



## PRIVACY NOTICE

### on data processing related to complaint handling

#### 1. Preamble

The purpose of this Privacy Notice is to inform you about the data processing of **Budapest Metropolitan University** (registered office: 1148 Budapest, Nagy Lajos király street 1-9., institutional identification: FI33842) (hereinafter: **Data Controller** or **METU**) in connection with the complaint handling as per its Complaint Handling Policy in compliance with applicable legal requirements:

- **Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation; GDPR)**
- **the applicable Hungarian legislation.**

#### 2. Data Controller

METU is considered to be a Data Controller regarding the data processing under this Privacy Notice.

Contact information:

address: 1148 Budapest, Nagy Lajos király street 1-9.

e-mail: [adatvedelmitisztviselo@metropolitan.hu](mailto:adatvedelmitisztviselo@metropolitan.hu)

During the data processing, the Data Controller complies with the regulations in force and fully respects the protection of the fundamental rights and privacy of individuals with special attention to the provisions of the General Data Protection Regulation.

If you have any questions or comments, please contact us at [adatvedelmitisztviselo@metropolitan.hu](mailto:adatvedelmitisztviselo@metropolitan.hu)

#### 3. The data processing activities

We inform the data subjects that data processing related to student academic and financial matters, student disciplinary matters, legal remedy procedures, ethical procedures, and reports made through the internal whistleblowing system does NOT fall within the scope of this privacy notice. Information regarding notifications and procedures made in this subject area is available on the following platforms:

- <https://metropolitan.hu/en/adatkezeles-adatvedelem>
- <https://metropolitan.hu/en/visszaelesi-szabalyzat>

This notice applies to the personal data processed during the course of handling and investigating matters falling under the scope of the Complaints Handling Policy (hereinafter: the Policy). The complainant (hereinafter: the data subject) may submit their complaint orally or in writing, in Hungarian or English, in accordance with the procedure set out in the Policy.

Except for anonymous reports, the submission of a complaint involves the processing of the data subject's personal data—particularly the collection, recording, storage and use of such data—as specified below. If an anonymous reporter provides the personal data of natural persons involved in the reported complaint, the provisions below shall likewise apply.

##### 3.1. The purpose of data processing

The **purpose** of the data processing is to record comments and complaints related to the Data Controller's operations and services, to identify such complaints, and to ensure the professional,

impartial and transparent handling of complaints submitted to the Data Controller, including the timely remedy of any grievances and the maintenance of complaint records.

### **3.2. The types of personal data**

- Identification and contact details (e.g. name, telephone number, email address)
- Contents of the power of attorney (authorised representative's or proxy's details, particularly identification data)
- Contents of the complaint (if a natural person is affected by the complaint, their identification data and data related to the complaint)
- Contents of the minutes recorded in relation to a verbal complaint:
  - i. identification and contact details (name of the complainant, postal address or email address, in the case of a student their NEPTUN code),
  - ii. in the case of acting through an authorised representative or proxy: the representative's / proxy's name and contact details,
  - iii. the complainant's / person submitting the complaint's declaration on whether they request the confidential processing of their personal data and identity,
  - iv. the place, time, and method of submitting the complaint,
  - v. a detailed description of the complaint, and a list of documents and other evidence presented by the complainant,
  - vi. the name of the employee recording the minutes,
  - vii. in the case of an in-person verbal complaint: the signatures of the employee recording the minutes and of the complainant – or, where applicable, the representative / proxy; in the case of a telephone complaint: the signature of the employee recording the minutes,
  - viii. the place and time of recording the minutes,
  - ix. in the case of a telephone complaint: the unique identification number of the complaint,
  - x. the warning given to the complainant.
- In the case of submitting a written complaint:
  - i. identification and contact details (name of the complainant, postal address or email address, in the case of a student their NEPTUN code),
  - ii. in the case of acting through an authorised representative or proxy: the name and contact details of the authorised representative or proxy,
  - iii. the complainant's / person submitting the complaint's declaration on whether they request the confidential processing of their personal data and identity,
  - iv. the clear identification of the matter, activity, service, or conduct affected by the complaint, along with a precise description of the case,
  - v. a brief and clear description of the contested conduct, procedure, or omission,
  - vi. copies of any supporting documents available, and all essential information that may assist in the investigation of the case,
  - vii. in the case of representation through a proxy: the submission of the power of attorney (in public or full-probative-value private document form),
  - viii. in the case of representation: proof of the representative's authority,
  - ix. the complainant's specific and unambiguous request (what action or remedy they seek),
  - x. in the case of submission on paper: the handwritten signature of the complainant / authorised representative / proxy,
  - xi. any other information provided by the complainant / person submitting the complaint.
- Identification data included in notes made during the investigation of the complaint
- Data contained in documents, records, and files relating to the complaint, as well as any additional information requested regarding a natural person
- The outcome of the complaint assessment and the content of the response provided to the complainant

### **3.3. Data subjects**

The complainant / person submitting the complaint to METU, and the natural persons affected by the reported complaint.

### **3.4. The legal basis of data processing**

The data processing carried out by the Data Controller is based on the Data Controller's legitimate interest (Article 6(1)(f) GDPR) to ensure a uniform, lawful and internally compliant complaint-handling system.

### **3.5. Source of data**

The complainant / person submitting the complaint and the persons involved in the investigation.

### **3.6. Data retention**

If the complainant submits their complaint to an improper forum, the competent colleague of METU shall, within 3 days following the notification of the data subject, take measures to forward the complaint to the organisational unit having the appropriate competence. In such cases, the retention period specified in the data processing notice applicable to the relevant forum / procedure shall apply.

The retention period for the personal data processed in the complaint-handling procedure covered by this notice is at least 3 years from the closure of the complaint case. If, as a result of the complaint, or thereafter, an administrative, judicial or other legal dispute arises, the data shall be retained until the final conclusion of such proceedings.

### **3.7. Data transfer, recipients**

The Data Controller does not transfer personal data to third countries.

The Data Controller pays particular attention to ensuring that only those employees or agents of the relevant organisational units who are authorised and responsible for performing the given task have access to the data. If, at the time of submitting the complaint, the complainant requests that their personal data be handled confidentially, the Data Controller will treat the personal data / identity provided accordingly, in a closed and confidential manner during the complaint-handling process. In such cases, only persons conducting the complaint-handling procedure — in particular those responsible for managing and recording the report — and who are bound by confidentiality obligations, shall have access to these data. However, the individuals conducting the investigation of the complaint shall not have knowledge of the complainant's identity.

The Data Controller transfers the processed data to the maintainer (BKF Fenntartó Korlátolt Felelősségű Társaság, registered office: 1117 Budapest, Gábor Dénes utca 4. Infopark. Building C. Ground Floor) and to the companies belonging to its corporate group, provided that, in the specific complaint case, their involvement can be established during the investigation, and in compliance with the provisions of the Policy.

## **4. Confidentiality and security of data**

The Data Controller processes personal data confidentially and takes all complementary IT measures required to a safe data processing.

The Data Controller and the Data Processor shall take appropriate technical and organizational measures – taking into account the state of science and technology and the costs of implementation, the nature, scope, circumstances and objectives of data management and the risk of varying probability and severity of natural persons' rights and freedoms – to guarantee a level of security that is appropriate to the degree of risk.

The Data Controller selects and manages the IT tools used to manage personal data in the provision of the service so that the data processed

- can only be accessed to the authorized person,
- are protected against unauthorized access through server-level and application-level security procedures,
- can be verified to be unaltered, and the verification of the changes is ensured,
- is available throughout the data processing period.

## **5. Your rights**

Please note that according to the law in force you can exercise your rights at [adatvedelmitisztviselo@metropolitan.hu](mailto:adatvedelmitisztviselo@metropolitan.hu) by e-mail - under the statutory terms -:

Pursuant to Article 21 of the GDPR, the data subject has the **right to object** to the processing of their

personal data as follows:

The data subject shall have the right to object, on grounds relating to their particular situation, **at any time to the processing of personal data concerning them which is based on points (e) or (f) of Article 6(1)**, including profiling based on those provisions. In such a case, the controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject, or which relate to the establishment, exercise or defence of legal claims.

Pursuant to Article 15 of the GDPR, the data subject may request **access** to personal data concerning them as follows:

The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning them are being processed, and, where that is the case, access to the personal data and to the following information:

- a) the purposes of the processing;
- b) the categories of personal data concerned;
- c) the recipients or categories of recipients to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
- d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing concerning the data subject, or to object to such processing;
- f) the right to lodge a complaint with a supervisory authority;
- g) where the personal data are not collected from the data subject, any available information as to their source;
- h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4), and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject submits the request by electronic means, the information shall be provided in a commonly used electronic form, unless otherwise requested by the data subject. The right to obtain a copy shall not adversely affect the rights and freedoms of others.

Pursuant to Article 16 of the GDPR, the data subject has the right to obtain from the controller the **rectification** of personal data concerning them.

At the request of the data subject, the controller shall rectify inaccurate personal data concerning them without undue delay. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

Pursuant to Article 17 of the GDPR, the data subject has the right to obtain from the controller the **erasure** of personal data concerning them as follows:

The data subject shall have the right to obtain from the controller the erasure of personal data concerning them without undue delay, and the controller shall be obliged to erase personal data without undue delay where one of the following grounds applies:

- a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- b) the data subject objects to processing for reasons of public interest, the exercise of official authority, or the legitimate interests of the controller (or a third party), and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing for direct marketing purposes;
- c) the personal data have been unlawfully processed;
- d) the personal data have to be erased for compliance with a legal obligation under Union or Member State law (Hungarian law) to which the controller is subject.

Where the controller has made the personal data public and is obliged to erase the personal

data pursuant to paragraph (1), the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure of any links to, or copies or replications of, those personal data.

The data subject's right to erasure may be restricted only where one of the following exceptions set out in the GDPR applies, meaning that further storage of the personal data shall be considered lawful:

- for exercising the right of freedom of expression and information;
- for compliance with a legal obligation;
- for the performance of a task carried out in the public interest;
- for the exercise of official authority vested in the controller;
- for reasons of public interest in the area of public health;
- for archiving purposes in the public interest;
- for scientific or historical research purposes or statistical purposes;
- for the establishment, exercise or defence of legal claims.

Pursuant to Article 18 of the GDPR, the data subject has the right to obtain **restriction of processing** from the controller as follows:

The data subject shall have the right to obtain restriction of processing where one of the following applies:

- a) the accuracy of the personal data is contested by the data subject, in which case the restriction shall apply for a period enabling the controller to verify the accuracy of the personal data;
- b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
- c) the controller no longer needs the personal data for the purposes of processing, but the data are required by the data subject for the establishment, exercise or defence of legal claims; or
- d) the data subject has objected to processing for reasons of public interest, the exercise of official authority, or the legitimate interests of the controller (or a third party), pending verification of whether the controller's legitimate grounds override those of the data subject.

Where processing has been restricted in accordance with the above, such personal data shall, with the exception of storage, only be processed with the data subject's consent, or for the establishment, exercise or defence of legal claims, or for the protection of the rights of another natural or legal person, or for reasons of important public interest of the Union or of a Member State.

Pursuant to Article 20 of the GDPR, the data subject has the right to **data portability** as follows:

The data subject shall have the right to receive the personal data concerning them, which they have provided to a controller, in a structured, commonly used and machine-readable format, and shall have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

- the processing is based on the data subject's consent or on a contract to which the data subject is a party,
- and the processing is carried out by automated means.

In exercising the right to data portability, the data subject shall have the right, where technically feasible, to have the personal data transmitted directly from one controller to another.

The exercise of the right to data portability shall not adversely affect the right to erasure. The right to data portability shall not apply where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

The right to data portability shall not adversely affect the rights and freedoms of others.

## **6. Questions, the right of appeal in court, complaints addressed to the supervisory authority**

If you have any questions or requests related to data protection, please contact us at the e-mail address [adatvedelmitisztviselo@metropolitan.hu](mailto:adatvedelmitisztviselo@metropolitan.hu).

If you request information, we will respond to your request within a maximum of 30 days, using the contact information you provided.

In case of illegal data processing experienced by the data subject, he or she may initiate a civil lawsuit against the Data Controller. The trial falls within the jurisdiction of the regional court. The lawsuit - at the option of the person concerned - can also be initiated before the court of the place of residence (you can see the list and contact details of the courts through the following link: <http://birosag.hu/torvenyszekek>).

Without prejudice to other administrative or judicial remedies, any data subject shall have the right to file a complaint to the supervisory authority, in particular in the Member State in which he or she has his or her habitual residence, place of employment or suspected infringement, if the data subject considers that the processing of personal data regarding him or her violates the GDPR.

National Authority for Data Protection and Freedom of Information

Address: H-1055 Budapest, Falk Miksa street 9-11.

Postal address: 1363 Budapest, Pf.: 9

E-mail: [ugyfelszolgalat@naih.hu](mailto:ugyfelszolgalat@naih.hu)

Phone no.: +36 (1) 391-1400

Website: [www.naih.hu](http://www.naih.hu)

Budapest, 2026.03.30.