Data Processing Agreement

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

between

Company / Organization
Address line 1
Address line 2
Country

“Controller”

and

EGI Foundation
Science Park 140
1098 XG Amsterdam
The Netherlands

“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).

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. Subject and duration of data processing

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

Provision of Service: EGI Single Sign On (SSO)

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: Affiliation, country, IP address

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

Data allowing conclusions on the personality:
☐ Hobbies
☐ Memberships
☐ Criminal record
☒ Other: Membership information on groups and communities

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:

Identify the users accessing services to support their delivery and track usage of resources for accounting and security management.

4. Categories of persons concerned

All legitimate users of the collaboration tools, including guest users (where applicable).

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 his own purposes.

(2) The processor assures that the persons employed by him 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 he is aware of the relevant general data protection regulations. He 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 him, 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 him 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, he 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 himself or third parties commissioned by him 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 his ability in carrying out the inspections. He is 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 he or the persons employed by him 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 him 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 his 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

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

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**
CESNET	Czech Republic	Resource provider, provision of virtual machines

Annex 2: Technical and organizational measures (TOM)

According to Art. 32 GDPR

This document describes the technical and organizational measures implemented by EGI Foundation to meet legal and contractual requirements when processing personal data.

The measures described in numbers 1 to 13 serve the purpose …

- to encrypt or pseudonymize personal data where necessary (see, inter alia, 6 to 8),
- to ensure the confidentiality, integrity, availability and resilience of systems and services in connection with the processing of personal data (see, inter alia, 1 to 10),
- to restore the availability of and access to personal data in the event of a physical or technical incident in a timely manner (see 11), and
- to regularly review, assess and evaluate the effectiveness of all technical and organizational measures to ensure the security of processing (see, inter alia, 12 and 13).

The following measures apply to all data processing activities that are under control of EGI Foundation, or where EGI Foundation is a subcontracted data processor on behalf of another data controller.

Please note: In federated service delivery scenarios, one or more data controllers and one or more subcontracted data processors may be entrusted with or involved in processing personal data.

(1) Access control

All access rights (both for access to IT systems and data and for access to buildings and rooms) are assigned according to the principle that employees and third-party users are only granted the level of access they need to perform their activities (need-to-know principle).

Access rights are granted according to defined (role-based) permission profiles. The access rights granted are reviewed regularly. Rights that are no longer required are withdrawn immediately.

Access to networks and network services is restricted by technical and physical measures. Access to wireless corporate networks that allow access to personal data is protected by personalized authentication (PKI, IEEE 802.1x). This applies in an analogous manner to wired access, unless it is from a secure area that is sufficiently protected and controlled by physical access control measures.

(2) Physical access control

Physical secure areas (zones) are defined on the basis of information security and data protection requirements and protected against unauthorized access by appropriate physical safeguards. The physical security concept distinguishes between public areas, controlled areas, restricted/internal areas, and high-risk zones. Secure zones are defined based on the protection needs of the information assets housed or made accessible within them.

Depending on the specific zone classification, selected or all of the following security features are implemented: Access restriction through personalized access medium, video surveillance and door-open sensors at access points, motion detection, privacy screens or view guards on potentially confidential information, and no photography policy.

For dealing with visitors and deliveries, procedures are used to prevent unauthorized persons from accessing security areas.

(3) Logical access control to processing systems

All data processing systems are equipped with a secure authentication mechanism (X509 certificate or password protection).

Defined procedures are used to authorize access to information, taking into account the need-to-know principle. Special procedures are in place for granting access rights to privileged systems (e.g., systems or applications used to control or administrate critical processes or to manage access rights for other systems).

For authentication on data processing systems (IT systems), secure passwords are used that have sufficient length, are robust against dictionary attacks, do not contain strings of consecutive letters or digits and are not based on facts that could be easily be guessed by others. Passwords must be changed whenever there is an indication that the password has been compromised. A changed password must not match or contain a password that has been used in the past. Where technically possible, the use of two-factor-authentication is enforced.

A " clear desk & screen policy" is implemented: When leaving the workplace, all computers in use must be locked (screen lock). In case of inactivity, the screen lock is automatically activated after a maximum of 10 minutes. Documents that may contain confidential information must not be kept open and unattended on desks or in other freely accessible storage areas.

(4) User activity control

All employees must attend mandatory basic training on information security and data privacy on an annual basis. Participation in this training is recorded. New employees are familiarized with the main regulations on information security and data privacy relevant to them at the start of their employment or assignment.

User activities, including logon attempts to data processing systems (IT systems), are logged to the extent required.

User accounts via which personal data can be accessed as part of processing activities must be personalized and must not be shared by more than one person.

Administrative activities on IT systems (such as changes to system configurations) are logged. Configuration files are historized, backed up and checked regularly and as required.

(5) Segregation control

It is ensured that personal data collected for different purposes are not mixed in their processing. To this end, multitenant systems are used where necessary, or systems are physically or logically separated.

(6) Data carrier and mobile device control

Data carriers containing personal data are stored in secure locations that prevent access to these carriers by unauthorized persons.

Personal data stored on mobile devices and data carriers (including laptops, smartphones, USB sticks) are required to be encrypted. The use of any type of private Internet/Cloud storage for the (temporary) storage of such data is prohibited. Confidential data will never be stored on private storage media or end devices.

Personal data that are no longer required are deleted. Electronic storage media and paper documents that are no longer required will be disposed of or destroyed / made unusable in such a way that it is no longer possible to gain knowledge of the data stored or contained on them.

The use of mobile devices is restricted and controlled. If personal data are accessed via mobile devices, suitable measures are taken to ensure that the devices cannot be used by unauthorized persons, for example in the event of loss or theft. All mobile devices used for business purposes are configured in such a way that they are protected by a query for a secret (e.g., PIN, pattern or biometric information) in the lock screen. The lock screen is automatically activated during inactivity. The corresponding mobile devices must never be left unattended. Modifications to the operating system software / firmware are prohibited. Security-relevant updates and patches are applied automatically. The devices are subject to comprehensive mobile device management (MDM), which technically implements these and other restrictions, policies, and measures.

(7) Pseudonymization and anonymization

Measures for pseudonymization or anonymization of personal data are implemented to the extent necessary. Data in development environments used for testing purposes is anonymized or pseudonymized wherever possible. Data on the usage of websites that is evaluated to generate usage statistics is anonymized.

(8) Transfer and dissemination control

Mechanisms for securing data traffic and communication connections, as well as for monitoring and logging activities in networks, have been established to the required extent. As appropriate, firewalls and intrusion detection and prevention systems (IDS / IPS) are in place.

When personal data is transmitted via public communication networks, secure end-to-end encryption of the communication is ensured. When establishing secure connections (VPN tunnels) offering access to IT resources via public networks, two-factor authentication is used as a matter of principle. If the exchange of confidential authentication information is required, this is done via a different communication path than the actual data transmission.

When transporting personal data stored on data carriers, the use of encryption, among other things, ensures that the data is protected against unauthorized access, manipulation or loss. After transport, the data is deleted from the storage media used for transport if it is no longer required on them.

Paper printouts and exports of confidential data from their source system are avoided whenever possible. Hard copies and electronic exports of confidential information leaving the business premises are handled with special care, taking into account the relevant confidentiality level - with the aim of preventing disclosure, loss and unauthorized copying. As soon as a paper printout is no longer required, it is destroyed. Electronic data exports that are no longer required are deleted again from the respective storage location and any transport data carrier used.

(9) Input control

Measures for subsequent verification of whether and by whom data has been entered, changed or removed (deleted) are implemented to the extent necessary. In systems used to collect and process personal data, access is categorized and automatically recorded. The integrity of log information is ensured.

(10) Availability control

A redundant design of communication and data processing systems (IT systems) and supporting facilities has been implemented to the required extent. An uninterruptible power supply (UPS) and high-availability Internet connection with automatic failover have been implemented at all relevant locations. Server and storage systems are designed redundantly (including redundant power supply units, disk mirroring). As appropriate, load balancing and failover are implemented for virtualized server systems.

(11) Recoverability

Data backups of databases and operating system images are taken to the extent required and with the aim of preventing the loss of personal data in the event of a technical malfunction or human error. Backups are performed for network drives and servers in productive operation, and the performance is recorded (logged) and monitored. The recovery of data backups is tested.

Processes or procedures for handling disruptions to IT systems and for restoring systems after a disruption have been established to the extent required.

Business continuity management (BCM) includes activities for business process impact analysis (BIA), definition and application of measures to ensure business continuity, taking into account information security and data protection aspects, as well as tests and reviews of the effectiveness of the measures implemented. A business process impact analysis is prepared or reviewed at least annually on the basis of the key business processes and services.

(12) Job control and subcontracting

The selection of subcontractors is carried out with the objective of ensuring that there is no increased risk to compliance with data protection objectives.

Depending on their role and the scope of access to confidential or personal data, subcontractors must, among other things, acknowledge and comply with regulations on secrecy / confidentiality as well as data protection (e.g., confidentiality / non-disclosure agreement), as well as an information security policy for suppliers.

In the case of security-critical subcontractors, service providers or suppliers, the following reporting and audit requirements are implemented: evaluation of contractually agreed reports (e.g., security events/incidents, availability statistics) as well as supplier audits using a self-assessment questionnaire, with an additional on-site inspection as necessary.

(13) Review, assessment and evaluation

Information on potential technical vulnerabilities or errors in data processing systems (IT systems) is evaluated at regular intervals and appropriate measures are initiated. Critical patches are deployed for both operating systems and software applications in use.

Data processing systems (IT systems) are checked regularly to the extent required and after changes to ensure that they are functioning properly.

An internal audit program is in place that covers regular system audits, process audits, IT security audits and data protection audits and controls.