Data processor agreement

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

as partner in Elixir Norway
and operator of the Norwegian Federated EGA service,
a node in the Federated EGA network of services[1]

[1] https://www.ebi.ac.uk/ega and https://ega-archive.org/

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).

Special categories of personal data will be processed, including genetic and phenotypic data. Limited individual level meta-data will also be processed. 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 Norwegian Federated EGA service (hereafter referred to as NFEGA).

In the event of conflict, the terms of this Agreement will take precedence over the data processor's privacy policy, or terms of any other agreement entered into between the data processor and the data controller in connection with the use of/processing in NFEGA.

2. Limiting clause

The purpose of the data processor's processing of personal data on behalf of the data controller is to pre-process and safely archive the data in encrypted form inside NFEGA 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 NFEGA helpdesk will provide advice to data submitters on which metadata[2] to include in a submission, but the data controller is solely and fully responsible for deciding which meta-data per subject to include in the dataset. 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.

Following approval by the data controller, the NFEGA service team may provide additional reformatted data files (genetic and phenotypic data) with updated standard formats to improve FAIR data quality, as part of the operation of NFEGA.

For the datasets deposited in NFEGA, the data controller is required to appoint a Data Access Committee (DAC) that will be responsible for processing requests for access to their deposited data.

Personal data that the data processor processes on behalf of the data controller may not be processed for any other purpose without the prior approval of the data controller.

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.

[2] Metadata are here considered being of two types: 1) Describing summary level data on experiments, and three variables that may be included are phenotype category, control/case, and sex; and 2) individual, per subject, level data that may be of different types, and are considered part of the sensitive data to be archived.

3. Instructions

The data processor will follow the written and documented instructions for the processing of personal data in NFEGA which the data controller has determined will apply.

[Name of institution/company] (data controller) and University of Oslo (data processor) are both obliged to comply with all obligations under the applicable Norwegian personal data legislation governing the use of NFEGA 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 are in conflict with the provisions of the applicable Norwegian personal data legislation.

The data controller undertakes to use the NFEGA services only as they are authorized 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 processor must receive documentation of the legal basis to share data from NFEGA to requesters the DAC approves for download access, in order to facilitate further data processing. It is thus the responsibility of the data controller through the DAC to organise any agreements needed for such further data processing.

4. Types of information and data subjects

The data processor processes the following personal data on behalf of the data controller:

- Dataset summary description: ……..
- NFEGA submission ID:..... ……
- Valid dataset reference (e.g. REK/IRB approval ID): ……...

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 version of the Terms of Service (ToS) at signing is included in annex I (current version: X) of this Data Processing Agreement. These may be updated and the most up to date version of these ToS will always be available here[3].

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.

[3] ega.elixir.no/tos

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

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.

NFEGA 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. The archived data is further encrypted for additional security to what is provided by the TSD design and architecture.

Security measures implemented in NFEGA (non-exhaustive):
Specific guarantees to minimize intervention:

- Informed consents as guided by Ethical review boards for each research project
- Lawful basis for data processing according to the data protection legislation
- Legitimate research purposes are necessary, as reviewed by the DAC for each requester asking for access to data for a deposited research project.
- Data are only archived and stored for the duration of the legal basis of each project

• Specific security measures relating to personal data to be processed:

- Pseudonymization is a process to minimize 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.
- DAC. Each research project will have a DAC, ensuring compliance with the terms of the project, and includes the PI of the research project.

• General safety measures implemented on the system in which the treatment is performed:

- 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 communication 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, 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.
- National secure infrastructure solutions - in Norway we have chosen to deploy an adapted version of the Nordic Sensitive Data Archive solution on top of TSD, that provide additional security around the archived data with minimal internet exposure.
- 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, we are performing extensive logging and monitoring of the micro-services deployed in the National Federated EGA services.

Organizational measures (management)

- A dedicated operational team will be managing the system, having the required technical level to handle the operation.
- Documentation - the team has access to a collection 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

Residual risk management:

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

> "The data processor agrees not to link or combine these Data to 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 in connection with their work, 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 will be able to limit 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 has a duty of confidentiality in respect of confidential security documentation which the data processor makes available to the controller.

9. Security Breach Notification

The data processor will 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 is 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.

The data processor may not contract any other sub-processors than those listed above without prior written approval by the data controller.

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 NFEGA to countries outside of EU/EEA, except as specified below.
- The data controller may authorise access to data in NFEGA for foreign citizens, through processing access requests in the appointed Data Access Committee. 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 DAC.
    - It is a prerequisite assumption from NFEGA that the data controller has the legal mandate to authorize 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 for download from NFEGA.
    - If the agreements between the DAC 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 NFEGA 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.

Erasure is to be carried out by the data processor within 60 days after the termination of the agreement. 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. Both parties are mutually responsible to initiate communication on this matter 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.

Visibility of the deposited data in NFEGA is automatically removed when 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.

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 as a consequence 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 as long as 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 NFEGA.

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.

12.05.2020

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

On behalf of the data controller	On behalf of the data processor
……..	……
(signature)	(signature)
	Professor Eivind Hovig
	Leader of Elixir Norway, sub-node at UiO

12.05.2020