

Revisions

Version	Date	Description	Authors
1.0	May 25 2020	First version based on version 1.0 of the Italian template	Andrea Ceravolo (IMT Lucca)
1.01	July 17 2020	Updated to the latest Italian version (1.01) and minor corrections.	Davide Vagheti (GARR)

Privacy Policy

(Privacy Policy pursuant to Articles 13 and 14 of the (EU) Regulation No. 679/2016 - from now on GDPR)

Definitions

- **Controller:** the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- **Processor:** a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. The Processor carries out the instructions of the Owner and accepts the supervision thereof, in particular on the effective adoption of adequate measures regarding the protection of personal data (correspond to the Legal Person who manages the "Resource").
- **Identity Provider:** a computer system that provides the federated authentication service for Users of a specific Organization.
- **Resources:** third party or Controller services to which the User of the federated authentication service intends to access.
- **Identity Federation:** a group of federated authentication service providers and resource access service providers that agree to interoperate according to a common set of rules.
- **User:** natural person who uses the service.
- **Subject:** natural person whose personal data are subject to processing by the Owner and any third parties (correspond to the User).

Service Name	Identity Provider (IdP)
Service Description	The federated authentication service that allows the Users of the <ORGANIZATION> to access federated Resources using their institutional credentials.

	<p>The Resources can be provided through the Italian Identity Federation of Universities and Research Institutions (IDEM), or directly.</p> <p>The federated Authentication Service is responsible for authenticating the User, issuing an authentication token and, if required, releasing a minimum set of personal data to access the Resource.</p>
<p>Controller</p>	<p>Name: <ORGANIZATION> Email: <CONTROLLER> Address: <ORGANIZATION MAILING ADDRESS></p> <p><ORGANIZATION> is the Controller of the personal data managed through the Service.</p>
<p>Data Protection Officer (GDPR Section 4) (if applicable)</p>	<p><INSTITUTIONAL DPO></p>
<p>Jurisdiction and supervisory authority</p>	<p>IT-IT Italian Data Protection Authority https://www.garanteprivacy.it</p>
<p>Categories of direct and indirect personal data processed and legal basis for processing</p>	<ol style="list-style-type: none"> 1. one or more unique identifiers; 2. identification credential; 3. first and last name; 4. e-mail address; 5. role in the organisation; 6. work group affiliation; 7. specific rights to resources; 8. name of the affiliated organisation; 9. IdP service log records: User identifier, date and time of use, requested Resource, submitted attributes; 10. Log records of the services necessary for the operation of the IdP service. <p>Any collected personal data is stored in Italy, in accordance with the GDPR. The data processing purpose is the provisioning of the authentication service. The legal basis for data processing is the fulfillment of contractual obligations (through the provisioning of the authentication service) and the legitimate interest of the Controller.</p>
<p>Purposes of personal data processing</p>	<p>To provide the federated authentication service in order to access the Resources requested by the User.</p> <p>To verify and monitor the proper functioning of the service and ensure its security (legitimate interest).</p> <p>To fulfil any legal obligations or requests from the judicial authorities.</p>

<p>Third parties to whom the data are communicated</p>	<p>The Controller, in order to provide the service correctly, communicates to the Resources providers to which the User intends to access proof of authentication and only the personal data (attributes) requested, in full compliance with the principle of minimization.</p> <p>Personal data is transmitted only when the subject requests access to the Resource of the third party.</p> <p>For purposes related to the legitimate interest of the Controller or the fulfilment of legal obligations, some log data may be processed by third parties (e.g. CERT, CSIRT, Judicial Authority).</p>
<p>Exercise of Subjects' rights</p>	<p>To request access to your personal data and their correction or deletion or to object to their processing, or to exercise the right to data portability (Articles 15 to 22 of the GDPR), contact the Controller at the above mentioned contact details.</p>
<p>Revocation of the consent of the interested party</p>	<p>The only data collected with the consent of the subject are preferences about the visualization of the attribute transmitted to the Resources. The preferences are collected at the time of the first access to the Resource and may be changed afterwards by starting over again the access procedure.</p>
<p>Data Portability</p>	<p>The Interested Party may request the portability of their data concerning the federated authentication service, including preferences regarding the visualization of the attributes transmitted to the Resources, which will be provided in open format and in accordance with Art. 20 of the GDPR. The data portability service is free of charge.</p>
<p>Duration of Data Storage</p>	<p>All personal data collected to provide the federated authentication service will be stored for the entire time it will be necessary to provide the service itself.</p> <p>After <N> months after deactivation, all personal data collected or generated by the use of the service will be deleted.</p>