Template for the Data Protection Concept of an
OSSE Bridgehead

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

\*Frankfurt University Hospital

Dept. of Pulmonology

69590 Frankfurt am Main, Germany

\*\*Johannes Gutenberg University Medical Center Mainz

Institute of Medical Biostatistics, Epidemiology, and Informatics (IMBEI)

55101 Mainz, Germany

Notes on Using this Template

The goal of this template for the data protection concept of an OSSE bridgehead is offer specific text passages by which an existing data protection concept has to be supplemented upon implementation of an OSSE bridgehead.

The template considers all components that are part of the OSSE bridgehead or are used in its context, along with the data flows between these components. Furthermore, it describes data protection measures that are part of the software features. Information to be complemented on organizational structures or processes or on further IT components used is marked in the texts. Technical measures not part of the software should be considered suggestions.

***Please note:*** *This document is a translation of the original German data protection template for OSSE bridgeheads based on German data protection law and regulations as well as published guidelines on the topic. When using this template, please be aware that you must identify and take into account the appropriate legal and regulatory requirements.*

### Markings and their Meaning

* *Passages in the text where information needs to be complemented or place holders to be substituted are marked gray* [*and put into square brackets as comments where necessary*]
* The beginnings and endings of those sections in the text that require different versions depending on the local conditions are identified by yellow markings in square brackets:
[*#beginning* ***version n*** *(version is described here)*] … [*#end* ***version n***]
[*Only applies to* ***version m***] …
* Notes on particular sections are also put in square brackets and marked yellow: [*This section should be edited in the following way…*]

### Adaptation Procedure

1. Substitute the placeholder “*Registry for Rare Disease X*” with the name of your registry throughout the template.
2. Answer the following questions for yourself, which are necessary for the choice of versions or information to be complemented.
3. *Who will run the OSSE bridgehead (i.e. usually controls the necessary central hardware)?*
4. *Which data are being transferred into the OSSE bridgehead (e.g. weight, date of birth, diagnosis as Orphacode)? (🡪 will result in an appendix)*
5. *Are the registry data already pseudonymized, or are identifying data stored along with the medical data?*
6. *In case the registry data are not pseudonymized, they have to be pseudonymized when transferred into the bridgehead. Who is in charge of the identity management for the pseudonymization of the data and who is running it? (The following options are possible:)*
	* *Identity management is handled centrally for all OSSE registries/bridgeheads for rare disease x (so that, in research projects involving other registries, identical patients can be recognized in various registries)[[1]](#footnote-2).*
	* *The OSSE bridgehead shall involve a proprietary identity management system.*
7. *Are data on biomaterial samples imported into the OSSE bridgehead (and which)?*

*If yes, □ from a biobank? □ directly from the sample source?*

1. Substitute the placeholders and complement the requested information.
2. Erase all unnecessary sections.
3. Erase the comments and markings.
4. Read through the template carefully and insert the passages adjusted based on your specific environment (IT infrastructure, organization etc.) into your data protection concept or add the adjusted template as an appendix.



OSSE Bridgehead for the Registry for Rare Disease X

Amendments to the Data Protection Concept[[2]](#footnote-3)

Project OSSE Bridgehead for the Registry for Rare Disease X

Authors [*Author(s)*]

 [*Institution(s)*]

[*Governing Body (Name and Address)*]

Version [Click to set date]

Content

[1. Introduction 6](#_Toc412628200)

[1.1 Overview of Data Processing When Using an OSSE Bridgehead 6](#_Toc412628201)

[2. Data Processing Components When Using an OSSE Bridgehead 6](#_Toc412628202)

[2.1 The OSSE Bridgehead 6](#_Toc412628203)

[2.2 Identity Management When Using an OSSE Bridgehead 7](#_Toc412628204)

[Pseudonyms 7](#_Toc412628205)

[Manual Linking 7](#_Toc412628206)

[2.3 Metadata Repository 8](#_Toc412628207)

[2.4 Registry of Registries 8](#_Toc412628208)

[3. Data Processing Procedures When Using an OSSE Bridgehead 8](#_Toc412628209)

[3.1 Data Import into the Bridgehead 8](#_Toc412628210)

[3.2 Pseudonymization 10](#_Toc412628211)

[Pseudonymization at Data Import 10](#_Toc412628212)

[Creating and Managing Keys 10](#_Toc412628213)

[3.3 Importing Biomaterial Data 10](#_Toc412628214)

[3.4 Data Export 14](#_Toc412628215)

[3.5 Decentralized Search 14](#_Toc412628216)

[3.6 Uploading Information to the Registry of Registries 15](#_Toc412628217)

[4. Organizational Framework 15](#_Toc412628218)

[4.1 Operation of Components 15](#_Toc412628219)

[4.2 Access by System Administrators 15](#_Toc412628220)

[4.3 Participating Researchers 15](#_Toc412628221)

[4.4 Data Protection Commission 15](#_Toc412628222)

[5. Data Protection Provisions 16](#_Toc412628223)

[5.1 Informational Separation of Powers 16](#_Toc412628224)

[5.2 Authorization and Authentication 16](#_Toc412628225)

[User Authorization 16](#_Toc412628226)

[Authorization of Components 16](#_Toc412628227)

[User Authentication 16](#_Toc412628228)

[Authentication of Components 16](#_Toc412628229)

[5.3 IT Infrastructure Provisions 16](#_Toc412628230)

[Security of Communication 16](#_Toc412628231)

[Logging 16](#_Toc412628232)

[6. Observing the Rights of Affected Individuals 17](#_Toc412628233)

[6.1 Information and Consent 17](#_Toc412628234)

[6.2 Information on Stored Data 17](#_Toc412628235)

[6.3 Revocation, Deletion, Anonymization 17](#_Toc412628236)

[7. Appendix 18](#_Toc412628237)

[7.1 Data Sets 18](#_Toc412628238)

[Transfer Data Set for the OSSE Bridgehead 18](#_Toc412628239)

[Identifying Data 18](#_Toc412628240)

# Introduction

## Overview of Data Processing When Using an OSSE Bridgehead

Data from the Registry for Rare Disease X with the option to be used for project cooperations with other registries are taken over into the OSSE bridgehead. To this end, the OSSE bridgehead supports “decentralized search,” an infrastructure for inquiries that allows networked OSSE registries and bridgeheads to be searched for specified cases. The inquiry, consisting of an exposé of the intended research question, the inquirer’s contact information, and the search criteria, is then automatically presented electronically to the [person(s) in charge of the registry data] together with the results. He/she/they has/have the option to check the inquiry for content criteria and legal legitimacy and, provided both are positive, to manually answer the inquiry and transmit the data sets if applicable. This method comes closest to a written inquiry, except that due to the cross-linking of registries, it is already clear where an inquiry concerning suitable data sets can make sense and therefore an assessment and response are supported by technical resources. To facilitate comparability and targeted inquiries for data content in different data sources, the data schema of an OSSE bridgehead is linked to a formal definition of all data fields registered as metadata in the central metadata repository (MDR). This equally applies to all participants in decentralized search (OSSE registries and OSSE bridgeheads).

Sections 2 and 3 provide a detailed description of the components and processes.

# Data Processing Components When Using an OSSE Bridgehead

## The OSSE Bridgehead

The OSSE bridgehead serves to make data in the Registry for Rare Disease X usable for decentralized search (see section 3.5, “Decentralized Search”). To this end, data from the Registry for Rare Disease X are extracted, transformed, and loaded into the OSSE bridgehead. During transformation, the data are harmonized based on the metadata of MDR, with a semantically corresponding MDR ID being assigned to each data field. In addition to the basic and longitudinal data from the Registry for Rare Disease X, data on biomaterial samples can be imported as well. The OSSE bridgehead does not store a patient’s identifying data (IDAT).

[*The following are two scenarios for data pseudonymization in the bridgehead:*]

[***Scenario 1*** *(Data in the registry are already pseudonymized):*] Since the data in the Registry for Rare Disease X are already pseudonymized, the pseudonyms are taken over identically.

[***Scenario 2*** *(Registry contains IDAT):*] The IDAT stored in the Registry for Rare Disease X together with the medical data (MDAT) are substituted by pseudonyms by way of the *Mainzelliste*[[3]](#footnote-4) during transformation.

The bridgehead consists of the following software components:

* The OSSE store: the data storage into which the data are imported, containing features for the data import and export as well as a query interface for decentralized search; and
* The OSSE share client: the client interface for decentralized search (see section 3.5, “Decentralized Search”). It retrieves inquiries placed via the search broker, communicates with the OSSE store and shows authorized users the inquiry and the output consisting of the inquiry exposé, the results and the inquirer’s contact data. In this, only pseudonymized and aggregated data are shown. The person in charge of the data can trigger a data export via the share client interface. The exported data contain non-traceable export pseudonyms instead of the pseudonyms stored in OSSE. The decision on the transfer of such “quasi-anonymized” research data is made by the [*specify the body in charge here*]. The transfer of the exported data must conform to the data use specified in the patient informed consent, since particularly in the area of rare diseases there is a high risk of re-identification based on medical data alone.

[*The following section does not apply to scenario 1 (no identity management system is used in the OSSE bridgehead.)*]

## Identity Management When Using an OSSE Bridgehead

Pseudonymization is a necessary measure to keep a high level of data protection in order to protect the patient from reverse identification. His/her identifying data (IDAT) are substituted by pseudonyms. When a pseudonym is requested, the data set is checked for correspondence with existing data sets (record linkage). Depending on the degree of IDAT correspondence and on the threshold values set, a new data set is created or an existing one returned.

### Pseudonyms

[*#Beginning* ***version 1*** *(Centralized ID management for all Registries for Rare Disease X):*]

For pseudonymization, the OSSE bridgehead uses an instance of the *Mainzelliste*that is managed centrally for all registries for all registries and bridgeheads for rare disease x by [manager of the central *Mainzelliste*]. It creates a unique identifier (PID) for each patient as well as one independent second-level pseudonym (PSN*OSSE*(#)) for each OSSE registry or each OSSE bridgehead which stores the patient’s data.

Furthermore, the *Mainzelliste* creates non-traceable export pseudonyms for the export of patient data for research purposes, with data of identical patients receiving the same export pseudonym if cases from different registries or bridgeheads for rare disease x are combined. The centralized ID management allows for a patient’s patient-relatable data collected or imported on different occasions at/from different locations (and into different registries) to be combined according to data protection rules.

[*#End version 1*]

[*#Beginning* ***version 2*** *(Local ID management for this Registry for Rare Disease X)*]

For pseudonymization, the OSSE bridgehead uses an instance of the *Mainzelliste* run by [manager of the *Mainzelliste*]. It creates a unique PID and a second-level pseudonym (PSN*OSSE*(#)) for each patient.

Furthermore, the *Mainzelliste* creates non-traceable export pseudonyms for the export of patient data for research purposes, with data of identical patients receiving different export pseudonyms if cases from different registries or bridgeheads for rare disease x are combined. This means that the local ID management allows for a patient’s patient-relatable data collected or imported on different occasions at/from different locations (and into different registries) to be combined according to data protection rules, but data on identical patients from different registries cannot be correlated.

[*#End version 2*]

### Manual Linking

An interface allows a person to check and, if necessary, correct the results of automated matching, i.e. to merge duplicates or separate falsely merged data sets. To do so, the match weights (reference values to compare the individual attributes of patients to be checked) are shown and it is possible to draw on medical data to make a decision.

## Metadata Repository

The Metadata Repository (MDR) stores the meaning (semantics) of all (reference) data elements used in the OSSE bridgehead. It offers a controlled vocabulary (syntax) and can provide machine-readable, structured information on data elements, e.g. conceptual domains or value ranges. Furthermore, it defines the fields of the registry forms specified in this concept (see section 7.1, “Data Sets”). Since the MDR does not process personal data, it will not be treated in more detail here.

## Registry of Registries

All OSSE registries and bridgeheads[[4]](#footnote-5) register in the registry of registries with a short description of the registry, contact persons and, if applicable, additional registry metadata and interesting core data (e.g. overall number of cases). The data are uploaded actively by the persons in charge. No patient data are transmitted. The registry of registries is managed by [*enter the manager of the registry of registries here*].

# Data Processing Procedures When Using an OSSE Bridgehead

## Data Import into the Bridgehead

Figure 1: Data Import into the Bridgehead

Data import into the bridgehead happens via a so-called ETL process[[5]](#footnote-6).

[*Beginning* ***scenario 1*** *(the existing registry contains pseudonyms that are taken over into the bridgehead):*]

To this end, the pseudonymized data are extracted from the existing registry [*and the biobank (if a biobank module exists)*] at regular intervals. Authenticating itself via a login and password, the ETL process loads the data into the OSSE bridgehead via a web interface.

[*End scenario 1*]

[*Beginning* ***scenario 2*** *(the existing registry contains IDAT):*]

Figure 1 shows the steps in which data are imported into the OSSE bridgehead:

1. Identifying, medical, and sample data are extracted from the existing registry [*and the biobank (if a biobank module exists)*] at regular intervals.
2. Identifying data are substituted by a pseudonym within the transformation step (see section 3.2, “Pseudonymization” for more detail)
3. Authenticating itself via a login and password, the ETL process loads the data into the OSSE bridgehead via a web interface. The ETL process loads the data into the OSSE via a web interface.

Figure 1: Data Import into the Bridgehead

## Pseudonymization

### Pseudonymization at Data Import

Upon data import from the existing registry, the IDAT are pseudonymized before the data sets are loaded. Data extraction and transformation are supported by data integration software (Talend Open Studio). The pseudonymization is part of the data transformation and carried out with a component developed particularly for this purpose. The process consists of the following steps:

1. For each data set, the data integration software launches the *Mainzelliste* and turns over the IDAT.
2. The *Mainzelliste* determines or creates the PSNOSSE and encrypts it with a public key of the OSSE bridgehead so that the OSSE pseudonym cannot be correlated with the IDAT outside the *Mainzelliste*.
3. The *Mainzelliste* sends the encrypted pseudonym, (PSNOSSE)tr, to the transformation component, where the IDAT are substituted by the (PSNOSSE)tr.
4. The import interface decrypts the (PSNOSSE)tr and stores the data with the PSNOSSE.

This procedure ensures that pseudonyms cannot be correlated during data import, since the data-providing party, which could correlate them to patients, can only see the encrypted (PSNOSSE)tr.

### Creating and Managing Keys

The pair of keys for the protected transfer of OSSE pseudonyms is created in the OSSE bridgehead upon startup and stored during runtime. A new pair of keys is produced upon re-start or through a registry feature. The current public key can be retrieved from the OSSE registry via a web interface at all times by way of an authorized component (e.g. the *Mainzelliste*).

[*End scenario 2*]

[*The following section (“Import from Biobanks”) is required if biomaterial samples are supposed to be imported directly into the bridgehead, i.e. not stored in the existing registry. It has to be distinguished here whether the sample data originate directly from the sample source or whether the research network uses a separate biobank. The latter case presumes that the biobank, according to the TMF Data Protection Concept for Biobanks[[6]](#footnote-7), does not pass on the LabID from the sample source in clear text but only in encrypted form and does not store any patient correlation itself. Differing implementations have to be adjusted accordingly in the following section.*]

## Importing Biomaterial Data[[7]](#footnote-8)

[*#Beginning* ***biobank exists***]

The link to a biobank should provide information on biomaterial samples facilitating the identification of those patients in the registry that are suitable for a particular research project. Data on biomaterial samples (IDAT, PID, LabID, further characteristics of the sample) are recorded in the treatment context (sample source) and transmitted to the biobank. The sample’s unique identifier, LabID, created at the sample source, is encrypted in the biobank (LabID)tr. The samples stored in the biobank are not patient-related; the samples’ link to the patient for the transfer to the bridgehead should therefore only be stored temporarily (until sample data are transferred). The sample data in the registry do not allow for information on the sample to be retrieved directly from the sample source. The following data are imported into the OSSE bridgehead from the biobank:

[*Delete items from this list as applicable!*]

* Existence and/or number of samples, respectively
* Sample characteristics
* (LabID)tr

Figure 1: Data flows during biomaterial data import

The import of biomaterial data consists of the following steps:

1. The patient is registered in the *Mainzelliste* via the sample source: the sample source sends IDAT and receives the encrypted OSSE pseudonym (PSNOSSE)tr and, if necessary, the universal PID.
2. The sample is transmitted to the biobank: the address label contains the (PSNOSSE)tr, which is stored temporarily for the data transfer to the registry.
3. The sample is registered in the biobank module: the biobank module stores the LabID and all necessary sample data (OrgDat). Through a cryptographic process, the LabID becomes the LabIDtr in order to avoid direct correlation of data set and sample. The correlation of (PSNOSSE)tr and LabIDtr is stored temporarily.
4. Transfer of sample data to the OSSE bridgehead: For each sample, the OSSE bridgehead receives a data set consisting of (PSNOSSE)tr, LabIDtr and further information on the sample that is supposed to be transmitted as well (see above). As described in section 3.1, “Data Import into the Bridgehead”, the data are transformed and loaded into the OSSE bridgehead. After successful transfer, the link between (PSNOSSE)tr and LabIDtr is deleted. This avoids a permanent correlation between sample and patient in the biobank.

[#*End biobank exists*]

[*#Beginning* ***biobank does not exist***]

The OSSE bridgehead for the Registry for Rare Disease X should provide information on biomaterial samples facilitating the identification of those patients in the registry that are suitable for a particular research project. Data on biomaterial samples (IDAT, PID, LabID, further characteristics of the sample) are recorded in the treatment context (sample source). The following data are imported into the OSSE bridgehead:

[*Delete items from this list as applicable!*]

* Existence and/or number of samples, respectively
* Sample characteristics

The import of biomaterial data consists of the following steps:

1. The patient is registered in the *Mainzelliste* via the sample source: the sample source sends IDAT and receives the encrypted OSSE pseudonym (PSNOSSE)tr and, if necessary, the universal PID.
2. Transfer of sample data from the sample source to the OSSE bridgehead: For each sample, the OSSE bridgehead receives a data set consisting of (PSNOSSE)tr, and further information on the sample that is supposed to be transmitted as well (see above). As described in section 3.1, “Data Import into the Bridgehead”, the data are transformed and loaded into the OSSE bridgehead.

[*In case storing the* (PSNOSSE)tr *in the sample source temporarily is not possible, it can be retrieved through the IDAT via the pseudonymization step in the ETL. The section needs to be adjusted accordingly.*]

[*#End biobank does not exist*]

Figure 2: Data flows during biomaterial data import

## Data Export

Data can be exported for analysis. For this purpose, the OSSE bridgehead’s internal pseudonym is substituted by an export pseudonym during export.

[*#Beginning* ***version 1*** *(a central* Mainzelliste *exists from which the bridgehead receives the pseudonyms)*]

If data from different registries are brought together in the context of decentralized search, uniform non-traceable export pseudonyms are queried with the central *Mainzelliste* upon export. These facilitate the matching of data sets from identical patients recorded in different registries, as well as consistent updates of the combined data sets. The export takes place in the following steps:

1. OSSE sends the internal pseudonym PSNOSSE(#) to the *Mainzelliste* along with a project identifier.
2. The *Mainzelliste* returns a uniform project-specific export pseudonym (PSNProjekt).
3. The data set is exported with the PSNProjekt.

[*#End version 1*]

[*#Beginning* ***version 2*** *(a local* Mainzelliste *exists from which the bridgehead receives the pseudonyms)*]

If data from different registries are brought together in the context of decentralized search, uniform non-traceable export pseudonyms are queried with the local *Mainzelliste* upon export. These facilitate consistent updates of the combined data sets, but identical patients from different registries are not recognized. The export takes place in the following steps:

1. OSSE sends the internal pseudonym PSNOSSE(#) to the *Mainzelliste* along with a project identifier.
2. The ID management returns a project-specific export pseudonym (PSNProjekt).
3. The data set is exported with the PSNProjekt.

[*#End version 2*]

Particularly in diseases with low case numbers, if the course of disease or additional data are known, medical data can be related to specific patients even without knowledge of the identifying data. Even the use of non-traceable export pseudonyms cannot always guarantee factual anonymity.

For this reason, the export of pseudonymized data and the purpose of their use are considered in the patient informed consent.

## Decentralized Search

Through decentralized search, OSSE researchers can search the databases of OSSE registries or bridgeheads in order to find locations with available patient data and samples potentially relevant to a research project. The search broker provides a web-based search form to record the inquiries that filter data elements by preset values or free-text search. Several search attributes can be combined at will via logical operators. The search form also transmits an abstract of the intended research project and the inquiring researcher’s contact information.

In a first step, the inquiry is saved and the inquiring researcher receives a corresponding notification. Each location’s share client fetches new inquiries from the search broker in regular intervals and determines which data sets in the OSSE bridgeheads match the search criteria. At each location, an authorized person can view the inquiry’s content and the data sets found and subsequently contact the inquiring researcher to arrange a potential data or sample transfer. This process and the data protection issues associated with it, e.g. the necessity to obtain further consent, have to be clarified for each individual case by the participating parties. Data transfer happens in a controlled way outside the OSSE bridgehead.

## Uploading Information to the Registry of Registries

Information on the OSSE bridgehead for the Registry for Rare Disease X (new registrations and update) can be uploaded to the registry of registries through a menu feature executed by an authorized user. The scope of information to be uploaded can be set in the bridgehead configuration. This does not apply to registry content data (see section 2.4, “Registry of Registries”).

# Organizational Framework

[*Together with the organizational framework, specify here the stipulations (e.g. bylaws or similar) legally reliable in case of a lawsuit.]*

## Operation of Components

The OSSE bridgehead is operated by [*insert location/institution running and managing the OSSE bridgehead here*]. Data recording locations for the registry include:

The central components installed in the context of using the OSSE bridgehead are managed by the following institutions:

* Identity Management: [*specify the manager of the* Mainzelliste *here*]
* MDR: [specify the MDR manager here]

For the purpose of the informational separation of powers, the organizational framework ensures independent operation of ID management and OSSE bridgehead (see section 5.1, “Informational Separation of Powers”).

## Access by System Administrators

Generally, the data stored in the OSSE bridgehead can be viewed by the administrators of the IT infrastructure used. Administrators may only access the data if it is essential to performing their duties. The data access procedure is regulated as follows: [*Describe here how such access takes place and how it is documented, e.g. beyond the usual logging and indicating the reasons*]. All administrators have to be instructed accordingly and agree to maintain confidentiality[[8]](#footnote-9).

## Participating Researchers

*Participating Researchers* are individuals who can place inquiries via decentralized search. Generally, all members of the registry locations can use the OSSE bridgehead as participating researchers, with each location deciding by itself which of its members are granted access (see also section 5.2, “Authorization and Authentication”).

Scientists who are not a member of a location of the Registry for Rare Disease X can request access from the data protection commission (see also section 4.4, “Data Protection Commission”). Access authorization should be adequately limited in time.

## Data Protection Commission

[*If the Registry for Rare Disease X features a data protection commission (or similar body), the following duties would be at their responsibility:*]

* Review and approval of requests to use OSSE bridgehead by external researchers[[9]](#footnote-10) (decentralized search)
* Review and approval of requests to export medical data for external research projects

# Data Protection Provisions

[*If the bridgehead does not use an existing ID management system, section 5.1 does not apply.*]

## Informational Separation of Powers

ID management is operated separately (logically, physically, and organizationally) from all components storing MDAT or data on biomaterial samples. [*The person/institution in charge of ID management (specify the person/institution in charge of ID management here)*] operates at his/her/its own legal responsibility and is not subject to the directives of the bridgehead and/or registry management. This ensures that individuals with access to clinical or biomaterial data in the OSSE bridgehead or in the Registry for Rare Disease X are not able to correlate the data to real patients.

## Authorization and Authentication

### User Authorization

User authorization (assigning defined roles to users) in the OSSE bridgehead is done through local administrators at the respective locations according to the local structures and requirements.

### Authorization of Components

Mutual access between IT components is defined in the respective configuration. To do so, the accessing system’s IP and a password are recorded.

### User Authentication

User Authentication for the OSSE bridgehead for the Registry for Rare Disease X is done via a username and password.

### Authentication of Components

Mutual access between IT components via the internet takes place only upon successful authentication. Authentication happens on the server side via server certificates and on the client side (depending on technical options) via IP address and username/password or via client certificates.

## IT Infrastructure Provisions

### Security of Communication

Communication between components generally occurs via encrypted connections (HTTPS). The keys and certificates used for this purpose must be generated in a way that corresponds to the current recognized requirements (e.g. key length). Current requirements can be found in the manuals for basic IT security of the German Federal Office for Information Security (<https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html>)

### Logging

Access by researchers to the OSSE bridgehead as well as access between components is logged. The record contains at least:

* The accessing person’s or component‘s identity
* Access date and time
* Access content (transmitted data, in aggregated form if necessary) or information from which the content can be reconstructed (e.g. reference to a database entry or similar)

The record is stored together with the respective server’s payload for a period of one to six months. The recorded data must only be viewed for technical administration (particularly for troubleshooting) and in to track abuse.

# Observing the Rights of Affected Individuals

## Information and Consent

[*The passages in the consent form have to be supplemented according to the use of the OSSE bridgehead.*]

The patient informed consent provides the legal basis for data processing. With it, the patient particularly agrees that

* his/her identifying data are transferred to ID management and stored there,
* medical data and data on biomaterial samples are transferred from the registry to the OSSE bridgehead in a pseudonymized way,
* Researchers of the Registry for Rare Disease X can analyze these data locally and search them via decentralized search,
* The patient’s medical data and data on biomaterial samples can be exported from the OSSE bridgehead via a non-traceable export pseudonym and transferred to external researchers for those research purposes as specified in the informed consent.

The patient is informed of his right to information and revocation upon obtaining consent.

## Information on Stored Data

[*The OSSE bridgehead for the Registry for Rare Disease X particularly contains data of the existing registry, so that information on these data can be given by the registry. If the bridgehead contains further data (e.g. biomaterial data) not included in the existing registry, the patient also receives a printout of these data as well. The procedure (“To whom does the patient address his/her request?”, “Who creates the printout?”, and “How is the printout transmitted to the patient?”) depend on the registry’s information procedure and has to be complemented in the data protection concept accordingly.*]

## Revocation, Deletion, Anonymization

Data erased from or anonymized in the Registry for Rare Disease X upon a patient’s revocation of consent are erased from or anonymized in the OSSE bridgehead as well. In case of anonymization, the data sets are deleted from the ID management and the patient’s PSNOSSE is substituted with a random pseudonym.

[*Provisions on the feasibility of anonymization of data sets, the handling of data forming the basis of a published study etc. should already be part of the data protection concept of the existing registry.*]

# Appendix

## Data Sets

### Transfer Data Set for the OSSE Bridgehead

### Identifying Data

1. For optimal use of the decentralized search, all participants (OSSE registries and OSSE bridgeheads) should employ a common identity management which can produce uniform export pseudonyms for the independent pseudonyms. It is crucial particularly in the area of rare diseases to not count identical patients multiple times in different registries. [↑](#footnote-ref-2)
2. This concept is based on the OSSE Data Protection Concept v1.2 by M. Muscholl, M. Lablans, A. Borg, F. Ückert and TOF Wagner. Translation by S. Buchberger. [↑](#footnote-ref-3)
3. *Mainzelliste* is the ID management software used in OSSE registries. It is a web-based pseudonymization service allowing for the creation of personal identifiers (PID). The term “*Mainzelliste”* will be used throughout this document to refer to an ID management concept implementing the Mainzelliste web interface. More information is available at [www.mainzelliste.de](http://www.mainzelliste.de). [↑](#footnote-ref-4)
4. With an OSSE bridgehead, registries not based on the OSSE registry software can be included in the decentralized search process. [↑](#footnote-ref-5)
5. ETL stands for “Extract-Transform-Load” and describes the technical and contentwise transfer of data from a source system to a target system. During the process, specific data adjustments (assignment to data fields, format changes, translation of values etc.) can be undertaken. [↑](#footnote-ref-6)
6. Pommerening, K, „Das Datenschutzkonzept der TMF für Biomaterialbanken“. ***it – Information Technology*** 49 (2007), 352–359. TMF is a German platform and umbrella organization for networked medical research. [↑](#footnote-ref-7)
7. The import of biomaterial data essentially follows the requirements of the TMF Data Protection Concept for Biobanks. [↑](#footnote-ref-8)
8. Usually, this should already have happened in the context of the individual’s work contract with the institution in charge. [↑](#footnote-ref-9)
9. I.e. individuals not affiliated with any of the OSSE Registry for Rare Disease X’s locations. [↑](#footnote-ref-10)