INFORMATION PURSUANT TO THE GENERAL DATA PROTECTION REGULATION - EU REGULATION 2016/679 AND LEGISLATIVE DECREE N. 196/2003 AND S.M.I. "CODE REGARDING THE PROTECTION OF PERSONAL DATA" - ACCESS TO THE IDEM FEDERATE SERVICES - EDU-GAIN FOR USERS OF THE UNIVERSITY OF INSUBRIA

The IDEM federation involves training and research institutions, both Italian and international, for the shared management of access to online resources. The federated authentication service allows users of the University of Insubria to access federated resources using their institutional credentials (University keyed identities).

The Resources can be provided through the Italian Identity Federation of Universities and Research Institutions (IDEM), or directly. The Federated Authentication Service is responsible for authenticating the user and consequently issuing an authentication token and, if requested by the service, a minimum set of personal data for access to the Resource.

Access and use of federated authentication services belonging to the IDEM and EduGain federations involves the processing of personal data, which are processed in accordance with the General Data Protection Regulation - EU Regulation 2016/679 and Legislative Decree no. 196/2003 and subsequent amendments. "Personal data protection code" as amended by Legislative Decree. 101/2018.

This information is provided pursuant to the General Data Protection Regulation - Regulation (EU) 2016/679.

1. Data Controller, Data Protection Officer

The Data Controller is the University of Insubria, in the person of the Rector, with legal seat in Varese (VA) Via Ravasi, 2, PEC: ateneo@pec.uninsubria.it.
The data subjects can contact the Data Protection Officer to exercise the rights provided for by the GDPR (articles 12 to 21) using the following e-mail address: privacy@uninsubria.it.
The updated list of data controllers and authorized data processors is kept at the headquarters of the Data Controller.

2. Data processing

Data subject:
Using the IDEM - EduGain federated services, the following data associated with the user's University digital identity are processed:

- one or more unique identifiers (schacPersonalUniqueCode)
- username associated with the University Digital Identity (eduPersonPrincipalName)
- name (given Name)
- surname (sn)
- electronic mail address (email)
- type of organization affiliation (eduPersonScopedAffiliation)
- specific rights on resources
- name of the relevant organization (schacHomeOrganization)
- the European student identifier (schacPersonalUniqueCode)

Activities Data:
following access to the services of the IDEM - EduGain federation, the technological infrastructure of the Federation, during its regular operation, collects the following data:

- Identity Provider (IdP) service log records: user identifier, date and time of use, requested resource, transmitted attributes;
- Log records of the services necessary for the operation of the IdP service.

Data are NOT collected for profiling or marketing purposes.

3. Processing tasks and legal basis

Legal Basis:
The data processing has its suitable legal basis in the execution of the service requested by the user (i.e. the use of digital services provided through the IDEM - EduGain federation) (Art. 6 (1) (b) GDPR); in the fulfillment of legal obligations or requests from the Authority of which the Data Controller is the recipient (for example, to follow up on the investigative needs of the Judicial or Public Security Authorities) (Legal basis: Art. 6 (1) (c) GDPR); in the legitimate interest of the University to obtain anonymous statistical information on the use of the service, check the correct functioning of the service, perform monitoring activities to support the security of the service (Legal basis: Art. 6 (1) (f) GDPR); in the exercise or defense of a right (Legal basis: Art. 9 (2) (f) GDPR)

Processing tasks:

- Purposes needed for the execution of the requested service: the data (in particular those linked to the account) are collected in order to allow the user to use the requested service;
- Troubleshooting malfunctions relating to access and use of federated services;
- Purposes required by law: the processing is based on a legal obligation relating to the processing of data required by law according to Legislative Decree. 30 May 2008, n. 109 concerning the implementation of Directive 2006/24/EC, relating to the conservation of data generated or processed in the context of the provision of electronic communication services accessible to the public or public communication networks and to fulfill the requests of the Judicial Authority and of the Judicial Police in relation to investigative activities;
- Purposes based on a legitimate interest: the access data are also used for the purposes of obtaining anonymous statistical information on the use of the service, checking the correct functioning of the service, performing monitoring activities to support the security of the service;
- Purposes based on the protection of rights: access data are collected to ascertain computer crimes.

4. Mandatory or non-mandatory provision of data

The provision of personal data associated with the identity is mandatory and needed to be able to use Federated services. The provision takes place with access to the services.

The provision of data relating to browsing activities is implicit in the use of communication protocols.

5. Data Processing Modalities

The data collection takes place in compliance with the principles of lawfulness, correctness, relevance, completeness and non-excess in relation to the purposes for which they are processed.

Personal data are processed in compliance with the principles of lawfulness, correctness and transparency, provided for by law, with the aid of tools suitable for recording and storing the data themselves and in any case in such a way as to guarantee their security and protect the maximum confidentiality of the data subject.

In this context, the personal data thus collected will be made accessible only to those within the University who need it due to their job or role.

These processors, whose number will be as limited as possible, will be appropriately trained in order to avoid loss, destruction, unauthorized access or unauthorized processing of the data themselves.

Extractions of the log files (relating to the activities performed through the service) may be carried out, also through cross-referencing and processing of such data to identify those responsible for abuse and/or illicit activities carried out by the data subjects or by third parties

6. Data storage period

In relation to the different purposes for which they were collected, your data will be kept for the time required by the relevant legislation or for the time strictly necessary to pursue the purposes.
In particular:

- the data aimed at managing telematic services and statistical analyzes are kept for a maximum of 3 months;
- the data collected for the detection of computer crimes are kept for 12 months, without prejudice to the longer term foreseen for the needs related to the notification of crimes, the definition of disputes or for the fulfillment of specific requests from the Judicial Authority and the Judicial Police in relation to investigative activities

7. Data recipients and authorized data processors

The data processed for the above purposes will be communicated or will in any case be accessible to employees and collaborators assigned to the competent offices of the University of Insubria, subjects authorized by the Data controller (art. 29 GDPR).

The management and storage of personal data collected takes place at the University; the suppliers of the federated services, for the sole purpose of the requested service, may become aware of the personal data.

In order to correctly provide the service, the Data Controller communicates to the suppliers of the Resources to which the User intends to access proof of authentication and only the strictly necessary personal data (attributes), in full compliance with the principle of minimization.

Personal data are transmitted only when the data subject requests access to the third party's resource.

In addition to the Service Providers to which the user intends to send their information to confirm their identity, the data may be sent to third parties, appointed as Data Processors pursuant to art. 28 of Regulation (EU) 2016/679, with reference to the management of the University IT services or systems.

The personal data collected could be transferred abroad if the user wants to access a Service Provider in a country not belonging to the European Economic Area.

For purposes related to the legitimate interest of the Data Controller or the fulfillment of legal obligations, the University may also communicate the controlled personal data to supervisory bodies, judicial authorities as well as to all other subjects to whom the communication is mandatory by law for the fulfillment of the aforementioned purposes, as well as to all those public bodies to whom, in the presence of the relevant conditions, communication is mandatorily required by EU laws, national laws or regulations.

The complete and updated list of data processors can be obtained upon request at the data controller seat.

8. Transfer of personal data to third countries

The data are stored on European territory.

9. Rights of the data subject

In cases where they are exercisable, on a case-by-case basis, the rights towards the University of Insubria (Data Controller) are as follows:

- right of access to personal data and to all the information referred to in art. 15 of the GDPR;
- right to rectification of inaccurate personal data and the integration of incomplete data;
- right to delete data, except for those contained in documents that must be retained by the University and unless there is a legitimate relevant reason to proceed with the processing;
- right to limit processing where one of the hypotheses referred to in the art. 18 of the GDPR occurs;
- right to data portability in a structured, commonly used and machine-readable format, such as .xml or similar;
- right to object to the processing of the personal data,
- right to revoke any consent given for non-mandatory data processing, without prejudice to the lawfulness of the processing based on the consent given before the revocation.

To exercise these rights, the data subject can contact the Data Protection Officer by sending the request via email to privacy@uninsubria.it.

10. Claim

The data subject also has the right to lodge a complaint with the Guarantor for the Protection of Personal Data (www.garanteprivacy.it) or with the Guarantor Authority of the EU State in which the data subject habitually resides or works, or of the place where the alleged violation has occurred, in relation to a treatment that is considered non-compliant.