Privacy Policy

(in compliance with Regulation EU 2016/679 - GDPR)

Definitions

- **Data controller**: person or other body that determines the purpose and means of personal data processing;
- **Data processor**: person or other body which processes personal data on the Data controller's behalf, according to given directions;
- **Identity Provider**: information system providing a controlled identity to the User;
- **Resource**: online service accessible through the Identity Provider;
- **Identity Federation**: a set of Institutions providing federate authentication and access to Resources, using common rules;
- **User**: person accessing Resources;
- **Interested Party**: person whose data are processed (the same as User).

Name of the Service	Federate Identity Provider (IdP) Service
Service Description	Federate authentication service allows Users to access Resources with their institutional credentials through the Federazione d'Identità italiana delle Università e degli Enti di ricerca (IDEM). Federate authentication service identifies Users, releases an authentication token and, if necessary, provides a minimum set of personal data to enable access to the Resource.
Data controller	Rector of the University of Milan Email: infoprivacy@unimi.it Address: Via Festa del Perdono n. 7, Milano
Data Protection Officer	Prof. Avv. Pierluigi Perri E-mail: dpo@unimi.it
Jurisdiction and control authority	The Italian Data Protection Authority https://www.garanteprivacy.it
Processed data and legal basis of treatment	1. One or more unique identifiers; 2. Personal credentials; 3. Name and surname; 4. E-mail address; 5. Role within the organization; 6. Affiliation to working groups; 7. Rights to specific Resources; 8. Name of User's organization; 9. Log data of IdP Service: user's ID, timestamp, user's name,

	requested Resource, other information about the User (attributes), as defined at the URL: https://www.sba.unimi.it/en/tools/16057.html; 10. Log data of other services necessary to IdP Service operation. Personal data are gathered in Italy, in compliance with GDPR, and their treatment is necessary in relation to the execution of the IdP Service. The legal basis of treatment is the User's consent, with which he/she agrees to access the IdP Service and to transfer personal data (attributes) to the Identity Federation.
Purpose of data processing	Personal data are processed to provide the IdP Service, to monitor its supply in a proper and secure way, for communications required by the public security regulations.
Third parties to whom personal data are disclosed	The Data controller provides Resources' suppliers with evidence of authentication and strictly necessary personal data (attributes), according to the principle of data minimisation. Personal data are delivered only when the Interested Party asks to access third parties' Resources. Data controller's legitimate interest and legal obligations are a valid basis to let some log data to be processed by third parties (e.g., in case of cybersecurity accidents, CERT, CSIRT, judicial authority).
Rights of the Interested Party	The Interested Party has the right to obtain from the Data controller access, correction and deletion of his/her personal data. The Interested Party has the right to limitation of processing and opposition to the processing of personal data.
Right to object to the treatment	The Interested Party agrees with the processing of personal data and the transmission of attributes to third parties at the first access to a Resource. The Interested Party can interrupt at any time the processing of personal information or can modify transmission preferences.
Data portability	The Interested Party has the right to portability of the personal data in a structured, commonly used and readable form. Data can be provided freely at the end of the service.
Retention time of personal data	User's personal data will be conserved as long as the Service is provided. 12 months after the end of the Service, personal data will be deleted. Log files can be processed for technical analysis in case of cybersecurity accidents.