DATA PROCESSING AGREEMENT
FOR THE SUBMISSION AND DISTRIBUTION OF PERSONAL DATA BY THE EUROPEAN GENOME-PHENOME ARCHIVE

Version 1.0, May 2020

Upon completion of the submission statement the Data Producer or any other organization upon Data Producer's mandate submits Personal Data (genetic and phenotypic data) of research participants to the European Genome-Phenome Archive (EGA). Personal Data is made accessible and distributed upon granted access by the Data Access Committee.

These Terms and Conditions (hereinafter Terms) address the requirements of Data Protection Laws for processing Personal Data by the EGA as the Data Processor and the relationship between and accountability of the Data Controller and Data Processor in processing Personal Data, normally determined by Data Processing Agreement.

1. INTRODUCTION

1. The European Genome-phenome Archive (EGA) is a service for permanent archiving and sharing of all types of personally identifiable genetic and phenotypic data (Personal Data) resulting from biomedical research projects, jointly managed by the European Molecular Biology Laboratory – and the Centre for Genomic Regulation (CRG). The submitted Personal Data are accessible and distributed under controlled access policy, whereby access decisions reside with the Data Access Committee (DAC), created or defined by the Data Producer for each dataset, and covered by a Data Access Agreement (DAA), defining the terms and conditions of the use of a specified dataset.
2. The European Molecular Biology Laboratory (EMBL) is an intergovernmental institution headquartered in Heidelberg, Germany, established by an agreement of 1973 (link) and enjoying privileges and immunities within the framework of its founding act of 1973, general principles of public international law and conventions signed with its host countries. Accordingly, it has the power to self-regulate data protection reflecting the essential principles of European Data Protection Law and focusing on scientific research as necessary for the fulfilment of its objectives and for the exercise of its functions by way of its Internal Policy No 68 on General Data Protection (IP No 68).
3. EMBL-EBI is the UK site of EMBL, established in Hinxton, UK, upon the Agreement of 1995 between the Government of the United Kingdom of Great Britain and Northern Ireland and EMBL concerning the European Bioinformatics Institute, enjoying the same position, privileges and immunities as EMBL and exercising the activities of EGA for EMBL.

4. The Centre for Genomic Regulation is a non-profit Spanish foundation, subject to GDPR according to Article 3(1) of the GDPR.
5. Personal Data submitted to and stored by EGA were collected by the Data Producer from individual Data Subjects (research participants) whose consent agreements authorise data release only for specific research use.

2. PURPOSE OF THESE TERMS

The purpose of these Terms is to identify processing activities of the Data Processor, whilst providing its service to the Data Controller and the global scientific community, to store submitted dataset(s) of genetic and phenotypic Personal Data with EGA and to distribute these dataset(s) upon DAC decision to various Recipients, requesting access to these data. Acceptance of these Terms implies the commitment to comply with the rights and obligations defined herein and with the requirements established by the legislation on data protection regarding processing of the Personal data defined in Section 3.

3. PROCESSING OF PERSONAL DATA

For the purposes outlined in Section 2 and further detailed in Appendix 1, EMBL and CRG act as Joint Data Processors (hereinafter the Data Processor) of Personal Data of research participants ("Data Subjects") embedded in the submitted dataset(s), and Data producer act as Data Controller (hereinafter the Data Controller).

The Data Processor provides contact details of the Data Protection Officer or any other person mandated to give information on data protection matters of the Data Processor on its internet page https://ega-archive.org/ .

4. TRANSFER OF DATA AND APPLICABLE DATA PROTECTION LAWS

Any Data Controller established within the European Economic Area, may transfer Personal Data to the Data Processor, partly being managed by an international organisation, upon relying on a derogation of the transfer being necessary for important reasons of public interest under Article 49(1)(d) and Article 49(4) of the GDPR.

Any Data Controller, exempted from the applicability of GDPR and/or subject to any other national law on data protection, shall duly rely on the appropriate legal basis for transfer of Personal Data to the Data Processor, under the Data Controller's applicable law.

Either party shall comply with Data Protection Laws applicable on its operations.

5. DATA PROCESSOR'S RESPONSIBILITIES:

1. The Data Processor shall only process Personal Data as instructed by the Data Controller as documented in these Terms, including with regard to transfers of Personal Data to a third country or an international organization, unless the Data Processor is required to do so by any applicable Data Protection Law; in such case, the Data Processor will inform the Data Controller of that legal requirement before Processing the relevant Personal data, unless that law prohibits such information on important grounds of public interest.
2. The Data Processor will use reasonable efforts to follow any other Data Controllers instructions as long as they are required by the Data Protection Laws, applicable to Data Processor, technically feasible and do not require changes to the EGA Service.
3. The Data Processor shall as soon as reasonably possible, inform the Data Controller if the Data Processor believes that any instruction of the Data Controller is in breach of Data Protection Laws, or is otherwise unable to implement it.
4. The Data Processor shall process Personal Data only for the purpose of providing it to the scientific community through the Data Processor.
5. The Data Processor shall implement and maintain appropriate technical and organisational measures as set out in Appendix 2. The Data Controller understands and agrees that these measures are subject to technical progress and development, and the Data Processor is therefore expressly allowed to implement alternative measures provided they maintain or exceed the general security level described in Appendix 2.
6. The Data Processor shall ensure that confidentiality applies to Personal Data and that access is strictly limited to the personnel who have committed themselves to confidentiality and have received appropriate training of their responsibilities.
7. The Data Processor shall not link or combine Personal Data to other information or archived data available in a way that could re-identify research participants.
8. Taking into account the nature of the Processing, Data Processor shall assist Data Controller by appropriate technical and organisational measures, insofar as this is reasonably possible, for the fulfilment of the Data Controller's obligation to respond to requests for exercising the Data subject's rights laid down in Chapter III of the GDPR.
9. The Data Processor shall keep all of the Personal data secure from any unauthorised or accidental use, access, disclosure, damage, loss or destruction.
10. The Data Processor shall without undue delay after becoming aware of and in accordance with Data Protection Laws, notify the Data Controller of any confirmed incident concerning unauthorized destruction, loss, alteration, disclosure of, or access to Personal data (“Security Incident”) via Data Controllers contact point, shared with the Data Processor at the time of the submission of data. The Data Processor shall together with the notification provide for contact details of the Data Protection Officer or other contact point where more information about the incident can be obtained.

11. Upon request of the Data Controller by way of re-submission, the Data Processor shall delete or return all Personal Data to the Data Controller.
12. The Data Processor shall make available to the Data Controller all information, where necessary and technically feasible, for the Data Controller to demonstrate compliance with its obligations.
13. Data Processor shall assist the Data Controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 of GDPR, taking into account the nature of the processing and the information available to the Data Processor.
14. Data Processor shall redirect all third party requests regarding Personal Data or information about the Processing activities to the Data Controller, whether the request is made by a Data subject, the Supervisory Authority or any other third party, unless such requests cannot legally be redirected to the Data Controller.
15. Data Processor shall distribute Personal Data submitted by Data Controller only upon decision to grant access to specific dataset(s) made by the relevant DAC.

6. USE OF SUB-PROCESSORS

The Data Processor may use one or more Sub-processors to process Personal Data during the course of submission and distribution of Personal Data. The Data Processor must enter into a written agreement with each Sub-processor, requiring the Sub-processor to comply with terms no less protective than these Terms.

Sub-processor(s) may only Process Personal Data for the purposes of these Terms. The Data Processor remains responsible for all Sub-processors it uses to carry out the Processing.

The Data Processor shall keep record of the list of Sub-processors that will be provided to the Data Controller upon request. Any changes thereof will be notified on Data Processor's website. Unless the Data Processor receives an objection to a change within 30 days of the notification, that change will be deemed approved. In case of Data Controller's objection, both Data Controller and Data Processor shall use all reasonable endeavours in good faith to resolve the objection.

7. DATA CONTROLLER'S RESPONSIBILITIES

Data Controller is responsible for ensuring that Personal Data embedded in datasets and transmitted to the Data Processor are pseudonymised and encrypted in transit and at rest.

Data Controller is responsible at each time:

- to demonstrate the existence of Data subject's informed consent for participation in the research project or any other suitable legal basis for processing Personal Data,

- to obtain appropriate ethical or other approvals for collecting Personal Data embedded in the submitted datasets and
- to comply with and to be able to demonstrate compliance with applicable Data Protection Laws
- to control distribution of Personal Data.

8. AUDIT

The Data Processor will contribute to audits conducted by the Data Controller by providing appropriate documentation. In exceptional cases and upon prior agreement with the Data Processor, the Data Controller may conduct on-site inspections. Any direct or indirect cost incurred by the Data Processor through an audit request will need to be reimbursed by the Data Controller, and any on-site inspection will need to be (i) pre-agreed in terms of objective, scope, timing and process, and (ii) without prejudice to the privileges and immunities granted to EMBL.

9. Term and Termination

These Terms take effect on the day of submission of data to the Data Processor and will remain in effect whilst any part of the Data Controller's data is stored by the Data Processor. It can be terminated by either party with 60 days' notice, provided that any Personal data provided by the Data Controller will be returned or deleted upon expiration of the notice period.

10. Liability and indemnification

Data Controller shall indemnify and hold harmless the Data Processor from and against any losses, damages and expenses (including without limitation legal fees) awarded against the Data Processor and arising from a claim brought as a result of the Data Controller's breach of its obligations under these Terms or applicable Data Protection Laws ("Claim"); provided, however, that the indemnity shall not extend to any Claim arising from (i) a negligent act or omission of the Data Processor and/or its personnel, (ii) any misconduct by the Data Processor and/or its personnel and/or (iii) any breach of these Terms or applicable Data Protection Laws by the Data Processor.

Each Party shall be deemed liable for the damage caused by any of its processing activities that do not comply with its obligations under these Terms and applicable Data Protection Laws.

The Data Processor shall be exempt from any liability under the previous paragraph if it proves that it is not in any way responsible for the event giving rise to the damage.

11. Dispute resolution

The Parties shall endeavor to settle their disputes amicably.

Any controversy or claim arising out of, or relating to, these Terms (including the enforceability or breach thereof, any question regarding its existence, validity or termination) or relating to the EGA Service shall be resolved using the internal dispute resolution mechanisms of EGA including those related to Data Protection.

Once those remedies have been exhausted they may be finally resolved by arbitration under the Rules of the LCIA ("Rules"), which Rules are deemed to be incorporated by reference into this section. Notwithstanding the foregoing, the arbitrator shall not be authorized to award punitive damages with respect to any such claim or controversy, nor shall any party seek punitive damages relating to any matter under, arising out of or relating to these Terms or the Service in any other forum. If any arbitration is commenced by either Party, the substantially prevailing Party in that arbitration or action is entitled to recover from the other Party its attorneys' fees and costs (including arbitration fees and costs and expert witness fees) incurred in connection therewith. The entire arbitration shall be conducted and concluded in no later than ninety (90) days after service of the arbitration demand, unless the arbitrator has reasonable grounds to extend this deadline, and it may do so without the approval of either party. The extension and the reasoning thereof shall be notified to both parties. A written demand for arbitration must be delivered within one (1) year from the date on which the Services to which the claim relates were provided. Failure to comply with this provision shall be a complete bar to any claim. The place of arbitration will be London, the language to be used in the arbitral proceedings shall be English, unless otherwise agreed upon, and the governed substantive law to be used shall be of England and Wales.

Nothing herein shall be deemed or interpreted as a waiver, express or implied, of any privileges or immunities accorded to EMBL, being one managing party of Data Processor by its constituent documents or international law.

12. DEFINITIONS.

Unless otherwise agreed or defined in these Terms, all capitalized terms used will have the meanings given to them below:

1. "Data Controller", "Data Processor", "Personal Data", "Processing", "Genetic data", "Pseudonymisation" shall have the same meaning as described in the GDPR.
2. "Data Producer" shall mean an organization that collected the samples and generated any associated analyses of the Personal Data, and submitted those data to the Data Processor, either alone or having mandated other institutions to complete the submission.
3. "DAC" means Data Access Committee, a body of one or more individuals, named by the Data Producer, granting data release to external requestors, these being Recipients.
4. "Data Protection Laws", the GDPR and any national implementing laws, regulations and secondary legislation and any other laws and regulations relating to the processing of Personal Data and privacy which apply to a Party; and, if applicable, the guidance and codes of practice issued by any competent data protection supervisory authority; and for the Data Processor, partly

managed by an intergovernmental institution, EMBL`s IP No 68 and any other rules regulating data protection, further provided that any reference to GDPR or any other national implementing law in relation to EMBL is simply for convenience and does not imply a waiver of any privileges and immunities applicable to EMBL.

5. “EGA service” means data center facilities, servers, networking equipment, and host software systems (e.g., virtual firewalls) that are under Data Processor's control and used to provide its Services.
6. “EGA Security Standards” means the security standards attached to these Terms as Appendix 2.
7. “Security Incident” means a breach of Data Processors' security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Data Controller`s data on systems managed or otherwise controlled by Joint Data Processors. Security incidents do not include unsuccessful attempts or activities that do not compromise the security of Data Controller`s data (including unsuccessful log-in attempts, pings, port scans, denial of service attacks and other network attacks on system firewalls or networked systems).
8. “Sub-processor” shall mean any processor which the Data Processor engages to carry out specific processing activities on behalf of the Data Processor.
9. “Effective date” means the date on which the Data Controller accepted these Terms.
10. “Recipient” means any natural or legal person, to which the Personal Data are disclosed upon DAC granted access to the data.
11. “Supervisory Authority”; as long as GDPR applies, a supervisory authority of a Member State concerned pursuant to Article 55(2) of the GDPR, for EMBL, the Data Protection committee pursuant to Article 20 of the Internal policy No 68.

SIGNED for and on behalf of:

Name:

Position:

Signature:

Date:

Appendix 1

Subject Matter and Details of the Data Processing

Subject Matter

Data Controller`s submission of Personal Data to EGA service, EGA processing of such data, and distribution to recipients upon DAC granted access.

Duration of the Processing:

Processing takes place from the submission of data from the Data Controller to the Data Processor and until the end of Data Processor`s services, including, if applicable, any period during which provision of the EGA Services may be suspended and any post-termination period during which the Data Processor may continue providing the Services requested by the Data Controller for transitional purposes, unless deletion or return of the data is requested by the Data Controller.

Nature and Purpose of the Processing

Provision of the EGA Services for the purpose of sharing deposited data with the international scientific community and the general public. EGA services may include the generation and provision of quality control metrics, facilitating data discovery, ensuring datasets are updated to current standards, or applying data compression.

Categories of Personal Data processed (special data)

Genetic and phenotypic data of research participants.

The Categories of Data Subjects to whom the Project Personal Data relate

Research participant - individuals/data subjects whose explicit consent for processing personal data is provided to the Data Controller in the relevant agreements that authorize data release for specific research purposes.

Appendix 2

European Genome-phenome Archive: Security Overview

Version 1.0, March 2019

Authors: Thomas Keane (EMBL-EBI), Dylan Spalding (EMBL-EBI), Jordi Rambla (CRG, Barcelona), Arcadi Navarro (CRG, Barcelona), Paul Flicek (EMBL-EBI), Helen Parkinson (EMBL-EBI)

The European Genome-phenome Archive (EGA) is a controlled access archive for consented human data. The EGA does not grant or deny access to data, this is done by the Data Access Committee (DAC) of the relevant Data Controller and EGA applies these permissions to the access to data on behalf of the Data Controller (Figure 1). This document provides an overview of EGA's practices in ensuring the security of data stored at EGA. As security is a prime concern of the EGA, the EGA is a member of the Global Alliance for Genomics and Health (GA4GH - https://www.ga4gh.org/) Data Security work stream. The EGA contributes and helps develop the recommendations outlined the GA4GH Security Technology Infrastructure document[1], which defines guidelines, best practices, and standards for building and operating an infrastructure that promotes responsible data sharing in accordance with the GA4GH Privacy and Security Policy[2].

[1] https://www.ga4gh.org/docs/ga4ghtoolkit/data-security/2016May10_REV_SecInfrastructure.pdf
[2] https://www.ga4gh.org/docs/ga4ghtoolkit/data-security/Privacy-and-Security-Policy.pdf

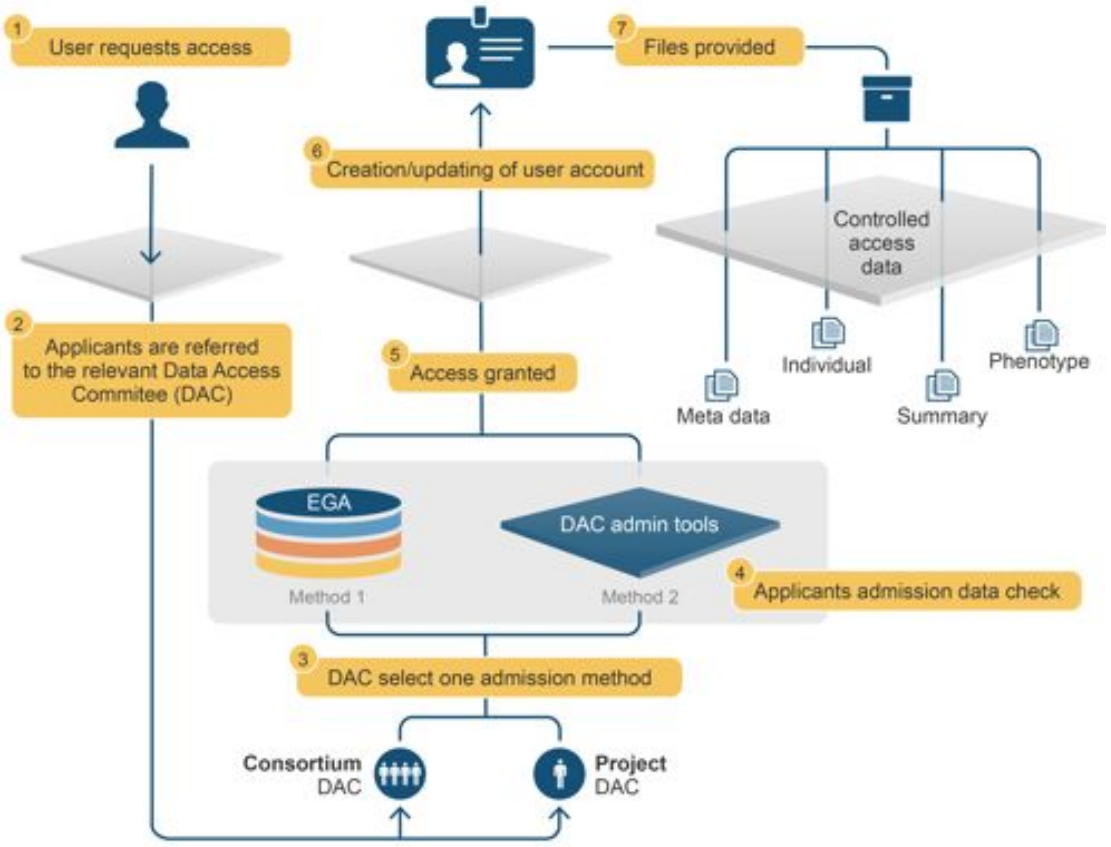

Figure 1: Process of applying for access to data held in the EGA. The user makes a request to access data controlled by a DAC. The DAC informs the EGA of the decision, and if access is granted, the EGA creates an account for the user (if the user does not already have an account) and grants permission to the data for that user.

The key points of EGA security strategy are:

1 Regular Risk Assessment

- The EGA regularly identifies and assesses risk related to the following:
    - Breach of confidentiality,
    - Breach of privacy or autonomy,
    - Malicious or accidental corruption or destruction of data archived at EGA,
    - Disruption of services provided by the EGA.

2 Risk mitigation

- The EGA implements and maintains safeguards to minimize the risks identified above in accordance with the 5 control objectives identified below and outlined in the GA4GH Security and Infrastructure document[3].
- If a data breach is discovered, the EGA applies a defined protocol to minimize damage.

3 Identity and authorisation management

- The EGA authenticates the identity of individuals or software accessing controlled access data held at the EGA.
- The EGA ensures an appropriate level of assurance (LoA) is applied to the identity consistent with the risk associated with that individual, such as multi-factor authentication for DACs.
- The EGA provides the minimum access rights and privileges consistent with the user's identity, allowing access consistent with the GA4GH Privacy and Security Policy, as determined by the appropriate DAC.

4 Audit Logs

- The EGA maintains a set of logs recording:
    - Changes to user access rights,
    - Data access requests,
    - Resource usage.

5 Cryptography, communication security, and data integrity

- The EGA ensures data transmission integrity using a hash function.
- All data transmitted to or from the EGA is end-to-end encrypted.
- All data at EGA is stored using strong encryption.
- Encryption keys are not stored in the same system as the encrypted data.
- All data archived at EGA must be accompanied by a signed submission statement ensuring appropriate consent or ethical approval has been obtained, and is in accordance with all applicable laws and regulations.

The EGA has a defined protocol defining the response in the event of a security breach, and is continuing to work with the GA4GH Data Security Work Stream to help define best practice and associated standards for breach responses.

[3] https://www.ga4gh.org/docs/ga4ghtoolkit/data-security/2016May10_REV_SecInfrastructure.pdf

Control Objectives

The following control objectives are defined with the aim to implement technology safeguards to prevent the incidences identified below:

- Control Objective 1: Unauthorized access, use, or disclosure of confidential and private data.
- Control Objective 2: The discovery, access,and use of individuals' genomic and health-related data, and individual identities, other than as authorized by applicable jurisdictional law, institutional policy, and individual consents.
- Control Objective 3: Accidental or malicious corruption or destruction of data.
- Control Objective 4: Disruption, degradation, and interruption of services enabling access to data.
- Control Objective 5: Potential security attacks and misuse of authorized accesses and privileges.

-