



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

Data controller
EGI Foundation

Place, DD.MM.YYYY

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) that 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



Annex 3: Standard contractual clauses

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

EGI Foundation
Science Park 140
1098 XG Amsterdam
The Netherlands

(the 'data exporter')

and

Company / Organization
Address line 1
Address line 2
Country

(the 'data importer')

each a 'party'; together 'the parties',

have agreed on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

1. Definitions

For the purposes of the Clauses:

(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1);

(b) 'the data exporter' means the controller who transfers the personal data;

(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on their behalf after the transfer in accordance with their instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) 'the sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with their instructions, the terms of the Clauses and the terms of the written subcontract;



(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

2. Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

3. Third-party beneficiary clause

(1) The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

(2) The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

(3) The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to their own processing operations under the Clauses.

(4) The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

4. Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that they have instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the



data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that they will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that their data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that they will ensure compliance with Clause 4(a) to (i).

5. Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with their instructions and the Clauses; if they cannot provide such compliance for whatever reasons, they agree to inform promptly the data exporter of their inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that they have no reason to believe that the legislation applicable to them prevent them from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, they will promptly notify the change to the data exporter as soon as they are aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;



(c) that they have implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that they will promptly notify the data exporter about:

- (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;
- (ii) any accidental or unauthorised access; and
- (iii) any request received directly from the data subjects without responding to that request, unless they have been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to their processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit their data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case they may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of sub-processing, they have previously informed the data exporter and obtained their prior written consent;

(i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

6. Liability

(1) The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

(2) If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or their sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if they were the data exporter, unless any successor entity has assumed the entire legal obligations of the data



exporter by contract or by operation of law, in which case the data subject can enforce their rights against such entity.

The data importer may not rely on a breach by a sub-processor of their obligations in order to avoid their own liabilities.

(3) If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to their own processing operations under the Clauses as if they were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce their rights against such entity. The liability of the sub-processor shall be limited to their own processing operations under the Clauses.

7. Mediation and jurisdiction

(1) The data importer agrees that if the data subject invokes against their third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

(2) The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

8. Cooperation with supervisory authorities

(1) The data exporter agrees to deposit a copy of this contract with the supervisory authority if they so request or if such deposit is required under the applicable data protection law.

(2) The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

(3) The data importer shall promptly inform the data exporter about the existence of legislation applicable to them or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

9. Governing law

The Clauses shall be governed by the law of the Member State in which the data exporter is established, namely the Netherlands.

10. Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

11. Sub-processing

(1) The data importer shall not subcontract any of their processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts their obligations under the Clauses, with the consent of the data exporter, they shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses (3). Where the sub-processor fails to fulfil their data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

(2) The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to their own processing operations under the Clauses.

(3) The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established, namely the Netherlands.

(4) The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

12. Obligation after the termination of personal data-processing services

(1) The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that they have done so, unless legislation imposed upon the data importer prevents them from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that they will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

(2) The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, they will submit their data-processing facilities for an audit of the measures referred to in paragraph 1.



Signatures

Amsterdam, DD.MM.YYYY

Data exporter
EGI Foundation

Place, DD.MM.YYYY

Data importer
Company / Organization



Appendix 1 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer): see Preamble and Section 1 of the Data Processing Agreement

Data importer

The data importer is (please specify briefly activities relevant to the transfer): see Preamble and Section 1 of the Data Processing Agreement

Data subjects

The personal data transferred concern the following categories of data subjects (please specify): see Section 4 of the Data Processing Agreement

Categories of data

The personal data transferred concern the following categories of data (please specify): see Section 2 of the Data Processing Agreement

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify): see Section 2 of the Data Processing Agreement

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify): see Section 1 of the Data Processing Agreement

Signatures

Amsterdam, DD.MM.YYYY

Data exporter
EGI Foundation

Place, DD.MM.YYYY

Data importer
Company / Organization



Appendix 2 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached): see Annex 2: Technical and organizational measures (TOM) of the Data Processing Agreement

Signatures

Amsterdam, DD.MM.YYYY

Data exporter
EGI Foundation

Place, DD.MM.YYYY

Data importer
Company / Organization