

PERSONAL DATA PROCESSOR AGREEMENT REGARDING REDIRIS SERVICES

BETWEEN

ALBERTO MARTÍNEZ LACAMBRA, acting in his capacity as General Director of the public corporate entity Red.es, M.P. (“Red.es” or “Data Processor”/”Processor”), with registered address at Plaza Manuel Gómez Moreno s/n, Edificio Bronce, 28020 Madrid, and tax identification number (NIF) Q-2891006-E, authorised to enter this agreement by virtue of the powers delegated to him in accordance with the provisions of Article 14.1 a) of Royal Decree 164/2002 of 8 February approving the Articles of Association of the public corporate entity Red.es.

AND: [NAME], acting in their capacity as [POSITION], of [INSTITUTION], as an Entity affiliated to RedIRIS and applicant for its services, with the status of “Data Controller” or “Affiliated institution”.

THEY DECLARE

- I. The Parties have signed an Affiliation Agreement for the provision of ICT services provided by RedIRIS to Spanish academic and scientific bodies; and this processing agreement is an appendix to the Affiliation Agreement. To provide these RedIRIS services, Red.es, as the entity delegated with RedIRIS powers, must collect or access the personal data for which the affiliated institution is controller.
- II. According to the provisions of Article 28 of Regulation (EU) 2016/679 (“GDPR”), the affiliated institution, as data controller (the “Controller”) and Red.es, as data processor (the “Processor”), have agreed to sign this personal data processing agreement (the “Agreement”), which shall be governed by the following

CLAUSES

1. PURPOSE OF THE PROCESSING

The purpose of this Agreement is to regulate access to the personal data for which the affiliated institution is data controller by Red.es for the provision of services included in the catalogue of services provided by RedIRIS under the Affiliation Agreement signed by the parties.

Services may include any of those contained in the RedIRIS service catalogue, available at http://www.rediris.es/servicios/serv_alfab.html.es; each of these services is governed by its relevant “Terms and Conditions of Use”, which shall be added as an Appendix, numbered in the relevant order, to this Agreement as the Terms and Conditions of Use are accepted. These documents regulate the technical specifications of the RedIRIS Services, including but not limited to:

- 1.1 Connectivity Services:
 - 1.1.1 Global Internet Access.
 - 1.1.2 Network Incident Management: IRIS-NOC
 - 1.1.3 Academic and research Internet.
 - 1.1.4 IP routing service.
 - 1.1.5 Multicast content distribution service.
 - 1.1.6 Device time synchronisation service: NTP.
 - 1.1.7 DNS Service.
 - 1.1.8 ipv6 Service.
- 1.2 Technical support to institutions:
 - 1.2.1 Consultancy.
 - 1.2.2 Network monitoring tools.
 - 1.2.3 Services panel.
- 1.3 Digital identity:
 - 1.3.1 Digital certificates: TCS.
 - 1.3.2 Federation of identities
 - 1.3.3 IRIS-SARA.
 - 1.3.4 Identifier registry: RID.
 - 1.3.5 PGP Key Server: Keyserver.
- 1.4 Private networks:
 - 1.4.1 Optical circuits: Lightpaths.
 - 1.4.2 Virtual circuits: VPN L2.

1.5 Promotion

1.6 Mobility: 1.6.1 Eduroam

1.7 Data transfer 1.7.1 Filesender.

1.7.2 Science data transfer.

1.8 Cloud 1.8.1 GÉANT IaaS Framework

1.8.2 Other collaboration agreements with providers

1.8.3 IrisMail (under testing)

1.9 Security 1.9.1 Unified anti-spam filter service (Washer).

1.9.2 Security incident management: IRIS-CERT.

1.9.3 Denial of service attack mitigation service – DDoS.

1.9.4 Security Incident Management – INCIBE.

1.10 Collaboration 1.10.1 Collaborative repository: BSCW.

1.10.2 Replica repository: FTP.

1.10.3 Distribution lists service: LISTSERV.

1.10.4 Autolist

Processing shall include but is not limited to collection, structuring, storage, consultation, comparison, transfer, erasure and any other processing necessary to provide the service in question.

2. IDENTIFICATION OF THE INFORMATION CONCERNED

To perform the provisions arising from compliance with this order, the Controller shall provide the Processor with the information necessary to provide RedIRIS services. These are generally employee or user data, i.e. full name, username and position, as well as members, providers and visitors receiving the services of the affiliated institution.

3. DURATION

The duration of the Agreement shall be as established in the Affiliation Agreement, and the duration established for acceptance and compliance with the terms and conditions of use of the different services.

Once the service has been provided, personal data must be returned by the Data Processor, as well as any medium or document containing any personal data subject to the processing, under the terms developed in this Agreement.

The return must include the complete deletion of existing data on the IT equipment used by the Processor. However, the Processor can keep a copy, with the data duly blocked, as long as responsibilities for the execution of the service can be derived.

4. OBLIGATIONS OF THE DATA PROCESSOR

4.1 Obligation to use data only for the purpose of the order and under the instructions of Controller

The Processor is obliged to use the personal data subject of the processing, or those collected for inclusion, only for the purpose of this order. Under no circumstances may they be used or applied for personal purposes or for purposes other than those contained in this Agreement.

The Processor shall process data in accordance with the instructions of the Controller. If the Processor considers any of the instructions to be in breach of the GDPR or any other applicable data protection provision, the Processor shall immediately inform the Controller.

4.2 Registration of processing activities on behalf of the Controller

The Processor shall keep a written record of all categories of processing activities carried out on behalf of the Controller, containing at least the contents of Article 30 GDPR.

4.3 Data transfer and assignment

The Processor shall not communicate data to third parties except with express

authorisation from the Controller, when accepted by law, and only to provide the services offered.

The Processor can communicate data to other data processors acting on behalf of the same Controller, following the latter's instructions. In this case, the Controller shall identify, in advance and in writing, the entity to which the data must be communicated, the data to be communicated and the security measures to be applied in order to proceed with the communication.

If the Processor is required by applicable law to transfer personal data to a third country, it shall inform the Controller of this legal requirement in advance, unless forbidden by this regulation for important reasons of public interest.

4.4 Subcontracting

The Processor is authorised to subcontract with the companies it deems appropriate as is necessary to provide the services covered in the Agreement.

In any case, the Processor shall only choose subcontractors that offer sufficient guarantees to apply appropriate technical and organisational measures, so that the processing is in accordance with the requirements of the GDPR and guarantees the protection of the rights of the data subject.

The subcontractor, which will also have the status of data processor, is also obliged to comply with the obligations established in this Agreement for the Processor and the instructions given by the Controller. The Processor is responsible for regulating the new relationship so that the new data processor is subject to the same conditions (instructions, obligations, security measures, etc.) and the same formal requirements as it, in relation to the appropriate processing of personal data and the guarantee of the rights of data subjects. In the event of non-compliance by the sub-processor, the Processor will remain fully accountable to the Controller for compliance with the obligations.

4.5 Duty of secrecy, confidentiality and security

The Processor is obliged to maintain secrecy with regard to personal data to which it has had access by virtue of this processing, even after the processing operation has been completed.

The Processor shall ensure that the persons authorised to process personal data issue an express written commitment to respect confidentiality and to comply with the relevant security measures, of which they must be duly informed.

The Processor shall provide the Controller with documentation accrediting compliance with the obligation established in the previous section.

4.6 Training

The Processor shall ensure the necessary training in personal data protection for the persons authorised to process personal data on behalf of the Controller, as well as inform them about the content of the order and any other information relevant to the completion of the processing.

4.7 Duty of information

The Processor is responsible for facilitating the right to information at the time of data collection.

4.8 Rights of the data subject

When the persons concerned exercise these rights before the Processor, it must inform the Data Protection Officer or the Data Protection Manager of the Affiliated Institution. Notification must be sent as soon as possible and in no case later than the working day following receipt of the request, together, where appropriate, with other information that may be relevant to the resolution of the request.

4.9 Security breaches

The Processor shall notify the Data Controller, without undue delay, and in any case before the maximum term of 48 hours, and by e-mail to the Data Protection Officer or Data Protection Manager of the Affiliated Entity, of personal data security breaches of which it is aware, together with all the relevant information for the documentation and communication of the incident. If sufficient information is available, the Processor shall provide at least the items listed in Article 33.3 GDPR.

4.10 Assisting the Controller

The Processor must support the Data Controller in:

- Conducting data protection impact assessments, where appropriate.
- Conducting prior consultations with the supervisory authority, where appropriate.

The Processor shall provide the Controller with all the necessary information to demonstrate compliance with its obligations under data protection regulations.

4.11 Security measures

The Processor shall take the necessary technical and organisational measures to ensure data security and to prevent any unauthorised alteration, loss, processing or access to personal data.

In particular, the Processor shall implement the relevant security measures as provided for in Annex II (Security measures) of Royal Decree 3/2010 of 8 January, which regulates the National Security Scheme in the field of Electronic Administration, and Information Security Management System security controls based on the Standard UNE-EN ISO/IEC 27001.

During the term of the Agreement, these security measures must be adapted to the results of a Risk Analysis or, failing this, to a Data Protection Impact Assessment, pursuant to Article 32 GDPR. Supplementary measures applied according to this Agreement shall be applied until a risk assessment is conducted.

4.12 Data Protection Officer

The Processor shall provide the Controller with the contact details of its Data Protection Officer.

5. SPECIFIC OBLIGATIONS OF THE CONTROLLER

The Controller is responsible for enforcing this Agreement:

- Providing the Data Processor with the data referred to in clause two of this Agreement.
- Conducting a personal data protection impact assessment of the processing operations to be carried out by the Processor, if necessary.

- iii. Making prior consultations, as appropriate.
- iv. Ensuring and supporting, in advance and throughout the processing, the Processor complies with the GDPR, the Spanish Data Protection Act (LOPD) and its implementing regulations.
- v. Obtaining, prior to the delivery of the data to the Processor, sufficient legitimacy for processing the personal data of data subjects.

6. LIABILITY

6.1. Without prejudice to the provisions of this Agreement and applicable regulations, the Processor shall only be liable for direct damages suffered by the Controller and directly caused by actions, omissions or deviations from the order instructions in relation to the obligations provided for in this Agreement or in the Law.

6.2. The Processor shall not be liable for direct or indirect damages caused by due and correct compliance with the instructions issued by the Controller regarding the order, or for actions or omissions by the Controller related to the obligations provided for in this Agreement or in the Law.

Notwithstanding the above, the Controller undertakes to compensate all expenses, legal costs, compensation, fines, penalties and any other costs incurred by the Processor to defend itself in or as a result of these proceedings, and which are caused by actions or omissions by the Controller, or correct and due compliance with the instructions issued by the Controller under this order.

6.3 The Processor shall not be liable for problems and/or damages caused by reasons beyond its control or that could not have been foreseen by the Parties or when, even if foreseeable, the Processor has taken all reasonable efforts and implemented the relevant measures to avoid them, or which are considered as force majeure or fortuitous.

6.4. The Processor is not involved in the creation, transfer nor disclosure of data provided by the Controller, has no prior control and does not guarantee the lawfulness, infallibility and usefulness of the content of the data or files transferred, disseminated, stored, received, obtained, provided or accessible by means of the services provided by the Controller, rejecting all liability that may arise from the above.

7. APPLICATION OF AGREEMENT PROVISIONS

The Affiliation Agreement, which the Parties expressly ratify, shall apply to any issue not expressly provided for in this Agreement, which is an integral and inseparable part of the former.

In witness whereof, the Parties sign two copies of this Agreement, in the place and on the date indicated above.

FOR THE PUBLIC CORPORATE ENTITY RED.ES, M.P.

Signed. ALBERTO MARTÍNEZ LACAMBRA
GENERAL DIRECTOR

FOR [INSTITUTION]

Signed. [NAME]
[POSITION]