Template for data processor agreements

Data Processor Agreement between a Norwegian Federated EGA-associated Data Access Committee

and

a Data Requester for a defined

NFEGA dataset

Pursuant to the applicable Norwegian personal data legislation 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 - institution/affiliation)

and

……

(data processor - institution/affiliation)

23.09.2020

Definitions

Authorised Personnel: The individuals at the User Institution to whom XXXXX grants access to the Data. This includes the User, the individuals listed in Appendix II and any other individuals for whom the User Institution subsequently requests access to the Data. Details of the initial Authorised Personnel are set out in Appendix II.

Data: The managed access datasets to which the User Institution has requested access.

Data Producers: XXXXX and the collaborators listed in Appendix I responsible for the development, organisation, and oversight of these Data.

External Collaborator: A collaborator of the User, working for an institution other than the User Institution.

Project: The project for which the User Institution has requested access to these Data. A description of the Project is set out in Appendix II.

Publications: Includes, without limitation, articles published in print journals, electronic journals, reviews, books, posters and other written and verbal presentations of research.

Research Participant: An individual whose data form part of these Data.

Research Purposes: Shall mean research that is seeking to advance the understanding of genetics and genomics, including the treatment of disorders, and work on statistical methods that may be applied to such research.

User: The principal investigator for the Project.

User Institution: The Institution that has requested access to the Data.

1. Purpose of the agreement

The purpose of the agreement is to regulate the rights and obligations under the applicable Norwegian personal data legislation, and regulation (EU) 2016/679 of 27th April 2016 in respect of the protection of physical persons in connection with the processing of personal data and the free exchange of such data, as well as the repeal of Directive 95/46/EC.

The agreement is intended to ensure that personal data is 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, compilation, storage, disclosure or combinations of these, in connection with the use of/processing in Project.

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 Project.

2. Limiting clause

The User Institution agrees to only use these Data for the purpose of the Project (described in Appendix II) and only for Research Purposes. The User Institution further agrees that it will only use these Data for Research Purposes which are within the limitations (if any) set out in Appendix I.

Personal data that the data processor processes on behalf of the data controller may not be used 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.

3. Instructions

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

The User Institution is obliged to comply with all obligations under the applicable Norwegian personal data legislation governing the use of computational infrastructure 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.

4. Types of information and data subjects

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

- Dataset with NFEGA Dataset ID: _____
- Genetic data from Research Participants
- Pseudonymized personal data on Research Participants relevant to the original study producing the Data.

- More details of the Data is specified in Appendix I

The personal data applies to the following data subjects:

- Research Participants that have consented to take part in the study, as documented by Legal basis reference (e.g. REK/IRB approval): ……..

5. The rights of registered subjects

The data processor is obliged to assist the data controller in safeguarding the rights of registered subjects in accordance with applicable Norwegian personal data legislation.

The rights of the data subjects include, but 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 corrections to, or erasure of their own personal data, 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 registered 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 registered 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.

- Comment: There may be a need to specify the most important safeguards that the data processor has implemented, possibly referring to documents or publications that explain how the data processor works with data security, and what safeguards are established for the service in question. These may be incorporated into the agreement, or as an appendix to the agreement.

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.

The data processor agrees to preserve, at all times, the confidentiality of these Data. In particular, it undertakes not to use, or attempt to use these Data to compromise or otherwise infringe the confidentiality of information on Research Participants. Without prejudice to the generality of the foregoing, the data processor agrees to use at least the measures set out in Appendix I to protect these Data.

The data processor agrees to protect the confidentiality of Research Participants in any research papers or publications that they prepare by taking all reasonable care to limit the possibility of identification.

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.

The data processor agrees only to provide access to these Data, in whole or part, or any material derived from these Data, to the Authorised Personnel. Should the data processor wish to share these Data with an External Collaborator, the External Collaborator must complete a separate application for access to these Data.

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 Norwegian Data Protection Authority is 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:

…….. (names of sub-processors)

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

- Comment: Personal data that the data processor is processing on behalf of the data controller may be transferred to countries outside the EU/EEA (third countries). Such transfer may take place on certain conditions, and the rules for transfer to third countries are found in Articles 45-47 and 49 of the EU data protection regulation. These rules imply, among other things, that the transfer will be lawful if it takes place to EU-approved third countries, to companies that have joined the Privacy Shield framework, or on the basis of the EU Commission's standard contractual clauses for transfer of personal data to data processors in third countries. The rules also apply to backup and other transfer of personal data that is carried out in connection with the administration of the service in question, such as support.

Personal data that the data processor processes in accordance with this agreement will be transferred to the following recipient countries outside the EU/EEA:
..... (name of recipient country)

The legal basis for transmitting personal data to the aforementioned recipient countries outside the EU/EEA is:

……...
(brief explanation of the transfer basis)

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.

Any additions: The parties may agree that the data controller itself, or an independent third party that the data controller chooses, performs security audits at the data processor, and how any costs incurred in connection with such an audit should be allocated.

13. Data Producer disclaimer

The data processor agrees that the Data Producers, and all other parties involved in the creation, funding or protection of these Data: a) make no warranty or representation, express or implied as to the accuracy, quality or comprehensiveness of these Data; b) exclude to the fullest extent permitted by law all liability for actions, claims, proceedings, demands, losses (including but not limited to loss of profit), costs, awards damages and payments made by the Recipient that may arise (whether directly or indirectly) in any way whatsoever from the Recipient's use of these Data or from the unavailability of, or break in access to, these Data for whatever reason and; c) bear no responsibility for the further analysis or interpretation of these Data.

14. Publications and Intellectual Property (IP) rights

The data processor agrees to follow the Fort Lauderdale Guidelines and the Toronto Statement. This includes but is not limited to recognising the contribution of the Data Producers and including a proper acknowledgement in all reports or publications resulting from the use of these Data.

The data processor agrees to follow the Publication Policy in Appendix III. This includes respecting the moratorium period for the Data Producers to publish the first peer-reviewed report describing and analysing these Data.

9. The data processor agrees not to make intellectual property claims on these Data and not to use intellectual property protection in ways that would prevent or block access to, or use of, any element of these Data, or conclusion drawn directly from these Data.

10. The data processor can elect to perform further research that would add intellectual and resource capital to these data and decide to obtain intellectual property rights on these downstream discoveries. In this case, the data processor agrees to implement licensing policies that will not obstruct further research on the Data.

15. Change management

The data processor will notify the data controller prior to any significant changes to the protocol for the Project.

The data processor accepts that it may be necessary for the Data Producers to alter the terms of this agreement from time to time. As an example, this may include specific provisions relating to the Data required by Data Producers other than XXXXX. In the event that changes are required, the Data Producers or their appointed agent will contact the data processor to inform it of the changes and the data processor may elect to accept the changes or terminate the agreement.

16. 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 (30) days after the termination of the agreement. This also applies to the backup of personal data.

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.

The data processor covers all costs associated with the return and erasure of the personal data covered by this agreement.

17. 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

or

the agreement applies until _____.

23.09.2020

The agreement may be terminated by both parties with a mutual deadline of ____.

16. Contacts

Contact person at the data processor for any questions related to this agreement is: ____.

Contact person at the data controller for any questions related to this agreement is: ____.

[Delete the alternative below – 17a or 17b – that is not applicable]

17a. Choice of Law and Legal Venue

The agreement is governed by Norwegian law and the parties accept (fill in the names of the court) as legal venue. This also applies after termination of the agreement.

- Comment: This point applies when the data processor is a private operator.

17b. 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 the parties do not reach agreement through negotiations, the dispute will be resolved with binding effect by the Ministry of Education and Research. Either party may require that the dispute be sent to the Ministry.

- Comment: This point applies when the data processor is another state university or university college.

***

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)

23.09.2020

23.09.2020

APPENDIX I – DATASET DETAILS
APPENDIX II —PROJECT DETAILS
APPENDIX III — PUBLICATION POLICY

APPENDIX I – DATASET DETAILS (to be completed by the data producer before passing to applicant)

Dataset reference (EGA Study ID and Dataset Details)

Name of project that created the dataset

Names of other data producers/collaborators

Specific limitations on areas of research

Minimum protection measures required

File access: *Data can be held in unencrypted files on an institutional compute system, with Unix user group read/write access for one or more appropriate groups but not Unix world read/write access behind a secure firewall. Laptops holding these data should have password protected logins and screenlocks (set to lock after 5 min of inactivity). If held on USB keys or other portable hard drives, the data must be encrypted.*

APPENDIX II – PROJECT DETAILS (to be completed by the Requestor)

Details of dataset requested i.e., EGA Study and Dataset Accession Number

Brief abstract of the Project in which the Data will be used (500 words max)

All Individuals who the User Institution to be named as registered users

Name of Registered User	***Email***	***Job Title***	***Supervisor****

All Individuals that should have an account created at the EGA

Name of Registered User	**Email**	**Job Title**

APPENDIX III – PUBLICATION POLICY

XXXXX intend to publish the results of their analysis of this dataset and do not consider its deposition into public databases to be the equivalent of such publications. XXXXX anticipate that the dataset could be useful to other qualified researchers for a variety of purposes. However, some areas of work are subject to a publication moratorium.

The publication moratorium covers any publications (including oral communications) that describe the use of the dataset. For research papers, submission for publication should not occur until XX months after these data were first made available on the relevant hosting database, unless XXXXX has provided written consent to earlier submission.

In any publications based on these data, please describe how the data can be accessed, including the name of the hosting database (e.g., The European Genome-phenome Archive at the European Bioinformatics Institute) and its accession numbers (e.g., EGAS00000000029), and acknowledge its use in a form agreed by the User Institution with XXXXX.