

INFORMATION ON PERSONAL DATA PROCESSING RELATING TO THE STAFF AREA

Dear user, please find the following information on how we will process your personal data under Article 13 of EU Regulation 2016/679, also known as GDPR.

We will process your data by following the principles of fairness, lawfulness, transparency and the protection of privacy and your rights. Data processing may occur manually or electronically or with the use of IT or automated devices. It may consist of any operation carried out with or without the use of automated processes, including the collection, recording, organisation, structuring, storage, elaboration, selection, blocking, adaptation, modification, extraction, consultation, use, communication via transmission, diffusion or any other means of making available, comparison, interconnection, limitation, cancellation or destruction of said data.

Who is the Data Controller?

The Data Controller - i.e. the body that determines how and why your data is processed - is the University of Milano-Bicocca, located in Piazza dell'Ateneo Nuovo 1, 20126 Milan, represented by its legal representative, the Rector Giovanna Iannantuoni (hereinafter the "Controller"). You can contact the Controller by writing to the address shown above or sending an email to rettorato@unimib.it or the certified email address ateneo.bicocca@pec.unimib.it

Who is the Personal data protection Officer?

The University of Milano-Bicocca has appointed a Personal data protection Officer you can contact with all queries relating to personal data processing and the exercise of any rights deriving from GDPR. You can contact the Personal data protection Officer at rpd@unimib.it or the following certified email address rpd@pec.unimib.it

Why do we process your data?

In accordance with Article 6, Paragraph 1 of GDPR, we process your personal data so that the relevant University department/bodies can fulfil all duties allocated to them. More specifically, the University will process your data to:

- Staff Selection and recruitment;
- Administrative and career management of the Staff;
- Activities related to the didactic and training for staff, including the provision of distance learning;
- Activation and management of tools made available to who work in the University in order to carry out their working duties;
- Planning and manage the welfare benefits offered to the administrative staff;
- Preparation and management of specific actions for the well-being of the staff;

- Detection of the satisfaction degree with the services offered by the Area

Who can we communicate your data to?

Only personnel belonging to the departments of the University and authorised by the Data Controller may process your data, in accordance with their functions and skills.

Moreover, the Data Controller can communicate your personal data to the following external third-party subjects, because their activities are essential to the achievement of the aforementioned purposes, including as regards functions attributed to them by law:

- European Commission
- Ministries (Ministry of the Education, Ministry of Economy)
- National and local public bodies
- Other Public University
- Private legal entities
- Judicial authority, ATS and ASST for medical teachers with assistance functions
- Chartered members of a profession
- International Bodies
- Other public or private entities to which the University entrusts services in out-sourcing, in limits established by law.

If your data is transferred out of the EU or to international organisations, you will be provided with specific information notice. If no decision on adequacy has been issued for the destination country, or if appropriate and adequate guarantees on personal data protection are not available, and/or no information as to how to obtain a copy of your data or the location is provided, you will be asked to grant your consent before we proceed with the transfer.

Is it compulsory for you to provide us with your data?

Yes, because if you fail to do so, the University will be unable to complete the required activities and deal with requests. However, no formal declaration of consent for data processing is required.

We will use the data of persons or children (under 16 years of age) who are unable to express their consent as long as the parent/s or the person with parental/legal responsibility consent.

How long will we store your data for?

Personal data in the database of the Data Controller is stored for an unlimited period of time.

If your personal data is contained in analogue documents and/or digital products or products owned by the Data Controller, this data is subject to legal storage time limits; the various time limits are contained in the “Disposal of analogue and digital documents guidelines”, which can be found on the University website.

Where present, authentication logs will be cleared after 180 days.

What are your rights and how can you exercise them?

You have the right to:

- access your data;
- obtain the correction or cancellation of data or the limitation of data processing;
- request data portability if data is in digital form;
- oppose data processing;
- make a complaint to the supervisory authorities.

You can exercise your rights by contacting the Data Controller and/or the Personal data protection Officer; the Data Controller must respond to you within 30 days from the date they receive your request (this period can be extended to 90 days if the request is particularly complex).

If you believe that your data processing violates relevant regulations, or if the response to a request in which you have exercised one or more of the rights set out in Articles 15-22 of GDPR fails to arrive within the time limit indicated or is unsatisfactory, you can contact the supervisory authority or the personal personal data protection authority.

Will you be subject to automated decision-making processes?

No, you will not be subject to any decisions based solely on automated processes (including profiling), unless you have explicitly provided your consent for this.

Is your data safe?

Your data is processed in a lawful, proper manner and we adopt appropriate security measures designed to prevent any unauthorised access, disclosure, modification or destruction of the data.

[This policy was last updated on 25/10/2021]