Data Processor Agreement

for depositing human genetic and phenotypic data for controlled access data archival and retrieval purposes in the Federated EGA Norway service

Pursuant to the applicable Norwegian personal data legislation, including but not limited to the Personal Data Act of 15th June 2018 no 38 and Regulation (EU) 2016/679 of 27th April 2016, Articles 28 and 29, cf. Article 32-36, the following agreement is entered into

between

.....

(Data Controller)

and

University of Oslo
(Data Processor)

29.03.2023

1. Purpose of the agreement

The purpose of the agreement is to regulate the rights and obligations under the applicable Norwegian personal data legislation, including, but not limited to, the Personal Data Act of 15th June 2018 no 38 and Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of **natural** persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Federated EGA Norway (hereafter referred to as FEGA Norway) is a service for archiving sensitive genome and phenotype data, as part of the distributed European network of interlinked services to provide FAIR[1] controlled access for such sensitive human data[2] . The FEGA Norway service is implemented in TSD[3] hosted by USIT at UiO, where all archived data in FEGA Norway is stored encrypted inside a dedicated TSD project for this service. UiO is a partner in ELIXIR Norway and UiO is the legal entity responsible for operating the FEGA Norway service.

Special categories of personal data will be processed, including data revealing ethnic origin data, genetic data and data concerning health. The agreement is intended to ensure that the personal data are not processed illegally, wrongfully, or processed in ways that result in unauthorised access, alteration, erasure, damage, loss, or unavailability.

The agreement governs the Data Processor's processing of personal data on behalf of the Data Controller, including collection, registration, structuring, retrieval, compilation, storage, disclosure, erasure, or combinations of these, in connection with the use of/processing in the FEGA Norway service.

2. Limiting clause

The purpose of the Data Processor's processing of personal data governed by this agreement is to pre-process and safely archive the data in encrypted form inside FEGA Norway on behalf of the Data Controller, and when instructed by the Data Controller, to re-encrypt the data and provide access to safe download functionality to requesters that are approved by the Data Controller.

The FEGA Norway helpdesk will provide advice to data submitters on which metadata to include in a submission, but the Data Controller is solely and fully responsible for deciding which metadata per subject to include in the dataset. Metadata are here considered being of two types: 1) Descriptive summary level data on experiments and study level to be made publicly available, and three variables that may be included are phenotype category, control/case, and sex; and 2) individual, per subject, level phenotype data that may be of different types including health information and are considered part of the sensitive data to be archived. Published descriptions of a dataset made available publicly (without controlled access) in the FEGA portal, will not be allowed to include information that, directly or indirectly, can identify individuals in the data set.

For further details on categories of data processing and permitted data processing tasks, please refer to Annex I.

[1] https://www.go-fair.org/
[2] https://ega-archive.org/
[3] https://www.uio.no/english/services/it/research/sensitive-data/

For the datasets deposited in FEGA Norway, the Data Controller has established a Data Access Committee (DAC) that will be the contact point for processing requests for access to their deposited data in FEGA Norway.

The Data Processor may not transfer personal data covered by this agreement to partners or other third parties without the prior approval of the Data Controller, cf. point 10 of this agreement.

3. Instructions

The Data Processor will follow the written and documented instructions for the processing of personal data in FEGA Norway which the Data Controller has determined will apply.

The Data Controller and the Data Processor are both obliged to comply with all obligations under the applicable Norwegian personal data legislation governing the use of FEGA Norway for the processing of personal data.

The Data Processor is obliged to notify the Data Controller if it receives instructions from the Data Controller that conflict with the provisions of the applicable Norwegian personal data legislation.

Data Controller undertakes to use the FEGA Norway services only as they are authorised in connection with their ongoing research / clinical activities. This is also related to the principle of data minimization with regard to access to and use of personal data. In particular, the Data Controller must be able to document the legal basis to share data from FEGA Norway to requesters the controller approves for download access, in order to facilitate further data processing. It is thus the responsibility of the Data Controller to organise and maintain any agreements needed for such further data processing. All communication regarding this required documentation to FEGA Norway shall be in accordance with instructions from the controller, administratively organised through DAC.

4. Types of information and data subjects

The Data Processor processes the following personal data on behalf of the Data Controller:

- Dataset summary description: ……..
- FEGA Norway submission ID:..... ……
- Ethics approval reference (e.g. REK/IRB approval ID): ……
- Lawful basis for data processing according to the data protection legislation:
    - ……

The personal data applies to the following data subjects:

- A brief summary of how many individuals are included in the dataset:.....
- These individuals are research subjects in a study on (fill in phenotype/disease/ purpose):.....

The Data Processor will in addition register and store information associated with the use of the service, both for data submitters and data requesters. The current version of the Terms of Service (ToS) and Privacy Policy (PP) at signing is included in Annex II of this Data Processing Agreement. These may be updated and the most up to date version of the ToS and PP are available on the FEGA Norway website[4], all users will be notified prior to any change for FEGA Norway ToS and PP.

5. The rights of data subjects

The Data Processor is obliged to assist the Data Controller in safeguarding the rights of data subjects in accordance with applicable Norwegian personal data legislation.

The rights of the data subjects include, but are not limited to, the right to information on how his or her personal data is processed, the right to request access to personal data, the right to request rectification to, or erasure of personal data about them, and the right to require restriction of processing of their personal data.

To the extent relevant, the Data Processor will assist the Data Controller in maintaining the data subject's right to data portability and the right to object to automated decision-making, including profiling.

The Data Processor is liable for damages to the data subject if errors or omissions by the Data Processor inflict financial or non-financial loss on the registered subject as a result of infringement of their rights or privacy protection.

6. Satisfactory data security

FEGA Norway utilises the national solution for processing sensitive data, Services for Sensitive Data (TSD) operated by USIT (Center for Information Technology, USIT) at UiO, as it's foundation (system and security docs[5]). The archived data is further stored encrypted for additional security to what is provided by the TSD design and architecture.

The Data Processor will implement appropriate technical, physical, and organisational safety measures to safeguard the personal data covered by this agreement from unauthorised or unlawful access, alteration, erasure, damage, loss, or unavailability.

The Data Processor will document its own security organisation, guidelines and routines for security, risk assessments and established technical, physical or organisational security measures. The documentation will be made available to the Data Controller on request.

The Data Processor will establish continuity- and contingency plans for effective handling of serious security incidents. The documentation will be made available to the Data Controller on request.

The Data Processor will document the training of its own employees in data security. The documentation will be made available to the Data Controller on request.

For a further non-exhaustive high-level overview of security measures implemented in FEGA Norway, please refer to Annex III.

[4] ega.elixir.no/tos.html ega.elixir.no/pp.html
[5] https://www.uio.no/english/services/it/research/sensitive-data/about/description-of-the-system.html

Residual risk management:

In our template for data access agreements between a Data Access Committee and a Data Requester, we advise including a paragraph on the risk of re-identification of individuals as follows:

> "The Data Processor agrees not to attempt to re-identify any individuals. The processor further agrees to not link or combine these Data with other information or archived data available in a way that could re-identify the Research Participants, even if access to that data has been formally granted to the Data Processor or is freely available without restriction."

7. Confidentiality

Only employees of the Data Processor, who need to access personal data that is processed on behalf of the Data Controller to operate the FEGA Norway services, may be granted such access. The Data Processor is required to document guidelines and routines for control of access. The documentation will be made available to the Data Controller on request.

Employees of the Data Processor have a duty of confidentiality in respect of documentation and personal data to which they gain access in accordance with this agreement. This provision also applies after termination of the agreement. The duty of confidentiality includes employees of third parties who perform maintenance (or similar tasks) on systems, equipment, networks or buildings that the Data Processor uses to provide the service.

The Data Controller shall provide equivalent access control and have equivalent duty of confidentiality concerning all documentation made available by the Data Processor in accordance with this agreement.

Norwegian legislation defines the scope of the duty of confidentiality for employees of the controller, for employees of the Data Processor and third parties.

8. Access to security documentation

The Data Processor is obliged to provide the Data Controller, upon request, with access to all security documentation that is necessary for the Data Controller to be able to meet its obligations under the applicable Norwegian personal data legislation.

The Data Processor is obliged to provide the Data Controller, upon request, with access to other relevant documentation that allows the Data Controller to assess whether the Data Processor complies with the terms of this agreement.

The Data Controller shall keep confidential any security documentation which the Data Processor makes available to the controller.

9. Security Breach Notification

The Data Processor shall notify the controller without undue delay, if personal data processed on behalf of the controller is exposed to a breach of security.

The Data Processor's notification should, at minimum, include information that describes the security breach, which registered subject is affected by the breach, what personal data are

affected by the breach, what immediate measures are implemented to address the breach and what preventive measures may have been established to avoid similar incidents in the future.

The Data Controller is responsible for ensuring that the data subjects and the Norwegian Data Protection Authority are notified when required.

10. Sub-processors

The Data Processor is obliged to enter into separate agreements with sub-processors that govern the sub-processor's processing of personal data in connection with this agreement.

In agreements between the Data Processor and sub-processors, the sub-processors will be required to comply with all the obligations to which the Data Processor is subject under this agreement and according to law. The Data Processor is obliged to submit the agreements to the Data Controller on demand.

The Data Processor will verify that sub-processors comply with their contractual obligations, in particular that data security is satisfactory and that employees of the sub-processors are familiar with their obligations and fulfil them.

The Data Controller approves that the Data Processor contracts the following sub-processors to satisfy this agreement:

- TSD service operated by USIT, University of Oslo, Norway.

Any change to the list of sub-processors must be informed in writing to the Data Controller minimum 30 days before the planned change. The Data Controller may object to FEGA Norway's use of a new sub-processor by notifying FEGA Norway promptly in writing within ten (10) business days after receipt of notice of change. In the event the Data Controller objects to a new sub-processor, as permitted in previous sentence, FEGA Norway will use reasonable efforts to make available a change in the services to not perform processing of personal data by the objected-to new sub-processor without unreasonably burdening the Data Controller. If FEGA Norway is unable to make available such a change in services, the Data Controller's sole remedy if the new sub-processor is not acceptable is to terminate this DPA.

The Data Processor is liable for damages to the Data Controller for any financial loss that is inflicted on the Data Controller, and that is due to illegal or improper processing of personal data or inadequate data security on the part of sub-processors.

11. Transfer to countries outside the EU/EEA

- The Data Processor will never carry out any transfers of personal data stored in FEGA Norway to countries outside of EU/EEA, except as specified below.
- The Data Controller may authorise access to data in FEGA Norway to non-EU/EEA citizens. Upon approval, the dataset will be made available for the requester in encrypted format to be further processed according to the conditions as agreed with the Data Controller.
    - It is a prerequisite assumption from FEGA Norway that the Data Controller has the legal mandate to authorise such data access, transfer and processing.
    - The Data Controller is responsible for establishing separate agreements as required for each recipient of their dataset that is being granted access to from FEGA Norway.

- If the agreements between the Data Controller and the data requester allows the dataset to be transferred to and stored in countries outside of EU/EEA, this is permitted directly from the FEGA Norway service.

12. Safety audits and impact assessments

The Data Processor will regularly implement security audits of its own work with safeguarding of personal data from unauthorised or unlawful access, alteration, erasure, damage, loss, or unavailability.

Security audits will include the Data Processor's security goals and security strategy, security organisation, guidelines, and routines for security work, established technical, physical, and organisational safeguards and the work of data security at sub-processors to this agreement. It will also include routines for warning the Data Controller in the event of security breaches, and routines for testing of emergency and continuity plans.

The Data Processor will document the security audits. The Data Controller will be granted access to the audit reports on request.

If an independent third-party conducts security audits at the Data Processor, the Data Controller will be informed of which auditor is being used and be given access to the summaries of the audit reports on request.

13. Return and erasure

Upon termination of this agreement, the Data Processor is obliged to return and erase any personal data that is processed on behalf of the Data Controller under this agreement. The Data Processor determines how the return of the personal data will take place, including the format to be used. Both parties are mutually responsible to initiate communication on the matter of return and erasure, in due time to allow the practical execution of return and erasure within the time frame of the legal approval for the deposited data set.

Erasure is to be carried out by the Data Processor within 30 days after the termination of the agreement for any reason. Backup of personal data will be automatically erased no later than 90 days after the original data is erased. The backup data will only be available to a few system administrators in this period. The Data Processor will normally execute erasure of the data in agreement with the Data Controller but reserves the right to complete the legally required erasure of the data if the Data Controller is not reachable.

Visibility of meta-data for the deposited data in FEGA Norway is automatically removed in due time before the legal approval for the submission expires. The Data Controller will be notified before and when this visibility change is executed. This can be reversed by documenting a legal basis for the extended approval period. If no extension documentation is provided, the above rules of erasure will be executed.

The Data Processor will document that the erasure of personal data has been carried out in accordance with this agreement. The documentation will be made available to the Data Controller on request.

Erasure of personal data such as user profiles and usage data of FEGA Norway web portal and services, is specified in the ToS and PP of these services (see Section 4 Types of information), and is not included in this agreement.

Similarly, erasure of personal data such as user profiles and usage data of other services in the Federated EGA network, is governed by the ToS and PP documents accepted by the users for these services and must be enforced by these service providers as Data Processors.

14. Breach of contract

In case of breach of the terms of this agreement caused by errors or omissions on the part of the Data Processor, the Data Controller may cancel the agreement with immediate effect. The Data Processor will continue to be obliged to return and erase personal data processed on behalf of the Data Controller pursuant to the provisions of Section 13 above.

The Data Controller may require compensation for financial loss suffered by the Data Controller because of errors or omissions on the part of the Data Processor, including breach of the terms of this agreement, cf. also points 5 and 10 above.

15. Duration of the Agreement

This agreement applies if the Data Processor processes personal data on behalf of the Data Controller, where the maximum duration is set in the approval for the Data Controller to store data in FEGA Norway.

The agreement may be terminated by both parties with a termination period of 60 days.

16. Contacts

Contact person at the Data Processor for any questions related to this agreement is: Eivind Hovig, email: ehovig@ifi.uio.no, telephone:+47-22858504.

Contact person at the Data Controller for any questions related to this agreement is: _____, email: _____, telephone: _____

17. Choice of Law and Resolution of Disputes

The Parties' rights and obligations under this agreement are determined in full by Norwegian law. Any disputes arising out of this Agreement shall be first sought to be resolved through negotiations. If unsuccessful, the matter shall be resolved through the Norwegian legal system.

***

This agreement is in 2 – two copies, one to each of the parties.

Place and date

29.03.2023

On behalf of the Data Controller	On behalf of the Data Processor
……..	……
(signature)	(signature) Professor Eivind Hovig, Centre for bioinformatics, Dept of Informatics, UiO

29.03.2023

Annex I - Categories of data processing and permitted data processing tasks

Categories of data processing as defined in GDPR Article 4(2), that will be performed on the data by the Data Processor:

- storage
- structuring
- making data available
- erasure or destruction

FEGA Norway will on behalf of the Data Controller pre-process and safely archive the data in encrypted form within our archival service. When instructed by the Data Controller, FEGA Norway staff will re-encrypt the data and provide access to safe download functionality to requesters that are approved by the Data Controller.

To improve FAIR data quality of a deposited data set, the FEGA Norway service team may continuously update the formats of datafiles to follow community standards. The original data files will remain in the dataset, and updated data files in new formats will be added as a supplement. The Data Controller will be informed in the event of such an update to a data set and given the opportunity to quality control the new data files.

Other standard data processing operations in FEGA Norway include re-encryption of data when rotating encryption keys for security reasons, performing data integrity checks and computation of non-identifiable quality control summary statistics.

Personal data that the Data Processor processes on behalf of the Data Controller may not be processed for any other purpose than stated above, without the prior written approval of the Data Controller.

Annex II - FEGA Norway Terms of Service and Privacy Policy

Current versions of FEGA Norway services Terms of Service and Privacy Policy are included for reference, both last updated 2020-05-20.

Terms of Service

Definitions:

“The Service”: any one of the Federated EGA Norway node sites provided to you by the Elixir Norway organisation and the partner organisations, including but not limited to:

- https://ega.elixir.no/
- https://ega.uio.no/

Use of Service

The Service is a free, public, Internet accessible resource. Data transfer is automatically encrypted by using the underlying HTTPS protocol. Data storage is encrypted with Crypt4GH encryption format. If there are restrictions on the way your research data can be stored and used, please consult your local institutional review board or the project principal investigator before uploading it to any public site, including The Service. Your access to the service may be revoked at any time for reasons deemed necessary by the operators of The Service. You acknowledge that you are responsible for compliance of all of your data processing activities carried out on The Service with applicable laws and regulations of Norway, the European Union as well as any laws or regulations of other legislations or any other restrictions that might be applicable due to the provenance, intended use, legal ownership of or any licensing or other legal restrictions imposed on the data being processed.

Accounts and Service Limitations

To use The Service, you must have an EGA Account and Elixir Account, and login to the service using Elixir AAI. Your registration data is primarily used so you may persistently store data on The Service. The operators of The Service will not provide your registration data to any third party (except for our partners, such as Elixir AAI and USIT) unless required to do so by law. Your access to The Service is provided under the condition that you abide by any published quotas on data storage, or any other limitations placed on The Service. Attempts to subvert these limits by using multiple accounts or through any other method may result in termination of all associated accounts.

Disclaimer

The Service is provided to you on an “AS IS” BASIS and WITHOUT WARRANTY, either express or implied, including, without limitation, the warranties of non-infringement, merchantability, or fitness for a particular purpose. THE ENTIRE RISK AS TO THE QUALITY OF THE SERVICE IS WITH YOU. This DISCLAIMER OF WARRANTY constitutes an essential part of this service agreement.

Privacy Policy

Definitions:

“The Service”: any one of the Federated EGA Norway node sites provided to you by the Elixir Norway organisation and the partner organisations, including but not limited to:

- https://ega.elixir.no/
- https://ega.uio.no/

This privacy policy will explain how The Service uses the personal data we collect from you when you use our website.

Topics:

- What data do we collect?
- How do we collect your data?
- How will we use your data?
- How do we store your data?
- What are your data protection rights?
- What are cookies?
- How do we use cookies?
- What types of cookies do we use?
- How to manage your cookies
- Privacy policies of other websites
- Changes to our privacy policy
- How to contact us
- How to contact the appropriate authorities

What data do we collect?

The Service collects the following data:

- Elixir ID, read more at https://elixir-europe.org/services/compute/aai
- Information about your data uploads to The Service or data retrievals from The Service
    - Including public keys provided by you for encryption purposes

How do we collect your data?

You directly provide The Service with most of the data we collect. We collect data and process data when you:

- Sign in with the "Elixir Login" button.
- Perform a dataset submission to the archive.
- Perform a dataset retrieval from the archive after access approval by the respective Data Access Committee.
- Voluntarily complete a customer survey or provide feedback on any of our message boards or via email.
- Use or view our website via your browser’s cookies.

29.03.2023

How will we use your data?

The Service collects your data so that we can:

- Facilitate the authentication and authorization to The Service. Since the authentication and authorization to The Service is based on Elixir AAI, we need to store your Elixir ID, to keep you logged in.
- Keep track of which submission was performed by which user.
- Security and audit purposes to track all data transfers of files under controlled access regime due to their sensitive content (human genome phenome information).

The Service will share your data with our partner(s) in order to facilitate authentication and authorization functionality.

- Elixir AAI
- USIT

Since the authentication attempts are processed by Elixir AAI, they will have to know your Elixir ID. The way Elixir AAI handles Elixir IDs is a subject of their Privacy Policy.

Elixir ID also will be stored at the USIT premises to keep track of all performed data submissions.

How do we store your data?

The Service stores your authentication data (session tokens) using the browser cookies mechanism. The information about the cookies and how The Service is using them is provided below.

Elixir ID is also securely stored in the database at the USIT server. This information is stored permanently but can be removed in accordance with the right to erasure, described below.

Additionally, Elixir ID is stored as part of the logs of The Service at the USIT-hosted web server. This information is stored for a maximum of 6 months following The Service's logging policies and can be removed in accordance with the right to erasure, described below.

As The Service depends on TSD for secure storage of deposited datasets to the archive, all dataset transfers in and out of The Service are also being logged and audited in the TSD infrastructure, as according to TSD Privacy Policy.

What are your data protection rights?

The Service would like to make sure you are fully aware of all your data protection rights. Every user of The Service is entitled to the following:

The right to information (GDPR Art. 13 and 14) - The Service shall provide you with information on the processing of your personal data at the time when your personal data is collected.

The right to access (GDPR Art. 15) – You have the right to request The Service for copies of your personal data and information of the data processing. We may charge you a small fee for this service.

The right to rectification (GDPR Art. 16) – You have the right to request that The Service correct any information you believe is inaccurate. You also have the right to request The Service to complete the information you believe is incomplete.

The right to erasure (GDPR Art. 17) – You have the right to request that The Service erase your personal data, under certain conditions.

The right to restriction of processing (GDPR Art. 18) – You have the right to request that The Service restrict the processing of your personal data, under certain conditions.

The right to data portability (GDPR Art. 20)– You have the right to request that The Service transfer the data that we have collected to another organisation, or directly to you, under certain conditions.

The right to object to processing (GDPR Art. 21)– You have the right to object to The Service's processing of your personal data, under certain conditions.

If you make a request, we have one month to respond to you. If you would like to exercise any of these rights, please contact us at our email:

Email us at: fega-norway-support@elixir.no

Cookies

Cookies are text files placed on your computer to collect standard Internet log information and visitor behaviour information. When you visit our websites, we may collect information from you automatically through cookies or similar technology.

For further information, visit https://allaboutcookies.org.

How do we use cookies?

The Service uses cookies in a range of ways to improve your experience on our website, including:

- Keeping you signed in
- Understanding how you use our website

What types of cookies do we use?

There are several different types of cookies, however, our website uses:

- Functionality – The Service uses these cookies so that we recognize you on our website and remember your previously selected preferences. These could include what language you prefer and location you are in. A mix of first-party and third-party cookies are used.

How to manage cookies

You can set your browser not to accept cookies, and the above website tells you how to remove cookies from your browser. However, in a few cases, some of our website features may not function as a result.

Privacy policies of other websites

The Service website contains links to other websites. Our privacy policy applies only to our website, so if you click on a link to another website, you should read their privacy policy.

Changes to our privacy policy

The Service keeps its privacy policy under regular review and places any updates on this web page. This privacy policy was last updated on 20 May 2020.

How to contact us

If you have any questions about The Service's privacy policy, the data we hold on you, or you would like to exercise one of your data protection rights, please do not hesitate to contact us.

Email us at: fega-norway-support@elixir.no

How to contact the appropriate authority

Should you wish to report a complaint or if you feel that The Service has not addressed your concern in a satisfactory manner, you may use the following contacts:

- Data Controller function: behandlingsansvarlig@uio.no
- Data protection officer: personvernombud@uio.no

Annex III - Summary overview of FEGA Norway security measures

Security measures implemented in FEGA Norway (non-exhaustive):

i) Specific guarantees to minimise intervention:

"Standard" TSD/UiO requirements such as:

- Informed consents as guided by Ethical review boards for each research project
- Lawful basis for data processing according to the data protection legislation

In addition, FEGA Norway requires:

- Data are only archived and stored for the duration of the legal basis of each project

ii) Specific security measures relating to the personal data to be processed:

- Pseudonymization is a process to minimise information while maintaining the possibility to re-identify data. Only pseudonymized data will be accepted within the service. No re-identification key is kept with the service.
- The Data Controller has established a Data Access Committee (DAC) that will be the contact point for processing requests for access. Each dataset in FEGA Norway is thus linked to one specific DAC.

iii) General safety measures implemented on the system in which the processing is performed:

- National secure infrastructure solutions - in Norway we have chosen to deploy an adapted version of the Federated EGA software solution (developed in a Nordic collaboration) on top of TSD. This both provides additional security around the archived data and minimal internet exposure of the archival services.
- Encryption - The service will store all data internally with separate encryption keys for each research project using the Global Alliance for Genomics and Health (GA4GH) encryption standard Encrypt4GH. The service also relies on this standard for all data transfers going in and out of the service over the internet.
- Security by design - The architecture and micro-services in the Norwegian Federated EGA services are developed in collaboration among the Nordic ELIXIR nodes with joint NordForsk funding[6], with a large development team of highly qualified developers. The encryption and design have been targeting the creation of a safe online system while being exposed to internet threats.
- Two-factor authentication is in place for all access to stored archival data, for submitters, requesters, and service operators.

Audit is performed on all transactions as per design in TSD. In addition, the FEGA Norway operations team performs extensive logging and monitoring of the micro-services deployed in the FEGA Norway services.

iv) Organisational measures (management)

[6] https://neic.no/heilsa/

A dedicated operational team of staff authorised by UiO as service owner manages the system, having the required technical level to handle the operation. The team includes experts from TSD, the Department of Informatics at the University of Oslo, and selected ELIXIR Norway partner universities.

- Documentation - the team has access to a collection of Standard Operating Procedures (SOPs) that is regularly subject to revision.
- We have restricted the access to encryption keys to core staff members.

Additional relevant security measures implemented in TSD (non-exhaustive):

- Annual update of Risk and Vulnerability Analysis
- Fully automated firewall configuration to avoid human error
- No openings to the internet from the project areas, except highly controlled export and import of data
- Regular penetration testing
- Backups and snapshots are taken every night