Schablone zur Ergänzung eines Datenschutzkonzepts bei Einsatz eines OSSE-Brückenkopfs

Dr. Marita Muscholl\*\*, Martin Lablans\*\*, Andreas Borg\*\*, Prof. Dr. Frank Ückert\*\*, Prof. Dr. TOF Wagner\*

\*Universitätsklinikum Frankfurt am Main

Abteilung Pneumologie

69590 Frankfurt am Main

\*\*Universitätsmedizin der Johannes Gutenberg-Universität Mainz

Institut für Medizinische Biometrie, Epidemiologie und Informatik

55101 Mainz

Hinweise zur Nutzung der Schablone

Ziel der Schablone zur Ergänzung des Datenschutzkonzepts bei Einsatz eines OSSE-Brückenkopfs ist es, individuelle Textpassagen anzubieten, um die ein bereits vorhandenes Datenschutzkonzept ergänzt werden muss, wenn ein OSSE-Brückenkopf eingesetzt wird. Die Schablone berücksichtigt alle Komponenten, die Teil des OSSE-Brückenkopfs sind oder im Zusammenhang mit diesem verwendet werden sowie die Datenflüsse zwischen diesen Komponenten. Maßnahmen zum Datenschutz, die Teil der Softwarefunktionen sind, werden beschrieben. Zu ergänzende Informationen zu organisatorischen Strukturen oder Abläufen oder zu darüber hinaus verwendeten, eigenen IT-Komponenten sind im Text markiert. Technische Maßnahmen, die nicht Teil der Software sind, sind als Vorschläge zu sehen.

### Markierungen und ihre Bedeutung

* *Stellen im Text, an denen Information zu ergänzen ist oder Platzhalter zu ersetzen sind, sind grau markiert* [*und als Kommentare ggf. in eckige Klammern gesetzt*]
* Abschnitte im Text, für die es je nach den lokalen Gegebenheiten verschiedenen Varianten gibt, sind mit gelb unterlegten Beginn- und Ende-Markierungen geklammert oder, wenn es sich nur um einen Satz handelt, durch eine Markierung am Satzanfang gekennzeichnet:   
  [*#Beginn* ***Variante n*** *(hier ist die Variante beschrieben)*] … [*#Ende* ***Variante n***]  
  [*Gilt nur für* ***Variante m***] …
* Hinweise zu einzelnen Abschnitten sind ebenfalls in eckigen Klammern und gelb hinterlegt: [*Dieser Abschnitt soll folgendermaßen bearbeitet werden …*]

### Vorgehen bei der Bearbeitung

1. Ersetzen Sie in der Schablone den Platzhalter „Register für „Seltene Erkrankung X“ durch den Namen Ihres Registers.
2. Beantworten Sie sich folgende Fragen, die für die Auswahl der Varianten oder zu ergänzenden Informationen notwendig sind:
3. *Wer wird den OSSE-Brückenkopf betreiben (hat üblicherweise die notwendige zentrale Hardware unter seiner Kontrolle)?*
4. *Welche Daten werden in den OSSE-Brückenkopf transferiert (z.B. Gewicht, Geburtsdatum, Diagnose als Orphacode)? (🡪 ergibt einen Anhang)*
5. *Sind die Daten im Register bereits pseudonymisiert, oder sind die identifizierenden Daten mit den medizinischen Daten zusammen gespeichert?*
6. *Falls die Daten im Register nicht pseudonymisiert sind, müssen sie beim Transfer in den Brückenkopf pseudonymisiert werden. Wo ist das Identitätsmanagement zur Pseudonymisierung der Daten angesiedelt und wer betreibt es? (folgende Varianten sind möglich)*
   * *Es gibt ein Identitätsmanagement, das für alle OSSE-Register/‑Brückenköpfe für „Seltene Erkrankung X“ zentral betrieben wird (damit bei Forschungsprojekten mit anderen Registern identische Patienten in verschiedenen Registern erkannt werden können)[[1]](#footnote-2).*
   * *Für den OSSE-Brückenkopf soll ein eigenes Identitätsmanagement betrieben werden.*
7. *Werden Daten zu Biomaterialproben in den OSSE-Brückenkopf importiert (und welche)?*
   * *Falls ja, □ aus einer Biomaterialbank? □ direkt von der Probenquelle?*
8. Ersetzen Sie die Platzhalter und ergänzen Sie die abgefragten Informationen.
9. Löschen Sie überflüssige Abschnitte.
10. Löschen Sie die Kommentare und Markierungen.
11. Lesen Sie dabei die gesamte Schablone sorgfältig durch und fügen Sie die hinsichtlich Ihrer spezifischen Umgebung (IT-Infrastruktur, Organisation, etc.) angepassten Textpassagen in Ihr Datenschutzkonzept ein oder fügen Sie die angepasste Schablone als Anhang an.

Logo_UKF_-_rgb

OSSE-Brückenkopf zum Register für „Seltene Erkrankung X“

Ergänzungen für das Datenschutzkonzept[[2]](#footnote-3)

Projekt OSSE-Brückenkopf zum Register für „Seltene Erkrankung X“

Autoren [*Autoren*]

[*Institution(en)*]

[*Träger (Name und Adresse)*]

Version [*Datum*]

Inhalt

[1. Einleitung 6](#_Toc395794485)

[1.1 Überblick über die Datenverarbeitung beim Einsatz eines OSSE-Brückenkopfs 6](#_Toc395794486)

[2. Datenverarbeitende Komponenten beim Einsatz des OSSE-Brückenkopfes 6](#_Toc395794487)

[2.1 Der OSSE-Brückenkopf 6](#_Toc395794488)

[2.2 Identitätsmanagement für die Nutzung des OSSE-Brückenkopfs 7](#_Toc395794489)

[Pseudonyme 7](#_Toc395794490)

[Manuelles Linken 8](#_Toc395794491)

[2.3 Metadaten-Repository 8](#_Toc395794492)

[2.4 Registerverzeichnis (Registry of Registries) 8](#_Toc395794493)

[3. Datenverarbeitende Prozesse beim Einsatz eines OSSE-Brückenkopfes 8](#_Toc395794494)

[3.1 Datenimport in den Brückenkopf 8](#_Toc395794495)

[3.2 Pseudonymisierung 10](#_Toc395794496)

[Pseudonymisierung beim Datenimport 10](#_Toc395794497)

[Schlüsselerzeugung und Schlüsselverwaltung 10](#_Toc395794498)

[3.3 Import von Biomaterialdaten 10](#_Toc395794499)

[3.4 Datenexport 13](#_Toc395794500)

[3.5 Dezentrale Suche 14](#_Toc395794501)

[3.6 Hochladen von Informationen an das Registerverzeichnis 15](#_Toc395794502)

[4. Organisatorische Rahmenbedingungen 15](#_Toc395794503)

[4.1 Betrieb der Komponenten 15](#_Toc395794504)

[4.2 Zugriff durch Systemadministratoren 15](#_Toc395794505)

[4.3 Teilnehmende Forscher 15](#_Toc395794506)

[4.4 Ausschuss für Datenschutz 15](#_Toc395794507)

[5. Maßnahmen zum Datenschutz 16](#_Toc395794508)

[5.1 Informationelle Gewaltenteilung 16](#_Toc395794509)

[5.2 Autorisierung und Authentifizierung 16](#_Toc395794510)

[Autorisierung von Benutzern 16](#_Toc395794511)

[Autorisierung von Komponenten 16](#_Toc395794512)

[Authentifizierung von Benutzern 16](#_Toc395794513)

[Authentifizierung von Komponenten 16](#_Toc395794514)

[5.3 Maßnahmen in der IT-Infrastruktur 16](#_Toc395794515)

[Sicherheit der Kommunikation 16](#_Toc395794516)

[Protokollierung 17](#_Toc395794517)

[6. Wahrung von Betroffenenrechten 17](#_Toc395794518)

[6.1 Aufklärung und Einwilligung 17](#_Toc395794519)

[6.2 Auskunft über gespeicherte Daten 17](#_Toc395794520)

[6.3 Widerruf, Löschung, Anonymisierung 17](#_Toc395794521)

[7. Anhang 19](#_Toc395794522)

[7.1 Datensätze 19](#_Toc395794523)

[Transfer-Datensatz für den Brückenkopf 19](#_Toc395794524)

[Identifizierende Daten 19](#_Toc395794525)

# Einleitung

## Überblick über die Datenverarbeitung beim Einsatz eines OSSE-Brückenkopfs

In den OSSE-Brückenkopf werden Daten aus dem Register für „Seltene Erkrankung X“ übernommen, die für Kooperationsprojekte mit anderen Registern genutzt werden können sollen. Zu diesem Zweck unterstützt der OSSE-Brückenkopf die „Dezentrale Suche“, eine Anfrage-Infrastruktur, mit der in vernetzten OSSE-Registern und ‑Brückenköpfen nach definierten Fällen gesucht werden kann. Die Anfrage, bestehend aus einem Exposé zur geplanten Forschungsfragestellung, den Kontaktdaten des Anfragenden[[3]](#footnote-4) und den Suchkriterien, wird zusammen mit den Ergebnissen [dem/den Datenverantwortlichen des Registers] elektronisch-automatisch vorgelegt. Diese(r) hat/haben dann die Möglichkeit, die Anfrage auf inhaltliche Kriterien und rechtliche Zulässigkeit zu prüfen und, falls beides positiv ausfällt, manuell auf diese Anfrage zu antworten und ggf. die Datensätze zu übermitteln. Diese Art der Suche kommt am ehesten einer klassischen schriftlichen Anfrage gleich, nur dass durch die Vernetzung der Register schon geklärt ist, wo eine Anfrage bezüglich geeigneter Datensätze sinnvoll sein kann und somit ihre Begutachtung und Beantwortung durch technische Hilfsmittel unterstützt werden. Um die Vergleichbarkeit und die gezielte Abfrage von Dateninhalten in verschiedenen Datenquellen zu ermöglichen, ist das Datenschema des OSSE-Brückenkopfes mit einer formalen Definition aller Datenfelder verknüpft, die in Form von Metadaten im zentralen Metadaten Repository (MDR) registriert ist. Dies gilt gleichermaßen für alle Teilnehmer der Dezentralen Suche (OSSE-Register und OSSE-Brückenköpfe).

Eine detaillierte Beschreibung der Komponenten und Prozesse wird in den Abschnitten 2 und 3 gegeben.

# Datenverarbeitende Komponenten beim Einsatz des OSSE-Brückenkopfes

## Der OSSE-Brückenkopf

Der OSSE-Brückenkopf dient dazu, die Daten des Registers für „Seltene Erkrankung X“ für die dezentrale Suche (siehe 3.5 Dezentrale Suche) nutzbar zu machen. Dazu werden Daten aus dem Register für „Seltene Erkrankung X“ extrahiert, transformiert und in den OSSE-Brückenkopf geladen. Im Transformationsschritt findet eine Datenharmonisierung auf der Basis der Metadaten des MDR statt, indem jedem Datenfeld eine semantisch zugehörige MDR-ID zugeordnet wird. Zusätzlich zu den medizinischen Stamm- und Verlaufsdaten aus dem Register für „Seltene Erkrankung X“ können auch Daten zu Biomaterialproben importiert werden. Der OSSE-Brückenkopf speichert keine identifizierenden Daten (IDAT) der Patienten.

[*Im Folgenden zwei Szenarien für die Pseudonymisierung der Daten im Brückenkopf:*]

[***Szenario 1*** *(Daten im Register liegen bereits pseudonymisiert vor)*] Da die Daten im Register für „Seltene Erkrankung X“ pseudonymisiert vorliegen, werden diese Pseudonyme identisch übernommen.

[***Szenario 2*** *(Das Register enthält IDAT)*] Die IDAT, die im Register für „Seltene Erkrankung X“ zusammen mit den medizinischen Daten (MDAT) gespeichert sind, werden bei der Transformation der Daten für den Datenimport mithilfe der Mainzelliste durch Pseudonyme ersetzt.

Der Brückenkopf besteht aus den folgenden Softwarekomponenten:

* dem OSSE-Store, dem Datenspeicher, in den die Daten importiert werden und der Funktionen für den Datenimport und ‑export besitzt sowie eine Abfrage-Schnittstelle für die „Dezentralen Suche“, und
* dem Teiler (OSSE-Share), dem Client-Interface für die dezentrale Suche (siehe 3.5 „Dezentrale Suche“). Er ruft über den Suchbroker gestellte Anfragen ab, kommuniziert mit dem OSSE-Store und zeigt einem berechtigten Benutzer Anfrage und Ergebnis bestehend aus dem Anfrage-Exposé, den Ergebnissen und den Kontaktdaten des Anfragenden an. Hierbei werden nur pseudonymisierte und aggregierte Daten angezeigt. Der Datenverantwortliche kann mit dem Teiler-Interface einen Datenexport anstoßen. Die exportierten Daten enthalten nicht-rückführbare Exportpseudonyme anstelle der in OSSE gespeicherten Pseudonyme. Über die Weitergabe von derart „quasi anonymisierten“ Forschungsdaten an Dritte entscheidet [*hier das zuständige Gremium angeben*]. Es muss sichergestellt werden, dass die Weitergabe der exportierten Daten mit der in den Einwilligungen beschriebenen Datennutzung konform ist, da speziell im Bereich seltener Erkrankungen allein durch die medizinischen Daten ein hohes Reidentifizierungs-Risiko besteht.

[*Falls für den OSSE-Brückenkopf kein Identitätsmanagement eingesetzt wird, entfällt der folgende Abschnitt*]

## Identitätsmanagement für die Nutzung des OSSE-Brückenkopfs

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.

### Pseudonyme

[*#Beginn* ***Variante 1*** *(Zentrales ID-Management für alle Register für „Seltene Erkrankung X“)*]

Für die Pseudonymisierung im OSSE-Brückenkopf wird eine Instanz der „Mainzelliste[[4]](#footnote-5)“ genutzt, die zentral für alle OSSE-Register und ‑Brückenköpfe für „Seltene Erkrankung X“ von [*Betreiber der zentralen Mainzelliste*] betrieben wird. Sie erzeugt für jeden Patienten einen eindeutigen PID und je ein unabhängiges Pseudonym zweiter Stufe (PSN*OSSE*(#)) für jedes OSSE-Register bzw. jeden OSSE-Brückenkopf, in dem Daten des Patienten gespeichert werden.

Die Mainzelliste erzeugt außerdem nicht-rückführbare Exportpseudonyme für den Export von Patientendaten zu Forschungszwecken, wobei im Fall einer Zusammenführung von Fällen aus verschiedenen Registern oder Brückenköpfen für „Seltene Erkrankung X“ Daten identischer Patienten, dasselbe Exportpseudonym erhalten. Das zentrale Identitätsmanagement ermöglicht eine datenschutzgerechte Zusammenführung der zu verschiedenen Zeitpunkten und von verschiedenen Standorten (und in verschiedene Register) erfassten bzw. importierten patientenbeziehbaren Daten eines Patienten.

[*#Ende Variante 1*]

[*#*Beginn ***Variante 2*** *(Lokal betriebenes ID-Management für dieses Register für „Seltene Erkrankung X“)*]

Für die Pseudonymisierung im OSSE-Brückenkopf wird eine Instanz der „Mainzelliste“ genutzt, die von [*Betreiber der Mainzelliste*] betrieben wird. Sie erzeugt für jeden Patienten einen eindeutigen PID und ein Pseudonym zweiter Stufe (PSN*OSSE*).

Die Mainzelliste erzeugt außerdem nicht-rückführbare Exportpseudonyme für den Export von Patientendaten zu Forschungszwecken, wobei im Fall einer Zusammenführung von Fällen aus verschiedenen Registern oder Brückenköpfen für „Seltene Erkrankung X“ Daten identischer Patienten, unterschiedliche Exportpseudonyme erhalten. Das lokale Identitätsmanagement ermöglicht also eine datenschutzgerechte Zusammenführung der zu verschiedenen Zeitpunkten und von mehreren Standorten erfassten bzw. importierten patientenbeziehbaren Daten, jedoch ohne dass Daten identischer Patienten aus verschiedenen Registern einander zugeordnet werden können.

[*#Ende Variante 2*]

### Manuelles Linken

Eine Schnittstelle erlaubt 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, zur Entscheidungsfindung auf medizinische Daten zuzugreifen.

## Metadaten-Repository

Das Metadaten-Repository (MDR) speichert die Bedeutung (Semantik) sämtlicher im OSSE-Brückenkopf für „Seltene Erkrankung X“ verwendeten (Nutz-)Datenelemente. Es bietet ein kontrolliertes Vokabular (Syntax) und kann maschinenlesbare, strukturierte Aussagen über Datenelemente treffen, beispielsweise konzeptuelle Domänen oder Wertebereiche. Hier sind auch die Felder der in diesem Konzept genannten Registerformulare (7.1 Datensätze) definiert. Da das MDR keine personenbezogenen Daten verarbeitet, wird innerhalb dieses Datenschutzkonzepts nicht weiter darauf eingegangen.

## Registerverzeichnis (Registry of Registries)

Im Registerverzeichnis registrieren sich alle OSSE-Register und ‑Brückenköpfe mit einer Kurzbeschreibung des Registers, den Ansprechpartnern und ggf. zusätzlich den Metadaten des Registers und interessanten Kerndaten (z.B. Anzahl der Fälle insgesamt). Die Daten werden von den Verantwortlichen aktiv hochgeladen. Es werden keine Patientendaten übertragen. Das Registerverzeichnis wird von [*Hier den Betreiber des Registerverzeichnisses angeben*] betrieben.

# Datenverarbeitende Prozesse beim Einsatz eines OSSE-Brückenkopfes

## Datenimport in den Brückenkopf

Für den Datenimport in den Brückenkopf wird ein sogenannter ETL[[5]](#footnote-6)-Prozess durchlaufen.

[*#Beginn Szenario 1 (Das bestehende Register enthält Pseudonyme, die in den Brückenkopf übernommen werden)*]

Dazu werden die **pseudonymisierten** Daten (in regelmäßigen Zeitabständen) aus dem existierenden Register [und der Biomaterialbank *(falls ein Biobankmodul existiert)*] extrahiert. Der ETL-Prozess lädt die Daten über eine Web-Schnittstelle in den OSSE-Brückenkopf, wobei er sich mit Login und Passwort authentisiert.

[*#Ende Szenario 1*]

Abbildung 1: Datenimport in den Brückenkopf

[*#Beginn Szenario 2 (Das bestehende Register enthält IDAT)*]

Abbildung 1: Datenimport in den Brückenkopf.

Abbildung 1: zeigt die Schritte, in denen Daten in den OSSE-Brückenkopf importiert werden:

1. Identifizierende, medizinische und Probendaten werden (in regelmäßigen Zeitabständen) aus dem existierenden Register [und der Biomaterialbank *(falls ein Biobankmodul existiert)*] extrahiert.
2. Identifizierende Daten werden innerhalb des Transformationsschrittes durch ein Pseudonym ersetzt (Details siehe Abschnitt 3.2 „Pseudonymisierung“).
3. Der ETL-Prozess lädt die Daten über eine Web-Schnittstelle in den OSSE-Brückenkopf, wobei er sich mit Login und Passwort authentisiert.

## Pseudonymisierung

### Pseudonymisierung beim Datenimport

Beim Datenimport aus dem bereits existierenden Register werden die IDAT vor dem Laden der Datensätze pseudonymisiert. Datenextraktion und -transformation werden durch eine Datenintegrations-Software (Talend Open Studio) unterstützt. Dabei ist die Pseudonymisierung Teil der Daten-Transformation und wird mit einer eigens dafür entwickelten Komponente durchgeführt. Folgende Schritte werden durchlaufen:

1. Für jeden Datensatz ruft die Datenintegrationssoftware die Mainzelliste auf und übergibt die IDAT.
2. Die Mainzelliste ermittelt oder erzeugt das PSNOSSE und verschlüsselt es mit einem öffentlichen Schlüssel des OSSE-Brückenkopfs, damit das OSSE-Pseudonym nicht außerhalb der Mainzelliste mit den IDAT zusammengeführt werden kann.
3. Die Mainzelliste liefert das verschlüsselte Pseudonym, (PSNOSSE)tr, an die Transformationskomponente, wo die IDAT durch das (PSNOSSE)tr ersetzt werden.
4. Die Importschnittstelle entschlüsselt das (PSNOSSE)tr und speichert die Daten mit dem PSNOSSE.

Durch dieses Verfahren ist sichergestellt, dass beim Datenimport keine Pseudonyme zugeordnet werden können, da die Daten liefernde Seite, die den Patientenbezug herstellen kann, nur das verschlüsselte (PSNOSSE)tr sieht.

### Schlüsselerzeugung und Schlüsselverwaltung

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

[*#Ende Szenario 2*]

[*Der folgende Abschnitt (Import von Biomaterialdaten) wird benötigt, falls Bioprobendaten direkt in den Brückenkopf importiert werden sollen, also nicht bereits im bestehenden Register gespeichert werden. Dabei wird unterschieden, ob die Probendaten direkt von der Probenquelle stammen oder der Verbund eine separate Biomaterialbank nutzt. Im zweiten Fall wird vorausgesetzt, dass die Biomaterialbank, gemäß dem „Datenschutzkonzept der TMF für Biomaterialbanken“[[6]](#footnote-7), die LabID von der Probenquelle nicht im Klartext sondern in verschlüsselter Form weitergibt und selbst keinen Patientenbezug speichert. Abweichende Realisierungen sind im folgenden Abschnitt entsprechend anzupassen.)*]

## Import von Biomaterialdaten

[#Beginn Biomaterialbank existiert]

Durch die Anbindung einer Biomaterialbank sollen Information über Bioproben zur Verfügung gestellt werden, die ermöglichen, aus dem Register geeignete Patienten für Forschungsvorhaben zu ermitteln. Daten zu Bioproben (IDAT, PID, LabID, weitere Charakteristika der Probe) werden im Behandlungszusammenhang erfasst (Probenquelle) und an die Biomaterialbank übertragen. Der an der Probenquelle erzeugte eindeutige Identifikator der Probe, LabID, wird in der Biomaterialbank verschlüsselt (LabID)tr. Die Biomaterialbank speichert Proben ohne Patientenbezug; deshalb soll der Patientenbezug der Probe für die Weitergabe an den Brückenkopf nur temporär (bis zur Übertragung der Probendaten) gespeichert werden. Die Daten im Brückenkopf erlauben keinen direkten Abruf von Informationen zur Probe von der Probenquelle. Folgende Daten aus der Biomaterialbank werden in den OSSE-Brückenkopf importiert: [*Unzutreffendes aus der Aufzählung streichen!*]

* Existenz bzw. Anzahl der Proben,
* Charakteristika zur Probe
* sowie die (LabID)tr

Abbildung 2: Datenflüsse beim Import von Biomaterialdaten

Beim Import von Biomaterialdaten werden folgende Schritte durchlaufen:

1. Der Patient wird durch die Probenquelle in der Mainzelliste registriert: Die Probenquelle schickt IDAT und erhält das verschlüsselte OSSE-Pseudonym (PSNOSSE)tr und, falls erforderlich, den allgemein gültigen PID.
2. Die Probe wird an die Biobank übermittelt: Das Adressetikett enthält das (PSNOSSE)tr das für die Datenübermittlung an das Register zwischengespeichert wird.
3. Die Probe wird im Biobankenmodul registriert: Das Biobankenmodul speichert die LabID und alle notwendigen Daten zur Probe (OrgDat). Aus der LabID wird durch eine kryptografische Operation die LabIDtr erzeugt, damit eine direkte Zuordnung von Datensatz und Probe vermieden werden kann. Eine Zuordnung von (PSNOSSE)tr und LabIDtr wird temporär gespeichert.

Übertragung der Probendaten an den OSSE-Brückenkopf: Der OSSE-Brückenkopf erhält zu jeder Probe einen Datensatz bestehend aus (PSNOSSE)tr, LabIDtr und weiteren Information zur Probe (siehe oben), die übermittelt werden sollen. Die Daten werden, wie unter 3.1 „Datenimport in den Brückenkopf“ beschrieben, transformiert und in den OSSE-Brückenkopf geladen. Nach erfolgreicher Übertragung wird die Zuordnung (PSNOSSE)tr und LabIDtr gelöscht. Dadurch wird verhindert, dass in der Biomaterialbank dauerhaft eine Zuordnung zwischen Probe und Patient hergestellt wird.

[#*Ende Biomaterialbank existiert*]

[#Beginn Biomaterialbank existiert nicht]

Im OSSE-Brückenkopf des Registers für „Seltene Erkrankung X“ sollen Information über Bioproben zur Verfügung gestellt werden, die ermöglichen, aus dem Register geeignete Patienten für Forschungsvorhaben zu ermitteln. Daten zu Bioproben (IDAT, PID, LabID, weitere Charakteristika der Probe) werden im Behandlungszusammenhang erfasst (Probenquelle). Folgende Daten werden in den OSSE-Brückenkopf importiert:

[*Unzutreffendes aus der Aufzählung streichen!*]

* Existenz bzw. Anzahl der Proben,
* Charakteristika zur Probe

Beim Import von Biomaterialdaten werden folgende Schritte durchlaufen:

1. Der Patient wird durch die Probenquelle in der Mainzelliste registriert: Die Probenquelle schickt IDAT und erhält das verschlüsselte OSSE-Pseudonym (PSNOSSE)tr und falls erforderlich, den allgemein gültigen PID.
2. Übertragung von Probendaten aus der Probenquelle an das OSSE-Brückenkopf: Der OSSE-Brückenkopf erhält zu jeder Probe einen Datensatz bestehend aus (PSNOSSE)tr und weiteren Information zur Probe (siehe oben), die übermittelt werden sollen. Daten von der Probenquelle werden, wie unter 3.1 „Datenimport in den Brückenkopf“ beschrieben, transformiert und in den OSSE-Brückenkopf geladen.  
   [*Falls es nicht möglich ist*,das (PSNOSSE)tr *in der Probenquelle zwischenzuspeichern, kann es mithilfe der IDAT über den Pseudonymisierungsschritt im ETL-Prozess abgerufen werden*. *Der Abschnitt ist entsprechend anzupassen.*]



Abbildung 2: Datenflüsse beim Import von Biomaterialdaten

[#*Ende Biomaterialbank existiert nicht*]

## Datenexport

Daten können zu Auswertungszwecken exportiert werden. Dafür wird das interne Pseudonym des OSSE-Brückenkopfs im Exportschritt durch ein Exportpseudonym ersetzt.

[*#Beginn Variante 1 (Es gibt eine zentrale Mainzelliste, von der der Brückenkopf die Pseudonyme erhält)*]

Werden im Rahmen der dezentralen Suche Daten aus verschiedenen Registern zusammengeführt, so werden beim Export einheitliche nicht-rückführbare Exportpseudonyme bei der zentralen Mainzelliste abgefragt. Diese erlauben, in den zusammengeführten Datenbeständen Datensätze identischer Patienten zuzuordnen, die in verschiedenen Registern erfasst wurden, sowie die konsistente Aktualisierung der zusammengeführten Datensätze. Folgende Schritte werden beim Export durchlaufen:

1. OSSE schickt das interne Pseudonym PSNOSSE(#) zusammen mit einer Projektkennung an die Mainzelliste.
2. Die Mainzelliste liefert ein einheitliches projektspezifisches Exportpeusonym (PSNProjekt) zurück.
3. Der Datensatz wird mit dem PSNProjekt ausgegeben.

[*#Ende Variante 1*]

[*#Beginn Variante 2 (Es gibt eine „lokale“ Mainzelliste, von der der Brückenkopf die Pseudonyme erhält)*]

Werden im Rahmen der dezentralen Suche Daten aus verschiedenen Registern zusammengeführt, so werden beim Export einheitliche nicht-rückführbare Exportpseudonyme bei der lokalen Mainzelliste abgefragt. Diese erlauben die konsistente Aktualisierung der zusammengeführten Datensätze, identische Patienten verschiedener Register werden dabei aber nicht erkannt. Folgende Schritte werden beim Export durchlaufen:

1. OSSE schickt das interne Pseudonym PSNOSSE zusammen mit einer Projektkennung an die Mainzelliste.
2. Die Mainzelliste liefert ein projektspezifisches Exportpeusonym (PSNProjekt) zurück.
3. Der Datensatz wird mit dem PSNProjekt ausgegeben.

[*#Ende Variante 2*]

Besonders bei Erkrankungen mit geringen Fallzahlen lassen sich medizinische Daten bei Kenntnis des Krankheitsverlaufs oder zusätzlicher Daten auch ohne Kenntnis der identifizierbaren Daten konkreten Patienten zuordnen. Auch bei der Verwendung nicht-rückführbarer Exportpseudonyme kann nicht immer sicher von faktischer Anonymität ausgegangen werden. Deshalb wird auch der Export pseudonymisierter Daten und der Zweck ihrer Nutzung in der informierten Einwilligung berücksichtigt.

## Dezentrale Suche

Mit der dezentralen Suche können OSSE-Forscher die Datenbestände der OSSE-Register oder ‑Brückenköpfe durchsuchen, um die Standorte zu ermitteln, an denen Daten und Proben von Patienten vorhanden sind, die für ein Forschungsvorhaben relevant sein könnten. Der Suchbroker stellt für die Suche ein Webformular bereit, in dem Suchanfragen erfasst werden können, die Datenelemente nach vorgegebenen Werten oder per Freitextsuche filtern. Mehrere Suchattribute können durch logische Operatoren frei kombiniert werden. Mit dem Suchformular wird außerdem eine Exposé des geplanten Forschungsvorhabens und die Kontaktdaten des anfragenden Forschers übermittelt.

Die Suchanfrage wird zunächst gespeichert und dem anfragenden Forscher lediglich die Speicherung der Suchanfrage mitgeteilt. Die Teiler der Standorte rufen in regelmäßigen Abständen neu hinzugekommene Suchanfragen vom Suchbroker ab und ermitteln, welche Datensätze im OSSE-Brückenkopf den Suchkriterien entsprechen. Der Inhalt der Anfrage sowie die gefundenen Datensätze können an jedem Standort von einer dazu berechtigten Person eingesehen werden. Diese kann nun den anfragenden Forscher kontaktieren, um eine mögliche Weitergabe von Daten oder Proben zu vereinbaren. Dieser Vorgang und die damit verbundenen datenschutzrechtlichen Fragen, wie z.B. die Notwendigkeit, weitere Einwilligungen einzuholen, müssen im Einzelfall von den beteiligten Personen geklärt werden. Eine Übermittlung von Daten findet kontrolliert außerhalb des OSSE-Brückenkopfes statt.

## Hochladen von Informationen an das Registerverzeichnis

Durch eine Menüfunktion, die von einem berechtigten Benutzer ausgeführt wird, können Informationen über den OSSE-Brückenkopf zum Register für „Seltene Erkrankung X“ an das Registerverzeichnis hochgeladen werden (Neuregistrierung und Aktualisierung). Der Umfang der hochzuladenden Informationen kann in der Konfiguration des Brückenkopfs eingestellt werden. Inhaltsdaten des Registers betrifft dies nicht (siehe 2.4 „Registerverzeichnis (Registry of Registries)“).

# Organisatorische Rahmenbedingungen

[*In Verbindung mit den organisatorischen Rahmenbedingungen sind auch die vertraglichen Regelungen (z.B. eine Satzung oder Vergleichbares) zu nennen, die im Falle eines Rechtsstreits belastbar sind.*]

## Betrieb der Komponenten

Der Betrieb des OSSE-Brückenkopfs erfolgt durch [*hier den Standort/die Institution angeben, die den OSSE-Brückenkopf betreibt und administriert*].

Den Betrieb der zentralen Komponenten, die im Zusammenhang mit der Nutzung des OSSE-Brückenkopfes eingesetzt werden, übernehmen folgende Institutionen:

* Identitätsmanagement: [*Betreiber der Mainzelliste hier angeben*]
* MDR: [*Betreiber des MDR hier angeben*]

Zum Zweck der informationellen Gewaltenteilung wird der organisatorisch unabhängige Betrieb von Identitätsmanagement und OSSE-Brückenkopf gewährleistet (vgl. Abschnitt 5.1, „Informationelle Gewaltenteilung“).

## Zugriff durch Systemadministratoren

Die im OSSE-Brückenkopf gespeicherten Daten können prinzipiell von den Administratoren der verwendeten IT-Infrastruktur eingesehen werden. Zugriffe auf die Daten durch Administratoren dürfen nur erfolgen, wenn dies zur Erfüllung ihrer Aufgaben zwingend erforderlich ist. Das Vorgehen beim Datenzugriff ist durch folgenden Prozess geregelt: [*Hier ist zu beschreiben, wie ein derartiger Zugriff abläuft, und wie der Zugriff beispielsweise über die übliche Protokollierung hinaus unter Angabe von Gründen dokumentiert wird*]. Alle Administratoren sind entsprechend zu instruieren und zur Verschwiegenheit zu verpflichten[[7]](#footnote-8).

## Teilnehmende Forscher

*Teilnehmende Forscher* sind die Personen, die über die dezentrale Suche Anfragen stellen können. Generell können alle Mitglieder der Registerstandorte als teilnehmende Forscher den OSSE-Brückenkopf nutzen, wobei jeder Standort selbst entscheidet, welche seiner Mitglieder eine Zugangsberechtigung erhalten (siehe auch Abschnitt 5.2, „Autorisierung und Authentifizierung“).

Wissenschaftler, die nicht Mitglieder eines der Standorte des Registers für „Seltene Erkrankung X“ sind, können auf Antrag vom Ausschuss für Datenschutz oder einem vergleichbaren Gremium (siehe auch Abschnitt 4.4) eine Zugangsberechtigung erhalten. Diese ist angemessen zu befristen.

## Ausschuss für Datenschutz

[*Falls im Register für „Seltene Erkrankung X“ ein Ausschuss für Datenschutz (oder ein vergleichbares Gremium) existiert*, *würden folgende Aufgaben in seinen Aufgabenbereich fallen:*]

* Prüfung und Bewilligung von Anträgen externer Forscher[[8]](#footnote-9) für die Nutzung des OSSE-Brückenkopfs (dezentrale Suche).
* Prüfung und Bewilligung von Anträgen auf Export medizinischer Daten für externe Forschungsprojekte.

Darüber hinaus ist der Ausschuss für Datenschutz erster Ansprechpartner für datenschutzrechtliche Angelegenheiten.

# Maßnahmen zum Datenschutz

[*Falls für den Brückenkopf kein „eigenes“ Identitätsmanagement eingesetzt wird, fällt 5.1. weg*]

## Informationelle Gewaltenteilung

Das Identitätsmanagement wird logisch, physikalisch und organisatorisch getrennt von allen Komponenten betrieben, die MDAT oder Daten zu Bioproben speichern. [*Der Betreiber des Identitätsmanagements* *(hier bitte den Betreiber angeben)*] steht unter eigener rechtlicher Verantwortung und ist dem Betreiber von Brückenkopf und/oder Register gegenüber nicht weisungsgebunden. So ist sichergestellt, dass Personen, die im Brückenkopf oder im Register für „Seltene Erkrankung X“ auf klinische oder Biomaterial-Daten Zugriff haben, keine Zuordnung von Daten zu realen Patienten treffen können.

## Autorisierung und Authentifizierung

### Autorisierung von Benutzern

Die Autorisierung von Benutzern (Zuweisung zu definierten Rollen) des OSSE-Brückenkopfs erfolgt durch lokale Administratoren der jeweiligen Standorte entsprechend den lokalen Strukturen und Erfordernissen.

### Autorisierung von Komponenten

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

### Authentifizierung von Benutzern

Die Authentifizierung von Benutzern gegenüber dem OSSE-Brückenkopf für „Seltene Erkrankung X“ erfolgt über Benutzername und Passwort.

### 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 Nutzername/Passwort oder über Clientzertifikate.

## Maßnahmen in der IT-Infrastruktur

### Sicherheit der Kommunikation

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 werden (siehe <https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html>).

### Protokollierung

Es erfolgt eine Protokollierung der Zugriffe von Forschern auf den OSSE-Brückenkopf sowie Zugriffe zwischen den Komponenten. Das Protokoll enthält mindestens:

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

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

# Wahrung von Betroffenenrechten

## Aufklärung und Einwilligung

[*Die Passagen der Einwilligungserklärung sind entsprechend für den Einsatz des Brückenkopfes zu ergänzen*]

Die informierte Einwilligung ist Rechtsgrundlage der Datenverarbeitung. Mit der Einwilligung erklärt sich der Patient insbesondere dazu bereit, dass

* seine identifizierenden Daten an das Identitätsmanagement übermittelt und dort gespeichert werden,
* medizinische Daten und Daten zu Biomaterialproben aus dem Register pseudonymisiert an den OSSE- Brückenkopf übertragen werden,
* diese Daten von Forschern des Register für „Seltene Erkrankung X“ lokal ausgewertet und gemäß der Funktionsweise der dezentralen Suche durchsucht werden können und
* medizinische Daten und Daten zu Biomaterialproben des Patienten aus dem OSSE-Brückenkopf mit einem nicht-rückführbaren Exportpseudonym exportiert und für Forschungszwecke, die in der Einwilligung näher definiert sind, an externe Forscher, die benannt sind, übermittelt werden.

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

## Auskunft über gespeicherte Daten

[*Der OSSE-Brückenkopf des Registers für die „Seltene Erkrankung X“ enthält insbesondere Daten des bestehenden Registers, so dass eine Auskunft über diese Daten, durch das Register erfolgen kann. Falls er weitere Daten enthält (z.B. Biomaterialdaten), die nicht im bestehenden Register enthalten sind, erhält der Patient auch einen Ausdruck dieser Daten aus dem Brückenkopf. Das Verfahren („An wen richtet der Patient seinen Antrag?“, „Wer stellt den Ausdruck her?“ und „Wie wird er an den Patienten übermittelt?“) richtet sich nach dem Auskunftsverfahren des Registers und muss im Datenschutzkonzept entsprechend ergänzt werden.*]

## Widerruf, Löschung, Anonymisierung

Daten, die im Register für die „Seltene Erkrankung X“ aufgrund eines Widerrufs der Einwilligung gelöscht oder anonymisiert werden, werden auch im OSSE-Brückenkopf gelöscht oder anonymisiert. Im Falle der Anonymisierung werden die Datensätze im Identitätsmanagement gelöscht und das PSNOSSE des Patienten durch ein zufälliges Pseudonym ersetzt.

[*In Bezug auf die Anonymisierbarkeit der Datensätze, dem Umgang mit Daten, die Grundlage einer bereits veröffentlichten Studie sind etc., sollten bereits Regelungen im Datenschutzkonzept des bestehenden Registers festgelegt sein.*]

# Anhang

## Datensätze

### Transfer-Datensatz für den Brückenkopf

### Identifizierende Daten

1. Für eine optimale Nutzung der dezentralen Suche sollten alle Teilnehmer (OSSE-Register und OSSE-Brückenköpfe) ein gemeinsames Identitätsmanagement nutzen, das für die unabhängigen Pseudonyme der verschiedenen Teilnehmer einheitliche Exportpseudonyme erzeugen kann. Gerade im Bereich der Seltenen Erkrankungen ist es entscheidend, identische Patienten in verschiedenen Registern nicht mehrfach zu zählen. [↑](#footnote-ref-2)
2. Dieses Konzept basiert auf dem OSSE-DSK v1.2 von M. Muscholl, M. Lablans, A. Borg, F. Ückert und TOF Wagner. [↑](#footnote-ref-3)
3. Gemeint sind grundsätzlich entsprechende Personen beiden Geschlechts; auf eine neutrale Formulierung wurde aus sprachlichen Gründen verzichtet. [↑](#footnote-ref-4)
4. „Mainzelliste“ steht hier wie auch im Folgenden für ein Identitätsmanagement, das die Schnittstelle der Mainzelliste erfüllt. [↑](#footnote-ref-5)
5. 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. [↑](#footnote-ref-6)
6. Pommerening, K, „Das Datenschutzkonzept der TMF für Biomaterialbanken“. **it – Information Technology** 49 (2007), 352–359 [↑](#footnote-ref-7)
7. Dies sollte in der Regel im Rahmen des Arbeitsverhältnisses an der zuständigen Institution ohnehin geschehen sein. [↑](#footnote-ref-8)
8. D.h. Personen, die nicht zu den Standorten des Registers für „Seltene Erkrankung X“ gehören. [↑](#footnote-ref-9)