Personal Data Processing Policy

(Personal Data Processing Policy, pursuant to Article 13 and Article 14 of EU Regulation 2016/679 on personal data protection - GDPR)

Definitions

- ‘Data Controller’: a natural or legal person, public authority, agency or other body who, alone or jointly with others, determines the purposes and means of personal data processing; where the purposes and means of such processing are determined by Union or Member State law, the Controller or the specific criteria for its nomination may be provided for by Union or Member State law.
- ‘Data Processor’: a natural or legal person, public authority, agency or other body who processes personal data on behalf of the Controller.
- Identity Provider: IdP system providing the federated authentication service for the Users of a specific Organization.
- Resources: services of third parties or of the Controller which the User of the federated authentication service intends to access.
- Federation of Identity: a group of organizations providing federated authentication services and organizations providing access services to Resources that decide to interoperate according to a set of common rules;
- User: any natural person who uses the service;
- Data Subject: any natural person whose personal data are being processed by the Data Controller and any third party (coincides with the User).

<table>
<thead>
<tr>
<th>Service</th>
<th>Identity Provider (IdP) eduGAIN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description of Service</td>
<td>The federated authentication service via eduGAIN allows teachers and students of the eduGAIN-federated universities to access the federated services of Università degli studi di Milano-Bicocca using their own institutional credentials. The Federated Authentication Service is responsible for authenticating the user and issuing an authentication token and, if required, a minimum set of personal data for access to the resource.</td>
</tr>
</tbody>
</table>
| **Data Controller** | Name: Università degli studi di Milano-Bicocca  
Email: rettorato@unimib.it - ateneo.bicocca@pec.unimib.it  
Address: Piazza dell'Ateneo Nuovo 1, 20126 Milan (Italy)  
The University is the Controller of personal data processing managed through the Service, in the person of the Rector Prof. Giovanna Iannantuoni, its Legal Representative, |
| **Data Protection Officer** | The Data Protection Officer is Dr. Emanuela Mazzotta, who can be contacted at the e-mail address rpd@unimib.it or at the certified email address rpd@pec.unimib.it |
| **Jurisdiction and supervisory Authority** | IT-IT  
The Italian Data Protection Authority  
[https://www.garanteprivacy.it](https://www.garanteprivacy.it) |
| **Categories of personal data processed and legal basis for the processing** | 1. one or more unique identifiers,  
2. recognition credential,  
3. name and surname,  
4. email address,  
5. role in the organization,  
6. membership in working groups,  
7. specific rights on resources,  
8. name of the belonging organization,  
9. IdP service log record: user identifier, date and time of use, requested resource, transmitted attributes,  
10. Log records of the services necessary for the functioning of the IdP service.  
The personal data collected are stored in Italy in accordance with the GDPR. Their processing is aimed at providing the authentication service. The legal bases for data processing are the provision of the authentication service (fulfilment of contractual obligations) and the legitimate interest of the Controller. |
<table>
<thead>
<tr>
<th><strong>Personal data are processed for</strong></th>
<th>Providing the federated authentication service to access the resources requested by the Data Subject. Verifying and monitoring the proper functioning of the service and guaranteeing its security (legitimate interest). Fulfilling any legal obligations or requests from the judicial authorities.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Third Parties to whom the data are disclosed</strong></td>
<td>In order to provide the service correctly, the Data Controller communicates the proof of authentication and only the personal data (attributes) required, in full compliance with the principle of minimization, to the suppliers of the Resources to which the User intends to access. Personal data are transmitted only when the Data Subject requests access to the third party's Resource. For purposes related to the legitimate interest of the Data Controller or the fulfilment of legal obligations, some log data may be processed by third parties (eg. CERT, CSIRT, Judicial Authority).</td>
</tr>
<tr>
<td><strong>Exercise of Data Subjects’ rights</strong></td>
<td>Contact the Data Controller at the addresses indicated above to request access to personal data and their correction or deletion, or restriction of processing concerning them, or to exercise the right to data portability (articles from 15 to 22 of the GDPR).</td>
</tr>
<tr>
<td><strong>Revocation of the Data Subject’s consent</strong></td>
<td>The only data collected with the consent of the Data Subject are preferences regarding the transmission of attributes to third parties. The preferences are collected on first access to the Resource and can be modified later by starting the access procedure again.</td>
</tr>
<tr>
<td><strong>Data portability</strong></td>
<td>Data Subjects may request the portability of their data relating to the federated authentication service, including preferences regarding the transmission of attributes to third parties, which will be provided in an open format and pursuant to Art. 20 of the GDPR. The portability service is free of charge upon termination of the service.</td>
</tr>
<tr>
<td>Duration of data retention</td>
<td>All personal data collected in order to provide the federated authentication service are retained for as long as it is necessary to provide the service itself. After 180 days from deactivation, all personal data collected or generated by use of the service are deleted.</td>
</tr>
</tbody>
</table>