

Processing of personal data

(Privacy Statement in accordance with Articles 13 and 14 of Regulation (EU) 679/2016 - hereinafter GDPR)

Definitions

- Data Controller: Legal or Natural Person who determines the ways and means of the processing of personal data of the specific Organisation to which the Users belong;
- Data Processor: a legal or natural person who processes the data on behalf of the Data Controller within the limits of agreed upon with the Data Controller. The Data Processor carries out the Data Controller's instructions and accepts controls from the Data Controller, in particular controls on the actual implementation of proper personal data protection measures (the Data Processor is the legal person managing the 'Resource');
- Identity Provider: a computer system that provides the federated authentication service for the Users of a specific Organisation;
- Resources: third-party or Data Controller's services that 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 using the service;
- Data Subject: natural person whose personal data are processed by the Data Controller and any third parties (the Data Subject is the User);

Name of Service	Identity Provider (IdP)
Service Description	The federated authentication service allows Politecnico di Milano users to access federated resources using their institutional credentials. Resources can be provided either through IDEM (the Italian national federation for universities and research institutions for authentication and authorization), or directly. 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 accessing the Resource.

Data Controller	Name: Politecnico di Milano - General Director delegated by the pro-tempore Rector Email: dirgen@polimi.it Address: Politecnico di Milano Piazza Leonardo da Vinci, 32 20133 Milano Politecnico di Milano is the Data Controller of personal data managed through the Service.
Data Protection Officer (GDPR Section 4) (if applicable)	Email: privacy@polimi.it
Jurisdiction and Spervisory Athorities	IT-IT Garante per la Protezione dei Dati Personali (Italian Data Protection Authority) https://www.garanteprivacy.it
Categories of direct and indirect personal data processed and legal basis for processing	1. one or more unique identifiers; 2. recognition credential; 3. name and surname; 4. email address; 5. role in the organisation; 6. membership in working groups; 7. specific rights on resources; 8. name of the relevant organisation; 9. IdP service log records: user ID, date and time of use, requested Resource, transmitted attributes; 10. Service log records necessary for the operation 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 basis for the processing of data is the provision of the authentication service (fulfilment of contractual obligations).

Purposes of personal data processing	Providing the federated authentication service for accessing the Resources requested by the data subject. Verifying and monitoring the proper functioning of the service and ensure its security. Fulfilling any legal obligations or requests by Judicial Authorities.
Third parties to whom the data are disclosed	The Data Controller, in order to provide the service correctly, communicates to the providers of the Resources to which the User intends to access proof of authentication and only the personal data (attributes) requested, in full compliance with the principle of minimisation. Personal data are only transmitted at the moment when the Data Subject requests access to the third party's Resource. For purposes related to the fulfilment of legal obligations, some log data may be processed by third parties (e.g., CERT, CSIRT, Judicial Authorities).
Exercise of Data Subjects' rights	The Data Subject has the right to request access to and rectification or erasure of his/her personal data or restriction of its processing, or to object to its processing, or to exercise the right to data portability (GDPR Articles 15 to 22 GDPR); to do so, the Data Subject should contact the Data Controller at the above-mentioned contact details.
Withdrawal of the Data Subject's consent	The only data that are collected with the consent of the Data Subject are preferences on the display of attributes transmitted to Resources. Preferences are collected when accessing the Resource for the first time and can be changed later by starting the access procedure again.
Data portability	The Data Subject may request the portability of his/her data relating to the federated authentication service, including preferences on the display of attributes transmitted to Resources, which will be provided in an open format and in accordance with GDPR Article 20. The data portability service is free of charge.

Duration of Data Retention	All personal data collected for the purpose of providing the federated authentication service are retained for as long as it is necessary to provide the service. Upon deactivation of the user, the personal data collected from or generated by his/her use of the service will be retained for the time period stipulated by the regulations in force.
----------------------------	---