

Datenschutzkonzept¹

Deutsches Mukoviszidose-Register

(Stand: 01..03.2025)

Version	3.1
Projekt	Deutsches Mukoviszidose-Register (DMR)
Medizinische Leitung	Prof. Dr. Lutz Nährlich Zentrum für Kinderheilkunde und Jugendmedizin Universitätsklinikum Giessen-Marburg GmbH
Autor/innen	Dr. Miriam Schlangen / Manuel Burkhart Mukoviszidose Institut gemeinnützige Gesellschaft für Forschung und Therapieentwicklung mbH Tochtergesellschaft des Mukoviszidose e.V. In den Dauen 6 53117 Bonn Dr. Kai Kronfeld (IZKS), Mainz UNIVERSITÄTSMEDIZIN der Johannes Gutenberg-Universität Mainz Interdisziplinäres Zentrum Klinische Studien (IZKS) Langenbeckstraße 1 55131 Mainz Dirk Schlüchter sicdata Unternehmensberatung Heiligenstock 34c 42697 Solingen Michael Volk axaris – software & systeme GmbH Max-Eyth-Weg 2 89160 Dornstadt
Betreiber ²	Mukoviszidose Institut gGmbH (MI) In den Dauen 6 53117 Bonn

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. Schuler 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

Versionshistorie

Versions-Nr.	Inhalte	Datum
3.01	Fehlerkorrekturen	01.01.2019
3.02	Löschung der Daten wurde spezifiziert	01.04.2019
3.03	MDAT Hosting Anbieterwechsel, Anpassung Adresse	01.11.2021
3.1	Integration der Datenströme des Patientenportals MUKOme, Technische Komponenten aktualisiert, Neustrukturierung des Dokuments und Anpassung an die überarbeitete Version des OSSE-Datenschutzkonzepts, Fehlerkorrekturen, redaktionelle Anpassungen, Entfernung des Abschnitts zum manuellen Importtool „MUKO Importer“, Ergänzung des Dokuments um eine DSFA	01.03.2025

Inhaltsverzeichnis

1	EINLEITUNG	6
1.1	Zielsetzung des vorliegenden Dokuments	6
1.2	Krankheitsbild Mukoviszidose	7
1.3	Zielsetzung und Zweck der Datenverarbeitung im Deutschen Mukoviszidose Register	7
1.4	Rechtsgrundlage	8
1.5	Überblick über die Datenverarbeitung	8
1.6	Bewertung der Zweckmäßigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge	9
1.7	Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen	9
1.8	Aufklärung und Einwilligung Registerteilnahme	10
2	ORGANISATIONSSTRUKTUR DES DEUTSCHEN MUKOVISZIDOSE-REGISTERS	11
2.1	Mukoviszidose e.V. - Träger	11
2.2	Mukoviszidose Institut - Registerbetreiber	11
2.3	Leitungsgremium (Registerstelle)	12
2.4	Wissenschaftlicher Beirat / Data Access Committee – AG Register	13
2.5	Registrierte Personen	13
2.6	Meldende Stellen - Teilnehmende Mukoviszidose Einrichtungen	13
2.7	Datennutzende	14
2.8	Vertrauensstelle	14
2.9	Systemadministration	15
2.10	Datenmanagement / Transferstelle	15
2.11	Deutsches Mukoviszidose-Register Historie	15
3	DATENVERARBEITENDE KOMPONENTEN	17
3.1	Registersoftware – MUKOweb	17
3.1.1	<i>Komponenten und Funktionen</i>	17
3.1.2	<i>Betrieb der Komponenten</i>	18
3.1.3	<i>Workflow</i>	19
3.1.4	<i>Benutzer, Rollen und Rechte</i>	19
3.2	Pseudonymisierungs- und Identitätsmanagement	20
3.2.1	<i>Pseudonyme</i>	20
3.2.2	<i>Manuelles Linken</i>	20
3.3	Einwilligungsmanagement	20
3.4	Registerverzeichnis	21

4	DATENVERARBEITENDE PROZESSE	22
4.1	Manuelle Dateneingabe	22
4.1.1	Anlegen eines Patienten.....	22
4.1.2	Erfassung der Einwilligung	22
4.1.3	Erfassung der medizinischen Daten	22
4.2	Datenimport	22
4.3	Pseudonymisierung.....	23
4.3.1	Manuelle Patientenregistrierung	23
4.3.2	Pseudonymisierung beim Datenimport über MUKO.Importer.....	24
4.3.3	Registrierungsverfahren MUKOme Patientenportal	25
4.4	Datenexport und Nutzung	26
4.4.1	Datenexport.....	26
4.4.2	Datennutzung.....	26
4.4.3	Datenzugriff durch Administrierende.....	27
5	WEITER MAßNAHMEN ZUM DATENSCHUTZ	28
5.1	Informelle Gewaltenteilung.....	28
5.2	Autorisierung und Authentifizierung	28
5.2.1	Autorisierung von Benutzern	28
5.2.2	Autorisierung von Komponenten	28
5.2.3	Authentifizierung von Benutzern	28
5.2.4	Authentifizierung von Komponenten	29
5.3	Maßnahmen in der IT-Infrastruktur	29
5.3.1	Sicherheit der gespeicherten Daten	29
5.3.2	Sicherheit der Kommunikation	29
5.3.3	Protokollierung.....	30
5.4	Maßnahmen in der IT-Infrastruktur	30
6	Wahrung von Betroffenenrechten	31
6.1	Aufklärung und Einwilligung	31
6.2	Auskunfts-, Berichtigungs- Widerspruchs- und Beschwerderechte	31
6.3	Widerruf, Löschung, Anonymisierung.....	33
6.4	Dauer der Speicherung.....	33
7	ANHANG	34
7.1	Patienteneinwilligung.....	34
7.2	Weitere mitgeltende Dokumente.....	34
7.3	Datensatz DMR.....	34

7.3.1 *Medizinische Daten* 34

7.3.2 *Identifizierende Daten* 34

7.4 Rollen und Aufgaben im DMR 35

7.5 Technische und organisatorische Maßnahmen (TOMs) 36

8 ANHANG: TABELLARISCHE DATENSCHUTZ-FOLGEABSCHÄTZUNG 37

8.1 Gesetzliche Vorschrift betreffend DSFA und Definition für vorliegendes Dokument 37

8.2 Festlegung Schutzbedarf..... 39

8.3 Einschätzung und Bewertung der Risiken 39

8.4 DSFA-Tabelle mit Datenverarbeitung und Risikominimierung 41

1 EINLEITUNG

1.1 Zielsetzung des vorliegenden Dokuments

Das Deutsche Mukoviszidose-Register (DMR) 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.

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 ist². Ferner wird der Deklaration der Datenschutzkonferenz gefolgt, wonach eine DSFA kein einmaliger Vorgang ist. In diesem Sinne befasst sich das vorliegende Datenschutzkonzept mit den Datenverarbeitungsstrukturen und -prozessen des DMR.

Als Grundlage der technischen Infrastruktur für das Register dient die Registersoftware MUKOweb (tripletrax) der Firma axaris³, die auch für andere Register, eingesetzt wird.

Das vorliegende Dokument beachtet die sieben Gewährleistungsziele des Standarddatenschutzmodells der Datenschutzkonferenz des Bundes und Länder und die darin abgebildeten zentralen Datenschutzerfordernisse der DSGVO. Die sieben angestrebten Gewährleistungsziele sind: Datenminimierung, Verfügbarkeit, Integrität, Vertraulichkeit, Nichtverkettung, Transparenz, Intervenierbarkeit⁴.

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 DMR dar.

² 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 Datenschutzerfordernisse der DSGVO. Die sieben angestrebten Gewährleistungsziele sind: Datenminimierung, Verfügbarkeit, Integrität, Vertraulichkeit, Nichtverkettung, Transparenz, Intervenierbarkeit.

³ www.axaris.de

⁴ Überprüfung und Wiederholung des DSFA bei Änderungen fordert Art. 35 Abs. 11 DSGVO

1.2 Krankheitsbild Mukoviszidose

In Deutschland sind rund 8.000 Kinder, Jugendliche und Erwachsene von der unheilbaren Erbkrankheit Mukoviszidose betroffen. Durch eine Störung des Salz- und Wassertransports in die Körperzellen bildet sich bei Menschen mit Mukoviszidose ein zähflüssiges Sekret, das Organe wie die Lunge oder die Bauchspeicheldrüse irreparabel schädigt. Jedes Jahr werden rund 200 Kinder mit der seltenen Krankheit geboren.

1.3 Zielsetzung und Zweck der Datenverarbeitung im Deutschen Mukoviszidose Register

Vor dem Hintergrund eines Mangels an Wissen über die Mukoviszidose verlangt die ärztliche und gesellschaftliche Verantwortung für die Betroffenen die Beobachtung von Krankheitsverläufen über lange Zeiträume. Nur durch die Forschung in standortübergreifenden Verbünden mit ausreichenden Fallzahlen kann auch bei Seltenen Erkrankungen wie bei der Mukoviszidose sinnvoll klinisch wie auf dem Gebiet der Grundlagen geforscht werden. Auch für die Versorgung und gesundheitspolitische Planung sind verlässliche Informationen zur Häufigkeit bestimmter Ausprägungsmuster, zum Gesundheitszustand, etc. von größter Wichtigkeit.

Ziel des DMR ist es, durch eine strukturierte und flächendeckende Erfassung und statistische Auswertung der Registerdaten, Mukoviszidose und damit verbundene Gesundheitsstörungen zu diagnostizieren, zu behandeln oder zu heilen und damit die Gesundheit von Patientinnen und Patienten der Klinik zu schützen, aufrechtzuerhalten oder wiederherzustellen. Primäre Ziele sind:

- die Versorgungssituation von Patienten mit Mukoviszidose in Deutschland zu erfassen, zu analysieren und zu verbessern,
- die erhobenen Daten als Grundlage für Versorgungsforschung, Therapieentwicklung und Arzneimittelsicherheitsüberwachung bereitzustellen,
- die Registerdaten für Patienten und Therapeuten in jährlich erscheinenden Berichtsbänden aufzubereiten und transparent darzustellen.

Im DMR kann die behandelnde Ärztin bzw. Arzt eine Zusammenstellung der gespeicherten Informationen zum Krankheitsverlauf (Mukoviszidose-Historie) und einen Patientenschnellstatus zum jeweiligen Verlauf der Mukoviszidose-Erkrankung abrufen. Dem Behandler werden die individuellen Patientendaten mit den im Register zusammengeführten Daten zum Krankheitsverlauf anderer Patienten, z.B. derselben Altersgruppe bzw. Schweregrades zurückgemeldet. Diese Vergleichsdaten dienen im Rahmen der patientenindividuellen Behandlung der Erkennung von Auffälligkeiten und Besonderheiten.

Des Weiteren dienen die Registerdaten als Grundlage für:

- Wissenschaftliche Forschungsvorhaben
- Projekt Benchmarking (Vergleich zwischen den Ambulanzen / Lernen von den Besten)
- Beteiligung am europäischen Mukoviszidose-Register (ECFS Patient Registry)
- Public Reporting für Mukoviszidose Betroffene
- Registry-embedded clinical Studies
- Post-Authorisation Efficacy Study (PAES)
- Post-Authorisation Safety Studies (PASS)

Die beschriebenen Projekte und wissenschaftlichen Forschungsvorhaben werden mit dem Ziel durchgeführt, zusätzliche Erkenntnisse über die Krankheit, die Sicherheit und den Nutzen von verabreichten Arzneimitteln im Vergleich zu anderen Therapien gewinnen zu können. Hierfür werden die pseudonymisierten medizinischen Daten ein weiteres Mal durch das Datenmanagement pseudonymisiert, so dass kein Rückschluss auf die **Personen und die betreuenden Ambulanzen möglich ist**. Die wissenschaftlichen Projekte werden durch das MI und die AG Register (ein wissenschaftliches Gremium des Mukoviszidose e.V.) inhaltlich bewertet und vertraglich mit den Antragstellern im Sinne des Patienten geregelt.

1.4 Rechtsgrundlage

Die informierte Einwilligung der zu registrierenden Personen (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 faktisch anonymisierten Daten zu Forschungszwecken wird in der Einwilligung berücksichtigt, da speziell im Bereich der Mukoviszidose 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 nachgeholt informierten Einwilligung zur Übermittlung in das und zur Nutzung im Deutschen Mukoviszidose-Register beruhen.

1.5 Überblick über die Datenverarbeitung

Im DMR werden Daten von Patienten⁵, die in den teilnehmenden Mukoviszidose Ambulanzen behandelt werden, erhoben und verarbeitet. Die Daten werden auf folgende Weise in das Register erfasst:

- manuell über die web-basierte MUKOweb-Benutzer-Schnittstelle

Folgende Arten von Daten werden erhoben:

- Identifizierende Daten (IDAT): Sie enthalten primär demografische Daten (Name, Vorname, Geburtsdatum, Geburtsort, Mobilfunknummer, eMailadresse), die eine eindeutige Identifikation des Patienten erlauben. Sie werden nicht im Register, sondern separat in einem Pseudonymisierungs- und Identitätsmanagement gespeichert und verwaltet.
- Medizinische Gesundheitsdaten (MDAT): Dazu gehören alle routinemäßig erhobenen Daten, die über die Erkrankung und deren Verlauf im Register 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 Abschnitt 7.1.

Alle Datenfelder, die im Register erfasst werden, sind in einem Metadaten-Repository registriert und definiert. Die erfassten Daten sind für alle Nutzer und Patienten zugänglich. Die Registerstruktur (Formulare zur strukturierten Erfassung von Daten) wird mithilfe von MUKOweb dynamisch festgelegt und zentral gespeichert.

Daten im DMR werden zu Auswertungszwecken ausschließlich mit nicht-rückführbaren Pseudonymen, anonymisiert oder in bereits aggregierten Berichten exportiert. Das Deutschen Mukoviszidose-

⁵ Gemeint sind grundsätzlich entsprechende Personen beider Geschlechter; auf eine neutrale Formulierung wurde aus sprachlichen Gründen verzichtet.

Register unterstützt interne und externe Registeranfragen, mit der im Register nach definierten Fällen gesucht werden kann.

1.6 Bewertung der Zweckmäßigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge

In Art. 35 Abs. 7 lit. b DSGVO wird gefordert, dass die „Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck“ vorgenommen wird: In Deutschland existieren nur Schätzungen, wie viele Menschen mit Mukoviszidose in Deutschland leben.

Es gibt im deutschen Gesundheitssystem mit vielen Tausenden Leistungserbringern und vielen Dutzend Leistungsfinanzierern, die jeweils getrennte Datensilos führen, keine epidemiologische Übersicht, die neben dem DMR verlässliche und/oder öffentlich zugänglichen Analysen der Versorgungssituation von Menschen mit Mukoviszidose ermöglichen. Für den Zweck der epidemiologischen Übersicht über die Inzidenz und Prävalenz von Menschen mit Mukoviszidose ist es notwendig und verhältnismäßig, ein nationales Register aufzubauen, das, unter anderem, von allen dem Registerbetreiber bekannten Mukoviszidose Ambulanzen unterstützt wird.

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.

Weiterhin dient das Register den unter Abschnitt 3.1 beschriebenen Zielsetzungen, die in Ihrer Gesamtheit, die Verbesserung der Versorgungssituation von Menschen mit Mukoviszidose zum Ziel haben.

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

Hier wird die in Art. 35 Abs. 7 lit. c DSGVO 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 DMR 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 DMR 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 DMR 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.

1.8 Aufklärung und Einwilligung Registerteilnahme

Für die Teilnahme am Deutschen Mukoviszidose-Register wird jeder Patient und/oder die Eltern/gesetzlichen Vertreter des Patienten vom behandelnden Arzt über Wesen, Ziele, erwartete Vorteile, mögliche Risiken und Zeitdauer des Registerverfahrens informiert (Einwilligungserklärungen siehe Anhang).

Vorgehen bei nicht-einwilligungsfähigen Patienten

Bei minderjährigen Patienten werden die Eltern/gesetzlichen Vertreter aufgeklärt und sofern sie der Teilnahme am Registerverfahren zustimmen möchten, können sie die Einwilligungserklärung unterschreiben. Der mutmaßliche Wille des Patienten ist zu berücksichtigen. Soweit der Minderjährige selbst in der Lage ist, Wesen, Bedeutung und die Tragweite der Einwilligung zu erkennen und seinen Willen hiernach zu bekunden, wird zusätzlich auch er in angemessener Form aufgeklärt und kann seine Einwilligung erteilen.

Einwilligung zur Registerteilnahme

Dem Patienten und/oder den Eltern/gesetzlichen Vertretern muss ausreichend Zeit und Gelegenheit gegeben werden, um vor der Registermeldung über seine Teilnahme zu entscheiden und offene Fragen zu klären. Die Einwilligungserklärung wird vom Patienten und/oder von beiden Elternteilen/gesetzlichen Vertretern sowie vom behandelnden Arzt eigenhändig datiert und unterzeichnet.

2 ORGANISATIONSSTRUKTUR DES DEUTSCHEN MUKOVISZIDOSE-REGISTERS

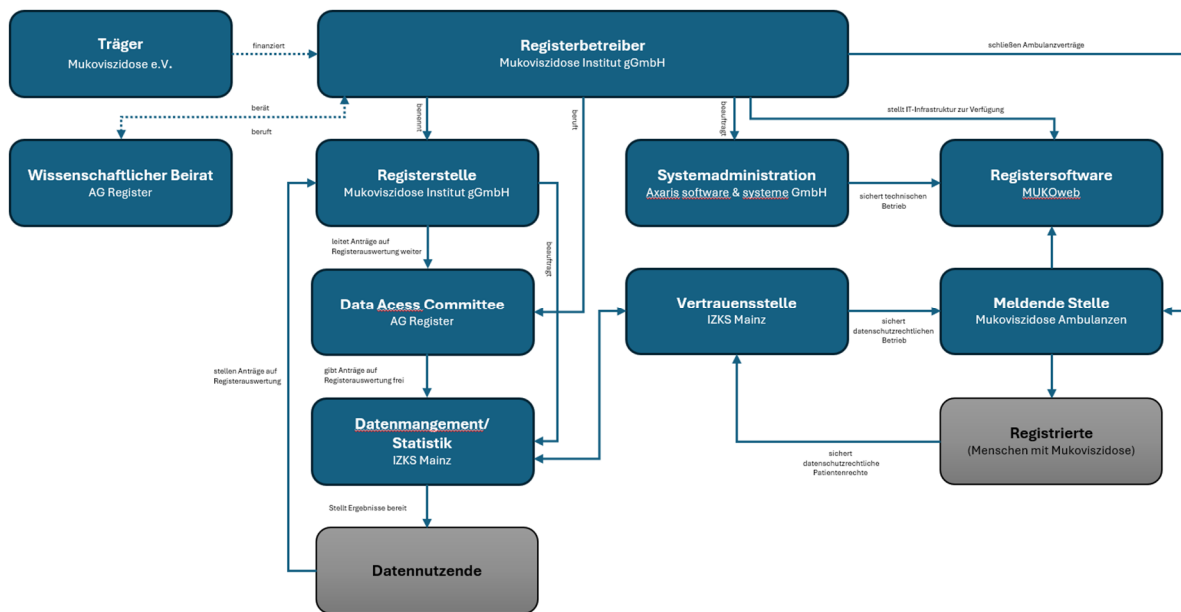


Abbildung 1 Organisationsstruktur Mukoviszidose-Register

2.1 Mukoviszidose e.V. - Träger

Aktueller Träger des Vorhabens ist der Mukoviszidose e.V. - Bundesverband Cystische Fibrose (CF) in Bonn.

Der Mukoviszidose e.V. vernetzt die Menschen mit Mukoviszidose, ihre Angehörigen, Ärzte, Therapeuten und Forscher. Er bündelt unterschiedliche Erfahrungen, Kompetenzen sowie Perspektiven mit dem Ziel, jedem Betroffenen ein möglichst selbstbestimmtes Leben mit Mukoviszidose ermöglichen zu können. Damit die gemeinsamen Aufgaben und Ziele erreicht werden können, ist der gemeinnützige Verein auf die Unterstützung engagierter Spender und Förderer angewiesen. Weitere Informationen hierzu finden Sie unter www.muko.info/spenden.

2.2 Mukoviszidose Institut - Registerbetreiber

Aktueller Registerbetreiber, und damit Verantwortlicher im Sinne des Art. 4 DSGVO ist die Mukoviszidose Institut gemeinnützige Gesellschaft für Forschung und Therapieentwicklung mbH (MI). Das MI ist eine gemeinnützige 100%ige Tochtergesellschaft des Mukoviszidose e.V. Sie erbringt professionell Dienstleistungen im Bereich der Forschung und des Qualitätsmanagements, um neue Therapieansätze zu ermöglichen und die bestehende Therapie zu optimieren mit dem Ziel, die Lebenszeit und die Lebensqualität von Patienten/innen mit Mukoviszidose zu verbessern. Das MI wurde durch den Mukoviszidose e.V. mit der Planung und Koordination des Mukoviszidose-Registers beauftragt und tritt gegenüber den beteiligten Mukoviszidose Einrichtungen als Ansprechpartner und Registerbetreiber auf.

Im Falle einer betriebswirtschaftlichen Auflösung des MI wird durch den Bundesvorstand des Mukoviszidose e.V. ein neuer Registerbetreiber bestimmt. Die Koordination des Registers obliegt in diesem Fall bis auf weiteres dem Mukoviszidose e.V. Bei der Auflösung des Mukoviszidose e.V. werden die medizinischen (MDAT) Daten an einen neu zu bestimmenden Datentreuhänder übergeben und nach

einer Sperrfrist von 1 Jahr gelöscht. Die Identitätsdaten der Patienten (IDAT) verbleiben bis zu diesem Zeitpunkt im Identitätsmanagement und werden zeitgleich gelöscht. Die Beauftragung erfolgt durch den neu zu bestimmenden Datentreuhänder.

Registrierte Personen werden über einen möglichen Wechsel der Trägerschaft rechtzeitig informiert und können in diesem Fall ihre Einwilligung in die Verarbeitung ihrer Daten im DMR widerrufen (vgl. Abschnitt 6.3 „Widerruf, Löschung, De-Identifizierung“).

Das gesamte Registerverfahren wurde durch die zuständigen Datenschutzbehörden, den Datenschutzbeauftragten der Mukoviszidose Institut gGmbH (Firma SicData, Solingen) datenschutzrechtlich geprüft und freigegeben. Die Fa. SicData - Datenschutz und IT-Sicherheit berät das MI als zuständiger Datenschutzbeauftragter.

Der Betreiber stellt die Registerinfrastruktur und die Registersoftware MUKOweb den teilnehmenden Zentren zur Verfügung. Der Betreiber koordiniert und organisiert Anfragen zur Auswertung von Registerdaten und/oder Erhebungen von studienspezifischen Registerdaten. Der Betreiber entscheidet über die Teilnahme am DMR. Er ist Vertragspartner gegenüber den durchführenden Dienstleistern (Datenmanagement, Datenhosting, Softwareentwickler etc.). Der Betreiber wird durch die AG-Register und dessen Leitungsgremium bei der Entwicklung, strategischen Planung und Durchführung des Registers unterstützt.

Registerbetreiber

Mukoviszidose Institut gGmbH
In den Dauen 6
53177 Bonn
Tel.: +49 (0) 228-9878-0
Fax: +49 (0) 228-9878-77
Mail: register@muko.info

2.3 Leitungsgremium (Registerstelle)

Der TFQ-Beirat⁶ des Mukoviszidose e.V. wählt den medizinischen Leiter und dessen medizinischen Stellvertreter mit einfacher Mehrheit aus dem Kreis der im TFQ-Beirat vertretenen AGAM-Mitglieder⁷. Geborenes Mitglied der des Leitungsgremiums ist die Geschäftsführung der Mukoviszidose Institut gGmbH oder deren benannte Vertretung. Das Leitungsgremium wird für die Dauer von drei Jahren bestimmt und muss anschließend durch den TFQ-Beirat bestätigt oder neu gewählt werden.

Das Leitungsgremiums des DMR ist die vom Registerbetreiber ernannte Arbeitsgruppe, die den Registerbetrieb des DMR sowie die Datennutzung koordiniert, einschließlich der Kommunikation mit

⁶ Der TFQ-Beirat ist das zentrale Beratungsgremium des Bundesvorstandes in allen Angelegenheiten der Therapieoptimierung und -qualität. Er setzt sich aus Vertretern der im Verein angesiedelten Gremien zusammen und verbindet so die Expertise der Behandler/innen mit der der in der Selbsthilfe engagierten Betroffenen und Angehörigen.

⁷ Die AGAM vertritt die Ärztinnen und Ärzte innerhalb des Mukoviszidose e.V. Zu ihren Aufgaben gehören die Optimierung der medizinischen Versorgung sowie die Verbesserung von Diagnostik und Therapie der Mukoviszidose. Darüber hinaus vertritt die AGAM die Interessen der AGAM-Mitglieder innerhalb des Mukoviszidose e.V. und nach außen.

der AG Register/Data Access Committee, des Datenmanagements/der Transferstelle, der Vertrauensstelle und der Systemadministration.

2.4 Wissenschaftlicher Beirat / Data Access Committee – AG Register

Die Mitglieder der AG-Register werden durch die Mitglieder des Leitungsgremiums vorgeschlagen und mit einfacher Mehrheit durch den TFQ-Beirat bestätigt. Die Teilnahme an der AG-Register ist nicht auf Mitglieder des TFQ-Beirats beschränkt. Interessierte können sich direkt mit dem Leitungsgremium in Verbindung setzen.

Die AG-Register Mitglieder werden für die Dauer von 3 Jahren benannt. Sollte für spezifische Projektanforderungen zusätzliche Expertise benötigt werden, können weitere Mitglieder als temporäre Mitglieder der AG-Register durch das Leitungsgremium vorgeschlagen werden. Auch zusätzliche Mitglieder müssen durch einfache Mehrheit des TFQ-Beirats bestätigt werden.

Das Leitungsgremium und die AG-Register beraten den Registerbetreiber bei der Entwicklung, strategischen Planung und Durchführung des Registers. Bei der finanziellen und strategischen Entwicklung des Deutschen Mukoviszidose-Registers einschl. externer Kooperationen sowie der Berichterstattung gegenüber dem Mukoviszidose e.V. sind die AG-Register, das Leitungsgremium der AG-Register und die Mukoviszidose Institut gGmbH zu gegenseitiger Information und Einvernehmen verpflichtet.

Die AG-Register und das Leitungsgremium entscheiden über alle internen und externen Registeranfragen (Nutzungsanträge). Die Regelungen sind in der „Verfahrensordnung Registerstudien“ beschrieben. Das Leitungsgremium erarbeitet und aktualisiert die Geschäfts-, Publikations- und Gebührenordnung. Der medizinische Leiter des Registers wird als Mitglied des Leitungsgremiums und im Einvernehmen mit dem Bundesvorstand des Mukoviszidose e.V., als „National Coordinator“ für die ECFS in den für das Register relevanten Gremien aktiv.

2.5 Registrierte Personen

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

Einschlusskriterien:

- Mukoviszidose
(gemäß AWMF-Leitlinie 026/023 Diagnose der Mukoviszidose vom Juli 2023)
- CFSPID
(CF – Screening positive, inconclusive diagnosis) (gemäß Munck, J Cyst Fibros 2015)
- CFTR-assoziierte Erkrankung
(gemäß AWMF-Leitlinie 026/023 Diagnose der Mukoviszidose vom Juli 2023)

2.6 Meldende Stellen - Teilnehmende Mukoviszidose Einrichtungen

Meldende Stellen sind die Mukoviszidose Einrichtungen (Kliniken/Zentren), welche Daten in das DMR eingeben. Eine aktuelle Liste der am DMR beteiligten Stellen ist unter <https://www.muko.info/leben-mit-cf/adressen/cf-einrichtungen> zu finden.

Die teilnehmenden Stellen identifizieren sich über ein durch das Datenmanagement bereitgestelltes Formular per Fax. Das Formular beinhaltet eine Erklärung zur Einhaltung der geltenden Regeln des Datenschutzes. Nach Erhalt des Faxes werden durch das Datenmanagement der Ambulanz personalisierte User-ID's und Passwörter zur Verfügung gestellt. Eine Übersicht über die eingetragenen Nutzer ist durch den Registerbetreiber jederzeit einsehbar. Die autorisierten Personen (Ärzte/Dokumente) dokumentieren die medizinischen Daten in der webbasierten Registersoftware.

Die am Registerverfahren beteiligten Mukoviszidose-Einrichtungen werden durch bereits bestehende Ambulanz- und Lizenzverträge vertraglich zur Dateneingabe verpflichtet. Für das medizinische und nicht-medizinische Personal gelten die datenschutzrechtlichen Regeln der Klinik.

Teilnehmende Mukoviszidose Einrichtungen können interne Registeranfragen an das Deutsche Mukoviszidose-Register stellen. Die Anträge werden durch die AG Register inhaltlich bewertet und freigegeben. Vgl. hierzu Abschnitt 7 „Geschäftsordnung des Deutschen Mukoviszidose-Registers“.

Generell können alle Mitglieder der meldenden Stellen als Registrierende das DMR nutzen, wobei die meldenden Stellen selbst entscheiden, welche Mitglieder, nach Prüfung und Zustimmung durch die Registerstelle des DMR, 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.

2.7 Datennutzende

Datennutzende sind natürliche oder juristische Personen, die an dem Registerprojekt beteiligt sind und durch Abschluss eines Ambulanzvertrags Vertragspartei zum DMR werden oder die im Rahmen einer genehmigten Registeranfrage Daten des DMR nutzen. Sie stellen Registeranfragen zur Nutzung von Daten des DMR für wissenschaftliche Zwecke an die Registerstelle.

2.8 Vertrauensstelle

Die Vertrauensstelle dient neben den behandelnden Ärzten als zentrale Anlaufstelle für die im Register dokumentierten Patienten. Die speziell autorisierten und zur Verschwiegenheit verpflichteten Beauftragten der Vertrauensstelle haben Einblicke in die durch den behandelnden Arzt dokumentierten Daten und können, soweit dies für den ordnungsgemäßen Betrieb des DMR notwendig ist, Einsicht in die medizinischen Gesundheitsdaten nehmen. Die Vertrauensstelle nutzt die personenidentifizierenden Daten für registerbezogene und administrative Prozesse, beispielsweise um doppelte Einträge von Patienten im Register zu vermeiden. Die Einhaltung aller datenschutzrechtlichen Aspekte wird durch den zuständigen Datenschutzbeauftragten der Universitätsmedizin Mainz sichergestellt.

Vertrauensstelle Mukoviszidose-Register

Universitätsmedizin der Johannes-Gutenberg-Universität Mainz
Interdisziplinäres Zentrum Klinische Studien (IZKS)
Langenbeckstraße 1
55131 Mainz
Tel.: +49 (0) 6131 17-9906
Fax: +49 (0) 6131 17-9925
Mail: vertrauensstelle-mukoviszidose@izks-mainz.de

An die Vertrauensstelle können sich die Patienten wenden, um von Ihren Rechten im Sinne der DSGVO (vgl. Abschnitt 6.2 Auskunft über gespeicherte Daten) Gebrauch machen zu können.

2.9 Systemadministration

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

2.10 Datenmanagement / Transferstelle

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

2.11 Historie

Seit 1995 bildet das Projekt „Qualitätssicherung Mukoviszidose“ die Grundlage zur Beurteilung der Versorgungsqualität von Mukoviszidose Patienten in Deutschland. Insgesamt wurden in den vergangenen Jahren kontinuierlich jährliche Verlaufsdatensätze und Stammdaten von aktuell mehr als 7.500 Mukoviszidose Patienten erfasst.

2007 wurde die bestehende Registersoftware CFAS (Cystic Fibrosis Quality Ambulanz System) durch die Ambulanz- und Registersoftware „MUKO.dok“ abgelöst. „MUKO.dok“ wurde von der Arbeitsgruppe MUKO.dok des TFQ Beirates (Beirat des Mukoviszidose e.V. Therapieförderung und Qualität) entwickelt und durch den Dienstleister - die Firma axaris - software & systeme GmbH - programmiert. Die Software „MUKO.dok“ war in 83 Mukoviszidose Einrichtungen installiert und wurde dort betrieben. Die Softwarelizenz ist in Besitz des Mukoviszidose e.V.

2014 wurde durch den Bundesvorstand des Mukoviszidose e.V. beraten und entschieden die Registerdaten ab 2015 zentral in einer webbasierten Erfassungssoftware (MUKOweb) zu dokumentieren.

Als Grundlage für das aktualisierte DMR diene das generische Datenschutzkonzept der Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V. (TMF).

Seit 2017 läuft das Mukoviszidose-Register im Regelbetrieb. Es beteiligen sich bundesweit über 85 Mukoviszidose Einrichtungen am DMR. Das bisherige Verfahren wurde durch die Landesdatenschutzbeauftragten der Länder, im Umlaufverfahren durch den Datenschutzbeauftragten des Landes NRW freigegeben. Ein positives Ethikvotum der Ethikkommission der Justus-Liebig Universität in Gießen liegt vom 01.04.2019 (AZ 24/19) für das DMR liegt vor.

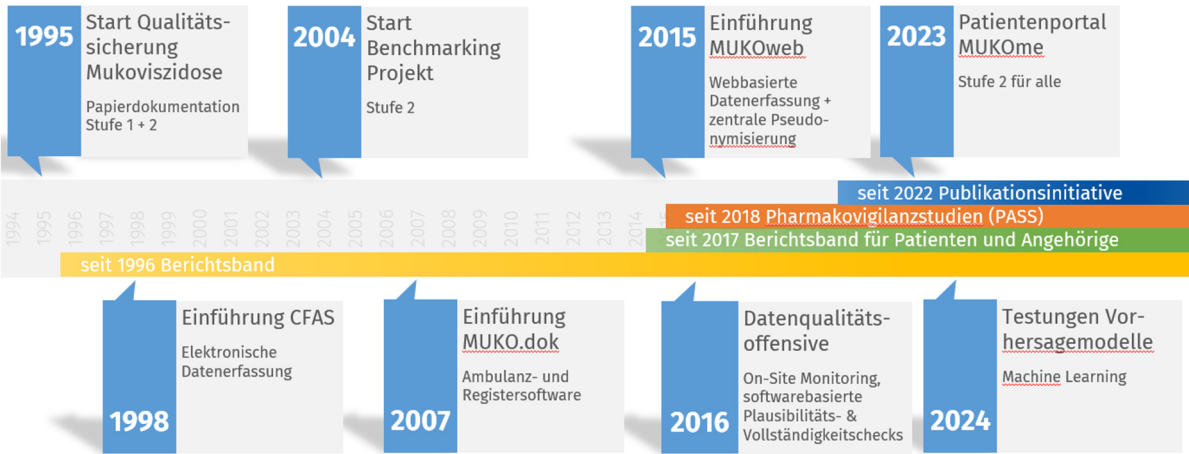


Abbildung 2: Meilensteine des Deutschen Mukoviszidose-Registers

3 DATENVERARBEITENDE KOMPONENTEN

Für die Erfassung, Verarbeitung, Pseudonymisierung und Speicherung der Daten sind im DMR verschiedene Stellen beauftragt. Durch eine institutionelle und organisatorisch getrennte Speicherung der identifizierenden und medizinischen Datenbestände, ist die Einhaltung des Datenschutzes jederzeit gewährleistet.

Das Datenschutzkonzept des DMR orientiert sich am generischen Datenschutzkonzept der Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V. (TMF) und der Schablone für OSSE-Datenschutzkonzepte in der überarbeiteten Fassung v2.0, Juni 2022. Ein positives Votum der TMF für das DMR liegt vor.

3.1 Registersoftware – MUKOweb

3.1.1 Komponenten und Funktionen

Im DMR werden die Registerdaten mit der speziell auf die Dokumentation von Mukoviszidose Patienten ausgelegten, webbasierten Registersoftware MUKOweb erfasst und auf unabhängigen Servern für IDAT und MDAT physisch getrennt voneinander gespeichert. Die Registersoftware MUKOweb dient der Erfassung und Speicherung medizinischer Stamm- und Verlaufsdaten (MDAT) von Menschen mit Mukoviszidose.

Die Eingabe der Daten erfolgt an den Standorten über die webbasierte Registersoftware MUKOweb; zusätzlich können Daten über ein Migrationstool für einen Datenimport erfasst werden. Alle Daten werden versioniert gespeichert, d.h. geänderte und gelöschte Werte bleiben in der Datenbank erhalten und können angezeigt werden.⁸

Identifizierende Daten (IDAT) werden nicht in der zentralen Registerdatenbank des DMR, sondern ausschließlich im Identitätsmanagement (vgl. Abschnitt 3.2 Pseudonymisierungs- und Identitätsmanagement) gespeichert. Die Kommunikation zwischen Identitätsmanagement und MUKOweb findet über den Webbrowser statt. Für den Benutzer erscheint die Eingabemaske des Identitätsmanagements integriert in die Benutzeroberfläche von MUKOweb. Das zurückgelieferte Pseudonym, wird mit den MDAT gespeichert. Da medizinische Daten behandlungsnah lokal erfasst werden, können IDAT und MDAT für den Behandler in der Mukoviszidose Einrichtung im Browser zusammen angezeigt werden. MUKOweb tauscht niemals Daten zwischen MDAT und IDAT direkt aus. Grundsätzlich wird jegliche Kommunikation zwischen dem lokalen Computer des Benutzers und den MDAT und IDAT-Datenbanken mit einem asymmetrisch operierenden Verschlüsselungsalgorithmus verschlüsselt. MUKOweb verwendet hierfür den Standard für verschlüsselte Kommunikationsverbindungen im Internet, das sog. https-Protokoll. Dieses basiert auf dem SSL/TLS-Algorithmus, einem hybriden Verschlüsselungsverfahren zur sicheren Datenübertragung.

MUKOweb erfüllt alle organisatorisch-technischen Maßnahmen des Datenschutzes. Das Konzept erfüllt zudem die Vorgaben des TMF-Datenschutzleitfadens für das klinische Modul zur versorgungs-/patientennahen klinischen Forschung. MUKOweb orientiert sich an den Leitlinien der „Good Clinical Practice (GCP)“.

⁸ Ausgenommen ist die Löschung auf Wunsch eines Patienten, siehe Anmerkungen zum Widerrufsrecht in Abschnitt 0.

Datenfelder und Formulare sind extern in einem DataDictionary registriert und beschrieben und können auch nach Start des laufenden Vorhabens modifiziert und ergänzt werden.

MUKOweb wird auf Basis der folgenden Kernkomponenten implementiert (Stand 01.01.2025):

MUKOweb/MUKOme Server
▪ Server Ubuntu 22.04 LTS ▪ Datenbanksystem: MariaDB 10.11.6 ▪ Webserver: Nginx 1.20.2 ▪ Programmlogik: PHP 8.3
MUKOweb Admin-Seite
▪ PHP Framework: Laravel 11.2 ▪ Layout von MUKOweb: SamrtAdmin (inkl. Bootstrap): 1.9.6
MUKOweb Dokumentations-Seite:
▪ PHP Framework: Laravel 11.23.3 ▪ Javascript Framework: Vue js 3.4.21 ▪ Inertia JS: 1.0.15 ▪ CSS Framework: Tailwind CSS 3.4.3
MUKOme
▪ PHP Framework: Laravel 11.16.0 ▪ Javascript Framework: Vue js 3.5.11 ▪ Layout von MUKOme: Vue Argon Dashboard PRO - 2.0.0

3.1.2 Betrieb der Komponenten

Den Betrieb der zentralen Komponenten des DMR übernehmen ausgewählte Institutionen, die in Absprache mit dem Registerbetreiber bestimmt werden. Dabei wird zum Zweck der informationellen Gewaltenteilung der organisatorisch unabhängige Betrieb von Identitätsmanagement und DMR gewährleistet (vgl. Abschnitt 5.1 Informelle Gewaltenteilung).

Der Betrieb des DMR erfolgt in der Verantwortung der Mukoviszidose Institut gGmbH

*Mukoviszidose Institut
gemeinnützige Gesellschaft für Forschung und Therapieentwicklung mbH
Tochtergesellschaft des Mukoviszidose e.V.
In den Dauen 6
53117 Bonn*

Die Registersoftware und Registerdatenbank des DMR werden auf einem angemieteten Server eines den Anforderungen des Bundesamts für die Sicherheit in der Informationstechnik (BSI) entsprechenden Rechenzentrum gehostet. Mit dem Anbieter besteht ein Vertrag zur Auftragsverarbeitung.

*Hetzner Online GmbH
Industriestr. 25
91710 Gunzenhausen*

Die Systemadministration der IT-Infrastruktur und der technische Support des DMR werden bereitgestellt durch

axaris – software & systeme GmbH
Max-Eyth-Weg 2
89160 Dornstadt

Der Betrieb des Pseudonymisierungs- und Identitätsmanagementstools Mainzliste⁹ sowie des zentralen Einwilligungsmanagements wird durch die Universitätsmedizin der Johannes-Gutenberg-Universität Mainz bereitgestellt

Universitätsmedizin der Johannes-Gutenberg-Universität Mainz
Interdisziplinäres Zentrum für Klinische Studien (IZKS)
Langenbeckstraße 1
55131 Mainz

3.1.3 Workflow

Medizinische Daten werden in Formularen für Stammdaten- und Verlaufsdaten erfasst. Die identifizierenden Daten werden in einem gesonderten Formular abgefragt.

3.1.4 Benutzer, Rollen und Rechte

MUKOweb verfügt über ein detailliertes Rollenkonzept, dass die Definition von lesende und/oder schreibende Zugriffsrechte bis auf Itemebene hinunter ermöglicht.

Die Zugriffsberechtigungen werden rollenbasiert durch die Systemadministration vergeben. Jeder Benutzer besitzt entsprechend seiner Funktion eine oder mehrere Rollen, mit denen er sich jeweils anmeldet. Für die Definition der Zugriffsrechte werden Daten insbesondere nach ihrer Zuordnung zu der informationellen Einheit in der sie erhoben klassifiziert. Für das DMR gibt es entsprechend der Einwilligungserklärung, den beteiligten Mukoviszidose Einrichtungen und organisatorischen Erfordernissen folgende Rollen:

- Administrator
- Dokumentar
- Observer
- Clinical Investigator
- Präsentationen

Die Rechte der einzelnen Rollen sind im Benutzerhandbuch für MUKOweb dokumentiert.

Alle Zugriffe werden protokolliert (vgl. Abschnitt 5.3 „Maßnahmen in der IT-Infrastruktur“).

⁹ <https://www.unimedizin-mainz.de/imbei/informatik/ag-verbundforschung/mainzliste.html>

3.2 Pseudonymisierungs- und Identitätsmanagement

Pseudonymisierung ist ein zur Aufrechterhaltung eines hohen Datenschutzniveaus notwendiger Schritt, um den Patienten vor Rückidentifizierung zu schützen. Anstelle seiner identifizierenden Daten (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 nach den eingestellten Schwellwerten, wird ein neuer Datensatz erzeugt oder ein vorhandener zurückgeliefert.

Bei unklaren Fällen muss die Mukoviszidose Einrichtung in Kontakt mit dem Identifikationsmanagement treten. Erst im Anschluss kann ein neuer Patient angelegt oder vervollständigt werden.

3.2.1 Pseudonyme

Das Identitätsmanagement nutzt als zentrale Komponente die ‚Mainzliste‘, einen webbasierten Pseudonymisierungsdienst erster Stufe. Sie erlaubt die Erzeugung von Personenidentifikatoren (PID) aus identifizierenden Attributen (IDAT). Die Mainzliste erfüllt die Anforderungen an die Patientenliste des revidierten Datenschutzkonzepts der TMF.

Die Mainzliste kommuniziert über eine REST-basierte Webschnittstelle mit der Onlineregistersoftware MUKOweb. Sie erzeugt für jeden Patienten einen eindeutigen Identifikator (PID) und je ein unabhängiges Pseudonym zweiter Stufe, in dem Daten des Patienten erfasst werden.

Die Mainzliste kann außerdem nicht-rückführbare Exportpseudonyme für den Export von Patientendaten zu Forschungszwecken erzeugen. Das zentrale Identitätsmanagement ermöglicht eine datenschutzgerechte Zusammenführung der zu verschiedenen Zeitpunkten und von verschiedenen Mukoviszidose Einrichtungen erfassten bzw. importierten patientenbeziehbaren Daten eines Patienten.

3.2.2 Manuelles Linken

Eine Schnittstelle der Mainzliste erlaubt es einem Menschen, Ergebnisse des automatischen Matching 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 Patienten) angezeigt und es besteht die Möglichkeit für das Datenmanagement und die Registerleitung, zur Entscheidungsfindung auf die pseudonymisierten medizinischen Daten zuzugreifen.

3.3 Einwilligungsmangement

Rechtsgrundlage der Datenverarbeitung im DMR 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 Einwilligungsmanagement im Identifikationsmanagement des DMR erfolgt mithilfe von MUKOweb. Dieses dient der Verarbeitung modular abgebildeter Einwilligungen und Widerrufe im Kontext des Registers. Die Erhebung der Einwilligungen als Rechtsgrundlage der Datenverarbeitung im DMR erfolgt bei den meldenden Stellen papierbasiert mit Verwahrung des Originals bei den meldenden Stellen. Im Anschluss werden die Informationen aus den Einwilligungserklärungen über eine webbasierte Benutzeroberfläche durch die meldenden Stellen in MUKOweb erfasst und gespeichert.

Die digitale Verwaltung der Einwilligungen und Dokumentation sowie die Verarbeitung der Widerrufe erfolgt unter Verantwortung des Identifikationsmanagements des DMR.

3.4 Registerverzeichnis

In einem Registerverzeichnis kann der Registerbetreiber das DMR 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 DMR ist in den folgenden Registerverzeichnissen registriert:

- HMA-EMA Catalogues of real-world data sources and studies¹⁰
- DKRS – Deutsches Register Klinischer Studien - Bfarm¹¹
- Registerdatenbank am BQS Institut¹²

¹⁰ <https://catalogues.ema.europa.eu/>

¹¹ https://www.bfarm.de/DE/Das-BfArM/Aufgaben/Deutsches-Register-Klinischer-Studien/_node.html

¹² <https://www.bqs.de/bqs-register/04-registersuche.php>

4 DATENVERARBEITENDE PROZESSE

4.1 Manuelle Dateneingabe

4.1.1 Anlegen eines Patienten

Eine berechnigte dateneingebende Person als Mitglied einer meldenden Stelle legt eine zu registrierende Person im DMR an, indem

- (1) der Benutzer die IDAT in die in MUKOweb integrierte Maske der Mainzelliste eingibt.
- (2) MUKOweb erhält ein Pseudonym (vgl. Abschnitt 4.3 „Pseudonymisierung“), das mit dem Datensatz gespeichert wird. Dabei erhält der Benutzer keine Rückmeldung, ob der Patient in der Mainzelliste bereits vorhanden war oder neu angelegt wurde.
- (3) Stellt die Mainzelliste Abweichungen bei der Eingabe der IDAT bei einem bereits gespeicherten Patienten fest, wird kein neues Pseudonym vergeben. Die Mukoviszidose Einrichtung muss in Kontakt mit dem Pseudonymisierungsdienst treten.

4.1.2 Erfassung der Einwilligung

Nach der Registrierung einer Person im DMR werden aus dem Einwilligungsmanagement die verfügbaren Vorlagen für Einwilligungen abgerufen (Template) und der dateneingebenden Person in einer in die Benutzeroberfläche des MUKOweb integrierte Eingabemaske angezeigt. Die dateneingebende Person dokumentiert die Einwilligung der registrierten Person (Consent) sowie das Einwilligungsdatum. Diese werden mit dem von der Mainzelliste generierten PID im Einwilligungsmanagement gespeichert. 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 DMR 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 in MUKOweb gespeichert werden.

4.2 Datenimport

Daten (z.B. Lungenfunktionsmessungen) aus vorhandenen Systemen können manuell in das DMR importiert werden. Die Datenübernahme durchläuft folgende Schritte eines sogenannten ETL¹³-Prozesses, wobei sich die Daten bis zum Import in das DMR immer auf den lokalen Systemen am jeweiligen Standort befinden:

- 1) Identifizierende, medizinische und Probanden werden aus den Quellsystemen extrahiert.
- 2) Identifizierende Daten werden innerhalb des Transformationsschrittes durch ein Pseudonym ersetzt (vgl. Abschnitt 4.3 „Pseudonymisierung“).

¹³ 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.

3) Der ETL-Prozess lädt die Daten über eine Web-Schnittstelle in das DMR.

4.3 Pseudonymisierung

Pseudonymisierung findet bei jeder Art von Datenerfassung in das DMR statt, der manuellen Dateneingabe wie auch dem automatisierten Datenimport.

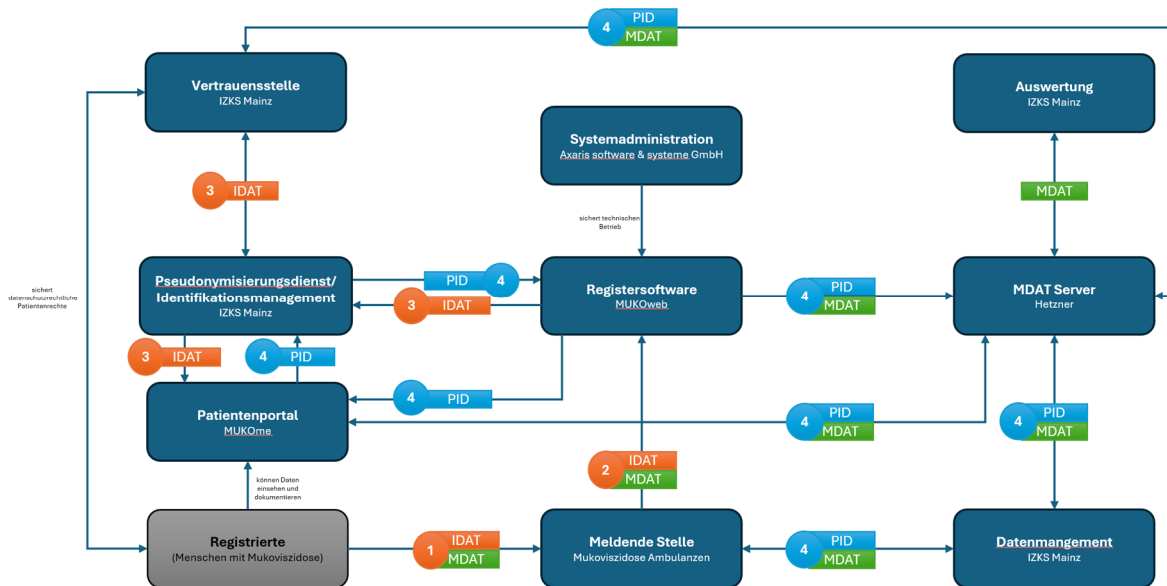


Abbildung 3 Workflow Pseudonymisierung des Deutschen Mukoviszidose Registers

4.3.1 Manuelle Patientenregistrierung

Gleichermaßen für die Registrierung eines neuen Patientendatensatzes wie auch für das Wiederfinden eines vorhandenen gibt der Benutzer die identifizierenden Daten in eine Eingabemaske der Mainzliste, die in MUKOweb angezeigt wird, ein. Die identifizierenden Daten 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 der Patient bereits in der Mainzliste registriert ist. Falls nicht, so wird der Patient neu angelegt, indem die IDAT gespeichert und ein Pseudonym erzeugt werden. Der Benutzer wird automatisch in MUKOweb zurückgeleitet, auf der MDAT zum neu angelegten oder ausgewählten Patienten eingegeben werden können. Browser und DMR kommunizieren dabei mittels temporärer Identifikatoren.

Während der Eingabe der MDAT im DMR, die lokal und behandlungsnah erfolgt, werden identifizierende Daten der Patienten im Browser angezeigt. Diese werden allerdings erst im Browser mit den MDAT zusammengeführt, so dass das DMR zu keinem Zeitpunkt Zugriff auf die IDAT bekommt. Dazu ruft die Registersoftware eine sessionbasierte temporäre ID ab, mit der der Browser die zugehörigen IDAT von der Mainzliste erhält.

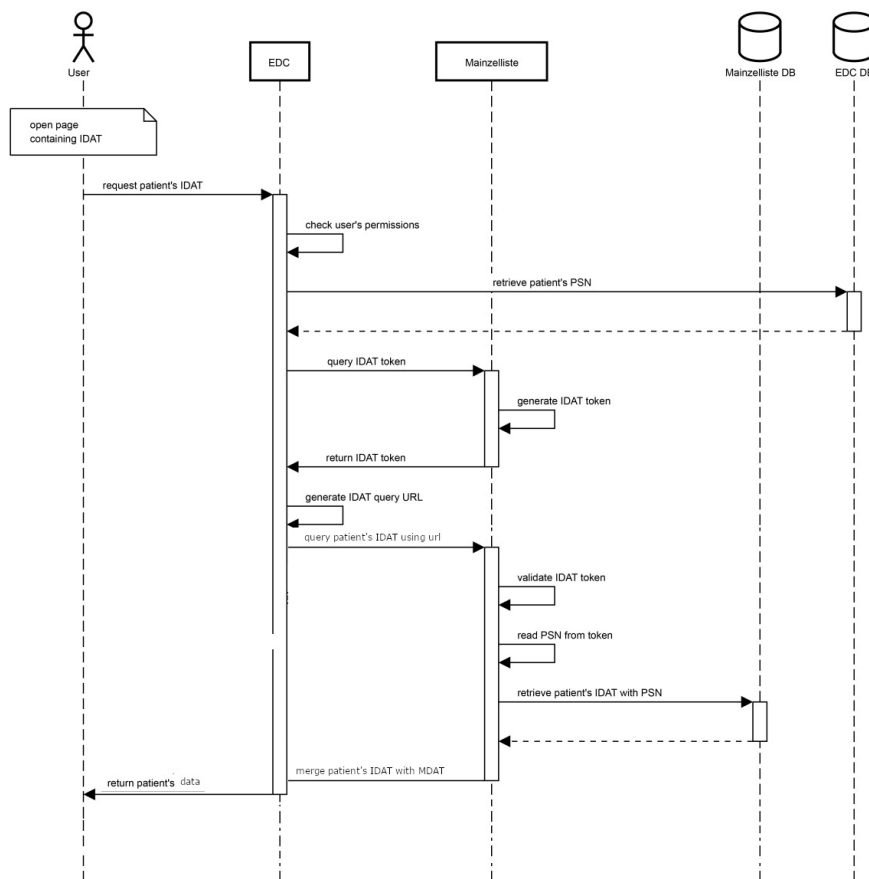


Abbildung 4 Abruf IDAT

Eine Re-Identifizierung (De-Pseudonymisierung) kann nur kontrolliert mithilfe der Mainzliste durchgeführt werden.

4.3.2 Pseudonymisierung beim Datenimport über MUKO.Importer

Beim manuellen Datenimport von Daten in MUKOweb über das eigens für diesen Zweck entwickelte Zusatzprogramm MUKO.Importer ist die Pseudonymisierung Teil der Daten-Transformation. Folgende Schritte werden hierbei durchlaufen:

- 1) MUKO.Importer erhält zwei Dateien: eine IDAT-Datei mit Patienten-ID und den IDAT, und eine Datendatei mit Patienten-ID und den Importdaten (MDAT).
- 2) Für jeden Datensatz in der IDAT-Datei ruft MUKO.Importer die Mainzliste auf und übergibt die IDAT.
- 3) Die Mainzliste ermittelt oder erzeugt das Pseudonym (analog zur manuellen Dateneingabe).
- 4) MUKO.Importer generiert für jedes aus der Mainzliste erhaltene (in diesem Zusammenhang als „privat“ bezeichnete) Pseudonym ein zusätzliches, zufälliges (in diesem Zusammenhang als „öffentlich“ bezeichnetes) Pseudonym. Patienten-ID, privates und öffentliches Pseudonym werden anschließend in einer verschlüsselten Datei gespeichert.
- 5) Diese Datei bildet den Zusammenhang zwischen den beiden Pseudonymen ab und muss nach jedem Datenimport gesichert werden. Sie wird bei jedem erneuten Import verwendet.

- 6) Beim Datenimport wird in der IDAT-Datei das öffentliche Pseudonym eingetragen und in der MDAT-Datendatei die Patienten-ID durch das private Pseudonym ersetzt. Diese Datei wird direkt an das DMR in MUKOweb hochgeladen und nicht lokal gespeichert.
- 7) Bei späteren Datenimporten muss die neue IDAT-Datei die öffentlichen Pseudonyme aus früheren Importen enthalten.

Durch dieses Verfahren ist sichergestellt, dass auch beim Datenimport keine Pseudonyme zugeordnet werden können, da die Daten liefernde Seite, die den Patientenbezug herstellen kann, nur das öffentliche Pseudonym sieht. Die Datei mit den privaten Pseudonymen wird nur im Hauptspeicher entschlüsselt bzw. verschlüsselt.

4.3.3 Registrierungsverfahren MUKOme Patientenportal

MUKOme ist das Patientenportal des DMR. Menschen mit Mukoviszidose und/oder Ihre Sorgeberechtigten können in diesem Portal Ihre im Register gespeicherten individuellen Gesundheitsdaten direkt einsehen. Hierzu gehören Daten aus den Bereichen Ambulanzbetreuung, körperliche Untersuchung, Mikrobiologie und Medikation.

MUKOme bietet Patienten außerdem die Möglichkeit, selbstständig Therapieerfolge (Outcome) in das DMR zu dokumentieren. Hierzu gehören z.B. Fragebögen zur Lebensqualität. Die Patienten werden durch die meldende Stelle zu MUKOme eingeladen. Hierzu werden die Patienten aus MUKOweb eingeladen. Im Patientenportal werden Mithilfe des Pseudonyms die benötigten IDAT (eMail + Mobilfunknummer) aus dem Pseudonymisierungsdienst abgerufen.

Die Patienten erhalten eine eMail mit einem Registrierungslink und über die Mobilfunknummer ein einmalig gültiger Code für den Registrierungsprozess. Nach der Vergabe eines individuellen Passworts können sich die Patienten mit Ihrem Nutzernamen, Geburtsdatum und Passwort in MUKOme anmelden.

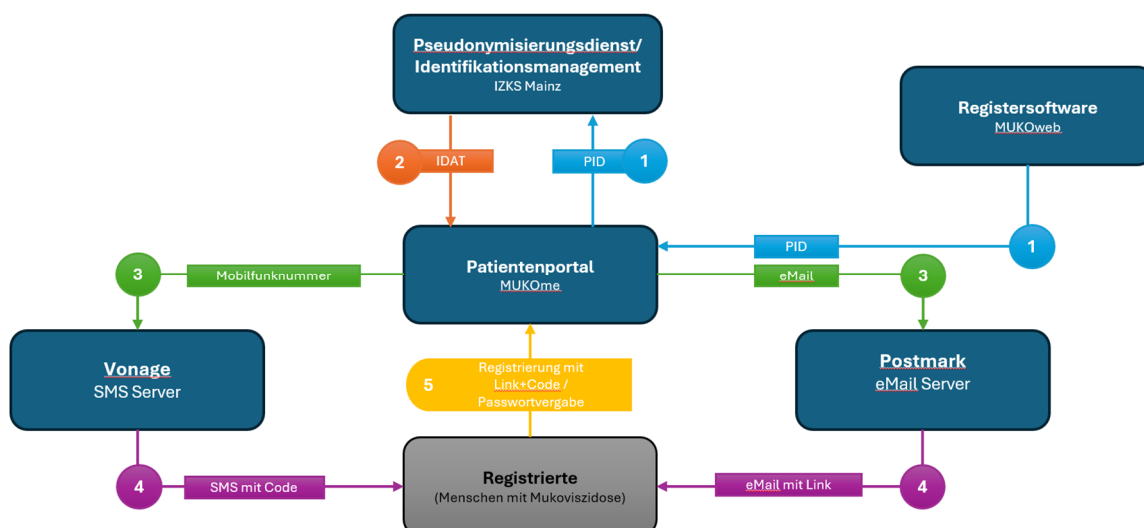


Abbildung 5 Registrierungsprozess MUKOme Patientenportal

4.4 Datenexport und Nutzung

Gemäß der gültigen Nutzungsordnung sind verschiedene Formen der Datennutzung vorgesehen. Dabei werden die On-Site-Nutzung in den geschützten Räumen des DMR („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 Off-Site-Nutzungen setzen gemäß Nutzungsordnung in einem durch die Registerstelle des DMR koordinierten Prozesses einen Nutzungsantrag mit Prüfung und positiver Empfehlung durch das Data Access Committee und Abschluss eines Nutzungsvertrags voraus.

Die Verantwortung für den Export bei der On-Site-Nutzung liegt bei der meldenden Stelle, bei der Off-Site-Nutzung beim Registerbetreiber. Sollten Daten an Dritte außerhalb des Registers weitergeleitet werden, müssen diese Daten ein weiteres Mal pseudonymisiert werden.

4.4.1 Datenexport

Medizinische Daten können zu Auswertungszwecken für alle Formen der Datennutzung durch das Datenmanagement/die Transferstelle aus der Registerdatenbank des DMR 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 DMR 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 und die meldenden Stellen des DMR können Datensätze bei Bedarf unter Verwendung des im DMR sichtbaren Pseudonyms (PID) exportiert werden.

4.4.2 Datennutzung

Externe Interessensgruppen (Wissenschaftler, Krankenkassen, etc.), die nicht aktiv am DMR beteiligt sind, können einen Antrag auf Registerauswertung bei der AG-Register einreichen. Die Anträge werden durch die AG-Register und das Leitungsgremium inhaltlich beurteilt und freigeben. Grundlage hierfür ist die Geschäftsordnung des Registers (vgl. Abschnitt 7.2 Geschäftsordnung).

Der Umfang und der Umgang der zur Verfügung gestellten Registerdaten wird vertraglich zwischen dem Antragsteller und dem MI fixiert. Dem Antragsteller kann nach Freigabe durch die AG-Register, ein durch das Datenmanagement aggregierter und anonymisierter Datenbankauszug zur Verfügung gestellt werden. Das Re-Identifikationsrisiko ist damit ausgeschlossen. Die Koordination des Antragsverfahrens und der Freigabe nach Beurteilung wird durch das MI gewährleistet.

Für Gastwissenschaftlerarbeitsplätze werden die beantragten und vom Data Access Committee freigegebenen Datensätze zur internen Nutzung von der Systemadministration des DMR zusammengestellt. Die weitere Verarbeitung und Analyse der Daten erfolgt an einem gegen unerlaubte und unlautere Datennutzung eingerichteten Arbeitsplatz im lokalen Safe Setting.

Für das European Cystic Fibrosis Registry (ECFS Register) wird das jeweilige Pseudonym des vollständigen Jahresdatensatzes durch das Datenmanagement mit einem zusätzlichen ExportPseudonym versehen.

4.4.3 Datenzugriff durch Administrierende

Die im DMR 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:
 - (1) den Zeitpunkt des Datenzugriffs,
 - (2) die beteiligten Administratoren und Administratorinnen,
 - (3) den Grund des Datenzugriffs.

Alle Administrierenden sind entsprechend zu instruieren und zur Verschwiegenheit zu verpflichten.

5 WEITER 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 Informelle Gewaltenteilung

Das Identitätsmanagement wird logisch, physikalisch und organisatorisch getrennt von allen Komponenten betrieben, die MDAT speichern. Die Systeme des Identitätsmanagements sind an Universitätsmedizin der Johannes-Gutenberg-Universität Mainz am Interdisziplinäres Zentrum für Klinische Studien (IZKS) lokalisiert und stehen unter eigener rechtlicher Verantwortung. So ist sichergestellt, dass Personen, die im DMR außerhalb des Behandlungszusammenhangs Zugriff auf medizinische Daten haben, keine Zuordnung von Daten zu realen Patienten treffen können.

Systembetreuer der MDAT haben zu keinem Zeitpunkt Zugriff auf die IDAT; die Systembetreuer der IDAT haben keinen Zugriff auf die MDAT der teilnehmenden Patienten. Die Systembetreuer der MDAT können im Auftrag des Registerbetreibers die gesamte oder Teile der Datenbank – beispielsweise für statistische Auswertungen – exportieren.

Der Export der IDAT ist zu keinem Zeitpunkt erlaubt. Veränderungen jeglicher Art in der Zentralen Patientenliste dürfen ausschließlich durch die Systembetreuer der IDAT durchgeführt werden.

5.2 Autorisierung und Authentifizierung

5.2.1 Autorisierung von Benutzern

Die Autorisierung von Benutzern (Zuweisung zu definierten Rollen) des DMR erfolgt durch das Datenmanagement entsprechend den lokalen Strukturen und Erfordernissen. Dabei können lokale Regelungen des Datenschutzes berücksichtigt werden. Sich überschneidende Rollen- und Rechtekonzepte zwischen den Systembetreuern von IDAT und MDAT sowie den Ärzten sind ausgeschlossen.

5.2.2 Autorisierung von Komponenten

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

5.2.3 Authentifizierung von Benutzern

Die Authentifizierung von Benutzern gegenüber dem DMR 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 in MUKOweb aktivieren.

Die Authentifizierungsdaten werden zur Sicherstellung der Identität des Kommunikationspartners beim Zugriff auf MDAT und IDAT während der Anwendersitzung in Form eines sog. Tokens ausschließlich am lokalen Arbeitsplatz gespeichert. Das Token stellt eine temporäre Zugangsberechtigung für

die aktuelle Benutzersitzung dar und verliert nach Benutzerabmeldung oder einer festgelegten Dauer der Inaktivität (15 Minuten) seine Gültigkeit.

In regelmäßigen Abständen wird durch das Datenmanagement kontrolliert, ob die Ärzte/Dokumente noch Mitarbeiter der Mukoviszidose Einrichtung sind. Fällt diese Kontrolle negativ aus, werden die Datenbankteilnehmer gelöscht.

Die Gültigkeit der Nutzerpasswörter ist auf 90 Tage beschränkt. Die Gültigkeit aller Nutzeraccounts wird jährlich durch das Datenmanagement überprüft.

5.2.4 Authentifizierung von Komponenten

Zugriffe zwischen verschiedenen IT-Komponenten über das Internet finden nur nach erfolgreicher Authentifizierung statt. Die Authentifizierung erfolgt serverseitig über Serverzertifikate und clientseitig (je nach technischer Möglichkeit) über IP-Adresse und Nutzernamen /Passwort oder über Clientzertifikate.

5.3 Maßnahmen in der IT-Infrastruktur

5.3.1 Sicherheit der gespeicherten Daten

Alle in den zentralen Komponenten des DMR erhobenen Daten werden auf verschlüsselten Festplattenpartitionen gespeichert. Der zugehörige Schlüssel befindet sich jeweils auf einem getrennten Medium pro Server (z.B. Papier, USB-Stick). Dieses Medium wird nur während des Mount- bzw. Bootvorgangs benötigt und wird ansonsten sicher verwahrt. Nur der Administrator des jeweiligen Servers hat Zugriff auf „sein“ Schlüsselmedium. Der Schlüssel kann nicht errechnet werden. Alle Server befinden sich in Rechenzentren, die über eine Zugangskontrolle per Chipkarte oder ähnlich sichere Token für jeweils berechtigte Personen verfügen. Die Serversysteme sind gegen unbefugten Zugang von außen über eine gemanagte Firewall geschützt. Der Zugang im Haus ist nur autorisierten Personen möglich. Diese erhalten den Zugang über Authentifizierung durch Benutzernamen und Passwort.

5.3.2 Sicherheit der Kommunikation

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

- Die Kommunikation zwischen den Komponenten erfolgt grundsätzlich über verschlüsselte Verbindungen (HTTPS). Die dafür eingesetzten Schlüssel und Zertifikate sind so zu erstellen, dass sie den aktuell anerkannten Anforderungen entsprechen (z.B. Schlüssellänge). Aktuelle Anforderungen können den IT-Grundschutz-Katalogen des Bundesamtes für Sicherheit in der Informationstechnik entnommen werden¹⁴.
- 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.

¹⁴https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html

Die Client-Computer der Mukoviszidose Einrichtungen werden durch die klinikinterne IT eigenverantwortlich gemanagt und durch aktuelle Virenschutzprogramme und persönliche Firewalls geschützt.

5.3.3 Protokollierung

Alle Zugriffe auf IDAT und MDAT werden nachvollziehbar und revisionssicher protokolliert und können von den Systembetreuern der jeweiligen Datenbank eingesehen werden. Das Protokoll enthält mindestens:

- Die Identität der zugreifenden Person oder Komponente.
- Datum und Uhrzeit des Zugriffs.
- Alle Daten im Audittrail bleiben erhalten
- Export Nutzerbezogen

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

5.4 Maßnahmen in der IT-Infrastruktur

Gemäß der Nutzungsordnung folgt das DMR 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 (vgl. Anhang 7.1 „Patienteneinwilligung Deutsches Mukoviszidose-Register“) ist Rechtsgrundlage der Datenverarbeitung.

Die Einwilligung des Patienten zur Teilnahme am DMR erfolgt in schriftlicher Form und wird durch den behandelnden Arzt eingeholt. Die unterschriebenen Patienteneinwilligungen werden im Original sowohl in der Patientenakte in der meldenden Stelle als auch im Identifikationsmanagement und in der Vertrauensstelle gespeichert. Das Datum der Patienteneinwilligung wird in der Registersoftware MUKOweb erfasst.

Mit der Einwilligung erklärt sich der Patient insbesondere dazu bereit, dass

- seine IDAT an das Identitätsmanagement und die Vertrauensstelle übermittelt und dort gespeichert werden,
- MDAT gemäß Registerdefinition im DMR erfasst werden,
- diese MDAT von Forschern des DMR lokal ausgewertet werden können und
- MDAT des Patienten aus dem DMR aggregiert, anonymisiert oder pseudonymisiert exportiert und für die in der Einwilligung näher definierten Zwecke, an Dritte übermittelt werden können. Hierzu gehören beispielsweise:
 - wissenschaftliche Registerevaluierungen,
 - interne Forschungsvorhaben (Benchmarking: Lernen von den Besten, Public Reporting Mukoviszidose) oder
 - externe Forschungsvorhaben/registerexterne Dritte (z.B. Krankenkassen, Pharmaindustrie). Registerevaluierungen werden z.B. mit dem Ziel durchgeführt zusätzliche Erkenntnisse über die Krankheit oder die Sicherheit und den Nutzen von verabreichten Arzneimitteln im Vergleich zu anderen Therapien gewinnen zu können.

Bei der Übermittlung medizinischer Gesundheitsdaten (MDAT) an ein Drittland oder eine Internationale Organisation außerhalb der EU, werden die Bedingungen und sonstigen Bestimmungen der Datenschutzgrundverordnung eingehalten.

Identifizierenden Daten (IDAT) werden hierbei zu keiner Zeit an Dritte weitergegeben. Sollte eine Zusammenführung von Daten im Rahmen von wissenschaftlichen Auswertungen anhand der IDAT notwendig werden, sind die in der Einwilligungserklärungen Prozesse durch den Registerbetreiber einzuhalten.

Bei Erreichen der Volljährigkeit wird der Patient durch den behandelnden Arzt gebeten, eine neue Einwilligungserklärung zu unterschreiben. Der Behandler wird durch die Registersoftware MUKOweb und die Vertrauensstelle auf die Erneuerung der Einwilligungserklärung hingewiesen.

Mit Einholen der Einwilligung wird der Patient über sein Recht auf Auskunft und Widerruf informiert.

6.2 Auskunfts-, Berichtigungs- Widerspruchs- und Beschwerderechte

Im DMR registrierte Personen haben das Recht, Auskunft darüber zu erhalten, ob und welche Daten von ihnen im gespeichert werden, und diese Daten einzusehen. Der Antrag auf Auskunft ist schriftlich

an die Vertrauensstelle oder meldende Stelle zu stellen. Daraufhin wird ein menschenlesbarer Ausdruck der Daten erzeugt und der erfassten Person ausgehändigt.

Betroffene Personen haben vor allem folgende Rechte:

das Auskunftsrecht nach Art.15 DSGVO, dies beinhaltet Informationen über...

- ...den Zweck der Datenverarbeitung/des Registerverfahrens
- ...die Kategorien der erhobenen Daten
- ...die Empfänger von Daten oder Kategorien von Empfängern
- ...die Dauer der Speicherung
- ...die Übermittlung Ihrer Daten in ein Drittland oder an internationale Organisation

das Recht auf Berichtigung nach Art. 16 und 19 DSGVO, dies beinhaltet z.B. ...

- ...die Vervollständigung Ihrer personenbezogenen und/oder Gesundheitsdaten
- ...Korrekturen an Ihren bestehenden personenbezogenen und/oder Gesundheitsdaten

das Recht auf Löschung und Widerspruch (Recht auf „Vergessenwerden“) nach Art. 17 und 19 DSGVO, dies tritt z.B. in Kraft wenn...

- ...der Betroffene seine Einwilligung zur Datenverarbeitung widerrufen hat
- ...die Speicherung der Daten nicht mehr notwendig ist
- ...eine Rechtspflicht zum Löschen nach EU- oder nationalem Recht besteht

das Beschwerderecht bei einer Aufsichtsbehörde nach Art. 77 DSGVO...

- ...wenn Sie der Ansicht sind, dass die Verarbeitung der Sie betreffenden personenbezogenen Daten gegen die DSGVO verstößt.

Die Kontaktdaten der für Sie zuständigen Aufsichtsbehörde finden Sie online unter: <https://www.bfdi.bund.de>

6.3 Widerruf, Löschung, Anonymisierung

Der Patient kann seine Einwilligung bei seinem behandelnden Arzt schriftlich zu jeder Zeit und ohne Angabe von Gründen zurückziehen. Der Widerruf wird in der Registersoftware MUKOweb dokumentiert und an das Identitäts- und Datenmanagement weitergegeben.

Im Falle eines Widerrufs wird die Zuordnung zu einer Person und Ihren identifizierenden Daten vernichtet. Es verbleiben ausschließlich anonymisierte medizinische Gesundheitsdaten, die keinen Rückschluss auf den Patienten zulassen, z.B. medizinische Gesundheitsdaten, die bereits Grundlage veröffentlichter Studien sind und denen Archivzwecke oder wissenschaftliche und historische Forschungszwecke entgegenstehen.

Im Falle der Anonymisierung werden die entsprechenden Datensätze in der zentralen Patientenliste (Mainzelliste) gelöscht und das bisherige Pseudonym des Patienten durch ein zufälliges Pseudonym ersetzt. Durch den Algorithmus zur Pseudonymerzeugung ist sichergestellt, dass die Pseudonyme eines gelöschten oder anonymisierten Patienten nicht mehr für neue Patienten verwendet werden. Die Anonymisierung ist von den zuständigen Betreibern zeitnah, maximal innerhalb von 14 Werktagen, vorzunehmen¹⁵. Der Abschluss der Löschung oder Anonymisierung wird dem Patienten schriftlich bestätigt.

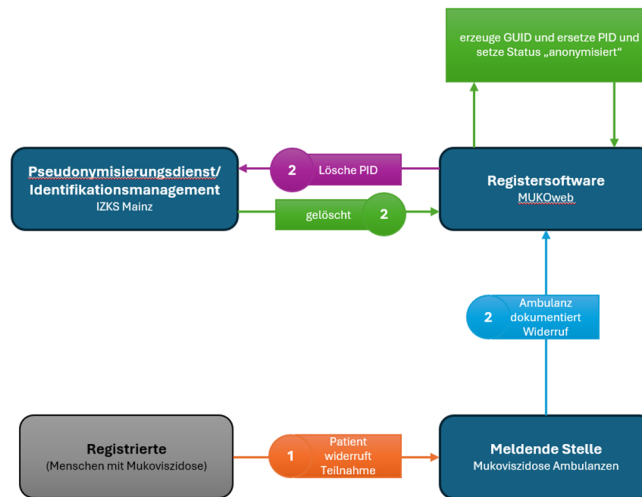


Abbildung 6 Ablauf des Widerrufs der Einwilligung

6.4 Dauer der Speicherung

Das DMR soll langfristig betrieben werden ohne ein festgelegtes Enddatum. Die erhobenen Daten bleiben im DMR gespeichert, solange es für sie eine sinnvolle wissenschaftliche Verwendung im Rahmen der Patienteneinwilligung gibt.

Die Daten bleiben gespeichert bis:

- Der Patient seine Einwilligung widerrufen (vgl. Abschnitt 6.3) oder
- bis zu 5 Jahren, nachdem sämtliche Projektaktivitäten eingestellt wurden.

Die Sinnhaftigkeit des Registerprojekts wird durch den Bundesvorstand des Mukoviszidose e.V. und die AG Register in regelmäßigen Abständen inhaltlich bewertet. Liegt keine Zweckmäßigkeit mehr vor oder wird der Registerbetrieb vor Ablauf der Überprüfung eingestellt, werden Ihre gesamten personenbezogenen Daten nach der Erreichung einer Sperrfrist von 5 Jahren unwiderruflich gelöscht.

¹⁵ Die meist impraktikable Löschung oder Anonymisierung in Datensicherungen ist verzichtbar, sofern die Sicherungen nur durch den zuständigen Systemadministrator eingesehen werden können und alte Sicherungen regelmäßig gelöscht werden.

7 ANHANG

7.1 Patienteneinwilligung

Die aktuelle Version der Patienteninformation und-einwilligung steht auf www.muko.info/register zur Verfügung. Version 2.1, Stand 01.01.2025

7.2 Weitere mitgeltende Dokumente

- Geschäftsordnung Deutsches Mukoviszidose-Register_2.0
- Publikationsordnung Deutsches Mukoviszidose-Register_1.7
- Verfahrensordnung Registerstudien Deutsches Mukoviszidose-Register-2.3

7.3 Datensatz DMR

Die aktuelle Version des DMR-Datensatzes steht auf www.muko.info/register zur Verfügung. Version 4.0, Stand 01.01.2025

7.3.1 Medizinische Daten

Aufgrund der hohen Anzahl der erhobenen Daten, ist die Einsichtnahme online unter www.muko.info/register realisiert.

7.3.2 Identifizierende Daten

Element	Ausprägung
Nachname (n)	
Vorname (n)	
Geburtsdatum	
Geburtsname	Optional
Gebrurstort	Optional
Geschlecht	
E-Mail	Optional
E-Mail Sorgeberechtigter	Optional
Mobilfunknummer	Optional
Mobilfunknummer Sorgeberechtigter	Optional
Ort, Straße & Hausnummer, PLZ	Optional
EGK Nummer	

7.4 Rollen und Aufgaben im DMR

Rolle	Wer	Aufgaben	Berechtigungen
Träger	Mukoviszidose e.V	▪ Bereitstellung finanzieller Mittel für die Entwicklung und den Betrieb des Registers	▪ Keine Einsicht in MDAT & IDAT
Registerbetreiber	Mukoviszidose Institut gGmbH	▪ Führung der Geschäfte des Registers ▪ Verantwortlicher im Sinne des Art. 4 DSGVO ▪ Entscheidungen rund um die Weiterentwicklung des Registers	▪ Keine Einsicht in MDAT & IDAT
Registerstelle	Mukoviszidose Institut gGmbH / Qualitätsmanagement	▪ technischer und administrativer Betrieb des Registers ▪ Einberufung von Data Access Committee und wissenschaftlichem Beirat ▪ Koordination des Registerbetriebs ▪ Ansprechpartner für meldende Stellen ▪ Ansprechpartner für inhaltliche Fragen ▪ zentrale Definition von Nutzerrollen ▪ zentrale Verwaltung der meldenden Stellen ▪ Koordination des Prozesses der Datennutzung	▪ Einsicht in MDAT
Datenmanagement/ Transferstelle	IZKS Mainz – Datenmanagement	▪ Zugriff auf alle medizinischen Daten aller teilnehmenden Einrichtungen ▪ Erstellung von Datenexporten und Auswertungen ▪ Beratung des Data Access Committees ▪ zentrale Nutzerverwaltung (Anlegen von Nutzerkonten, Zuweisung von Rollen) ▪ Prüfung der Zulassungsberechtigung von Nutzern	▪ Einsicht in MDAT ▪ Datenexport
Vertrauensstelle	IZKS Mainz – Vertrauensstelle	▪ Betrieb des zentralen Identitätsmanagements und Pseudonymisierungstools (Mainzelliste) ▪ Betrieb des zentralen Einwilligungsmanagements (glCS) ▪ Ansprechpartner für datenschutzrechtliche Angelegenheiten (Betroffenenrechte) ▪ Bearbeitung von Anfragen zu Identifikation eines Patienten ▪ Unterstützung der Transferstelle bei der datenschutzkonformen Bereitstellung von Daten	▪ Einsicht in IDAT ▪ Einsicht in MDAT, wenn dies für den ordnungsgemäßen Betrieb des Registers notwendig ist

Systemadministratoren	Axaris GmbH	▪ 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 Mukoviszidose Einrichtungen	▪ Erfassung von Daten im DMR ▪ Stellung von Nutzungsanträgen oder Nutzungsanzeigen	▪ Einsicht in IDAT und MDAT ihrer registrierten Personen ▪ erhalten beantragte Auswertungen entsprechend Nutzungsantrag / Nutzungsanzeige ▪ erhalten beantragte Daten entsprechend Nutzungsantrag / Nutzungsanzeige
Datennutzende	Externe Interessensgruppen	▪ Stellung von Nutzungsanträgen	▪ keine Einsicht in IDAT und MDAT ▪ erhalten beantragte Auswertungen entsprechend Nutzungsantrag / Nutzungsanzeige

7.5 Technische und organisatorische Maßnahmen (TOMs)

- Technische und organisatorische Maßnahmen (Vertrauensstelle/Datenmanagement/Transferstelle):
2024_05_06_TOMs_IZKS_1.0.pdf
- Technische und organisatorische Maßnahmen des Dienstleisters (Hosting MDAT):
2025-02-19_TOM_Hetzner.pdf
- Technische und organisatorische Maßnahmen des Dienstleisters (Systemadministration):
2025-01-01_TOM_Axaris.pdf

8 ANHANG: TABELLARISCHE DATENSCHUTZ-FOLGEABSCHÄTZUNG

8.1 Gesetzliche Vorschrift betreffend DSFA und Definition für vorliegendes Dokument

Bei der Erstellung des Datenschutzkonzeptes für das Deutsche Mukoviszidose-Register (DMR) wurden die Anforderungen an ein Datenschutzkonzept auf Bundesebene laut dem Gutachten von Thilo Weichert „Datenschutzrechtliche Rahmenbedingungen medizinischer Forschung“¹⁶ im Frühjahr 2022 berücksichtigt. Hier wird darauf verwiesen, dass in § 22 Abs. 2 Bundesdatenschutzgesetz (BDSG) die Inhalte eines Datenschutzkonzeptes benannt werden.¹⁷

Der Hauptteil des vorliegenden Dokuments (Kapitel 1 bis 7) erfüllt die Anforderungen der Bundesebene an ein 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 DSGVO¹⁸, muss die Abschätzung „vorab“ durchgeführt und dokumentiert werden.

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“].

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) Nichtverketzung
- (6) Transparenz
- (7) Intervenierbarkeit

¹⁶ Thilo Weichert 2022: Datenschutzrechtliche Rahmenbedingungen medizinischer Forschung. S.200. Gutachten für den TMF e.V.

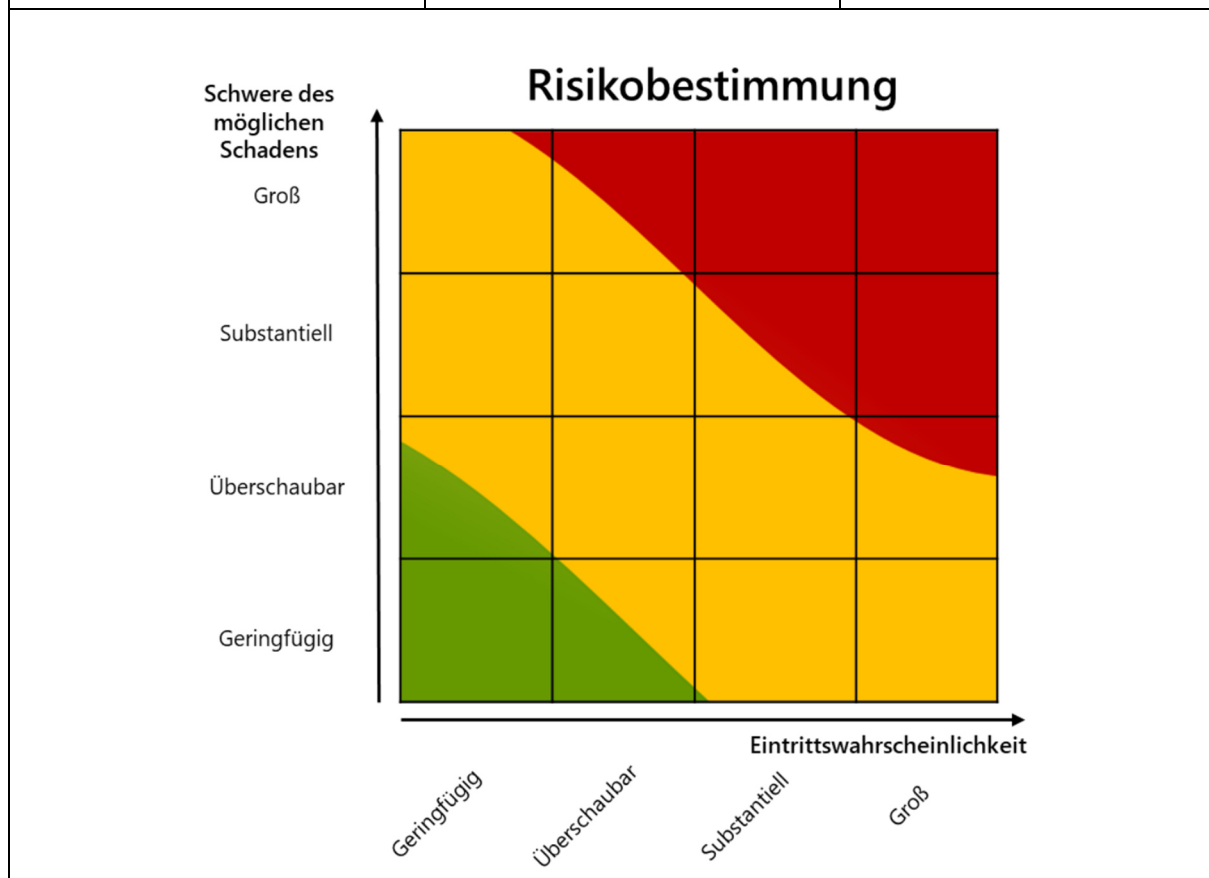
¹⁷ 8 „Die Pflicht, ein Datenschutzkonzept für ein Forschungsvorhaben vorzulegen, besteht nicht generell, sondern nur gemäß einigen speziellen Gesetzen. Eine entsprechende Pflicht kann generell allenfalls aus den Dokumentationspflichten nach Art. 5 Abs. 2 DSGVO abgeleitet werden. Eine präzise Festlegung 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“

¹⁸ 9 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.“

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 DMR das Datenschutzkonzept und die angehängte tabellarische DSFA mit gleicher Versionierung synchronisiert fortzuschreiben.

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. Perspektivisch 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).¹⁹

Die sieben Gewährleistungsziele des Standarddatenschutzmodells sind:	Schweregrade des möglichen Schadens	Eintrittswahrscheinlichkeiten
(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



¹⁹ TMF AG Datenschutz 2022: DSFA Template

8.2 Festlegung Schutzbedarf

Gemäß ErwGr. 51 DSGVO beinhaltet, dass die Verarbeitung der besonderen Kategorien von personen-identifizierenden Daten, dies sind

- Daten, aus denen die rassische und ethnische Herkunft, hervorgeht,
- Daten bzgl. politischer Meinungen,
- Daten hinsichtlich religiöser oder weltanschaulicher Überzeugungen,
- Daten, aus denen die Gewerkschaftszugehörigkeit hervorgeht,
- genetischen Daten,
- biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person,
- Gesundheitsdaten,
- Daten zum Sexualleben oder der sexuellen Orientierung,

immer einen besonderen Schutz verdienen, da „im Zusammenhang mit ihrer Verarbeitung erhebliche Risiken für die Grundrechte und Grundfreiheiten auftreten können.“. Daraus folgt zweierlei:

- (1) Es muss bei der Verarbeitung dieser Daten ein „besonderer“ Schutz vorhanden sein; Standardmaßnahmen, wie sie für den Schutz bei der Verarbeitung „normaler“ Daten ausreichen, müssen durch zusätzliche Maßnahmen ergänzt werden, die der Anforderung bzgl. des „besonderen“ Schutzbedarf genügen.
- (2) In ErwGr. 75 und 76 werden Risiken als abhängige Größe von der Eintrittswahrscheinlichkeit und der Schwere der Beeinträchtigung der Rechte und Freiheiten der betroffenen Person beschrieben. Die in ErwGr. 51 dargestellten möglichen erheblichen Risiken basieren somit einerseits auf der Schwere der Beeinträchtigung, die einer Verarbeitung dieser besonders sensiblen Daten innewohnt, andererseits auf der Wahrscheinlichkeit, mit welcher die Beeinträchtigung der Rechte und Freiheiten der betroffenen Personen eintreten könnte.

Der in ErwGr. 51 DSGVO angesprochene „besondere“ Schutz muss also geeignet sein, die Eintrittswahrscheinlichkeit so weit zu reduzieren, dass durch diese Maßnahmen für die Dauer der Verarbeitung kein hohes Risiko vorliegt. Andernfalls muss der Verantwortliche, wenn auf die Verarbeitung nach Feststellung des Ergebnisses nicht verzichtet wird, vor Beginn der Verarbeitung gemäß Art. 36 Abs. 1 die zuständige Aufsichtsbehörde konsultieren.

8.3 Einschätzung und Bewertung der Risiken

Die Erfüllung der Anforderungen von Art. 32 DSGVO wird detailliert in Abschnitt 8.4 dargestellt.

Die genannten Risiken können in folgende Kategorien eingeteilt werden:

- (1) Unbefugte Offenbarung personenbezogener Gesundheitsdaten mit Diskriminierungspotential
- (2) Datenerhebung und Datenerfassung
- (3) Probandenmanagement
- (4) Empfang der verschlüsselten personenidentifizierenden Daten oder pseudonymisierten medizinischen Daten durch Unberechtigte
- (5) Hohe Informationsdichte in der Vertrauensstelle
- (6) Berichterstattung
- (7) Datenmanagement (Organisation und Pflege der Daten)
- (8) Bereitstellung von probandenbezogenen Informationen

- (9) Unbefugte Veränderung personenbezogener Gesundheitsdaten mit Diskriminierungspotential
- (10) Unerwartete Einschränkung der Datenverfügbarkeit
- (11) Unerwarteter Datenverlust
- (12) Einschränkung des Auskunftsrechts
- (13) Einschränkung des Löschrechts (inkl. Widerruf und Widerspruch)
- (14) Statistische Analyse
- (15) Studienunterstützung
- (16) Diese Risiken müssen anhand der Wahrscheinlichkeit des Auftretens dieser Risiken und der Schwere der Auswirkungen bewertet werden.

8.4 DSFA-Tabelle mit Datenverarbeitung und Risikominimierung

Verarbeitungstätigkeit				Risikoanalyse & Maßnahmenfestlegung				Ergebnis	
lfd. Nr.	Verarbeitungsphase / Verarbeitungsrubrik (Top-Level-Aufgabe, TL=VR) / Verarbeitungsvorgang (Use Case)	Risikobeispiele / -beschreibung	Gewährleistungsziele	Schadenshöhe	Eintrittswahrscheinlichkeit	Risikobewertung	Maßnahmen	Bewertung der Gegenmaßnahme	Verfahren kann durchgeführt werden
			(1) Datenminimierung (2) Verfügbarkeit (3) Integrität (4) Vertraulichkeit (5) Nichtverkettung (6) Transparenz (7) Interventionsfähigkeit	Geringfügig Überschaubar Substantiell Groß	Geringfügig Überschaubar Substantiell Groß	- Kein Risiko - Voraussichtlich kein Risiko - (Normales) Risiko - Erhebliches Risiko - Hohes Risiko - untragbares Risiko			
1	Unbefugte Offenbarung personenbezogener Gesundheitsdaten mit Diskriminierungspotential	• Unbefugte interne Personen bekommen Einsicht in Patientenakte mit Diskriminierungspotential (Bsp. HIV-Diagnose) • Speichermedium mit Patienten-/ Probandendaten mit Diskriminierungspotential (Bsp. HIV-Diagnose) gelangt in Besitz von unbefugten externen Personen • Re-Identifizierung von Personen durch unbefugte externe Personen infolge unzureichender Pseudonymisierung/Anonymisierung • Social Engineering • Schadprogramm-Attacke oder externer Angriff auf IT-Infrastruktur zu Patienten-/ Probandendaten (digitale Patientenakte) mit Diskriminierungspotential (Bsp. HIV-Diagnose) • Erbeutung von personenbezogenen Gesundheitsdaten mit Diskriminierungspotential (Bsp. HIV-Diagnose) während des elektronischen Transports durch Zwischenschaltung des Angreifers (Man-In-The-Middle Attacken)	Vertraulichkeit	Substantiell	Überschaubar		Wahrung von Maßnahmen des Datenschutzes und der Informationssicherheit in den einzelnen Einrichtungen gemäß der TOMs Vertraulichkeit / Zugriffskontrolle, Zugangs- und Verarbeitungskontrolle, Protokollierung Schulung / Informationssystem, Datenschutz	Aufgrund der technischen und organisatorischen Maßnahmen (TOMs) der einzelnen Projektpartner sowie den in diesem Datenschutzrahmenkonzept getroffenen Maßnahmen dürfte vom jetzigen Stand der Technik aus betrachtet ein Zugriff auf unverschlüsselte personenidentifizierende Daten durch Unberechtigte unwahrscheinlich sein	Restrisiko akzeptabel

2	Datenerhebung und Datenerfassung		Datenminimier. Verfügbarkeit Integrität Vertraulichkeit	Substantiell	Überschaubar		Allgemeine TOM a. Umsetzung durch geschultes Personal b. DV in Geschützten Räumen Spez. TOM wg. Datenminimierung c. Erfassung eines abgestimmten Datensatzes d. Erfassung von genetischen Informationen mit Einwilligung Spez. TOM wg. Verfügbarkeit e. Ergonomie und Usability der Datenerfassung f. proaktive Entwicklung der Datenzugänge (z.B. Satellitendokum.) g. Gewährleistung der Verfügbarkeit und Belastbarkeit der Server durch Dienstleister (Hetzner TOMs) h. regelmäßige Backups entsprechend eines Backup-Konzepts Spez. TOM wg. Integrität i. Identitätsmanagement mit Vertrauensstelle j. Protokollierung aller Änderungen innerhalb der MUKOweb Software in Audit Trail k. Dokumentation aller manuellen Änderungen in der MUKOweb-Datenbank l. Datenübertragung zwischen Browser und Server mit sicherer Verschlüsselung Spez. TOM wg. Vertraulichkeit m. informationelle Gewaltenteilung mit Vertrauensstelle n. Pseudonymisierung und Trennung von IDAT und MDAT o. Zutritts- und Zugangskontrolle zu Servern (Hetzner TOMs) p. Zugangskontrolle: Authentifizierung in MUKOweb mit Passwort + 2FA q. Zugriffskontrolle innerhalb der MUKOweb-Software über modulares Berechtigungskonzept r. Trennungskontrolle innerhalb der MUKOweb-Software über modulares Berechtigungskonzept	Aufgrund der technischen und organisatorischen Maßnahmen (TOMs) sowie der vertraglichen Verpflichtungen mit den am Register beteiligten Dienstleistern und den in diesem Datenschutzrahmenkonzept getroffenen Maßnahmen dürfte vom jetzigen Stand der Technik aus betrachtet keine weitere Maßnahmen erforderlich sein.	Restrisiko akzeptabel
---	----------------------------------	--	--	--------------	--------------	--	---	---	-----------------------

3	Probandenmanagement		Verfügbarkeit Integrität Vertraulichkeit	Überschaubar	Überschaubar		Allgemeine TOM a. Umsetzung durch geschultes Personal b. DV in Geschützten Räumen Spez. TOM wg. Verfügbarkeit c. Datenerhebungskommunikation (Krankenhäuser, Niedergelassene, Patientengruppen, weitere) d. proaktive Entwicklung der Datenzugänge e. proaktive Probandenkommunikation f. Gewährleistung der Verfügbarkeit und Belastbarkeit der Server durch Dienstleister (Hetzner TOMs) g. regelmäßige Backups entsprechend eines Backup-Konzepts Spez. TOM wg. Vertraulichkeit h. Umsetzung bzw. Veranlassung nur d. Behandelnde und Erfüllungsgehilfen i. Informationelle Gewaltenteilung mit Vertrauensstelle j. Pseudonymisierung und Trennung von IDAT und MDAT k. Zutritts- und Zugangskontrolle zu Servern (Hetzner TOMs) l. Zugangskontrolle: Authentifizierung in MUKOweb-Software mit Passwort + 2FA m. Zugriffskontrolle innerhalb der MUKOweb-Software über modulares Berechtigungskonzept Spez. TOM wg. Integrität n. Protokollierung aller Änderungen innerhalb der MUKOweb-Software o. Dokumentation aller manuellen Änderungen in der MUKOweb-Datenbank		
4	Empfang der verschlüsselten personenidentifizierenden Daten oder pseudonymisierten medizinischen Daten durch Unberechtigte	Es besteht das Risiko, dass beim Versand verschlüsselte personenidentifizierende Daten oder pseudonymisierte medizinische Daten durch unberechtigte Dritte abgefangen werden oder an unberechtigte Personen versandt werden	Vertraulichkeit	Substantiell	Überschaubar		Personenidentifizierende Daten werden nur verschlüsselt versandt	Aufgrund der verschlüsselten Übermittlung der Daten sowie den in diesem Datenschutzrahmenkonzept getroffenen Maßnahmen ist der Empfang der Daten durch Unberechtigte unwahrscheinlich. Die Verwendung von Verschlüsselung und Pseudonymisierung reduziert das Risiko für die Rechte und Freiheiten der betroffenen Personen, da die Daten nicht direkt einer Person zugeordnet werden können	Restrisiko akzeptabel
5	Hohe Informationsdichte in der Treuhandstelle	Es besteht das Risiko, dass die in der Vertrauensstelle vorliegenden personenidentifizierende Daten als auch die medizinischen Daten von unberechtigten Personen eingesehen werden.	Vertraulichkeit Nichtverkettung	Substantiell	Überschaubar		Wahrung von Maßnahmen des Datenschutzes und der Informationssicherheit in den einzelnen Einrichtungen gemäß der TOMs Vertraulichkeit / Zugriffskontrolle, Zugangs und Verarbeitungskontrolle, Protokollierung Schulung / Informationssystem, Datenschutz	Aufgrund der technischen und organisatorischen Maßnahmen (TOMs) sowie der vertraglichen Verpflichtungen in den am Register beteiligten Dienstleister und den in diesem Datenschutzrahmenkonzept getroffenen Maßnahmen dürfte vom jetzigen Stand der Technik aus betrachtet eine zu hohe Informationsdichte in der Vertrauensstelle keine weiteren Maßnahmen erforderlich machen.	Restrisiko akzeptabel

Datenschutzkonzept Deutsches Mukoviszidose-Register – Version 3.1

6	Berichterstattung		Vertraulichkeit	Überschaubar	Überschaubar		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		Restrisiko akzeptabel
7	Datenmanagement (Organisation und Pflege der Daten)		Verfügbarkeit Integrität Vertraulichkeit	Überschaubar	Überschaubar		Allgemeine TOM a. Umsetzung durch geschultes Personal b. DV in Geschützten Räumen c. Umsetzung bzw. Veranlassung nur d. Behandelnde und Erfüllungsgehilfen		Restrisiko akzeptabel
8	Bereitstellung von probandenbezogenen Informationen		Vertraulichkeit	Überschaubar	Überschaubar		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. Rekontakting von Probanden nur durch Vertrauensstelle		Restrisiko akzeptabel
9	Unbefugte Veränderung personenbezogener Gesundheitsdaten mit Diskriminierungspotential	• Unautorisierte Personen nehmen Veränderungen an Patienten- / Probanden- / Mitarbeiterlisten vor, so dass fehlerhafte Zuweisungen (Record Linkage) von entsprechenden Gesundheitsdaten zu erwarten sind • Fehler bei der Dateneingabe (z.B. Fehler in der Schreibweise von Namen, Adressen etc)	Integrität	Substantiell	Überschaubar		Wahrung von Maßnahmen des Datenschutzes und der Informationssicherheit in den einzelnen Einrichtungen gemäß der TOMs Vertraulichkeit / Zugriffskontrolle, Zugangs und Verarbeitungskontrolle, Protokollierung Schulung / Informationssystem, Datenschutz		Restrisiko akzeptabel
10	Unerwartete Einschränkung der Datenverfügbarkeit	• Passwort für Zugang zu personenbezogenen Daten durch autorisierte Person nicht verfügbar • Temporärer Verlust von personenbezogenen Daten während privater Lagerung mobiler Speichermedien	Verfügbarkeit	Substantiell	Überschaubar		Belastbarkeit / Ausfallsicherheit / Technische Maßnahmen: Wiederherstellbarkeit in Zeitspanne, die keine Gefährdung der Patientenbehandlung sicherstellt, gewährleistet und Verfahren wird regelmäßig auf Funktionsfähigkeit geprüft; Prüfung wird dokumentiert Backup garantiert eine zusätzliche Möglichkeit der Wiederherstellung, allerdings mit einem höheren Zeitaufwand	Verfügbarkeit / Recoverykonzept	Restrisiko akzeptabel
11	Unerwarteter Datenverlust	• Verlust/Zerstörung von digitalen personenbezogenen Daten (z.B. Verlust oder Zerstörung des Speichermediums) durch interne Personen • Verlust/Zerstörung von personenbezogenen Daten im Papierformat (z.B. Verlust von ausgefüllten Erhebungsbögen)	Verfügbarkeit	Substantiell	Überschaubar		Verfügbarkeit / Backupkonzept, Verschlüsselung auf Datenträger Belastbarkeit / Ausfallsicherheit / Technische Maßnahmen: Unterbrechungsfreie Stromversorgung		Restrisiko akzeptabel

Datenschutzkonzept Deutsches Mukoviszidose-Register – Version 3.1

12	Einschränkung des Auskunftsrechts	• Ansprechperson in der verantwortlichen Stelle für betroffene Person temporär nicht verfügbar • Passwort für Zugang zu personenbezogenen Daten durch autorisierte Person nicht verfügbar • Temporärer Verlust von personenbezogenen Daten während privater Lagerung mobiler Speichermedien • Berechtigung zur Herausgabe der personenbezogenen Daten liegt nicht vor	Transparenz	Überschaubar	Überschaubar		Wahrung von Maßnahmen des Datenschutzes und der Informationssicherheit in den einzelnen Einrichtungen gemäß der TOMs Vertraulichkeit / Zugriffskontrolle, Zugangs- und Verarbeitungskontrolle, Protokollierung Schulung / Informationssystem, Datenschutz		Restrisiko akzeptabel
13	Einschränkung des Löschrchts (inkl. Widerruf und Widerspruch)	• Verarbeitung von Patienten- oder Probandendaten ohne Wissen der betroffenen Person • Verantwortliche Stelle verarbeitet personenbezogene Daten trotz erfolgtem Widerspruchs/Widerrufs unbegründet weiter • zuständige Stelle für das Löschrcht der betroffenen Person nicht bekannt • Ansprechperson in der verantwortlichen Stelle für betroffene Person temporär nicht verfügbar • unberechtigte Löschung der betreffenden Patienten-/Probandendaten • bei eingegangenem Widerruf/Widerspruch unzureichende Löschung der Daten, z.B. aufgrund der Nutzung in verschiedenen Datensätzen • Verantwortliche Stelle unterlässt Information der betroffenen Person über Art. 21 Absätze 1 und 2 DSGVO des Widerspruchsrechts	Vertraulichkeit	Überschaubar	Überschaubar		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	Aufgrund der technischen und organisatorischen Maßnahmen (TOMs) sowie der vertraglichen Verpflichtungen mit den am Register beteiligten Dienstleistern und den in diesem Datenschutzrahmenkonzept getroffenen Maßnahmen dürfte vom jetzigen Stand der Technik aus betrachtet keine weitere Maßnahmen erforderlich sein.	Restrisiko akzeptabel
14	Statistische Analyse		Integrität Vertraulichkeit Nichtverkettung Intervenierbarkeit.	Überschaubar	Überschaubar		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	Aufgrund der technischen und organisatorischen Maßnahmen (TOMs) sowie der vertraglichen Verpflichtungen mit den am Register beteiligten Dienstleistern und den in diesem Datenschutzrahmenkonzept getroffenen Maßnahmen dürfte vom jetzigen Stand der Technik aus betrachtet keine weitere Maßnahmen erforderlich sein.	Restrisiko akzeptabel

15	Studienunterstützung		Integrität Vertraulichkeit	Überschaubar	Überschaubar		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 (ggf. 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 MUKOweb-Software in pseudonymisierter Form i. weitere Verarbeitung und Bereitstellung der Daten nach SOPs mit Dokumentation für Nachvollziehbarkeit	Aufgrund der technischen und organisatorischen Maßnahmen (TOMs) sowie der vertraglichen Verpflichtungen mit den am Register beteiligten Dienstleistern und den in diesem Datenschutzrahmenkonzept getroffenen Maßnahmen dürfte vom jetzigen Stand der Technik aus betrachtet keine weitere Maßnahmen erforderlich sein.	Restrisiko akzeptabel
----	----------------------	--	-------------------------------	--------------	--------------	--	--	--	-----------------------