Data Processing Agreement

According to Art. 28, EU General Data Protection Regulation (GDPR)

EGI DPA Template Version: v.7

between

EGI Foundation
Science Park 140
1098 XG Amsterdam
The Netherlands

“Controller”

and

Company / Organization
Address line 1
Address line 2
Country

“Processor”

Preamble

The controller commissions the processor to process personal data on behalf of the controller in accordance with Art. 28 of the EU General Data Protection Regulation 2016/679 (EU-GDPR).

For the purpose of this agreement the controller may either process personal data directly from the data subject or act as a processor on behalf of another controller.

This Agreement on the processing of personal data on behalf of the data controller regulates the conditions to be satisfied by the data processor when processing personal data on behalf of the data controller.

The definitions in Article 4 of the GDPR apply.

1. Nature and duration of data processing

The performance of the following activities by the processor is subject to this Agreement:

Description of the activities performed by the processor

The data processing will commence on DD.MM.YYYY and

☒ is for an indefinite period.
☐ expires on DD.MM.YYYY.

2. Categories of personal data

Categories of personal data processed by the processor on behalf of the controller:

Identification data:
☐ Name
☐ Identification number
☐ E-mail address
☐ Phone number
☐ Address
☐ Bank details
☐ Other: Please specify

Behavioural data:
☐ Usage data (websites, services, social media)
☐ Data on purchase or payment transactions
☐ Location / positioning data
☐ Working time data
☐ Individual performance data
☐ Other: Please specify

Data allowing conclusions on the personality:
☐ Hobbies
☐ Memberships
☐ Criminal record
☐ Other: Please specify

Biographical data:
☐ CV data
☐ Education, degrees
☐ References
☐ Other: Please specify

Sociodemographic data:
☐ Age
☐ Gender
☐ Nationality
☐ Health data
☐ Family status
☐ Religion
☐ Sexual orientation
☐ Other: Please specify

3. Purpose of data processing

The purpose of the collection, processing and use of the personal data mentioned is:

Description of the purpose(s) of data processing

4. Categories of persons concerned

List of the categories of persons affected

5. Obligations of the processor

(1) The processor is obliged to maintain strict confidentiality during processing and shall process personal data only as contractually agreed or as instructed by the controller, unless the processor is required by law to carry out a specific processing activity. If such obligations exist for the processor, the processor shall notify the controller thereof prior to processing, unless such notification is prohibited by law. Furthermore, the processor shall not use the data provided for processing for any other purpose, in particular for their own purposes.

(2) The processor assures that the persons employed by them for processing have been made familiar with the relevant provisions of data protection and this Agreement prior to commencement of processing. Appropriate training and awareness-raising measures shall be repeated at regular intervals. The processor shall ensure that persons assigned to data processing activities are instructed and monitored appropriately on an ongoing basis with regard to the fulfilment of data protection requirements as well as the provisions resulting from this Agreement, such as the controller's authority to issue directives and purpose limitation.

(3) Persons who may gain knowledge of the data processed on behalf of the controller must commit in writing to maintain confidentiality, unless they are already legally subject to a relevant confidentiality obligation.

(4) The processor confirms that they are aware of the relevant general data protection regulations. They shall comply with the principles of proper data processing and ensure proper data processing by means of ongoing monitoring and regular checks.

(5) In connection with the commissioned data processing, the processor shall assist the controller in drawing up and updating the record of data processing activities and in carrying out the data protection impact assessment. All necessary information and documentation shall be provided and forwarded to the controller upon request.

(6) If the controller is subject to an inspection by supervisory authorities or other bodies, or if data subjects claim rights against them, the processor is obliged to support the controller to the extent necessary, as far as the data processing activities carried out by the processor are concerned.

(7) The processor shall inform the controller of inspections carried out by or on behalf of supervisory authorities for data protection without delay.

(8) The processor shall not provide information to third parties or to the data subject without the prior consent of the controller. Requests addressed directly to them shall be forwarded to the controller without delay.

(9) To the extent required by law, the processor shall appoint a competent and reliable person as data protection officer. It must be ensured that there are no conflicts of interest for the data protection officer. The controller may contact the data protection officer directly. The processor shall inform the controller of the contact details of the data protection officer or of the reasons why no officer has been appointed. The processor shall immediately inform the controller of any changes in the person of the data protection officer.

(10) The data processing shall generally take place within the EU or the EEA. Any relocation to a third country may only take place with the consent of the controller and under the conditions contained in Chapter V of the GDPR and in compliance with the provisions of this Agreement.

(11) If the processor is not established in the European Union, they shall appoint a responsible contact person in the European Union in accordance with Art. 27 GDPR. The contact details of the contact person as well as all changes in the contact person must be communicated to the controller without delay.

(12) The processor shall comply with all principles set out by the GÉANT Data Protection Code of Conduct in its most current version, which will be made available to the processor by the controller upon request.

6. Technical and organizational measures (TOM)

(1) The processor shall implement and document the technical and organisational measures (TOM) listed in Annex 2 to this Agreement prior to commencement of data processing and hand them over to the responsible party for inspection upon request. The measures described in the Annex 2 are defined as binding. They define the minimum required from the processor.

(2) The implementation of and compliance with all technical and organisational measures required in accordance with Art. 32 GDPR shall also be performed by the processor beyond the measures specified in Annex 2.

(3) The technical and organisational measures are subject to technical progress and further development and may be updated in the course of the contractual relationship. In doing so, the processor shall not fall below the security level of the specified measures.

(4) If fundamental changes are made to the technical and organisational measures, these shall be agreed with the controller. The changes shall be fixed in writing and the Annex 2 shall be adapted accordingly by the processor. However, no Agreement is required if the changes lead to an improvement of the data protection level agreed within the context of this Agreement and the controller is informed of these changes.

(5) If the measures taken do not meet or no longer meet the requirements of the controller, the processor shall notify the controller without delay.

(6) If personal data are processed in private homes or in the context of teleworking, the processor shall ensure that the necessary special measures for data protection within the meaning of Art. 32 GDPR are complied with.

(7) Upon request, the processor shall give evidence to the controller that the technical and organizational measures have been implemented effectively. For this purpose, he may also submit reports or extracts from reports of independent bodies or a suitable certification according to information security or data protection standards.

(8) Considering the type of data processing and the information made available to the processor, the processor shall provide adequate support to the controller in fulfilling his responsibilities under Articles 32 to 36 GDPR (concerning the security of the processing, notification obligations, data protection impact assessments and consultations with relevant supervisory authorities).

7. Correction, deletion and return of data

(1) The processor shall correct, delete or block data processed on behalf of the controller only in accordance with the Agreements made or in accordance with the instructions of the controller.

(2) At the latest upon termination of the contractual relationship or before upon request by the controller, the processor shall return to the controller all personal data, documents handed over and processing results to him or, after prior consent of the controller, shall destroy them in accordance with data protection regulations and provide evidence of this.

(3) Documentation which serves as evidence of proper data processing shall be stored by the processor in accordance with the respective retention periods beyond the end of the contract. He may hand these over to the controller at the end of the contract in order to relieve himself of the responsibility.

(4) The parties to the contract mutually undertake, even beyond the end of the contractual relationship, to maintain confidentiality with regard to any data.

8. Subcontracting

(1) The commission of further subcontractors (in addition to the subcontractors listed in Annex 1) for the purpose of processing personal data falling in the scope of this Agreement requires the prior written consent of the controller. The processor is obliged to apply the regulations and obligations set out in this Agreement to subcontractors and to assure the control rights of the controller also towards subcontractors in accordance with the contractual regulations set out herein. This shall apply in particular to the right of performing an inspection also directly vis-à-vis subcontractors.

(2) Upon request, the processor shall provide the controller with information about the essential contractual content of a subcontracting relationship and the implementation of the data protection-relevant obligations in the subcontracting relationship, if necessary, by inspecting the relevant contractual documents. The processor may black out those parts of the contract documents which are not necessary for a data protection check.

(3) Not to be regarded as a subcontracting relationship within the meaning of this provision are those services which the processor uses from third parties as an auxiliary service to support the execution of the commission. This includes e.g. telecommunication services, maintenance and user support (if no access to data of the controller can occur), cleaning or auditing services.

(4) The commissioning of subcontractors who do not process data exclusively from the territory of the EU or the EEA is only possible if the conditions stated in Sections 5 (10) and (11) of this Agreement are observed. In particular, it shall only be permissible to the extent that and as long as the subcontractor offers appropriate data protection guarantees. The processor shall inform the controller of the specific data protection guarantees offered by the subcontractor and how proof of such guarantees can be obtained.

9. Inspections by the controller

(1) The controller shall be entitled to convince themselves or third parties commissioned by them of the effective implementation of the technical and organizational measures taken by the processor on site prior to the commencement of data processing by the processor and then on a regular basis.

(2) During on-site inspections, the controller shall take the operational processes of the processor into consideration and announce inspections at least two weeks in advance.

(3) The processor shall be obliged to support the controller to the best of their ability in carrying out the inspections. They are obliged to provide the controller, upon request, with the information and evidence necessary to comply with his obligation to carry out inspections in connection with the processing of personal data.

10. Notification about violations of the data processor

(1) The processor and the controller shall inform each other immediately if breaches, irregularities or suspicions of data protection violations occur. The parties shall make all reasonable efforts to remedy any breaches without delay.

(2) In all cases, the processor shall notify the controller if them or the persons employed by them have committed violations of the provisions for the protection of personal data of the controller.

(3) The processor understands that according to Art. 33 and/or 34 GDPR information obligations may exist in the event of a breach of data protection. For this reason, such incidents (including loss, unauthorised disclosure or unauthorised access to data) must be reported to the controller immediately and within 48 hours at the latest, regardless of the cause. This shall also apply in the event of serious disruptions to business operations or suspicion of other violations of regulations for the protection of personal data of the controller. In consultation with the controller, the processor shall take appropriate measures to secure the data and to mitigate possible adverse consequences for data subjects. As far as the controller faces obligations according to Art. 33 and/or 34 GDPR, the processor will support them in this.

11. Authority of the controller to issue directives

(1) The processor shall be strictly bound by the instructions of the controller at all stages of processing personal data on behalf of the controller. The controller reserves the right to issue instructions on the type, scope and procedure of data processing.

(2) The processor shall immediately inform the controller if according to their opinion an instruction violates data protection regulations. The processor shall be entitled to suspend the execution of the corresponding instruction until it has been confirmed or amended by the controller following notification.

12. Final provisions

Upon conclusion of this Agreement, any (framework) regulations on data processing concluded between the parties shall be replaced by this Agreement.

Amendments to this Agreement must be made in writing. (Oral) supplementary agreements do not exist.

Should any of the above provisions be or become invalid or incomplete in whole or in part, the validity of the remaining provisions shall remain unaffected thereby. The parties agree to replace the invalid or incomplete provision with a valid provision that comes as close as possible to the economic intent and purpose of the parties.

The descriptions of the subcontracting relationships in Annex 1 and of the technical and organisational measures (TOM) in Annex 2 are an integral part of this Agreement.

Independent from the provisions made in Section 1, the controller or processor may only terminate this agreement after effective termination of all data processing activities that are subject to this agreement. Confidentiality of any data that the processor gained knowledge of during the execution of data processing activities shall remain in force indefinitely after the termination of this agreement.

Signatures

Amsterdam, DD.MM.YYYY	Place, DD.MM.YYYY
Data controller EGI Foundation	Data processor Company / Organization

Annex 1: Subcontracting relationships

Relevant subcontracting relationships as defined in Section 8 of this Agreement that fall into the scope of the data processing covered by this Agreement:

☐ No third parties are subcontracted for data processing.
☐ The following parties are subcontracted for data processing:

Company name	Company location	Subject to subcontracting

Annex 2: Technical and organizational measures (TOM)

According to Art. 32 GDPR

The processor commits towards the controller to effectively implement and monitor the technical and organisational measures included in or referenced from this Annex.

The measures set out below serve the following purposes:

- the pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

☐ The processor provides the following complete documentation describing in a meaningful manner the implementation of the technical and organisational measures (TOM) hat have been implemented for the purposes mentioned above: Reference / title of the submitted TOM documentation

☐ The processor does not provide a separate, complete documentation of the technical and organizational measures that have been implemented. In this case, the section "Description of the implementation by the processor" in each of the following paragraphs (1 to 13) **must be completed** in a meaningful way **by the processor**.

(1) Access control (general)

Description of the implementation by the processor:

To be completed by the processor, if no separate documentation of the technical and organisational measures that have been implemented is provided

(2) Physical access control

Description of the implementation by the processor:

To be completed by the processor, if no separate documentation of the technical and organisational measures that have been implemented is provided

(3) Access control to networks, applications and information

Description of the implementation by the processor:

To be completed by the processor, if no separate documentation of the technical and organisational measures that have been implemented is provided

(4) Control of user activities

Description of the implementation by the processor:

To be completed by the processor, if no separate documentation of the technical and organisational measures that have been implemented is provided

(5) Control of segregation

Description of the implementation by the processor:

To be completed by the processor, if no separate documentation of the technical and organisational measures that have been implemented is provided

(6) Control of data carriers and mobile devices

Description of the implementation by the processor:

To be completed by the processor, if no separate documentation of the technical and organisational measures that have been implemented is provided

(7) Pseudonymisation and anonymisation

Description of the implementation by the processor:

To be completed by the processor, if no separate documentation of the technical and organisational measures that have been implemented is provided

(8) Transmission control

Description of the implementation by the processor:

To be completed by the processor, if no separate documentation of the technical and organisational measures that have been implemented is provided

(9) Input control

Description of the implementation by the processor:

To be completed by the processor, if no separate documentation of the technical and organisational measures that have been implemented is provided

(10) Control of availability and access

Description of the implementation by the processor:

To be completed by the processor, if no separate documentation of the technical and organisational measures that have been implemented is provided

(11) Recoverability

Description of the implementation by the processor:

To be completed by the processor, if no separate documentation of the technical and organisational measures that have been implemented is provided

(12) Control of subcontracting

Description of the implementation by the processor:

To be completed by the processor, if no separate documentation of the technical and organisational measures that have been implemented is provided

(13) Testing, assessing and evaluation

Description of the implementation by the processor:

To be completed by the processor, if no separate documentation of the technical and organisational measures that have been implemented is provided