarbeiten und nutzen dürfen. Auch die Weitergabe von anonymisierten oder pseudonymisierten Daten zu Forschungszwecken wird in der Einwilligung berücksichtigt, da speziell im Bereich der Seltenen Erkrankungen nicht ausgeschlossen werden kann, dass durch die Krankheitsdaten Rückschlüsse auf die Identität der registrierten Person gezogen werden können. Die Datenübernahme aus anderen Datenbeständen wird in der Regel auf einer nachgeholten informierten Einwilligung zur Übermittlung in das und zur Nutzung im NARSE beruhen.

1.4 Überblick über die Datenverarbeitung

Im NARSE werden Daten von Betroffenen einer Seltenen Erkrankung, die in den teilnehmenden Kliniken, Zentren, Praxen oder Patientenorganisationen (auch als „Meldende Stellen“ bezeichnet) behandelt werden, erhoben, verarbeitet und genutzt. Darunter fallen auch minderjährige Personen oder Personen mit eingeschränkter Willensbildung; dies wird in Bezug auf die informierte Einwilligung berücksichtigt.

Die Daten werden auf folgende Weise im Register erfasst:

- manuell über die web-basierte OSSE-Benutzerschnittstelle (OSSE EDC)
- per Datenimport über die Importschnittstelle des OSSE EDC

Folgende Arten von Daten werden unter Beachtung des Grundsatzes der Datensparsamkeit und Datenminimierung gemäß Art. 5 DSGVO erhoben:

- Identifizierende Daten (IDAT): Sie enthalten Daten (z.B. Name, Geburtsdatum und -ort, Kontaktdaten), die eine eindeutige Identifikation einer Person erlauben. Sie werden nicht im Register, sondern separat in einem Pseudonymisierungs- und Identitätsmanagement gespeichert und verwaltet.
- Medizinische Daten (MDAT): Dazu gehören routinemäßig erhobene Daten (genetische und Gesundheitsdaten) über die Erkrankung und deren Verlauf, die in der Registerdatenbank des NARSE erfasst werden. Hierbei handelt es sich um besonders schützenswerte Daten. Es werden keine weiteren Datenarten (z.B. bildgebende Daten, biometrische Daten) erfasst und gespeichert.

Genauere Informationen zum Umfang der Daten finden sich im Anhang unter 7.3 „Datensatz NARSE“.

Alle Datenfelder, die im NARSE erfasst werden, sind in einem für alle OSSE-Register zentral betriebenen Metadaten-Repository registriert und definiert. Die Registerstruktur (Formulare zur strukturierten Erfassung von Daten) wird mithilfe eines Formulareditors dynamisch festgelegt und zentral gespeichert.

Daten aus dem NARSE werden zu Auswertungszwecken je nach Erforderlichkeit und Art der Datennutzung mit nicht-rückführbaren Exportpseudonymen oder mit den im Register sichtbaren Pseudonymen exportiert und in einem in der Nutzungsordnung festgelegten Verfahren für die wissenschaftliche Nutzung bereitgestellt (siehe Abschnitt 4.4 „Datenexport und Datennutzung“, Anhang 7.2 „Nutzungsordnung NARSE“).

Eine detaillierte Beschreibung der Komponenten und Prozesse wird in den Abschnitten 3 („Datenverarbeitende Komponenten“) und 4 („Datenverarbeitende Prozesse“) gegeben.

1.5 Bewertung der Zweckmäßigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge

Hier wird die in Art. 35 Abs. 7 lit. b DSGVO geforderte *„Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck“* vorgenommen:

Es existieren nur Schätzungen, wie viele Menschen mit Seltenen Erkrankungen in Deutschland leben. Es wird von einer Zahl in der Größenordnung von 4 Millionen Personen ausgegangen. Es wird ein Spektrum von 6.000 bis 10.000 verschiedenen Krankheiten angenommen, bei denen das Spektrum der Zahl der Betroffenen von mehreren zehntausend bis hinunter zu wenigen Einzelpersonen reicht. Es gibt im deutschen Gesundheitssystems mit vielen Tausenden Leistungserbringern und vielen Dutzend Leistungsfinanzieren, die jeweils getrennte Datensilos führen, keine epidemiologische Übersicht.

Für den Zweck der epidemiologischen Übersicht über die Inzidenz und Prävalenz Seltener Erkrankungen ist es notwendig und verhältnismäßig, ein nationales Register aufzubauen, das, unter anderem, von allen Zentren für Seltene Erkrankungen unterstützt wird.

Oft vergehen Jahre, bis Menschen mit Seltenen Erkrankungen eine Diagnose und eine Therapie erhalten. Letzteres gilt auch, wenn eine Diagnose bestimmt werden konnte, aber Informationen über veränderte Behandlungsoptionen, beispielsweise über neue kausale Therapien oder neue Enzymersatztherapien, die Betroffenen nicht erreichen. Beim Versuch der Rekrutierung von Betroffenen für klinische Studien für Diagnostik und Therapien wird regelmäßig die für eine statistisch gesicherte Aussagekraft (Power, Evidenz) notwendige Probandenzahl nicht erreicht.

Für den Zweck der Kommunikation von Diagnostik- und Therapieoptionen (einschließlich der Einladung zu klinischen Studien), ist es notwendig und verhältnismäßig, Betroffenen, potentiell Betroffenen, ihren Eltern und/oder Betreuern die Möglichkeit anzubieten, sich in ein nationales Register einzutragen oder eintragen zu lassen, das als Grundlage dafür dient, die Behandelnden, die Behandelbaren und deren Eltern oder Betreuer spezifisch über konkrete Entwicklungen von Diagnostik- und Therapieoptionen zu informieren.

1.6 Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen

Hier wird die in Art. 35 Abs. 7 lit. c DSGO geforderte „*Bewertung der Risiken für die Rechte und Freiheiten der betroffenen* Personen“ vorgenommen, deren Daten gemäß Art. 35 Abs. 1 DSGVO in einer Weise verarbeitet werden, in der ohne Schutzmaßnahmen voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen entsteht.

Im NARSE werden personenbezogen sensible Gesundheits-, Erkrankungs- und genetische Daten im Sinne des Art. 9 DSGVO gespeichert und verarbeitet. Bei nicht-erlaubtem individuellem Bekanntwerden einzelner Angaben können den registrierten Personen soziale und wirtschaftliche Schäden entstehen. Das Recht auf informationelle Selbstbestimmung würde verletzt. Freiheitsgrade des persönlichen Handelns wären bedroht. Gemäß Art. 6 DSGVO ist die Verarbeitung dieser Daten untersagt, wenn das Verbot nicht durch eine gehaltvolle Erlaubnis aufgehoben wird. Beim NARSE erfolgt durch die dokumentierte, informierte Einwilligung die Erlaubnis der Verarbeitung durch einen definierten Personenkreis und für definierte Zwecke.

Technische und organisatorische Schutzmaßnahmen, die in den Kapiteln 2 bis 6 des vorliegenden Datenschutzkonzepts näher beschrieben sind, stellen sicher,

- dass die Verarbeitung nur durch den berechtigten Personenkreis erfolgt,

- dass die Verarbeitung nur zu den erlaubten Zwecken erfolgt,
- dass die sensiblen Angaben keinen unberechtigten Personen bekannt werden.

Unter Einhaltung dieser Bedingungen dürfen die Risiken für die Rechte und Freiheiten der betroffenen Personen beim angestrebten Betrieb des NARSE als im geforderten und notwendigen Maß reduziert gelten. Diese Einschätzung wird mit den zuständigen Behördlichen Beauftragten für Datenschutz und Informationsfreiheit per Antrag auf Stellungnahme abgestimmt. Monita werden in einem kontinuierlichen Datenschutz-Assessment-Prozess aufgearbeitet.

2. ORGANISATIONSSTRUKTUR DES NARSE

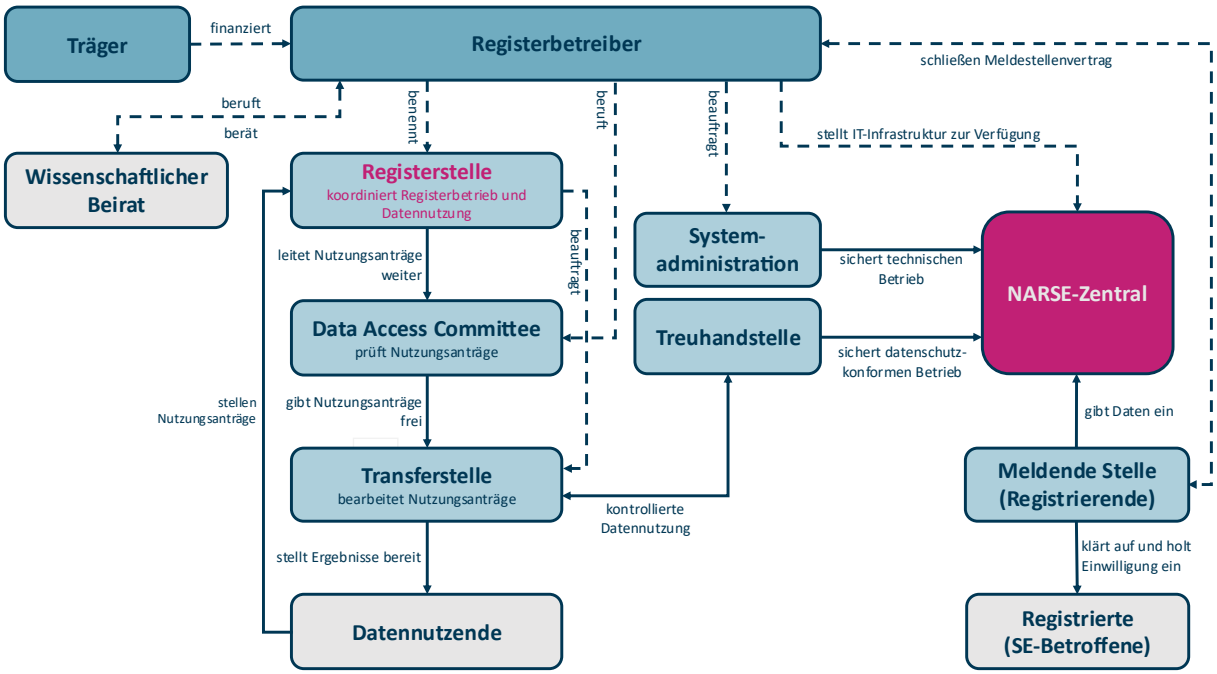


Abbildung 1: Registerorganisation des NARSE

2.1 Träger und Registerbetreiber

Aktueller Träger des Vorhabens und Registerbetreiber, und damit Verantwortlicher im Sinne des Art. 4 DSGVO, ist das Berlin Institute of Health (BIH) der Charité – Universitätsmedizin Berlin als Körperschaft des öffentlichen Rechts.

Berlin Institute of Health at Charité (BIH)
Charité – Universitätsmedizin Berlin
Anna-Louisa-Karsch-Str. 2
10178 Berlin

Vor dem Ende der zugesagten Finanzierung bis Ende 2026 wird der Registerbetreiber sich rechtzeitig um Findung von Möglichkeiten zur Weiterführung und einer Verstetigung des NARSE bemühen. Registrierte Personen werden über einen möglichen Wechsel der Trägerschaft rechtzeitig informiert und können in diesem Fall ihre Einwilligung in die Verarbeitung ihrer Daten im NARSE widerrufen (siehe Abschnitt 6.4 „Widerruf, Löschung, De-Identifizierung“).

2.2 Wissenschaftlicher Beirat

Die Weiterentwicklung des NARSE in den skizzierten Entwicklungsstufen erfolgt in beratender Funktion durch einen wissenschaftlichen Beirat, der sich unter anderem aus Vertreterinnen und Vertretern des Registerbetreibers, Vertreterinnen und Vertretern der ELHKS und Betroffenenvertretungen zusammensetzt. Die Mitglieder des wissenschaftlichen Beirats werden vom Registerbetreiber berufen.

2.3 Registerstelle

Die Registerstelle des NARSE ist die vom Registerbetreiber ernannte Arbeitsgruppe, die den Registerbetrieb des NARSE sowie die Datennutzung koordiniert, einschließlich der Kommunikation mit dem Data Access Committee, der Transferstelle, der Treuhandstelle und der Systemadministration.

Als Registerstelle wurden am 13.12.2024 berufen:

Dr. Franziska Krause und Dr. Mara Hartung
BIH at Charité | Charité – Universitätsmedizin Berlin
Geschäftsbereich Strategisches Wissenschaftsmanagement
Anna-Louisa-Karsch-Str. 2
10178 Berlin

2.4 Registrierte Personen

Registrierte Personen sind von einer Seltenen Erkrankung betroffene Personen, die in ihre Aufnahme in das NARSE eingewilligt haben oder diese veranlasst haben und deren Daten einwilligungsbasiert durch meldende Stellen im NARSE erfasst werden.

2.5 Meldende Stellen (Registrierende)

Meldende Stellen sind die Personen oder Einrichtungen wie Ärztinnen und Ärzte, Kliniken/Zentren, Patientenorganisationen, welche Daten in das NARSE eingeben. Eine aktuelle Liste der am NARSE beteiligten Kliniken, Zentren und Patientenorganisationen ist unter www.narse.de zu finden. Generell können alle Mitglieder der meldenden Stellen als Registrierende das NARSE nutzen, wobei die meldenden Stellen selbst entscheiden, welche Mitglieder, nach Prüfung und Zustimmung durch die Registerstelle des NARSE, eine Zugangsberechtigung erhalten sollen. Der zu schließende Meldestellenvertrag zwischen Registerbetreiber und meldenden Stelle regelt die Pflichten der meldenden Stelle zur sicheren und zuverlässigen Übermittlung von Daten an den Registerbetreiber, der für die ordnungsgemäße Verwaltung, Verarbeitung und den Schutz dieser Daten verantwortlich ist.

2.6 Datennutzende

Datennutzende sind natürliche oder juristische Personen, die an einem Nutzungsprojekt beteiligt sind und durch Abschluss eines Nutzungsvertrags Vertragspartei zum NARSE werden oder im Rahmen einer genehmigten Nutzungsanzeige Daten des NARSE nutzen. Sie stellen Nutzungsanträge oder Nutzungsanzeigen zur Nutzung von Daten des NARSE für wissenschaftliche Zwecke an die Registerstelle.

2.7 Treuhandstelle

Die Treuhandstelle des NARSE übernimmt die Verwaltung der personenidentifizierenden Daten (IDAT), die Erzeugung und Verwaltung von Pseudonymen für verschiedene Zwecke sowie das zentrale digitale Einwilligungsmanagement, einschließlich der Dokumentation von Änderungen der Einwilligungen bei Widerrufen. Sie unterstützt die Transferstelle bei der datenschutzkonformen Bereitstellung von Daten. Die Treuhandstelle ist organisatorisch unabhängig vom Registerbetreiber und hat keinen Zugriff auf die im NARSE erfassten medizinischen Daten (MDAT).

2.8 Systemadministration

Die Systemadministration des NARSE ist für die Bereitstellung und Wartung der verwendeten Registersoftware sowie die technische Speicherung und Verarbeitung der medizinischen Daten (MDAT) im NARSE zuständig, hat aber keinen Zugriff auf identifizierende Daten (IDAT). Sie verwaltet außerdem die Metadaten aller Datenelemente oder Variablen des NARSE in Form eines Data Dictionaries, unterstützt die Transferstelle bei der Bereitstellung von Daten aus dem NARSE und den Registerbetreiber bei der Umsetzung der Betroffenenrechte (Löschung von Daten im Rahmen eines Widerrufs, Auskunft über gespeicherte Daten).

2.9 Data Access Committee

Der Registerbetreiber benennt in Absprache mit dem wissenschaftlichen Beirat ein Data Access Committee, das für die Prüfung und Bewilligung von Nutzungsanträgen auf Bereitstellung medizinischer Daten für wissenschaftliche Zwecke verantwortlich ist. Leitfaden des Data Access Committees ist die vom Registerbetreiber verabschiedete Nutzungsordnung in der jeweils gültigen Fassung. Diese regelt unter anderem, wie das Antrags- und Genehmigungsverfahren aussieht, welche Kriterien ein Datennutzungsantrag erfüllen muss und in welcher Weise Behandelnde die Registerdaten für eigene Forschungszwecke nutzen können.

2.10 Transferstelle

Die Transferstelle übernimmt und koordiniert den gesamten Prozess der Bereitstellung von Daten aus dem NARSE für wissenschaftliche Auswertungen. Ferner gehört zu ihren Aufgaben die Beratung des Data Access Committees in Bezug auf die Machbarkeit von Nutzungsanträgen.

3. DATENVERARBEITENDE KOMPONENTEN

3.1 OSSE-Registersystem

3.1.1 Komponenten und Funktionen

Die OSSE-Software (Abbildung 2) dient der Erfassung und Speicherung medizinischer Daten von registrierten Personen im NARSE. Datenfelder und Formulare sind zentral in einem Metadaten-Repository bzw. Formulareditor definiert und beschrieben und können auch nach Start des laufenden Vorhabens modifiziert und ergänzt werden.

Die Eingabe der Daten erfolgt in den meldenden Stellen über die webbasierte Benutzerschnittstelle des OSSE EDC. Zusätzlich können Daten aus externen Quellen über Schnittstellen für den Datenimport erfasst werden. Alle medizinischen Daten werden versioniert in der Datenbank des OSSE EDC gespeichert. Über die Benutzeroberfläche geänderte und gelöschte Werte bleiben in der Datenbank erhalten und können bei Bedarf abgerufen werden.

Personenbezogene IDAT werden nicht im OSSE EDC, sondern direkt im Pseudonymisierungs- und Identitätsmanagement „Mainzelliste“ unter Verantwortung der Treuhandstelle des NARSE erfasst. Die Kommunikation zwischen Mainzelliste und dem OSSE EDC findet auf eine Weise statt, die keine IDAT an das OSSE EDC überträgt. Für Benutzerinnen und Benutzer erscheint die Eingabemaske der Mainzelliste integriert in die webbasierte Benutzeroberfläche des OSSE EDC. Das zurückgelieferte Pseudonym, „PSN_{OSSE}“ (siehe Abschnitt 3.2 „Pseudonymisierungs- und Identitätsmanagement“), wird mit den MDAT gespeichert, aber nicht angezeigt, sodass auch manuell keine Zuordnung der IDAT mit dem PSN_{OSSE} außerhalb des Pseudonymisierungs- und Identitätsmanagements möglich ist. Da MDAT behandlungsnah lokal erfasst werden, können IDAT und MDAT aber im Browser zusammen angezeigt werden. Dies geschieht mithilfe temporärer Identifikatoren, über die der Browser z.B. Name und Vorname der registrierten Person abruft und die sicherstellen, dass die Zuordnung zwischen dem PSN_{OSSE} und den IDAT der registrierten Person außerhalb des Pseudonymisierungs- und Identitätsmanagements nicht bekannt wird.

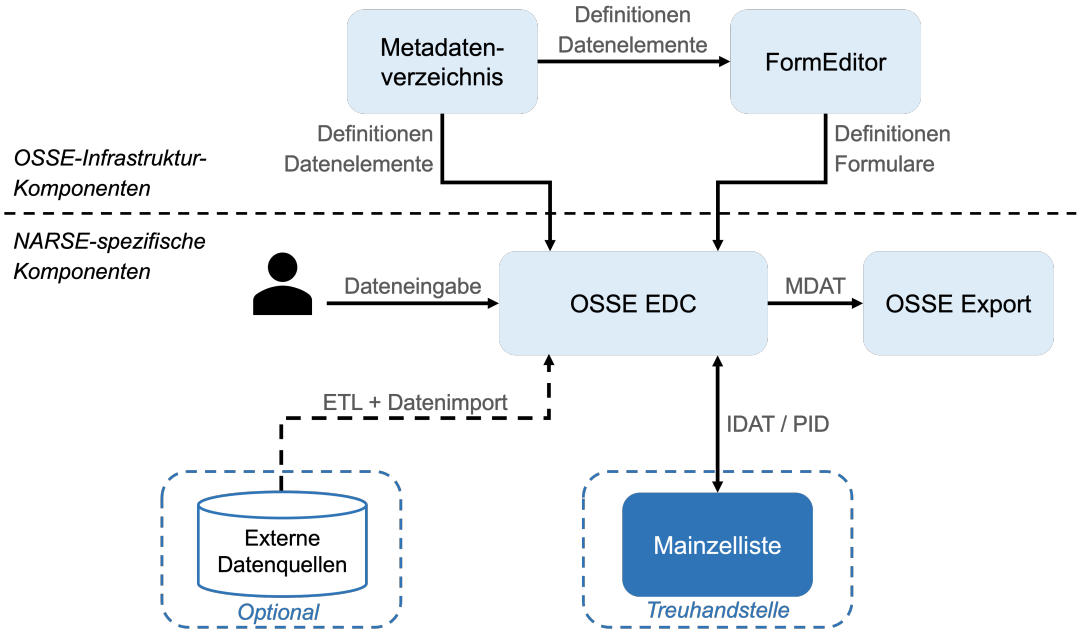


Abbildung 2: Aufbau des OSSE-Registersystems

3.1.2 Betrieb der Komponenten

Der Betrieb des NARSE erfolgt in der Verantwortung des Berlin Institute of Health (BIH) der Charité – Universitätsmedizin Berlin.

Berlin Institute of Health at Charité (BIH)
Charité – Universitätsmedizin Berlin
Anna-Louisa-Karsch-Str. 2
10178 Berlin

Die Registersoftware und Registerdatenbank des NARSE werden auf einem angemieteten Server eines den Anforderungen des Bundesamts für die Sicherheit in der Informationstechnik (BSI) entsprechenden Rechenzentrums gehostet. Mit dem Anbieter wird vom Betreiber des NARSE ein Vertrag zur Auftragsverarbeitung abgeschlossen.

Hetzner Online GmbH
Industriestr. 25
91710 Gunzenhausen
Deutschland

Die Systemadministration der IT-Infrastruktur der OSSE-Komponenten und der technische Support des NARSE wird im Rahmen eines Joint Controllers Vertrags zwischen Betreiber des NARSE, Systemadministration und Treuhandstelle an das Institut für Medizininformatik (IMI) der Goethe-Universität Frankfurt überantwortet.

Institut für Medizininformatik (IMI)
Goethe-Universität Frankfurt
Universitätsmedizin Frankfurt
Theodor-Stern-Kai 7
60590 Frankfurt am Main

Der Betrieb des Pseudonymisierungs- und Identitätsmanagementstools Mainzelliste[8] sowie des zentralen Einwilligungsmanagements gICS (generic Informed Consent Service)[9] wird im Rahmen eines Joint Controller Vertrags zwischen Betreiber des NARSE, Systemadministration und Treuhandstelle an die Unabhängige Treuhandstelle der TU Dresden (UTHS Dresden) überantwortet.

Unabhängige Treuhandstelle Dresden
Bereich Medizin der
Technischen Universität Dresden
Fetscherstraße 74
01307 Dresden

[8] https://www.unimedizin-mainz.de/imbei/informatik/ag-verbundforschung/mainzelliste.html

[9] https://www.ths-greifswald.de/forscher/gics/

3.1.3 Workflow

MDAT werden in Formularen erfasst, die im Bearbeitungsablauf folgende Statuswerte annehmen können:

- Unused: Das Formular wurde noch nicht geöffnet oder bearbeitet.
- Open: MDAT wurden in das Formular eingegeben und gespeichert.
- Reported: Die Eingabe der MDAT ist vorerst beendet und zur Validierung freigegeben (OSSE-Berechtigung „DataReport"). Änderungen sind temporär nicht möglich; über die OSSE-Berechtigung „DataValidation" kann der Status in „Open" oder „Validated" geändert werden.
- Validated: Die im Formular erfassten MDAT wurden validiert (über die notwendige OSSE-Berechtigung „DataValidation"). Eine nachträgliche Änderung ist nur mit erweiterten Zugriffsrechten möglich (OSSE-Berechtigung „RemoveValidation").

3.1.4 Zugänge, Rollen und Rechte

Zugriffsberechtigungen werden rollenbasiert durch einen Administrator oder eine Administratorin des NARSE vergeben, damit jede nutzende Person (Registrierende/r) des NARSE nur die ihr zugeordneten und für sie relevanten Daten einsehen kann (siehe Abschnitt 5.2 „Autorisierung und Authentifizierung"). Registrierende besitzen entsprechend ihrer Funktion eine oder mehrere Rollen, mit denen die Anmeldung erfolgt. Für die Definition der Zugriffsrechte werden Daten insbesondere nach ihrer Zuordnung zur meldenden Stelle und nach den beteiligten Berufsgruppen bzw. Funktionen klassifiziert. Eine detaillierte Liste der Rollen im NARSE und ihrer Beschreibung sowie der zugeordneten Berechtigungen findet sich im Anhang 7.4 „Rollen & Berechtigungen".

3.2 Pseudonymisierungs- und Identitätsmanagement

Pseudonymisierung ist ein zur Aufrechterhaltung eines hohen Datenschutzniveaus notwendiger Schritt, um eine im NARSE erfasste Person vor Re-Identifizierung zu schützen. Anstelle ihrer IDAT treten Pseudonyme. Bei der Anforderung eines Pseudonyms wird der Datensatz auf Übereinstimmung mit schon vorhandenen Datensätzen überprüft (Record Linkage). Je nach Grad der Übereinstimmung der IDAT und den eingestellten Schwellwerten, wird ein neuer Datensatz erzeugt oder ein vorhandener zurückgeliefert.

3.2.1 Pseudonyme

Für die Pseudonymisierung im NARSE wird eine Instanz der Mainzelliste genutzt, die von der Treuhandstelle des NARSE betrieben wird. Sie erzeugt für jede registrierte Person im Register einen eindeutigen Identifikator (PID) und ein Pseudonym zweiter Stufe (PSN_{OSSE}) sowie ein Pseudonym zur Verwendung im digitalen Einwilligungsmanagement (PSN_{gICS}). Die Mainzelliste kann außerdem nicht-rückführbare Exportpseudonyme für den Export von Registerdaten zu Forschungszwecken erzeugen.

3.2.2 Manuelles Linken

Eine Schnittstelle der Mainzelliste erlaubt den Administrierenden der Treuhandstelle, Ergebnisse des automatischen Matchings manuell zu überprüfen und ggf. zu korrigieren, d.h. Duplikate zusammenzuführen oder fälschlicherweise zusammengeführte Datensätze zu trennen. Hierfür werden die Matchgewichte (Vergleichswerte zwischen den einzelnen Attributen von zu prüfenden Personen) angezeigt. Zur Entscheidungsfindung bei unklaren Fällen können in einem protokollierten Prozess auch MDAT hinzugezogen werden. Die Administrierenden der Mainzelliste teilen einer verantwortlichen Person des Registerbetreibers die betroffenen Pseudonyme mit. Seitens des Registerbetreibers werden die

zugehörigen MDAT auf Übereinstimmung geprüft und der Treuhandstelle mitgeteilt, ob es sich mit hoher Wahrscheinlichkeit um dieselbe Person handelt oder nicht.

3.3 Einwilligungsmanagement

Rechtsgrundlage der Datenverarbeitung im NARSE sind die informierte Einwilligung der registrierten Personen oder durch deren gesetzliche Vertretenden mit den in Abschnitt 6.1 („Aufklärung und Einwilligung“) beschriebenen optionalen Differenzierungen.

Das zentrale digitale Einwilligungsmanagement in der Treuhandstelle des NARSE erfolgt mithilfe des Open-Source Tools gICS. Dieses dient der Verarbeitung modular abgebildeter Einwilligungen und Widerrufe im Kontext eines Registers und lässt sich sowohl in papierbasierte als auch rein digitale Arbeitsabläufe integrieren.

Die Erhebung der Einwilligungen als Rechtsgrundlage der Datenverarbeitung im NARSE erfolgt bei den meldenden Stellen papierbasiert mit Verwahrung des Originals bei den meldenden Stellen. Im Anschluss werden die Informationen aus den modularen Einwilligungserklärungen über eine in das OSSE EDC integrierte webbasierte Benutzeroberfläche durch die meldenden Stellen in gICS erfasst und gespeichert. Die digitale Verwaltung der Einwilligungen und Dokumentation sowie die Verarbeitung der Widerrufe erfolgt unter Verantwortung der Treuhandstelle des NARSE.

3.4 Metadaten-Repository

Das Metadaten-Repository speichert die Bedeutung (Semantik) sämtlicher im NARSE verwendeten Datenelemente. Es bietet ein kontrolliertes Vokabular (Syntax) und kann maschinenlesbare, strukturierte Aussagen über Datenelemente treffen, beispielsweise konzeptuelle Domänen oder Wertebereiche. Da das Metadaten-Repository keine personenbezogenen Daten verarbeitet, wird innerhalb dieses Dokuments nicht weiter darauf eingegangen.

3.5 Registerverzeichnis

In einem Registerverzeichnis kann der Registerbetreiber das NARSE mit einer Kurzbeschreibung des Registers, den Ansprechpartnern und ggf. zusätzlich Metadaten und aggregierten Kerndaten registrieren. Die Daten werden von den Verantwortlichen aktiv hochgeladen. Es werden keine Patientendaten übertragen. Das NARSE ist in den folgenden Registerverzeichnissen registriert:

- Registerdatenbank am BQS Institut[10]
- ERDRI.dor[11]

[10] https://www.bqs.de/bqs-register/04-registersuche.php

[11] https://eu-rd-platform.jrc.ec.europa.eu/erdridor/

4. DATENVERARBEITENDE PROZESSE

4.1 Manuelle Dateneingabe

Die manuelle Datenerfassung im NARSE erfolgt über die webbasierte Benutzeroberfläche der OSSE-Registersoftware.

4.1.1 Registrieren einer Person im Register

Eine berechtigte dateneingebende Person als Mitglied einer meldenden Stelle legt eine zu registrierende Person im NARSE an, indem sie die IDAT der zu registrierenden Person über die in die Benutzeroberfläche des OSSE EDC integrierte Maske der Mainzelliste eingibt (Abbildung 3, grün). Die Mainzelliste generiert mehrere nicht-sprechende Pseudonyme:

- PID als für die Registrierenden in der Nutzeroberfläche sichtbares Pseudonym,
- PSN_{OSSE} zur Verwendung im OSSE EDC,
- PSN_{gICS} zur Verwendung im Einwilligungsmanagement gICS.

Die PID wird den Registrierenden im Browser angezeigt. PSN_{OSSE} und PSN_{gICS} werden an das OSSE-Treuhandmodul (OSSE TTP) gesendet, über das die Kommunikation zwischen Mainzelliste, gICS und OSSE EDC erfolgt. Das OSSE EDC erhält das PSN_{OSSE}, das mit den dort erfassten MDAT gespeichert wird. Bei der Übergabe an das OSSE EDC erhält die dateneingebende Person keine Rückmeldung, ob die registrierte Person in der Mainzelliste bereits vorhanden war oder neu angelegt wurde.

4.1.2 Erfassung der Einwilligung

Nach der Registrierung einer Person im NARSE werden aus dem Einwilligungsmanagement gICS die verfügbaren Vorlagen für Einwilligungen abgerufen (Template) und der dateneingebenden Person in einer in die Benutzeroberfläche des OSSE EDC integrierte Eingabemaske angezeigt. Die dateneingebende Person dokumentiert die eingewilligten Module der registrierten Person (Consent) sowie das Einwilligungsdatum. Diese werden mit dem von der Mainzelliste generierten PSN_{gICS} im Einwilligungsmanagement gICS gespeichert (Abbildung 3, blau). Ohne eine Erfassung der Einwilligung ist keine weitere Erfassung von medizinischen Daten möglich.

4.1.3 Erfassung der medizinischen Daten

Die dateneingebende Person als Mitglied einer meldenden Stelle erhält eine Liste der im NARSE registrierten Personen entsprechend den eigenen Berechtigungen (Sichtbarkeit von IDAT, Sichtbarkeit von registrierten Personen anderer meldenden Stellen). Bei Vorliegen der entsprechenden Berechtigung werden im Browser die zugehörigen IDAT angezeigt. Nach Erfassung der Einwilligung kann die dateneingebende Person den Datensatz der registrierten Person öffnen und MDAT eingeben bzw. abrufen, die mit dem über das OSSE-TTP erhaltenen PSN_{OSSE} im OSSE EDC gespeichert werden (Abbildung 3, lila). Nicht abgebildet sind die für die interne Kommunikation mit der Mainzelliste erforderlichen Requests und Tokens (siehe Abschnitt 4.3 „Pseudonymisierung“).

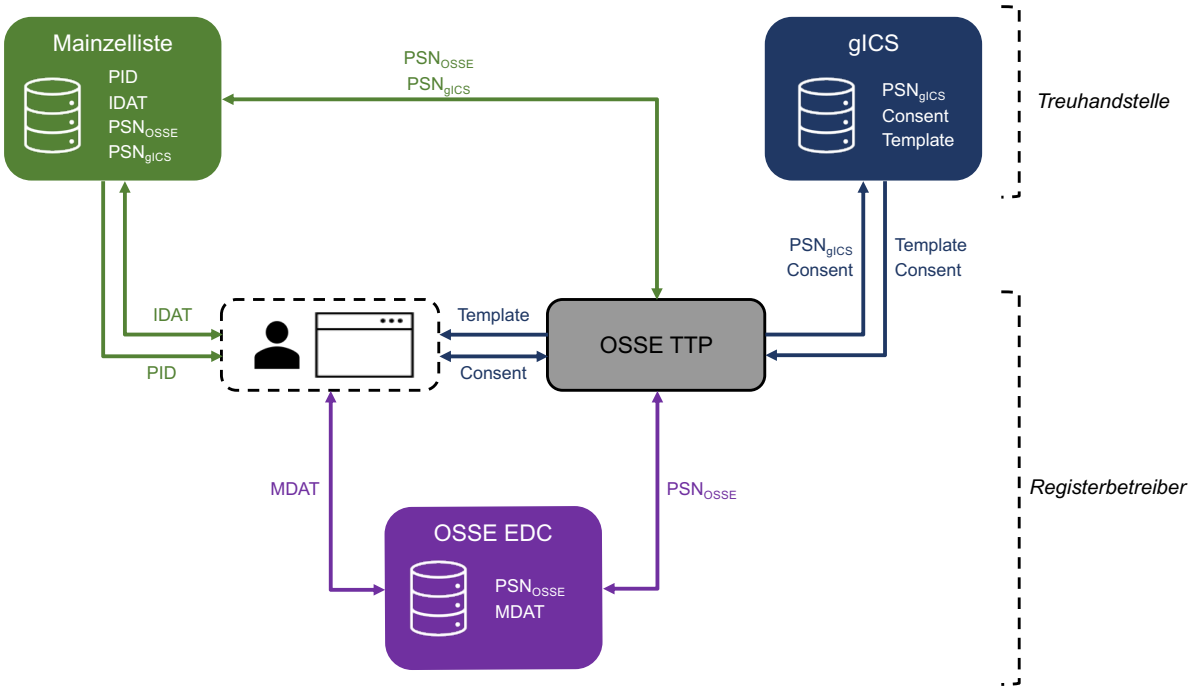


Abbildung 3: Datenströme im NARSE

4.2 Datenimport

Daten aus vorhandenen Datenverarbeitungssystemen oder Datensammlungen, z.B. aus Datenintegrationszentren oder anderen EDC-Systemen, können bei Vorliegen der entsprechenden Einwilligungen in das NARSE übernommen werden. Die Datenübernahme durchläuft folgende Schritte eines sogenannten ETL-Prozesses[12]:

1) IDAT und MDAT werden aus den Quellsystemen extrahiert.
2) IDAT werden im Rahmen der Transformation an das durch die Treuhandstelle des NARSE betriebene Pseudonymisierungs- und Identitätsmanagement übergeben und durch ein temporäres Import-Pseudonym ersetzt (siehe Abschnitt 4.3.2 „Pseudonymisierung beim Datenimport“).
3) Die in elektronischer Form vorliegenden Einwilligungsinformationen werden im Rahmen der Transformation an das durch die Treuhandstelle des NARSE betriebene Einwilligungsmanagement übergeben.
4) Der ETL-Prozess lädt die pseudonymisierten MDAT über eine Webschnittstelle in das NARSE, wobei das temporäre Import-Pseudonym durch das PSN_{OSSE} ersetzt wird (siehe Abschnitt 4.3.2 „Pseudonymisierung beim Datenimport“).

4.3 Pseudonymisierung

Pseudonymisierung findet bei jeder Art von Datenerfassung in das NARSE statt, sowohl bei der manuellen Dateneingabe als auch dem Datenimport.

[12] ETL steht für „Extract-Transform-Load“ und meint den technischen und inhaltlichen Transfer von Daten aus einem Quell-System in ein Ziel-System, wobei spezifische Anpassungen an den Daten (Zuweisung zu Datenfeldern, Formatänderungen, Übersetzung von Werten etc.) vorgenommen werden können.

4.3.1 Manuelle Patientenregistrierung

Gleichermaßen für die Registrierung eines neuen Patientendatensatzes wie auch für das Wiederfinden eines vorhandenen Datensatzes geben Registrierende die IDAT in eine Eingabemaske der Mainzelliste ein, die im Browserfenster der OSSE-Benutzeroberfläche angezeigt wird. Die IDAT müssen vollständig eingegeben werden, da hier nicht, wie beispielsweise in einem klinischen Arbeitsplatzsystem, Auswahllisten nach Eingabe von Namensteilen angezeigt werden können. Ein Record-Linkage-Algorithmus prüft, ob die eingegebene Person bereits in der Mainzelliste registriert ist. Falls nicht, so wird ein neuer Datensatz angelegt, indem die IDAT gespeichert und ein nicht-sprechender PID sowie das PSN_{OSSE} und das PSN_{gICS} als Pseudonyme zweiter Stufe erzeugt werden. Nach Erfassung der Einwilligungsinformationen (siehe Abschnitt 4.1.2 „Erfassung der Einwilligung“) wird die dateneingebende Person automatisch zur Patientenliste des OSSE EDC zurückgeleitet, wo die von der Mainzelliste generierte PID angezeigt wird und die MDAT zur neu angelegten oder ausgewählten Person eingegeben werden können. Browser und OSSE EDC kommunizieren dabei mittels temporärer Identifikatoren und das OSSE EDC erhält keine Kenntnis der PID. Das PSN_{OSSE} wird für Registrierende nicht sichtbar, d.h. es erscheint auch nicht im HTML-Code der angezeigten Formulare oder in HTTP-Anfragen des Webbrowsers. Mit diesem Verfahren ist sichergestellt, dass PSN_{OSSE} und IDAT zu keinem Zeitpunkt außerhalb der Mainzelliste einander zugeordnet werden können.

Während der Eingabe der MDAT im NARSE, die lokal und behandlungsnah erfolgt, werden neben der PID auch die IDAT der registrierten Person im Browser angezeigt, vorausgesetzt die dateneingebende Person hat die entsprechende Berechtigung, IDAT zu sehen. Diese werden allerdings erst im Browser mit den MDAT zusammengeführt, sodass das OSSE EDC zu keinem Zeitpunkt Zugriff auf IDAT bekommt. Dazu ruft die Registersoftware für jedes PSN_{OSSE} bei der Mainzelliste eine sessionbasierte temporäre ID (Token) ab, mit der der Browser die zugehörigen IDAT von der Mainzelliste erhält (Abbildung 3).

Das im OSSE EDC gespeicherte PSN_{OSSE} wird zu keiner Zeit angezeigt oder ausgegeben, sodass es weder bei der Dateneingabe im Behandlungsumfeld noch durch Zusammenführen exportierter Daten einer registrierten Person zugeordnet werden kann. Eine Re-Identifizierung (De-Pseudonymisierung) kann nur kontrolliert mithilfe der Mainzelliste durchgeführt werden.

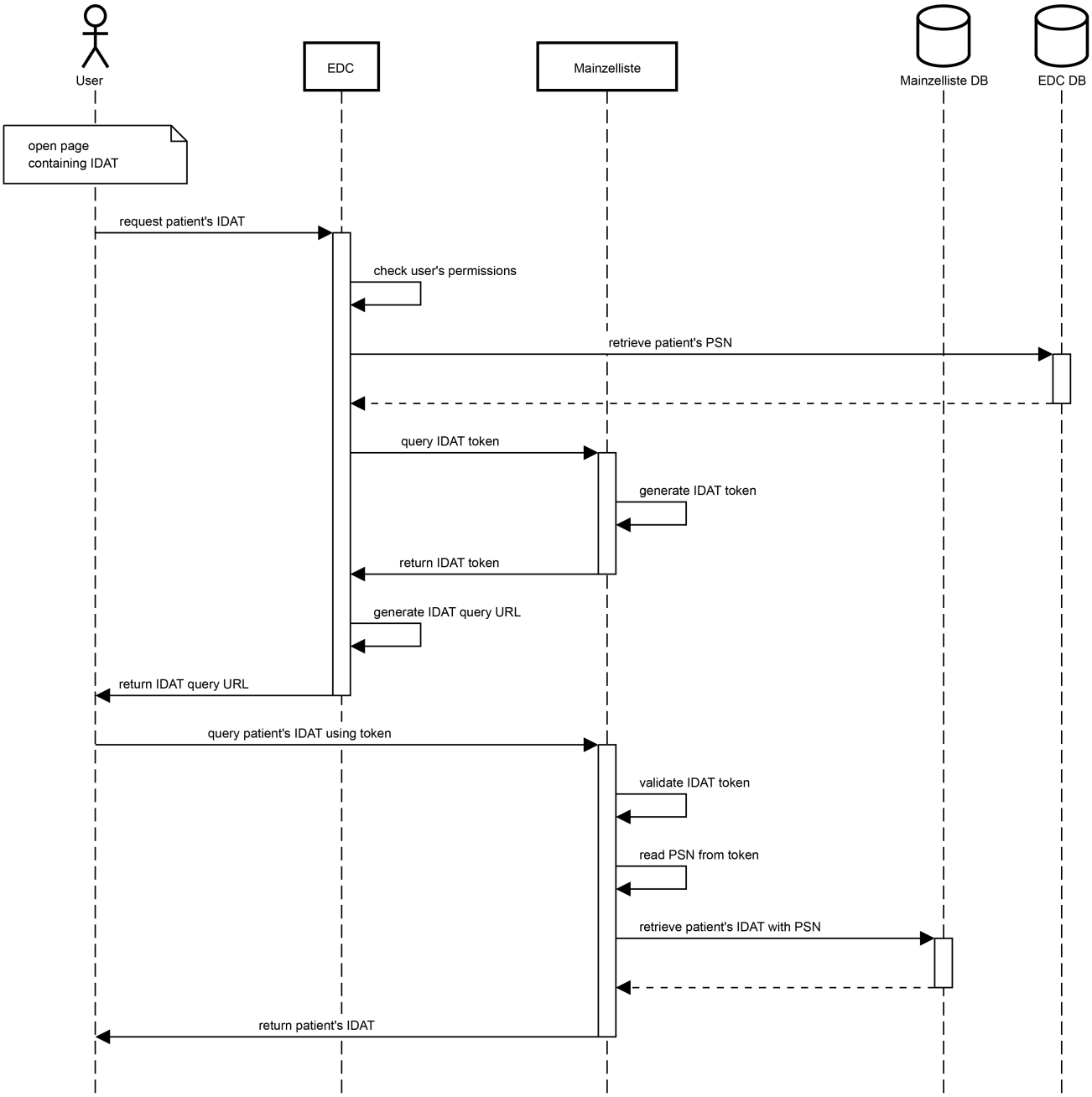


Abbildung 4: Abruf von IDAT

4.3.2 Pseudonymisierung beim Datenimport

Beim Datenimport werden die IDAT vor dem Import der Datensätze in das NARSE (siehe Abschnitt 4.2„Datenimport“) durch Pseudonyme ersetzt. Datenextraktion und -transformation werden durch eine Datenintegrationssoftware unterstützt. Dabei ist die Pseudonymisierung Teil der Transformation des ETL-Prozesses und wird mit einer eigens dafür entwickelten Komponente durchgeführt. Folgende Schritte werden durchlaufen:

1) Für jeden Datensatz ruft der ETL-Prozess die Mainzelliste auf und übergibt die IDAT sowie das lokale Pseudonym.
2) Die Mainzelliste legt die zu registrierende Person an und erzeugt die notwendigen Pseudonyme (analog zur manuellen Dateneingabe).

3) Die Mainzelliste liefert das Import-Pseudonym (PSN_{Import}) mit dem zugehörigen lokalen Pseudonym an die Transformationskomponente, wo die IDAT und das lokale Pseudonym durch das PSN_{Import} ersetzt werden.
4) Die Importschnittstelle des OSSE EDC entschlüsselt das PSN_{Import} über die Mainzelliste und speichert die Daten mit dem PSN_{OSSE}

Durch dieses Verfahren ist sichergestellt, dass beim Datenimport keine Pseudonyme zugeordnet werden können, da die datenliefernde Seite, die den Personenbezug herstellen kann, nur das lokale Pseudonym sowie das Import-Pseudonym PSN_{Import} und das OSSE EDC nicht das lokale Pseudonym sieht.

4.3.3 Schlüsselerzeugung und Schlüsselverwaltung

Das Schlüsselpaar für die asymmetrisch verschlüsselte Übertragung der OSSE-Pseudonyme wird im OSSE-Register bei Systemstart erzeugt und nur zur Laufzeit im Speicher gehalten. Bei Neustart oder durch eine Funktion des Registers kann ein neues Schlüsselpaar erzeugt werden. Der aktuelle öffentliche Schlüssel kann durch eine dazu berechtigte Komponente (z.B. das Pseudonymisierungs- und Identitätsmanagement) jederzeit über eine Webschnittstelle beim OSSE-Register abgerufen werden.

4.4 Datenexport und Datennutzung

Gemäß der gültigen Nutzungsordnung (siehe Anhang 7.2 „Nutzungsordnung NARSE“) sind verschiedene Formen der Datennutzung vorgesehen. Dabei werden die On-Site-Nutzung in den geschützten Räumen des NARSE („Algorithm to Data“) und die Off-Site-Nutzung („Data to Algorithm“) unterschieden, entsprechend des „Five Safes“ Konzepts zur sicheren Nutzung von Daten (siehe Abschnitt 5.4 „Five Safes“). Alle Formen der Datennutzung setzen gemäß Nutzungsordnung in einem durch die Registerstelle des NARSE koordinierten Prozesses einen Nutzungsantrag mit Prüfung und positiver Empfehlung durch das Data Access Committee und Abschluss eines Nutzungsvertrags oder eine genehmigte Nutzungsanzeige voraus. Die Verantwortung für den Export sowie die Aufbereitung und Bereitstellung von Daten aus dem NARSE liegt bei der Transferstelle des NARSE; die Umpseudonymisierung der Daten erfolgt unter Einbindung der Treuhandstelle des NARSE.

4.4.1 Datenexport

Medizinische Daten können zu Auswertungszwecken für alle Formen der Datennutzung durch die Transferstelle aus der Registerdatenbank des NARSE exportiert werden. Für die Herausgabe von Datensätzen an externe Datennutzende, auch für die Bereitstellung an Gastwissenschaftlerarbeitsplätzen oder die kontrollierte Datenfernverarbeitung, erfolgt mindestens eine projektspezifische Umpseudonymisierung der Daten, um zu verhindern, dass die im NARSE verwendeten Pseudonyme von externen Datennutzenden oder Analyseskripten eingesehen werden können oder mehrere herausgegebene Datensätze anhand der verwendeten Pseudonyme verknüpft werden können. Für interne Nutzungszwecke durch die Registerstelle des NARSE können Datensätze bei Bedarf unter Verwendung des im NARSE sichtbaren Pseudonyms (PID) exportiert werden; das intern im OSSE EDC gespeicherte PSNOSSE wird zu keinem Zeitpunkt herausgegeben.

Folgende Schritte werden für die Umpseudonymisierung im Rahmen des Exports von Datensätzen aus dem NARSE durchlaufen:

1) Das OSSE EDC schickt das interne Pseudonym PSN_{OSSE} zusammen mit einer Projektkennung an das Einwilligungsmanagement sowie das Pseudonym- und Identitätsmanagement in der Treuhandstelle des NARSE.

2) Das Einwilligungsmanagement überprüft für das jeweilige Pseudonym PSN_{OSSE} die Gültigkeit der vorliegenden Einwilligung.
3) Das Pseudonymisierungs- und Identitätsmanagement liefert ein einheitliches projektspezifisches Exportpseudonym ($PSN_{Projekt}$) zurück.
4) Der Datensatz wird mit dem $PSN_{Projekt}$ ausgegeben.

4.4.2 Datennutzung

Für die kontrollierte Datenfernverarbeitung werden von der Transferstelle des NARSE extern erstellte Algorithmen oder Skripte geprüft und auf einem Datenauszug aus der Registerdatenbank des NARSE ausgeführt, der die beantragten und vom Data Access Committee freigegebenen Daten mit einem projektspezifischen $PSN_{Projekt}$ enthält. Die Ergebnisse werden gemäß Nutzungsvertrag überprüft zur Verfügung gestellt.

Für Gastwissenschaftlerarbeitsplätze werden die beantragten und vom Data Access Committee freigegebenen Datensätze zur internen Nutzung von der Transferstelle des NARSE zusammengestellt. Die Herausgabe von pseudonymisierten Datensätzen an Gastwissenschaftlerarbeitsplätzen erfolgt mit einem projektspezifischen $PSN_{Projekt}$. Die weitere Verarbeitung und Analyse der Daten erfolgt an einem gegen unerlaubte und unlautere Datennutzung eingerichteten Arbeitsplatz im lokalen Safe Setting.

Für die Off-Site-Nutzung („Data to Algorithm“) werden die beantragten und vom Data Access Committee freigegebenen Datensätze zu Auswertungszwecken nach dem Export aus dem NARSE durch die Transferstelle des NARSE aufbereitet und bereitgestellt. Die Herausgabe von pseudonymisierten Datensätzen an externe Datennutzende erfolgt mit einem projektspezifischen $PSN_{Projekt}$. Besonders bei Erkrankungen mit geringen Fallzahlen lassen sich MDAT bei Kenntnis des Krankheitsverlaufs oder zusätzlicher Daten auch ohne Kenntnis der IDAT konkreten registrierten Personen zuordnen. Auch bei der Verwendung nicht-rückführbarer projektspezifischer Exportpseudonyme kann nicht immer sicher von absoluter Anonymität ausgegangen werden. Dieser Umstand der möglichen Re-Identifizierung anhand von MDAT wird auch in der informierten Einwilligung berücksichtigt und erläutert.

Für die NARSE-interne Datennutzung durch die Registerstelle des NARSE, beispielsweise zwecks Qualitätsüberprüfung und -sicherung, die Erstellung von Berichten oder die Erstellung von Pseudonymlisten für die meldenden Stellen (beschränkt auf registrierte Personen der jeweiligen meldenden Stelle), werden die im Rahmen einer Nutzungsanzeige vom Data Access Committee freigegebenen Datensätze von der Transferstelle des NARSE zusammengestellt und ausgewertet. Je nach Nutzungszweck werden im Rahmen der internen Datennutzung projektspezifische Exportpseudonyme oder die im NARSE sichtbaren Pseudonyme (PID) verwendet.

4.4.3 Datenzugriff durch Administrierende

Die im NARSE gespeicherten Daten können prinzipiell von den Administrierenden der verwendeten IT-Infrastruktur eingesehen werden. Zugriffe auf die Daten durch Administrierende dürfen nur erfolgen, wenn dies zur Erfüllung ihrer Aufgaben zwingend erforderlich ist. Dies kann bei den folgenden Tätigkeiten der Fall sein:

- Systemkonfiguration und -wartung (z.B. Updates des Betriebssystems oder der Software)
- Manuelle Änderungen in der Datenbank (z.B. Standort einer registrierten Person)
- Unterstützung beim Datenexport
- Unterstützende Dienstleistung zur Erfüllung der Betroffenenrechte im Auftrag des Registerbetreibers

Das Vorgehen beim Datenzugriff ist durch folgenden Prozess geregelt:

- Vor dem Zugriff wird geklärt, ob der Datenzugriff tatsächlich notwendig ist.
- Der Datenzugriff wird protokolliert. Das Protokoll umfasst dabei mindestens die folgenden Inhalte:
    - den Zeitpunkt des Datenzugriffs,
    - die beteiligten Administratoren und Administratorinnen,
    - den Grund des Datenzugriffs,
    - die involvierten Nutzdaten (nach Möglichkeiten anonymisiert oder pseudonymisiert).

Alle Administrierenden sind entsprechend zu instruieren und zur Verschwiegenheit zu verpflichten[13].

[13] Dies sollte in der Regel im Rahmen des Arbeitsverhältnisses an der zuständigen Institution ohnehin geschehen sein.

5. WEITERE MAßNAHMEN ZUM DATENSCHUTZ

Um den Datenschutz bei der Verarbeitung von personenbezogenen Daten zu gewährleisten, werden weitere Maßnahmen getroffen. Über die in diesem Abschnitt genannten Maßnahmen hinaus finden sich die relevanten gültigen technischen und organisatorischen Maßnahmen (TOMs), um die Sicherheit der erhobenen und verarbeiteten personenbezogenen Daten zu gewährleisten, in Abschnitt 7.5 „Technische und organisatorische Maßnahmen (TOMs)“.

5.1 Informationelle Gewaltenteilung

Das Pseudonymisierungs- und Identitätsmanagement sowie das Einwilligungsmanagement werden logisch und physikalisch getrennt von allen Komponenten betrieben, die MDAT speichern. So ist sichergestellt, dass Personen, die im NARSE außerhalb des Behandlungszusammenhangs Zugriff auf MDAT haben, keine Zuordnung zu realen Personen treffen können. Die Verantwortung für den Betrieb des Pseudonymisierungs- und Identitätsmanagement sowie des Einwilligungsmanagements wird im Rahmen eines Joint Controller Vertrags mit dem Registerbetreiber und der Systemadministration an die UTHS Dresden übergeben, die kein eigenes Interesse an der Nutzung der im NARSE erfassten MDAT hat. Diese Institution steht prinzipiell unter eigener rechtlicher Verantwortung und ist dem Registerbetreiber gegenüber bei Weisungen, die die Datenschutzziele wie Vertraulichkeit, Verfügbarkeit und Integrität gefährden, nicht weisungsgebunden. Im Joint Controller Vertrag wird geregelt, welche Verarbeitungsschritte ein eigener Verantwortlichkeit durchgeführt werden und welche in gemeinsamer Verantwortlichkeit mit den anderen beteiligten Stellen.

5.2 Autorisierung und Authentifizierung

5.2.1 Autorisierung von Registrierenden

Die Autorisierung von Registrierenden, also die Zuweisung von definierten Rollen zu Mitgliedern der meldenden Stellen, des NARSE erfolgt durch Administrierende der jeweiligen meldenden Stelle oder Administrierende des Registerbetreibers entsprechend den lokalen Strukturen und Erfordernissen.

5.2.2 Autorisierung von Komponenten

Der Zugriff von IT-Komponenten untereinander wird in der jeweiligen Konfiguration festgelegt. Dazu werden ab Beginn der Inbetriebnahme des NARSE die IP-Adresse des zugreifenden Systems und ein Passwort erfasst.

5.2.3 Authentifizierung von Registrierenden

Die Authentifizierung von Registrierend gegenüber dem NARSE erfolgt über Benutzername und Passwort mit der Möglichkeit, durch eine Zwei-Faktor-Authentifizierung ein erhöhtes Maß an Sicherheit zu erreichen. Der zweite Faktor besteht aus einem zeitlich begrenzt gültigen Einmal-Passwort, das nach dem TOTP-Verfahren auf einem Endgerät des oder der Registrierenden erzeugt wird. Registrierende müssen die Verwendung des zweiten Faktors selbständig aktivieren und erhalten bei der Aktivierung drei unbefristet gültige Einmal-Passwörter für den Fall, dass das Endgerät zur Erzeugung der Passwörter unbrauchbar wird.

5.2.4 Authentifizierung von Komponenten

Zugriffe zwischen verschiedenen IT-Komponenten über das Internet finden nur nach erfolgreicher Authentifizierung statt. Die Authentifizierung des OSSE EDCs gegenüber dem Metadaten-Repository und Formulareditor erfolgt über Login und Passwort, die bei der Initialisierung bzw. der Installation des

Registers festgelegt werden. Die Authentifizierung des OSSE EDCs gegenüber dem Pseudonymisierungs- und Identitätsmanagement Mainzelliste sowie dem Einwilligungsmanagement gICS erfolgt über einen bei der Installation festgelegten API-Key.

5.3 Maßnahmen in der IT-Infrastruktur

5.3.1 Sicherheit der gespeicherten Daten

Alle in den zentralen Komponenten des NARSE erhobenen Daten werden lokal in Datenbanken auf virtuellen Servern gespeichert. Nur Administrierende des jeweiligen Servers haben Zugriff auf die Daten. Alle Server befinden sich in Rechenzentren mit Standort in Deutschland, die über eine Zugangskontrolle per Chipkarte oder ähnlich sichere Token für jeweils berechtigte Personen verfügen. Darüber hinaus sind die Daten auf dem Server in einem nach dem Stand der Technik verschlüsselten Container gespeichert. Das Kennwort zur Entschlüsselung ist ausschließlich den Systemadministratoren/Systemadministratorinnen bekannt.

5.3.2 Sicherheit der Kommunikation

Die Vertraulichkeit der Kommunikation zwischen den Komponenten wird durch folgende Maßnahmen sichergestellt:

- Die Kommunikation zwischen den Komponenten, ebenso wie die Kommunikation zwischen dem Browser von Registrierenden und dem OSSE EDC bzw. dem OSSE Treuhandmodul (OSSE TTP) oder dem Pseudonymisierungsdienst Mainzelliste bzw. Einwilligungsmanagement gICS in der UTHS Dresden, erfolgt grundsätzlich über verschlüsselte Verbindungen (HTTPS). Die dafür eingesetzten Schlüssel und Zertifikate sind so zu erstellen, dass sie den aktuell anerkannten Anforderungen entsprechen. Die Verschlüsselung folgt den Maßstäben des Bundesamtes für Sicherheit in der Informationstechnik (BSI)[14].
- Durch Firewalls ist sichergestellt, dass die Server, auf denen die zentralen Komponenten laufen, nur über diejenigen Protokolle und Ports erreichbar sind, die für die Kommunikation mit Benutzern oder anderen Komponenten erforderlich sind (in der Regel HTTPS-Verbindungen). Der administrative Zugang ist auf das Intranet des Betreibers beschränkt.

5.3.3 Protokollierung

Es erfolgt eine Protokollierung der Zugriffe von Registrierenden auf die Komponenten sowie Zugriffe zwischen den Komponenten. Das Protokoll enthält mindestens:

- Die Identität der zugreifenden Person oder Komponente.
- Datum und Uhrzeit des Zugriffs.
- Den Inhalt des Zugriffs (die übermittelten Daten, ggf. aggregiert) oder Informationen, aus denen dieser rekonstruiert werden kann (z.B. Verweis auf einen Datenbankeintrag o.ä.).

Das Protokoll wird zusammen mit den Nutzdaten des entsprechenden Servers gespeichert und zwischen einem und sechs Monaten aufbewahrt. Die aufgezeichneten Daten dürfen nur im Rahmen der technischen Administration (insbesondere zur Fehlersuche) und bei der Verfolgung von Missbrauch eingesehen werden.

[14] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf?__blob=publicationFile&v=10

5.4 Five Safes

Gemäß der Nutzungsordnung folgt das NARSE dem Konzept der Five Safes mit dem Ziel der sicheren Nutzung von Daten, wobei mehr Strenge in einer Dimension zu mehr Freiheitsgraden in einer anderen führen kann: Sichere Projekte, Sichere Menschen, Sichere Umgebungen, Sichere Daten und Sichere Ergebnisse. Die Kombination der Kontrollen führt zu einer „sicheren Nutzung“.

6. WAHRUNG VON BETROFFENENRECHTEN

6.1 Aufklärung und Einwilligung

Die informierte Einwilligung (siehe Anhang 7.1 „Patienteneinwilligung NARSE“) ist Rechtsgrundlage der Datenverarbeitung. Mit der Einwilligung erklärt sich die registrierte Person insbesondere dazu bereit, dass

- ihre IDAT an das Pseudonymisierungs- und Identitätsmanagement übermittelt und dort gespeichert werden,
- ihre MDAT gemäß Registerdefinition im NARSE erfasst werden,
- diese MDAT von Forschenden des NARSE, die benannt und an die Nutzungsbedingungen gebunden sind, lokal ausgewertet werden können und
- MDAT aus dem NARSE anonymisiert oder mit einem nicht-rückführbaren Exportpseudonym exportiert und für Forschungszwecke, die in der Einwilligung näher definiert sind, an externe Forscher oder Institutionen, die benannt und an die Nutzungsbedingungen gebunden sind, übermittelt werden.
- In den Einwilligungen sind Differenzierungen möglich, die
    - die Datennutzung in der gesamten Europäischen Union,
    - die Erfassung genetischer Informationen,
    - die erneute Kontaktaufnahme zwecks Vernetzung
    - die erneute Kontaktaufnahme zwecks Information zu neuen Therapien oder Studien,
    - die Fallbesprechung mit Ärztinnen oder Ärzten an anderen Gesundheitseinrichtungen,

  jeweils einschließen oder ausschließen.

Mit Einholen der Einwilligung wird die registrierte Person über ihre Betroffenenrechte (Recht auf Auskunft, Widerruf, Berichtigung, Einschränkung der Verarbeitung und Beschwerde bei einer Aufsichtsbehörde) informiert.

6.2 Auskunft über gespeicherte Daten

Im NARSE registrierte Personen haben das Recht, Auskunft darüber zu erhalten, ob und welche Daten von ihnen im NARSE gespeichert werden, und diese Daten einzusehen. Der Antrag auf Auskunft ist schriftlich an den Registerbetreiber zu stellen. Daraufhin wird ein menschenlesbarer Ausdruck der Daten erzeugt und der erfassten Person ausgehändigt. Betroffene Personen haben das Recht auf Auskunft folgender Daten und Informationen (Art. 15 Abs. 1 lit. e-h DSGVO):

- Verarbeitungszwecke
- Kategorien der personenbezogenen Daten, die verarbeitet werden
- Empfänger oder Kategorien von Empfängern, die die personenbezogenen Daten erhalten haben
- Geplante Dauer der Speicherung
- Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung durch den Verantwortlichen oder eines Widerspruchsrechts gegen diese Verarbeitung
- Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde
- Verfügbare Informationen über die Herkunft der Daten
- Im Register gespeicherte Daten

6.3 Datenübertragbarkeit

Im NARSE registrierte Personen haben das Recht, die sie betreffenden personenbezogenen Daten, die sie selbst einem Verantwortlichen bereitgestellt haben, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten. Sofern von einer registrierten Person Daten in das NARSE eingetragen worden sind und die Person die Datenübertragung in einen anderen Datenbestand anfordert, wird der Betreiber des NARSE die Person nach Möglichkeit unterstützen.

6.4 Widerruf, Löschung, De-Identifizierung

Registrierte Personen haben das Recht, die Einwilligung in die Verarbeitung ihrer Daten im NARSE zu widerrufen. Der Widerruf ist als eindeutige Willensbezeugung direkt an die Treuhandstelle des NARSE oder an den behandelnden Arzt bzw. die behandelnde Ärztin zu richten, welche den Widerruf an die Treuhandstelle weiterleitet. Es ist möglich, den Widerruf in schriftlicher Form an die auf www.narse.de angegebenen Kontaktmöglichkeiten zu kommunizieren.

Im Falle eines Widerrufs entscheidet die widerrufende Person, wie mit ihren Daten verfahren werden soll (Abbildung 5). Die im NARSE erfassten MDAT können vollständig gelöscht oder durch Löschen der zugehörigen IDAT und des Pseudonyms de-identifiziert werden, in welchem Fall sie weiterhin für Auswertungen zur Verfügung stehen. Wenn eine Löschung der Daten voraussichtlich die Verwirklichung eines bereits gestarteten oder die Nachvollziehbarkeit eines beendeten Forschungsprojekts unmöglich macht oder ernsthaft beeinträchtigt, werden die Daten im Rahmen gesetzlich bestehender Ausnahmeregelungen nicht gelöscht. In diesen Fällen werden die Daten so gesperrt, dass sie nur noch für die den gesetzlichen Ausnahmeregelungen zugrundeliegenden notwendigen Zwecken verarbeitet werden können.

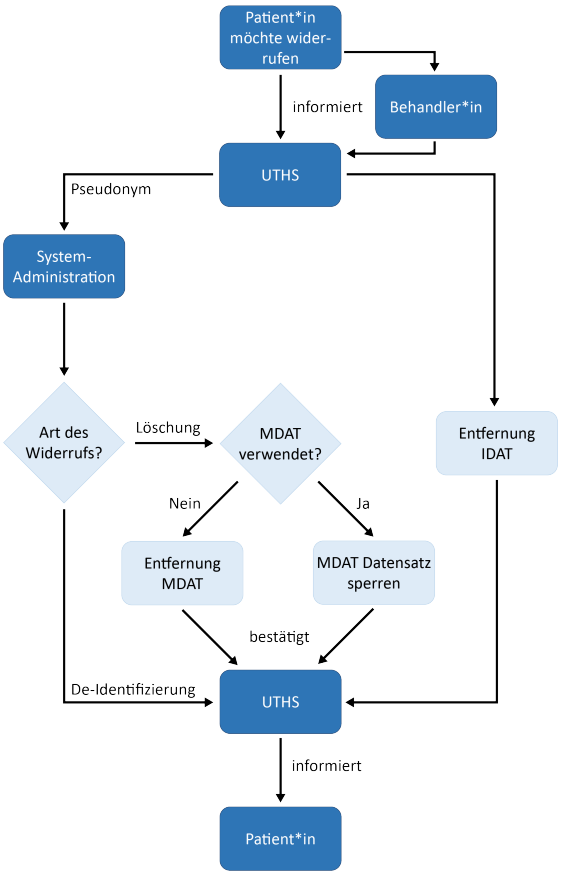


Abbildung 5: Ablauf des Widerrufs der Einwilligung

Im Fall einer De-Identifizierung werden die IDAT einer registrierten Person inklusive zugehöriger Pseudonyme vernichtet. Es verbleiben nur die MDAT, die in der Regel keinen Rückschluss auf eine Person zulassen[15]. Speziell im Bereich der ultraseltenen Erkrankungen kann aber nicht ausgeschlossen werden, dass durch MDAT-Rückschlüsse auf die Identität einer registrierten Person gezogen werden können.

Zur De-Identifizierung werden die Datensätze im Pseudonymisierungs- und Identitätsmanagement Mainzelliste durch die Treuhandstelle gelöscht und das bisherige PSN_{OSSE} der widerrufenden Person durch ein zufälliges Pseudonym ersetzt. Für den Fall, dass Daten archiviert wurden, wird dieser Vorgang ebenso für die archivierten Datensätze durchgeführt. Durch den Algorithmus zur Erzeugung von

[15] Anonymisierte Daten fallen nicht unter den Anwendungsbereich der DSGVO.

Pseudonymen ist sichergestellt, dass die Pseudonyme einer de-identifizierten Person nicht mehr für neu erfasste Personen verwendet werden. Die Treuhandstelle informiert die Systemadministration des NARSE, um sicherzustellen, dass die im OSSE EDC verbleibenden MDAT entsprechend umpseudonymisiert werden.

Im Falle der vollständigen Löschung werden die IDAT analog zur De-Identifizierung durch die Treuhandstelle gelöscht. Zusätzlich informiert die Treuhandstelle die Systemadministration des NARSE anhand des verwendeten Pseudonyms der widerrufenden Person, um die Löschung der im OSSE EDC erfassten MDAT zu veranlassen; dies umfasst auch die Löschung der Daten im Audit Trail des OSSE EDC. Die Systemadministration des NARSE führt die Löschung durch und bestätigt der Treuhandstelle die erfolgte Löschung der MDAT.

Die vollständige Löschung oder De-Identifizierung ist von der zuständigen Treuhandstelle, mit Unterstützung der Systemadministration des NARSE, unverzüglich nach Bekanntwerden des Widerrufs, vorzunehmen[16]. Der Erhalt des Widerrufs wird der widerrufenden Person schriftlich oder per E-Mail an die für den Widerruf verwendete Kontaktadresse bestätigt, unter Angabe eines Zeitpunkts, bis wann die Daten gelöscht werden. Eine Bestätigung erfolgt innerhalb eines Monats nach Bekanntwerden des Widerrufs.

6.5 Dauer der Speicherung

Das NARSE soll langfristig betrieben werden ohne ein festgelegtes Enddatum. In einem internen Prozess wird regelmäßig überprüft, ob das NARSE weiterlaufen soll oder ob die Registeraktivitäten eingestellt werden sollen.

Die erhobenen Daten bleiben bis auf weiteres im NARSE gespeichert, bis eine registrierte Person ihre Einwilligung widerruft (siehe Abschnitt 6.4„Widerruf, Löschung, De-Identifizierung“) oder bis zu 10 Jahren, nachdem sämtliche Registeraktivitäten eingestellt wurden.

Falls der Datenbestand nicht mehr in der vorgesehenen Form genutzt werden kann, prüft der Registerbetreiber, ob eine Rechtsgrundlage für eine anderweitige Verwendung der Daten, gegebenenfalls in anonymisierter Form, besteht. Falls diese Prüfung negativ ausfällt, sind die Daten zu löschen.

[16] Die meist impraktikable Anonymisierung in Datensicherungen ist verzichtbar, sofern die Sicherungen nur durch zuständige Systemadministrator/innen eingesehen werden können und alte Sicherungen regelmäßig gelöscht werden.

7. ANHANG: MITGELTENDE DOKUMENTE

7.1 Patienteneinwilligung NARSE

Die aktuelle Version der Patienteninformation und-einwilligung, ebenso die für Sorgeberechtigte und Jugendliche, steht auf www.narse.de zur Verfügung.

Version 2.0, Stand 30.01.2025

- 2025-01-30_NARSE_Patienteninfo-Einwilligung_V2.0
- 2025-01-30_NARSE_Elterninfo-Einwilligung_V2.0
- 2025-01-30_NARSE_Jugendliche-Einwilligung_V2.0

7.2 Nutzungsordnung NARSE

Die aktuelle Version der Nutzungsordnung des NARSE steht auf www.narse.de zur Verfügung.

Version 2.0, Stand 30.01.2025

- 2025-01-30_NARSE_Nutzungsordnung_V2.0

7.3 Datensatz NARSE

Die aktuelle Version des NARSE-Datensatzes steht auf www.narse.de zur Verfügung.

Version 1.2, Stand 30.01.2025

- 2025-01-30_NARSE_Datenelemente_DE_V1.2

7.3.1 Medizinische Daten

	Datenelement	Format	Pflicht	Kommentar
Formale Kriterien	Einschlussdatum	Datum (YYYY-MM-DD)	X	
	Diagnose Seltene Erkrankung(en): ORPHAcode	ORPHAcode (Katalog angebunden)	X	Mehrfacheingabe
	Diagnose Seltene Erkrankung(en): ICD Version	Auswahlmenü	X	Mehrfacheingabe
	Diagnose Seltene Erkrankung(en): ICD Code	ICD Code (Kataloge hinterlegt)	X	Mehrfacheingabe
	Diagnose Seltene Erkrankung(en): Diagnosesicherheit	Gesicherte Diagnose / Verdachtsdiagnose / Unbekannt	X	Mehrfacheingabe
Persönlicher und Familiärer Hintergrund	Alterskategorie bei Einschluss	Unbekannt / Säugling (<1 Jahr) / Kleinkind (>1 bis <6 Jahre) / Schulkind (>6 bis <12 Jahre) / Jugendliche*r (>12 bis <18 Jahre) / Erwachsene*r (≥18 bis <50 Jahre) / Erwachsene*r (≥50 Jahre)	X	
	Biologisches Geschlecht bei Geburt	Weiblich / Männlich / Anderes / Unbekannt	X	
	Administratives Geschlecht bei Einschluss	Weiblich / Männlich / Divers / Offen / Unbekannt		
	Aktueller Status: Datum	Datum (YYYY-MM-DD)		Mehrfacheingabe
	Aktueller Status: Status	Lebend / Verstorben / Nicht weiterverfolgt		Mehrfacheingabe
	Sterbealter	Zahl (0<=x<=100) in Jahren		Wenn Status = Verstorben
	An SE verstorben	Ja / Nein / Unbekannt		Wenn Status = Verstorben
	Andere Todesursache	Freitext		Wenn An SE verstorben = Nein
	Betroffene Familienangehörige: Verwandtschaftsbeziehung	Vater / Mutter / Bruder / Schwester / Sohn / Tochter		Mehrfacheingabe
	Betroffene Familienangehörige: Seltene Erkrankung	Ja, die gleiche seltene Erkrankung / Ja, eine andere seltene Erkrankung / Ja, die gleiche und eine andere seltene Erkrankung / Unbekannt		Mehrfacheingabe
	Betroffene Familienangehörige: Verstorben?	Ja / Nein / Unbekannt		Mehrfacheingabe

Anamnese & Diagnostik	Alter bei ersten Symptomen: Auswahl der Altersangabe	Unbekannt / Alter / Bei Geburt / Pränatal	X	
	Alter bei ersten Symptomen: Alter	Zahl (0<=x<=100) in Jahren + Monaten		Wenn Auswahl = Alter
	Alter bei Diagnose: Auswahl der Altersangabe	Unbekannt / Alter / Bei Geburt / Pränatal	X	
	Alter bei Diagnose: Alter	Zahl (0<=x<=100) in Jahren + Monaten		Wenn Auswahl = Alter
	Diagnosestellung	(Molekular-)Genetik / klinischer Phänotyp / Bildgebung / Histopathologie / Neugeborenenscreening (Stoffwechsel) / Neugeborenenscreening (genetisch) / Labordiagnostik / Sonstiges / Unbekannt	X	Mehrfachauswahl
	Sonstige Absicherung der Diagnose	Freitext		Wenn Diagnosestellung = Sonstiges
	(Molekular-)Genetische Diagnose: Betroffenes Gen	Freitext		Wenn Diagnosestellung = (Molekular-)Genetik, Mehrfacheingabe, nur mit Einwilligung
	(Molekular-)Genetische Diagnose: Genvariante	Freitext		Wenn Diagnosestellung = (Molekular-)Genetik, Mehrfacheingabe, nur mit Einwilligung
	Labordiagnostik: Laborparameter	Freitext		Wenn Diagnosestellung = Labordiagnostik, Mehrfacheingabe
	Phänotyp: HPO Term	HPO Code (Katalog angebunden)		Wenn Diagnosestellung = klinischer Phänotyp, Mehrfacheingabe
	Therapiestatus	Keine / Pharmakotherapie / Gentherapie / mRNA Therapie / Antikörpertherapie / CAR-T-Zelltherapie / Stammzelltransplantation / Stoffwechseltherapie / Sonstiges / Unbekannt	X	Mehrfachauswahl
	Sonstige spezifische Therapie	Freitext		Wenn Therapiestatus = Sonstiges

7.3.2 Identifizierende Daten

Datenelement	Format
Vorname(n)	
Nachname(n)	
Geburtsname	optional
Geburtsdatum	
Geburtsort	
Adresse (Straße, Hausnummer, PLZ, Wohnort)	optional
E-Mail-Adresse	optional

Telefonnummer	optional

7.3.3 Einwilligungsdaten

Datenelement	**Format**
Einwilligungsdatum	Datum (YYYY-MM-DD)
Einwilligung Datennutzung	Ja / Nein
Einwilligung Datennutzung international (EU)	Ja / Nein, optional
Einwilligung Re-Kontaktierung für Informationszwecke	Ja / Nein, optional
Einwilligung Re-Kontaktierung für Vernetzung	Ja / Nein, optional
Einwilligung Erfassung genetischer Informationen	Ja / Nein, optional
Einwilligung Fallbesprechung	Ja / Nein, optional

7.4 Rollen & Berechtigungen

7.4.1 Rollen und Aufgaben im NARSE

Rolle	Wer	Aufgaben	Berechtigungen
Träger	Berlin Institute of Health at Charité (BIH)	• Bereitstellung finanzieller Mittel für die Entwicklung und den Betrieb des Registers	• keine Einsicht in IDAT und MDAT
Registerbetreiber	Berlin Institute of Health at Charité (BIH)	• technischer und administrativer Betrieb des Registers • Verantwortlicher im Sinne des Art. 4 DSGVO • Führung der Geschäfte des Registers • Entscheidungen rund um die Weiterentwicklung des Registers • Einberufung von Data Access Commitee und wissenschaftlichem Beirat	• keine Einsicht in IDAT und MDAT
Registerstelle	Berlin Institute of Health at Charité (BIH)	• Koordination des Registerbetriebs • Ansprechpartner für meldende Stellen • Ansprechpartner für inhaltliche Fragen • zentrale Definition von Nutzerrollen • zentrale Verwaltung der meldenden Stellen • zentrale Nutzerverwaltung (Anlegen von Nutzerkonten, Zuweisung von Rollen) • Prüfung der Zulassungsberechtigung von Nutzern • Koordination des Prozesses der Datennutzung	• Einsicht in MDAT • Definition von Nutzerrollen • Verwaltung der Standorte (teilnehmende Einrichtungen) • Nutzerverwaltung (Anlegen von Nutzerkonten, Zuweisung von Rollen)
Transferstelle	Berlin Institute of Health at Charité (BIH)	• Zugriff auf alle medizinischen Daten aller teilnehmenden Einrichtungen • Erstellung von Datenexporten und Auswertungen • Beratung des Data Access Committees	• Einsicht in MDAT • Datenexport
Treuhandstelle	UTHS Dresden	• Betrieb des zentralen Identitätsmanagements und Pseudonymisierungstools (Mainzelliste) • Betrieb des zentralen Einwilligungsmanagements (gICS) • Ansprechpartner für Widerruf der Einwilligung • Ansprechpartner für datenschutzrechtliche Angelegenheiten (Betroffenenrechte) • Bearbeitung von Anfragen zu Identifikation eines Patienten • Unterstützung der Transferstelle bei der datenschutzkonformen Bereitstellung von Daten	• Einsicht in IDAT

System-administration	Institut für Medizininformatik, Goethe-Universität Frankfurt	• Second Level Support bei technischen Problemen oder Unklarheiten • dokumentierte manuelle Anpassungen in der Datenbank • Unterstützung bei Datenexporten und Wahrnehmung von Betroffenenrechten	• Einsicht in MDAT, wenn erforderlich (dokumentierter Zugriff)
Meldende Stellen	teilnehmende Einrichtungen des NARSE	• Erfassung von Daten im NARSE • Stellung von Nutzungsanträgen oder Nutzungsanzeigen	• Einsicht in IDAT und MDAT ihrer registrierten Personen • erhalten beantragte Daten entsprechend Nutzungsantrag / Nutzungsanzeige
Datennutzende	externe Interessensgruppen	• Stellung von Nutzungsanträgen	• keine Einsicht in IDAT und MDAT • erhalten beantragte Daten entsprechend Nutzungsantrag / Nutzungsanzeige

7.4.2 OSSE-Berechtigungen

- CreatePatients Permission to add new patients to your own location
- DataEntry Permission to enter and edit medical data of your own location
- See my location's patients Permission to read data of your own location
- See other locations' patients Permission to read data of any patient, i.e. also those of other locations
- See my IDAT Permission to see the IDAT of patients of your own location
- See all IDAT Permission to see the IDAT of any patient, i.e. also those of other locations
- DataExport Permission to export all medical data
- DataReport Permission to change the form status from open to reported
- DataValidation Permission to change the form status from reported to validated
- RemoveValidation Permission to change the form status from validated to open again
- PatientAccounts Permission to handle patient accounts

- Manage locations Permission to view, create and edit locations.
- Manage user roles Permission to view, create and edit user roles of all locations.
- Manage my location's user accounts Permission to view, create and edit user accounts of the own location, including allocation of roles and passwords.
- Manage all user accounts Permission to view, create and edit user accounts of all locations, including allocation of roles and passwords.

7.4.3 OSSE-Rollen: Zuordnung von Berechtigungen

Role	**Global Admin**	**Location Admin**	**Daten-eingabe**	**Daten-ansicht**	**Daten-export**	**IT Admin**
Location	*zentral*	*pro Standort*	*pro Standort*	*pro Standort*	*zentral*	*zentral*
CreatePatients	-	-	X	-	-	-
DataEntry	-	-	X	-	-	-
See my location's patients	-	-	X	X	X	X
See other locations' patients	-	-	-	-	X	X
See my IDAT	-	-	X	-	-	-
See all IDAT	-	-	-	-	-	-
DataExport	-	-	-	-	X	-
DataReport	-	-	-	-	-	-
DataValidation	-	-	-	-	-	-
RemoveValidation	-	-	-	-	-	-
PatientAccounts	-	-	-	-	-	-
Manage locations	X	-	-	-	-	-
Manage user roles	X	-	-	-	-	-
Manage my location's user accounts	-	X	-	-	-	-
Manage all user accounts	X	-	-	-	-	-
Change software settings	X	-	-	-	-	-

7.5 Technische und organisatorische Maßnahmen (TOMs)

- Technische und organisatorische Maßnahmen (TOMs) OSSE: 2023-01-13_TOM_OSSE_v2.pdf
- Technische und organisatorische Maßnahmen des Dienstleisters: 2024-01-25_TOM_Hetzner.pdf

8. ANHANG: TABELLARISCHE DATENSCHUTZ-FOLGENABSCHÄTZUNG

8.1 Gesetzliche Vorschrift betreffend DSFA und Definition für vorliegendes Dokument

Bei der Abfassung und Umsetzung eines Datenschutzkonzeptes für das Nationale Register für Seltene Erkrankungen (NARSE) ist eine gesetzliche Vorschrift im Berliner Landesdatenschutzgesetz §26 Absatz (2) zu beachten, die eine entsprechende Dokumentation vor der Inbetriebnahme der *„automatisierten Verarbeitung personenbezogener Daten"* vorsieht. Für die Anforderungen der Bundesebene an Datenschutzkonzepte hat Thilo Weichert im Gutachten „Datenschutzrechtliche Rahmenbedingungen medizinischer Forschung"[17] im Frühjahr 2022 dargestellt, dass in § 22 Abs. 2 Bundesdatenschutzgesetz (BDSG) die Inhalte eines Datenschutzkonzepts benannt werden.[18] Der Hauptteil des vorliegende Dokument (Kapitel 1 bis 7) erfüllt die Anforderungen der Bundesebene und der Berliner Landesebene an eine Datenschutzkonzept.

Daneben ist zu beachten, dass auf der Europaebene mit der DSGVO, deren Regelungen bei umfangreichen Verarbeitungen von besonderen Kategorien personenbezogener Daten (z.B. Gesundheitsdaten) ebenfalls einzuhalten sind, im Jahr 2018 der neue Begriff der **„Datenschutz-Folgenabschätzung"** (DSFA, Art. 35) eingeführt worden ist, ohne explizit einen Bezug zu Datenschutzkonzepten herzustellen. DSFA steht für die „Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten". Eine verpflichtend geforderte DSFA muss gemäß Art. 35 Abs. 7 DSGVO neben der Beschreibung von Verarbeitungsvorgängen und deren „Risiken für die Rechte und Freiheiten der betroffenen Personen" auch die Darstellung von „Abhilfemaßnahmen" zur Bewältigung der Risiken vorstellen. Der Begriff „Datenschutzkonzept" kommt in der DSGVO nicht vor. Gemäß Art. 35 Abs. 1 DSGVO[19], muss die Abschätzung **„vorab"** durchgeführt und dokumentiert werden.Aufgrund von Absprachen mit der Behördlichen Datenschutzbeauftragten der Charité und mit der AG Datenschutz des TMF e.V. erfolgt im vorliegenden **Datenschutzdokument für das NARSE** eine bedingte Zusammenführung

- des **Datenschutzkonzepts** gemäß Berliner (§ 26) und Bundes-Datenschutzgesetz (§ 22) und
- der **Datenschutz-Folgenabschätzung (DSFA)** gemäß Art. 35 DSGVO.

Im Sinne der Pflege in einem Dokument wird eine tabellarische DSFA als auswechselbare Anlage integriert [Kapitel 8 „Tabellarische Datenschutz-Folgenabschätzung" mit Abschnitt 8.2 „DSFA-Tabelle"]. Es wird verabredet, dass die Stellungnahme der TMF AG Datenschutz zum Datenschutzkonzept sich primär auf den Hauptteil des vorliegenden Dokumentes [Kapitel 1 bis 7] bezieht, dass ein vollständiges klassisches Datenschutzkonzept umfasst. Allfällige Änderungen des Kapitels 8 werden so abgefasst, dass die Gültigkeit des Hauptdokumentes und der Stellungnahme der TMF AG Datenschutz unberührt bleiben.

Die beiden folgenden Kästen dienen der Erläuterung des Vorgehens.

Exkurs 1

[17] Thilo Weichert 2022: Datenschutzrechtliche Rahmenbedingungen medizinischer Forschung. S.200. Gutachten für den TMF e.V.

[18] „Die Pflicht, ein Datenschutzkonzept für ein Forschungsvorhaben vorzulegen, besteht nicht generell, sondern nur gemäß einigen speziellen Gesetzen. Eine entsprechende Pflicht kann generell allenfalls aus den Dokumentationspflichten nach Art. 5 Abs. 2 DSGVO abgeleitet werden. Eine präzise Festlegung der notwendigen Inhalte ergibt sich aus den Gesetzen nicht. Als den Datenschutz umfassendes Dokument sollte es das Verarbeitungsverzeichnis, die Darstellung der technisch-organisatorischen Maßnahmen, die Datenschutz-Folgenabschätzung, die Einschränkung der Betroffenenrechte und die kompensierenden Garantien sowie, soweit es hierauf ankommt, die nötigen Interessenabwägungen enthalten. Kap. 11.3, Kap. 11.4)"

[19] DSGVO Artikel 35 (1): „Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, **so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch.** Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden."

Erläuterungen zur bedingten Zusammenführung von Datenschutzkonzept und Datenschutz-Folgenabschätzung (DSFA) für das NARSE im vorliegenden Dokument

Bei der Abfassung und Umsetzung eines Datenschutzdokumentes für das in Berlin vom BIH betriebenen NARSE sind das Landesdatenschutzgesetz (insbesondere § 26), das Bundesdatenschutzgesetz (insbesondere § 22) und die europäische DSGVO (insbesondere Artikel 35) zu beachten.

Das Berliner Landesdatenschutzgesetz fordert in §26 Absatz (2) die Abfassung eines Datenschutzkonzepts:

> *„[1]Vor einer Entscheidung über den Einsatz oder eine wesentliche Änderung einer automatisierten Verarbeitung personenbezogener Daten sind die zu treffenden technischen und organisatorischen Maßnahmen auf der Grundlage einer Risikoanalyse zu ermitteln und in einem Datenschutzkonzept zu dokumentieren. [2]Entsprechend der technischen Entwicklung und bei Änderungen der mit den Verarbeitungsvorgängen verbundenen Risiken ist die Ermittlung der Maßnahmen in angemessenen Abständen zu wiederholen.“*

Thilo Weichert verweist im Gutachten „Datenschutzrechtliche Rahmenbedingungen medizinischer Forschung“[20] auf § 22 Abs. 2 Bundesdatenschutzgesetz (BDSG) [21] das Inhalte eines Datenschutzkonzepts erläutert, ohne abschließend den Anwendungsbereich festzulegen. *Die Pflicht, ein Datenschutzkonzept für ein Forschungsvorhaben vorzulegen, besteht nicht generell, sondern nur gemäß einigen speziellen Gesetzen. Eine entsprechende Pflicht kann generell allenfalls aus den Dokumentationspflichten nach Art. 5 Abs. 2 DSGVO abgeleitet werden. Eine präzise Festlegung der notwendigen Inhalte ergibt sich aus den Gesetzen nicht. Als den Datenschutz umfassendes Dokument sollte es das Verarbeitungsverzeichnis, die Darstellung der technisch-organisatorischen Maßnahmen, die Datenschutz-Folgenabschätzung, die Einschränkung der Betroffenenrechte und die kompensierenden Garantien sowie, soweit es hierauf ankommt, die nötigen Interessenabwägungen enthalten.* Kap. 11.3, Kap. 11.4). „Typischerweise enthalten solche Konzepte die Darstellung der Zwecke und Rechtsgrundlagen der Verarbeitung, die Regelung der Verantwortlichkeit, die Prozesse und Da-

[20] Thilo Weichert 2022: Datenschutzrechtliche Rahmenbedingungen medizinischer Forschung. S.200. Gutachten für den TMF e.V.

[21] Bundesdatenschutzgesetz (BDSG); § 22 Verarbeitung besonderer Kategorien personenbezogener Daten

(2) In den Fällen des Absatzes 1 sind angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person vorzusehen. Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen können dazu insbesondere gehören:

1. technisch organisatorische Maßnahmen, um sicherzustellen, dass die Verarbeitung gemäß der Verordnung (EU) 2016/679 erfolgt,
2. Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt worden sind,
3. Sensibilisierung der an Verarbeitungsvorgängen Beteiligten,
4. Benennung einer oder eines Datenschutzbeauftragten,
5. Beschränkung des Zugangs zu den personenbezogenen Daten innerhalb der verantwortlichen Stelle und von Auftragsverarbeitern,
6. Pseudonymisierung personenbezogener Daten,
7. Verschlüsselung personenbezogener Daten,
8. Sicherstellung der Fähigkeit, Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten, einschließlich der Fähigkeit, die Verfügbarkeit und den Zugang bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen,
9. zur Gewährleistung der Sicherheit der Verarbeitung die Einrichtung eines Verfahrens zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen oder
10. spezifische Verfahrensregelungen, die im Fall einer Übermittlung oder Verarbeitung für andere Zwecke die Einhaltung der Vorgaben dieses Gesetzes sowie der Verordnung (EU) 2016/679 sicherstellen.

tenflüsse sowie insbesondere eine ausführliche Beschreibung der zum Schutz der Daten getroffenen technischen und organisatorischen Maßnahmen. Im Regelfall ist das Datenschutzkonzept damit auch Grundlage der in einem Verarbeitungstätigkeitenverzeichnis zu einem Projekt zu dokumentierenden Daten."

Weichert fährt fort, dass mit der DSGVO im Jahr 2018 der neue Begriff der Datenschutz-Folgenabschätzung (DSFA, Art. 35) eingeführt wurde, die zwingend bei umfangreichen Verarbeitungen von besonderen Kategorien personenbezogener Daten (z.B. Gesundheitsdaten) einzuhalten ist (vgl. Art. 35 Abs. 3 lit. b DSGVO).

Inhalte eines Datenschutzkonzeptes (den Datenschutz umfassendes Dokument) nach Th. Weichert 2022 Kap. 11.3, Kap. 11.4)	**Inhalte einer Datenschutz-Folgenabschätzung** Gemäß DSGVO Art. 35 Absatz (7)
• *(der Eintrag in) das Verarbeitungsverzeichnis,* • *die Darstellung der technisch-organisatorischen Maßnahmen,* • *die Datenschutz-Folgenabschätzung,* • *die Einschränkung der Betroffenenrechte und* • *die kompensierenden Garantien sowie,* • *soweit es hierauf ankommt, die nötigen Interessenabwägungen enthalten.*	*a) „eine systematische **Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung**, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen;* *b) eine **Bewertung** der Notwendigkeit und Verhältnismäßigkeit **der Verarbeitungsvorgänge** in Bezug auf den Zweck;* *c) eine **Bewertung der Risiken** für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 und* d) *die zur Bewältigung der Risiken geplanten **Abhilfemaßnahmen**, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird."*

Besonders zu beachten ist, dass sowohl ein Datenschutzkonzept gemäß § 26 (2) des Berliner Landesdatenschutzgesetzes als auch eine **DSFA vor Aufnahme der Verarbeitungsvorgänge** erstellt werden müssen.

Vorgehen beim NARSE

- Die verantwortlichen Autoren für das Datenschutzkonzept und die DSFA gehen von einer sehr großen Überschneidung der Anforderungen von Datenschutzkonzept und DSFA aus. Beide fordern mit teilweise geringfügig unterschiedlichen Begriffen die Beschreibung der Verarbeitungsvorgänge,
- die Feststellung von Risiken für Betroffenenrechte,
- Interessenabwägungen (einschließlich der Berufung auf Rechtsgrundlagen) und
- die Beschreibung von technischen und organisatorischen Abhilfemaßnahmen.

Während der Hauptteil des Datenschutzkonzepts als Fließtext formuliert ist, wird die tabellarische DSFA als kommentierte Liste der Verarbeitungsvorgänge dargestellt. Die Tabelle beruht auf einer Liste von Verarbeitungsvorgängen aus dem TMF-Bericht „Von der Evaluierung zur Konsolidierung: Anforderungen an Kohortenstudien und Register-IT (KoRegIT)" aus dem Jahre 2015. In dem TMF-Bericht liegt eine hierarchische Gliederung in „Phasen", „Top-Level-Aufgaben" und „Use Cases" vor, die im Prinzip übernommen wird. Allerdings

erfolgt eine Umbenennung der „Top-Level-Aufgaben“ in „Verarbeitungsgruppen“ und der „Use Cases“ in „Verarbeitungsvorgänge“.

In der tabellarischen DSFA wird die Betrachtung der Risiken, die es durch Abwehrmaßnahmen zu bewältigen gilt, auf die Gefährdung der sieben Gewährleitungsziele des Standarddatenschutzmodells der Konferenz der Datenschutzbeauftragten des Bundes und der Länder (Datenschutzkonferenz) fokussiert:

(1) Datenminimierung
(2) Verfügbarkeit
(3) Integrität
(4) Vertraulichkeit
(5) Nichtverkettung
(6) Transparenz
(7) Intervenierbarkeit

Die Technischen und Organisatorischen Schutzmaßnahmen, hier DSGVO-konform „Abhilfemaßnahmen“ genannt, werden mit Verweis auf das vorliegende Datenschutzkonzept benannt, aber noch nicht ausführlich beschrieben. Es ist vorgesehen, im Zuge der schrittweisen Weiterentwicklung des NARSE das Datenschutzkonzept und die angehängte tabellarische DSFA mit gleicher Versionierung synchronisiert fortzuschreiben.

Allerdings erhält die Versionsnummer der angehängten tabellarischen DSFA beginnend mit „a“ einen kleinen Buchstaben als Suffix, so dass Anpassungen der tabellarischen DSFA auch zwischenzeitlich erfolgen können, wenn dies notwendig erscheint.

Exkurs 2

Datenschutzkonzept und DSFA als kontinuierlicher Prozess

Das Berliner Landesdatenschutzgesetz fordert in § 26 die Wiederholung der *„Ermittlung* [und Dokumentation] *der Maßnahmen in angemessenen Abständen“*. Anpassungen des Datenschutzkonzeptes sollen *„Entsprechend der technischen Entwicklung und bei Änderungen der mit den Verarbeitungsvorgängen verbundenen Risiken“* erfolgen.

Im gleichen Sinn hat die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz) im Kurzpapier Nr. 5 mit dem Titel „Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO“ [22] die Interpretation erarbeitet, dass es sich bei der Abfassung einer DSFA nicht um einen einmaligen Vorgang handelt. Es wird ausgeführt: „Sollten sich z.B. neue Risken ergeben, die Bewertung bereits erkannter Risiken ändern oder wesentliche Änderung im Verfahren ergeben, die in der DSFA bisher nicht berücksichtigt wurden, so ist die DSFA zu überprüfen und ebenso anzupassen. Um dies zu garantieren, wird ein stetiger, iterativer Prozess der Prüfung und Anpassung empfohlen.

Diese Interpretation trifft beim NARSE mit der Absicht zusammen, eine kontinuierliche Weiterentwicklung und Erfahrungsaustausch zu betreiben.

[22] https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_5.pdf

Dieses Kurzpapier dient als erste Orientierung insbesondere für den nicht-öffentlichen Bereich, wie nach Auffassung der Datenschutzkonferenz die Datenschutz-Grundverordnung (DS-GVO) im praktischen Vollzug angewendet werden sollte. Diese Auffassung steht unter dem Vorbehalt einer zukünftigen - möglicherweise abweichenden - Auslegung des Europäischen Datenschutzausschusses.

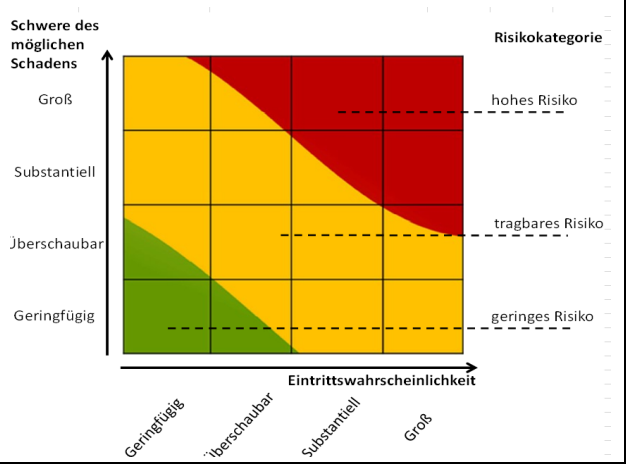
8.2 DSFA-Tabelle mit Verarbeitungsrubriken und Verarbeitungsvorgängen

Die „Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten“ orientiert sich an der Beschreibung der Verarbeitungsrubriken (Top-Level-Aufgaben, VR=TL) und Verarbeitungsvorgänge (Detailaufgaben, Use Cases, VV=UC) des TMF-Projektes KoRegIT[23].

Die hier vorliegende Folgenabschätzung beschränkt sich auf die Erhebung von Daten über die manuelle Patientenregistrierung und analysiert dies in Hinblick auf die Verarbeitungsrubriken (Top-Level-Aufgaben), die sieben Gewährleistungsziele des Standarddatenschutzmodells der Datenschutzkonferenz des Bundes und Länder und die darin abgebildeten zentralen Datenschutzanforderungen der DSGVO.

Im Zuge des Aufbaus des NARSE und des iterativ-zyklischen DSFA-Vorgehens können einzelne Detailaufgaben und ihre Risiken stärkere Beachtung finden.

Die Kategorisierung der Risiken orientiert sich am DSFA-Entwurf der TMF-AG Datenschutz (Stand November 2022)[24].

Die sieben **Gewährleistungsziele des Standarddatenschutzmodells** sind:	**Schweregrade des möglichen Schadens**	**Eintrittswahrscheinlichkeiten**	**Risikomatrix**
(1) Datenminimierung (2) Verfügbarkeit (3) Integrität (4) Vertraulichkeit (5) Nichtverkettung (6) Transparenz (7) Intervenierbarkeit	(1) Geringfügig (2) Überschaubar (3) Substantiell (4) Groß	(1) Geringfügig (2) Überschaubar (3) Substantiell (4) Groß	

[23] Aufbauend auf: Claudia Michalik M.A., Dipl.-Inform. Med. Sylvie Ngouongo, Prof. Dr. med. Jürgen Stausberg 2015: Von der Evaluierung zur Konsolidierung: Anforderungen an Kohortenstudien und Register-IT (KoRegIT). Anforderungskatalog. Version 1.0; Januar 2015. © TMF e.V.

[24] TMF AG Datenschutz 2022: DSFA Template

Tabelle 1: Tabelle der NARSE-Verarbeitungsrubriken und Verarbeitungsvorgänge mit Risikoanalyse und Abhilfemaßnahmen

Nr.	Typ TL/UC=	Iden-tifier	Verarbeitungsphase Verarbeitungsrubrik (Top-Level-Aufgabe, TL=VR) / Verarbeitungsvorgang (Use Case, UC=VV)	Risiken Gef. = Gefährdung der … Gef. = besondere Gefährd.	Abhilfemaßnahme [Techn. und Organisat. Maßn.: TOM]	Eintrittsw. Restrisiko	Schweregr. Restrisiko	Risiko-kategorie
3. Betrieb / Umsetzung								
145	TL= VR	TL022	**Probandenmanagement** Details zur Verarbeitungsrubrik Probandenmanagement finden sich in der nachfolgenden Auflistung der Verarbeitungsvorgänge [Use Case].	(1) Gef. Datenminimier. **(2) Gef. Verfügbarkeit** **(3) Gef. Integrität** **(4) Gef. Vertraulichkeit** (5) Gef. Nichtverkettung (6) Gef. Transparenz (7) Gef. Intervenierbark.	**Allgemeine TOM** a. Umsetzung durch geschultes Personal b. DV in Geschützten Räumen **Spez. TOM wg. Verfügbarkeit** c. Datenerhebungskommunikation (ZSE, Krankenhäuser, Niedergelassene, Patienten-gruppen, weitere) d. proaktive Entwicklung der Datenzugänge (z.B. Satellitendokum.) e. proaktive Probandenkommunikation f. Gewährleistung der Verfügbarkeit und Be-lastbarkeit der Server durch Dienstleister (Hetzner TOMs) g. regelmäßige Backups entsprechend eines Backup-Konzepts (OSSE TOMs 5b) **Spez. TOM wg. Vertraulichkeit** h. Umsetzung bzw. Veranlassung nur d. Be-handelnde und Erfüllungsgehilfen i. Informationelle Gewaltenteilung mit Ver-trauensstelle (UTHS) j. Pseudonymisierung und Trennung von I-DAT und MDAT k. Zutritts- und Zugangskontrolle zu Servern (Hetzner TOMs)	Über-schaubar	Über-schaubar	**Tragbares Risiko**

Nr.	Typ TL/UC=	Iden-tifier	Verarbeitungsphase Verarbeitungsrubrik (Top-Level-Aufgabe, TL=VR) / Verarbeitungsvorgang (Use Case, UC=VV)	Risiken Gef. = Gefährdung der … Gef. = besondere Gefährd.	Abhilfemaßnahme [Techn. und Organisat. Maßn.: TOM]	Eintrittsw. Restrisiko	Schweregr. Restrisiko	Risiko-kategorie
					l. Zugangskontrolle: Authentifizierung in OSSE-Software mit Passwort + 2FA (OSSE TOMs 3b) m. Zugriffskontrolle innerhalb der OSSE-Software über modulares Berechtigungs-konzept (OSSE TOMs 3c) **Spez. TOM wg. Integrität** n. Protokollierung aller Änderungen inner-halb der OSSE-Software (OSSE TOMs 4b) o. Dokumentation aller manuellen Änderun-gen in der OSSE-Datenbank (OSSE TOMs 4b)			
146	UC=VV	UC0080	Informationsmaterial an potentielle Probanden versenden		Siehe TOM zu Verarbeitungsrubrik TL022			
147	UC=VV	UC0081	Eignung potentieller Probanden prüfen		Siehe TOM zu Verarbeitungsrubrik TL022			
148	UC=VV	UC0084	Probanden aufklären und Einwilligungen einholen		Siehe TOM zu Verarbeitungsrubrik TL022			
149	UC=VV	UC0250	Screeningliste führen		Siehe TOM zu Verarbeitungsrubrik TL022			
150	UC=VV	UC0179	Probanden einschließen		Siehe TOM zu Verarbeitungsrubrik TL022			
151	UC=VV	UC0085	Probandenpass erstellen		Siehe TOM zu Verarbeitungsrubrik TL022			
152	UC=VV	UC0075	Probandenpass ausgeben		Siehe TOM zu Verarbeitungsrubrik TL022			
~~153~~	~~UC=VV~~	~~UC0251~~	~~Dezentrale Probandenliste führen~~		~~Siehe TOM zu Verarbeitungsrubrik TL022~~			
154	UC=VV	UC0244	Zentrale Probandenliste führen		Siehe TOM zu Verarbeitungsrubrik TL022			
155	UC=VV	UC0100	Widerruf einer Einwilligungserklärung bearbeiten		Siehe TOM zu Verarbeitungsrubrik TL022			
156	UC=VV	UC0235	Einwilligungserklärung des Probanden modifizieren		Siehe TOM zu Verarbeitungsrubrik TL022			

Nr.	Typ TL/UC=	Iden-tifier	Verarbeitungsphase Verarbeitungsrubrik (Top-Level-Aufgabe, TL=VR) / Verarbeitungsvorgang (Use Case, UC=VV)	Risiken Gef. = Gefährdung der … Gef. = besondere Gefährd.	Abhilfemaßnahme [Techn. und Organisat. Maßn.: TOM]	Eintrittsw. Restrisiko	Schweregr. Restrisiko	Risiko-kategorie
157	**TL= VR**	**TL037**	**Unterstützung und Betreuung von Probanden**	(1) Gef. Datenminimier. (2) Gef. Verfügbarkeit (3) Gef. Integrität **(4) Gef. Vertraulichkeit** (5) Gef. Nichtverkettung (6) Gef. Transparenz (7) Gef. Intervenierbark.	**Allgemeine TOM** a. Umsetzung durch geschultes Personal b. DV in Geschützten Räumen **Spez. TOM wg. Vertraulichkeit** c. Umsetzung bzw. Veranlassung nur d. Behandelnde und Erfüllungsgehilfen d. Rekontaktierung von Probanden nur mit Opt-in Einwilligung unter Einbindung der UTHS	Über-schaubar	Über-schaubar	**Tragbares Risiko**
158	UC=VV	UC0070	Termine mit Probanden vereinbaren		Siehe TOM zu Verarbeitungsrubrik TL037			
159	UC=VV	UC0071	Benachrichtigung bei Terminverschiebung erstellen		Siehe TOM zu Verarbeitungsrubrik TL037			
160	UC=VV	UC0073	Probanden auf Basis vereinbarter Termine einbestellen		Siehe TOM zu Verarbeitungsrubrik TL037			
161	UC=VV	UC0086	Zentrumswechsel eines Probanden verarbeiten		Siehe TOM zu Verarbeitungsrubrik TL037			
162	UC=VV	UC0206	Probanden Über Befunde informieren		Siehe TOM zu Verarbeitungsrubrik TL037			
163	UC=VV	UC0207	Informationsveranstaltung für Probanden ausrichten		Siehe TOM zu Verarbeitungsrubrik TL037			
164	**TL= VR**	**TL021**	**Datenerhebung und Datenerfassung**	**(1) Gef. Datenminimier.** **(2) Gef. Verfügbarkeit** **(3) Gef. Integrität** **(4) Gef. Vertraulichkeit** (5) Gef. Nichtverkettung (6) Gef. Transparenz (7) Gef. Intervenierbark.	**Allgemeine TOM** a. Umsetzung durch geschultes Personal b. DV in Geschützten Räumen **Spez. TOM wg. Datenminimierung** c. Erfassung eines abgestimmten Minimaldatensatzes d. Erfassung von genetischen Informationen nur mit Opt-in Einwilligung **Spez. TOM wg. Verfügbarkeit** e. Ergonomie und Usability der Datenerfassung f. proaktive Entwicklung der Datenzugänge (z.B. Satellitendokum.)	Über-schaubar	Über-schaubar	**Tragbares Risiko**

Nr.	Typ TL/UC=	Iden-tifier	Verarbeitungsphase Verarbeitungsrubrik (Top-Level-Aufgabe, TL=VR) / Verarbeitungsvorgang (Use Case, UC=VV)	Risiken Gef. = Gefährdung der … Gef. = besondere Gefährd.	Abhilfemaßnahme [Techn. und Organisat. Maßn.: TOM]	Eintrittsw. Restrisiko	Schweregr. Restrisiko	Risiko-kategorie
					g. Gewährleistung der Verfügbarkeit und Belastbarkeit der Server durch Dienstleister (Hetzner TOMs) h. regelmäßige Backups entsprechend eines Backup-Konzepts (OSSE TOMs 5b) **Spez. TOM wg. Integrität** i. Identitätsmanagement mit Vertrauens-stelle UTHS Dresden j. Protokollierung aller Änderungen inner-halb der OSSE-Software in Audit Trail (OSSE TOMs 4b) k. Dokumentation aller manuellen Änderun-gen in der OSSE-Datenbank (OSSE TOMs 4b) l. Datenübertragung zwischen Browser und Server mit sicherer Verschlüsselung (OSSE TOMs 4a) **Spez. TOM wg. Vertraulichkeit** m. informationelle Gewaltenteilung mit UTHS n. Pseudonymisierung und Trennung von I-DAT und MDAT o. Zutritts- und Zugangskontrolle zu Servern (Hetzner TOMs) p. Zugangskontrolle: Authentifizierung in OSSE-Software mit Passwort + 2FA (OSSE TOMs 3b) q. Zugriffskontrolle innerhalb der OSSE-Soft-ware über modulares Berechtigungskonzept (OSSE TOMs 3c)			

Nr.	Typ TL/UC=	Iden-tifier	Verarbeitungsphase Verarbeitungsrubrik (Top-Level-Aufgabe, TL=VR) / Verarbeitungsvorgang (Use Case, UC=VV)	Risiken Gef. = Gefährdung der … Gef. = besondere Gefährd.	Abhilfemaßnahme [Techn. und Organisat. Maßn.: TOM]	Eintrittsw. Restrisiko	Schweregr. Restrisiko	Risiko-kategorie
					r. Trennungskontrolle innerhalb der OSSE-Software über modulares Berechtigungs-konzept (OSSE TOMs 3d)			
165	UC=VV	UC0088	Daten erheben		Siehe TOM zu Verarbeitungsrubrik TL021			
~~166~~	~~UC=VV~~	~~UC0089~~	~~Daten importieren~~		~~Siehe TOM zu Verarbeitungsrubrik TL021~~			
167	UC=VV	UC0090	Probanden registrieren		Siehe TOM zu Verarbeitungsrubrik TL021			
~~168~~	~~UC=VV~~	~~UC0208~~	~~Probanden zu Kollektiv zuordnen~~		~~Siehe TOM zu Verarbeitungsrubrik TL021~~			
169	UC=VV	UC0092	Probandendatensatz bearbeiten		Siehe TOM zu Verarbeitungsrubrik TL021			
170	UC=VV	UC0093	Probandendatensatz deaktivieren/sperren		Siehe TOM zu Verarbeitungsrubrik TL021			
171	UC=VV	UC0094	Probandendatensatz endgültig löschen		Siehe TOM zu Verarbeitungsrubrik TL021			
~~172~~	~~UC=VV~~	~~UC0095~~	~~Visiten anzeigen~~		~~Siehe TOM zu Verarbeitungsrubrik TL021~~			
~~173~~	~~UC=VV~~	~~UC0096~~	~~Visite anlegen~~		~~Siehe TOM zu Verarbeitungsrubrik TL021~~			
~~174~~	~~UC=VV~~	~~UC0099~~	~~Visite löschen~~		~~Siehe TOM zu Verarbeitungsrubrik Nr. 164~~			
175	UC=VV	UC0242	Probandenberichte implementieren		Siehe TOM zu Verarbeitungsrubrik Nr. 164			
176	**TL=VR**	**TL023**	**Monitoring**	(1) Gef. Datenminimier. (2) Gef. Verfügbarkeit (3) Gef. Integrität **(4) Gef. Vertraulichkeit** (5) Gef. Nichtverkettung (6) Gef. Transparenz (7) Gef. Intervenierbark.	**Allgemeine TOM** a. Umsetzung durch geschultes Personal b. DV in Geschützten Räumen **Spez. TOM wg. Vertraulichkeit** c. Umsetzung bzw. Veranlassung nur d. Be-handelnde und Erfüllungsgehilfen	Über-schaubar	Gering-fügig	**Geringes Risiko**
177	UC=VV	UC0101	Monitore schulen		Siehe TOM zu Verarbeitungsrubrik TL023			
178	UC=VV	UC0102	Monitoring vor Ort vorbereiten		Siehe TOM zu Verarbeitungsrubrik TL023			

Nr.	Typ TL/UC=	Iden-tifier	Verarbeitungsphase Verarbeitungsrubrik (Top-Level-Aufgabe, TL=VR) / Verarbeitungsvorgang (Use Case, UC=VV)	Risiken Gef. = Gefährdung der … Gef. = besondere Gefährd.	Abhilfemaßnahme [Techn. und Organisat. Maßn.: TOM]	Eintrittsw. Restrisiko	Schweregr. Restrisiko	Risiko-kategorie
179	UC=VV	UC0103	Monitoring vor Ort durchführen		Siehe TOM zu Verarbeitungsrubrik TL023			
180	UC=VV	UC0104	Zentrales Monitoring durchführen		Siehe TOM zu Verarbeitungsrubrik TL023			
181	UC=VV	UC0105	Monitoringbericht erstellen		Siehe TOM zu Verarbeitungsrubrik TL023			
182	UC=VV	UC0209	Monitoringbericht abstimmen		Siehe TOM zu Verarbeitungsrubrik TL023			
183	UC=VV	UC0210	Monitoringbericht an Zentrum versenden		Siehe TOM zu Verarbeitungsrubrik TL023			
184	UC=VV	UC0106	Umsetzung der Maßnahmen zur Behebung oder Vorbeugung von Auffälligkeiten kontrollieren		Siehe TOM zu Verarbeitungsrubrik TL023			
185	**TL=VR**	**TL024**	**Bereitstellung von probandenbezogenen Informationen**	(1) Gef. Datenminimier. (2) Gef. Verfügbarkeit (3) Gef. Integrität **(4) Gef. Vertraulichkeit** (5) Gef. Nichtverkettung (6) Gef. Transparenz (7) Gef. Intervenierbark.	**Allgemeine TOM** a. Umsetzung durch geschultes Personal b. DV in Geschützten Räumen **Spez. TOM wg. Vertraulichkeit** c. Umsetzung bzw. Veranlassung nur d. Behandelnde und Erfüllungsgehilfen d. Rekontaktierung von Probanden nur mit Opt-in Einwilligung unter Einbindung der UTHS	Über-schaubar	Gering-fü-gig.	**Geringes Risiko**
186	UC=VV	UC0108	Befunddokumentation generieren		Siehe TOM zu Verarbeitungsrubrik TL024			
187	UC=VV	UC0109	Gutachten/Briefe erstellen		Siehe TOM zu Verarbeitungsrubrik TL024			
188	UC=VV	UC0110	Dokument verschicken		Siehe TOM zu Verarbeitungsrubrik TL024			
189	**TL=VR**	**TL025**	~~**Abrechnung mit Erhebungszentren und Probanden**~~ **(zurückgestellt)**	~~(1) Gef. Datenminimier.~~ ~~(2) Gef. Verfügbarkeit~~ ~~(3) Gef. Integrität~~ ~~(4) Gef. Vertraulichkeit~~ ~~(5) Gef. Nichtverkettung~~ ~~(6) Gef. Transparenz~~ ~~(7) Gef. Intervenierbark.~~	~~**Allgemeine TOM**~~ ~~a. Umsetzung durch geschultes Personal~~ ~~b. DV in Geschützten Räumen~~ ~~**Spez. TOM wg. Vertraulichkeit**~~ ~~c. Umsetzung bzw. Veranlassung nur d. Behandelnde und Erfüllungsgehilfen~~	~~Gering-fügig.~~	~~Über-schaubar~~	~~**Geringes Risiko**~~

Nr.	Typ TL/UC=	Iden-tifier	Verarbeitungsphase Verarbeitungsrubrik (Top-Level-Aufgabe, TL=VR) / Verarbeitungsvorgang (Use Case, UC=VV)	Risiken Gef. = Gefährdung der … Gef. = besondere Gefährd.	Abhilfemaßnahme [Techn. und Organisat. Maßn.: TOM]	Eintrittsw. Restrisiko	Schweregr. Restrisiko	Risiko-kategorie
190	UC=VV	UC0113	~~Umfang und Qualität der von den Zentren erbrachten Leistungen prüfen~~	-	~~Siehe TOM zu Verarbeitungsrubrik TL025~~			
191	UC=VV	UC0114	~~Abrechnung erstellen~~	-	~~Siehe TOM zu Verarbeitungsrubrik TL025~~			
192	UC=VV	UC0115	~~Abrechnung verschicken~~	-	~~Siehe TOM zu Verarbeitungsrubrik TL025~~			
193	UC=VV	UC0116	~~Auszahlungen prüfen~~	-	~~Siehe TOM zu Verarbeitungsrubrik TL025~~			
194	**TL=VR**	**TL045**	**~~Abrechnung von Dienstleistungen~~** **(Zurückgestellt)**	~~(1) Gef. Datenminimier.~~ ~~(2) Gef. Verfügbarkeit~~ ~~(3) Gef. Integrität~~ ~~**(4) Gef. Vertraulichkeit**~~ ~~(5) Gef. Nichtverkettung~~ ~~(6) Gef. Transparenz~~ ~~(7) Gef. Intervenierbark.~~	~~**Allgemeine TOM**~~ ~~a. Umsetzung durch geschultes Personal~~ ~~b. DV in Geschützten Räumen~~ ~~**Spez. TOM wg. Vertraulichkeit**~~ ~~c. Umsetzung bzw. Veranlassung nur d. Behandelnde und Erfüllungsgehilfen~~	~~Gering-fügig.~~	~~Über-schaubar~~	~~**Geringes Risiko**~~
~~195~~	~~UC=VV~~	~~UC0213~~	~~Abrechnung erstellen~~	-	~~Siehe TOM zu Verarbeitungsrubrik TL045~~			
~~196~~	~~UC=VV~~	~~UC0214~~	~~Abrechnung verschicken~~	-	~~Siehe TOM zu Verarbeitungsrubrik TL045~~			
~~197~~	~~UC=VV~~	~~UC0215~~	~~Zahlungseingang prüfen~~	-	~~Siehe TOM zu Verarbeitungsrubrik TL045~~			
198	**TL=VR**	**TL026**	**Datenmanagement (Organisation und Pflege der Daten)**	(1) Gef. Datenminimier. **(2) Gef. Verfügbarkeit** **(3) Gef. Integrität** **(4) Gef. Vertraulichkeit** (5) Gef. Nichtverkettung (6) Gef. Transparenz (7) Gef. Intervenierbark.	**Allgemeine TOM** a. Umsetzung durch geschultes Personal b. DV in Geschützten Räumen c. Umsetzung bzw. Veranlassung nur d. Behandelnde und Erfüllungsgehilfen	Über-schaubar.	Gering-fügig	**Geringes Risiko**
199	UC=VV	UC0122	Datensicherheit entsprechend dem Datenschutzkonzept umsetzen		Siehe TOM zu Verarbeitungsrubrik TL026			
200	UC=VV	UC0118	Datenbestand einfrieren		Siehe TOM zu Verarbeitungsrubrik TL026			
201	UC=VV	UC0119	Daten exportieren und bereitstellen		Siehe TOM zu Verarbeitungsrubrik TL026			

Nr.	Typ TL/UC=	Iden-tifier	Verarbeitungsphase Verarbeitungsrubrik (Top-Level-Aufgabe, TL=VR) / Verarbeitungsvorgang (Use Case, UC=VV)	Risiken Gef. = Gefährdung der … Gef. = besondere Gefährd.	Abhilfemaßnahme [Techn. und Organisat. Maßn.: TOM]	Eintrittsw. Restrisiko	Schweregr. Restrisiko	Risiko-kategorie
202	UC=VV	UC0121	Zentrales Monitoring unterstützen		Siehe TOM zu Verarbeitungsrubrik TL026			
4. Betrieb / Nutzung								
204	**TL=VR**	**TL028**	**Studienunterstützung**	(1) Gef. Datenminimier. (2) Gef. Verfügbarkeit **(3) Gef. Integrität** **(4) Gef. Vertraulichkeit** (5) Gef. Nichtverkettung (6) Gef. Transparenz (7) Gef. Intervenierbark.	**Allgemeine TOM** a. Umsetzung durch geschultes Personal b. DV in Geschützten Räumen **Spez. TOM wg. Vertraulichkeit** c. Umsetzung bzw. Veranlassung nur d. Behandelnde und Erfüllungsgehilfen d. Prüfung und Freigabe durch Data Access Committee (erg. durch EK und DSB) e. reguläre Beschränkung auf Daten mit Einwilligung f. reguläre Beschränkung auf Daten auf vorgegebene Nutzungszwecke g. reguläre Beschränkung auf Auswertung pseudonymisierter Daten **Spez. TOM wg. Integrität** h. Export aus OSSE-Software in pseudonymisierter Form (OSSE TOMs 4a) i. weitere Verarbeitung und Bereitstellung der Daten nach SOPs mit Dokumentation für Nachvollziehbarkeit	Über-schaubar	Über-schaubar	**Tragbares Risiko**
205	UC=VV	UC0127	Studienanfragen prüfen		Siehe TOM zu Verarbeitungsrubrik TL028			
206	UC=VV	UC0128	Feasibility-Analysen erstellen		Siehe TOM zu Verarbeitungsrubrik TL028			
207	UC=VV	UC0129	Daten bereitstellen		Siehe TOM zu Verarbeitungsrubrik TL028			
208	UC=VV	UC0131	Berichterstattung/statistische Analyse unterstützen		Siehe TOM zu Verarbeitungsrubrik TL028			

Nr.	Typ TL/UC=	Iden-tifier	Verarbeitungsphase Verarbeitungsrubrik (Top-Level-Aufgabe, TL=VR) / Verarbeitungsvorgang (Use Case, UC=VV)	Risiken Gef. = Gefährdung der … Gef. = besondere Gefährd.	Abhilfemaßnahme [Techn. und Organisat. Maßn.: TOM]	Eintrittsw. Restrisiko	Schweregr. Restrisiko	Risiko-kategorie
209	UC=VV	UC0224	Zentren potentielle Probanden melden		Siehe TOM zu Verarbeitungsrubrik TL028			
210	**TL=VR**	**TL029**	**Statistische Analyse**	(1) Gef. Datenminimier. (2) Gef. Verfügbarkeit **(3) Gef. Integrität** **(4) Gef. Vertraulichkeit** **(5) Gef. Nichtverkettung** (6) Gef. Transparenz **(7) Gef. Intervenierbark.**	**Allgemeine TOM** a. Umsetzung durch geschultes Personal b. DV in Geschützten Räumen **Spez. TOM wg. Vertraulichkeit** c. Freigabe nur durch Data Access Committee **Spez. TOM wg. Integrität** d. weitere Verarbeitung und Bereitstellung der Daten nach SOPs mit Dokumentation für Nachvollziehbarkeit	Über-schaubar	Über-schaubar	**Tragbares Risiko**
211	UC=VV	UC0134	Daten für Analyse aufbereiten		Siehe TOM zu Verarbeitungsrubrik TL029			
212	UC=VV	UC0135	Analyse durchführen		Siehe TOM zu Verarbeitungsrubrik TL029			
213	UC=VV	UC0136	Analysebericht erstellen		Siehe TOM zu Verarbeitungsrubrik TL029			
214	UC=VV	UC0139	Zentrenbezogene Auswertung erstellen		Siehe TOM zu Verarbeitungsrubrik TL029			
215	**TL=VR**	**TL030**	**Berichterstattung**	(1) Gef. Datenminimier. (2) Gef. Verfügbarkeit (3) Gef. Integrität **(4) Gef. Vertraulichkeit** (5) Gef. Nichtverkettung (6) Gef. Transparenz (7) Gef. Intervenierbark.	**Allgemeine TOM** a. Umsetzung durch geschultes Personal b. DV in Geschützten Räumen **Spez. TOM wg. Vertraulichkeit** c. Umsetzung bzw. Veranlassung nur d. Behandelnde und Erfüllungsgehilfen d. Veröffentlichung von Daten nur in aggregierter Form	Über-schaubar	Über-schaubar	**Tragbares Risiko**
216	UC=VV	UC0141	Berichte vorbereiten		Siehe TOM zu Verarbeitungsrubrik TL030			
217	UC=VV	UC0142	Berichte erstellen		Siehe TOM zu Verarbeitungsrubrik TL030			
218	UC=VV	UC0143	Berichte abstimmen		Siehe TOM zu Verarbeitungsrubrik TL030			
219	UC=VV	UC0237	Berichte finalisieren		Siehe TOM zu Verarbeitungsrubrik TL030			

Nr.	Typ TL/UC=	Iden-tifier	Verarbeitungsphase Verarbeitungsrubrik (Top-Level-Aufgabe, TL=VR) / Verarbeitungsvorgang (Use Case, UC=VV)	Risiken Gef. = Gefährdung der … Gef. = besondere Gefährd.	Abhilfemaßnahme [Techn. und Organisat. Maßn.: TOM]	Eintrittsw. Restrisiko	Schweregr. Restrisiko	Risiko-kategorie
220	UC=VV	UC0144	Berichte veröffentlichen		Siehe TOM zu Verarbeitungsrubrik TL030			
221	**TL=VR**	**TL031**	**Organisation von Publikationen und Präsentationen**	(1) Gef. Datenminimier. (2) Gef. Verfügbarkeit (3) Gef. Integrität **(4) Gef. Vertraulichkeit** (5) Gef. Nichtverkettung (6) Gef. Transparenz (7) Gef. Intervenierbark.	**Allgemeine TOM** a. Umsetzung durch geschultes Personal b. DV in Geschützten Räumen **Spez. TOM wg. Vertraulichkeit** c. Umsetzung bzw. Veranlassung nur d. Behandelnde und Erfüllungsgehilfen	Über-schaubar	Über-schaubar	**Tragbares Risiko**
222	UC=VV	UC0145	Relevante Journals und Kongresse recherchieren		Siehe TOM zu Verarbeitungsrubrik TL031			
223	UC=VV	UC0146	Publikationen und Präsentationen planen		Siehe TOM zu Verarbeitungsrubrik TL031			
224	UC=VV	UC0148	Autorenschaft abstimmen		Siehe TOM zu Verarbeitungsrubrik TL031			
225	UC=VV	UC0147	Publikationen und Präsentationen erstellen		Siehe TOM zu Verarbeitungsrubrik TL031			
226	UC=VV	UC0226	Publikationen und Präsentationen abstimmen		Siehe TOM zu Verarbeitungsrubrik TL031			
227	**TL=VR**	**TL033**	**Datenintegration, Datenzusammenführung** Ausarbeitung folgt vor der Inangriffnahme der Stufe 2 des NARSE: Import aus Satellitendokumentationen.	(1) Gef. Datenminimier. **(2) Gef. Verfügbarkeit** **(3) Gef. Integrität** **(4) Gef. Vertraulichkeit** **(5) Gef. Nichtverkettung** **(6) Gef. Transparenz** **(7) Gef. Intervenierbark.**	**Allgemeine TOM** a. Umsetzung durch geschultes Personal b. DV in Geschützten Räumen **Spez. TOM wg. Vertraulichkeit** c. Umsetzung bzw. Veranlassung nur d. Behandelnde und Erfüllungsgehilfen	Über-schaubar	Über-schaubar	**Tragbares Risiko**
228	UC=VV	UC0249	Anfragen nach Datenintegration oder Datenzusammenführung prüfen		Siehe TOM zu Verarbeitungsrubrik TL033			
229	UC=VV	UC0152	Datenkompatibilität prüfen		Siehe TOM zu Verarbeitungsrubrik TL033			
230	UC=VV	UC0153	Datenformat abstimmen		Siehe TOM zu Verarbeitungsrubrik TL033			
231	UC=VV	UC0154	Datenintegration/Datenzusammenführung durchführen		Siehe TOM zu Verarbeitungsrubrik TL033			

Nr.	Typ TL/UC=	Iden-tifier	Verarbeitungsphase Verarbeitungsrubrik (Top-Level-Aufgabe, TL=VR) / Verarbeitungsvorgang (Use Case, UC=VV)	Risiken Gef. = Gefährdung der … Gef. = besondere Gefährd.	Abhilfemaßnahme [Techn. und Organisat. Maßn.: TOM]	Eintrittsw. Restrisiko	Schweregr. Restrisiko	Risiko-kategorie
232	**TL= VR**	**TL046**	**Unterstützung der Patientenversorgung**	(1) Gef. Datenminimier. **(2) Gef. Verfügbarkeit** (3) Gef. Integrität **(4) Gef. Vertraulichkeit** (5) Gef. Nichtverkettung (6) Gef. Transparenz (7) Gef. Intervenierbark.	**Allgemeine TOM** a. Umsetzung durch geschultes Personal b. DV in Geschützten Räumen **Spez. TOM wg. Verfügbarkeit** c. vollständige Minimaldatensätze d. breite Kommunikation der Registernut-zung d. Standardisierung von Satellitendokumen-tation **Spez. TOM wg. Vertraulichkeit** e. Umsetzung bzw. Veranlassung nur d. Be-handelnde und Erfüllungsgehilfen f. Informationelle Gewaltenteilung	Über-schaubar	Über-schaubar	**Tragbares Risiko**
233	UC=VV	UC0218	Qualitätssicherung unterstützen		Siehe TOM zu Verarbeitungsrubrik TL046			
234	UC=VV	UC0219	Diagnose und Therapie unterstützen		Siehe TOM zu Verarbeitungsrubrik TL046			

5. Betrieb / Weiterentwicklung								
236	**TL= VR**	**TL032**	**Weiterentwicklung Register/Kohorte**	(1) Gef. Datenminimier. (2) Gef. Verfügbarkeit (3) Gef. Integrität **(4) Gef. Vertraulichkeit** (5) Gef. Nichtverkettung (6) Gef. Transparenz (7) Gef. Intervenierbark.	**Allgemeine TOM** a. Umsetzung durch geschultes Personal b. DV in Geschützten Räumen **Spez. TOM wg. Vertraulichkeit** c. Umsetzung bzw. Veranlassung nur d. Be-handelnde und Erfüllungsgehilfen	Über-schaubar	Über-schaubar	**Tragbares Risiko**
237	UC=VV	UC0149	Aktualisierungen und Projekte abstimmen		Siehe TOM zu Verarbeitungsrubrik TL032			
238	UC=VV	UC0245	Change Request bearbeiten		Siehe TOM zu Verarbeitungsrubrik TL032			

Nr.	Typ TL/UC=	Iden-tifier	Verarbeitungsphase Verarbeitungsrubrik (Top-Level-Aufgabe, TL=VR) / Verarbeitungsvorgang (Use Case, UC=VV)	Risiken Gef. = Gefährdung der … Gef. = besondere Gefährd.	Abhilfemaßnahme [Techn. und Organisat. Maßn.: TOM]	Eintrittsw. Restrisiko	Schweregr. Restrisiko	Risiko-kategorie
239	UC=VV	UC0247	Datenbank versionieren		Siehe TOM zu Verarbeitungsrubrik TL032			
6. Abschluss								
241	**TL= VR**	**TL034**	**Archivierung**	(1) Gef. Datenminimier. (2) Gef. Verfügbarkeit (3) Gef. Integrität **(4) Gef. Vertraulichkeit** (5) Gef. Nichtverkettung (6) Gef. Transparenz **(7)** Gef. Intervenierbark.	**Allgemeine TOM** a. Umsetzung durch geschultes Personal b. DV in Geschützten Räumen **Spez. TOM wg. Vertraulichkeit** c. Umsetzung bzw. Veranlassung nur d. Be-handelnde und Erfüllungsgehilfen	Über-schaubar	Über-schaubar	**Tragbares Risiko**
242	UC=VV	UC0157	Archivierung der Datenbank vorbereiten		Siehe TOM zu Verarbeitungsrubrik TL034			
243	UC=VV	UC0158	Abschließende Datenexporte durchführen		Siehe TOM zu Verarbeitungsrubrik TL034			
244	UC=VV	UC0159	Daten bzw. Dokumente archivieren		Siehe TOM zu Verarbeitungsrubrik TL034			
245	UC=VV	UC0160	Auf archivierte Dokumente zugreifen		Siehe TOM zu Verarbeitungsrubrik TL034			
246	UC=VV	UC0161	Archivierte Dokumente vernichten		Siehe TOM zu Verarbeitungsrubrik TL034			
247	**TL= VR**	**TL035**	**Vernichtung der Daten, Anonymisierung**	(1) Gef. Datenminimier. (2) Gef. Verfügbarkeit (3) Gef. Integrität **(4) Gef. Vertraulichkeit** (5) Gef. Nichtverkettung (6) Gef. Transparenz (7) Gef. Intervenierbark.	**Allgemeine TOM** a. Umsetzung durch geschultes Personal b. DV in Geschützten Räumen **Spez. TOM wg. Vertraulichkeit** c. Umsetzung bzw. Veranlassung nur d. Be-handelnde und Erfüllungsgehilfen	Über-schaubar	Über-schaubar	**Tragbares Risiko**
248	UC=VV	UC0162	Daten vernichten		Siehe TOM zu Verarbeitungsrubrik TL035			
249	UC=VV	UC0163	Daten anonymisieren		Siehe TOM zu Verarbeitungsrubrik TL035			
250	UC=VV	UC0246	Daten an Nachfolge-Organisation weitergegeben		Siehe TOM zu Verarbeitungsrubrik TL035			
251	UC=VV	UC0164	Daten deaktivieren		Siehe TOM zu Verarbeitungsrubrik TL035			

Nr.	Typ TL/UC=	Iden-tifier	Verarbeitungsphase Verarbeitungsrubrik (Top-Level-Aufgabe, TL=VR) / Verarbeitungsvorgang (Use Case, UC=VV)	Risiken Gef. = Gefährdung der … Gef. = besondere Gefährd.	Abhilfemaßnahme [Techn. und Organisat. Maßn.: TOM]	Eintrittsw. Restrisiko	Schweregr. Restrisiko	Risiko-kategorie
225	**TL= VR**	**TL036**	**Close Out**	(1) Gef. Datenminimier. (2) Gef. Verfügbarkeit (3) Gef. Integrität **(4) Gef. Vertraulichkeit** (5) Gef. Nichtverkettung (6) Gef. Transparenz (7) Gef. Intervenierbark.	**Allgemeine TOM** a. Umsetzung durch geschultes Personal b. DV in Geschützten Räumen **Spez. TOM wg. Vertraulichkeit** c. Umsetzung bzw. Veranlassung nur d. Be-handelnde und Erfüllungsgehilfen	Über-schaubar	Über-schaubar	**Tragbares Risiko**
253	UC=VV	UC0165	Schließung eines Zentrums vorbereiten		Siehe TOM zu Verarbeitungsrubrik TL036			
254	UC=VV	UC0166	Zentrum schließen		Siehe TOM zu Verarbeitungsrubrik TL036			
255	UC=VV	UC0167	Schließung Zentrum nachbereiten und dokumentieren		Siehe TOM zu Verarbeitungsrubrik TL036			