



Privacy Statement – for data management in connection with the CEEPUS Programme

1. PURPOSE OF THE STATEMENT

The purpose of this Statement is to provide information about the principles of data protection and data management applied by the Tempus Public Foundation regarding the CEEPUS Programme.

The Tempus Public Foundation (hereafter referred to as Data Controller) – as joint controller together with the National CEEPUS Offices (NCO) of the CEEPUS countries – manages the personal data of those who apply, and successfully participate in the CEEPUS Programme.

2. THE DATA CONTROLLER'S NAME

Name: Tempus Public Foundation

Headquarters and mailing address: 1077 Budapest Kéthly Anna tér 1.

Phone number: + 36-1-237-1300

Represented by: Károly Czibere, president

Data protection officer: Dr. Eszter Margit Szabó

E-mail address: adatvedelem@tpf.hu

3. SCOPE OF THE PERSONAL DATA MANAGEMENT

We will manage the following personal data:

- title
- name
- e-mail address
- phone no.
- gender
- date and place of birth
- citizenship
- address
- educational attainment (field of study, institution, level)
- sending higher education institution
- position at the sending higher education institution (student or academic position)
- host higher education institution
- tendered period
- tendered field of study
- language knowledge (language, level)

If any modification or change occurs during the data management period of the data handled by the Data Controller, please notify us immediately at the above availability.

4. THE LEGAL BASIS, OBJECTIVE AND METHOD OF DATA MANAGEMENT

4.1. Data management in the framework of the application process

4.1.1. The Management of data is based on your information-based statement, which includes your agreement for the use of your personal data provided during the submission of your application in the system. Legal Basis for the management of data: Article 6 (1) (b) of Regulation (EU) 2016/679 (General Data Protection Regulation) – preparation of contract signing.

For applications addressed to the National CEEPUS Offices in Albania, Bosnia-Herzegovina, Moldova, Montenegro, North Macedonia, Serbia and Kosovo, the legal basis for the management of data: Article 49 (1) (b) of Regulation (EU) 2016/679 (General Data Protection Regulation) – preparation of contract signing.

4.1.2. The purpose of data management is to evaluate your submitted application. The Data Controller uses the data you have provided exclusively for the purpose of evaluating your application.

4.2. Data management in the framework of the realization of your scholarship

4.2.1. The Management of data is based on the performance of the scholarship contract between you and the entitled Higher Education Institution. Legal Basis for the management of data: the performance of a contract according to Article 6 (1) (b) of Regulation (EU) 2016/679 (General Data Protection Regulation) and Article 49 (1) (b) of Regulation (EU) 2016/679 (General Data Protection Regulation) in the case of applications addressed to third countries as referred to in Point 4.1.1.

4.2.2. The purpose of data management is to realize your scholarship. The Data Controller uses the data you have provided exclusively for this purpose.

4.3. The Data Controller may not use or use the provided personal data for purposes other than those set out in these points. Disclosure of personal data to a third party – unless otherwise provided by law – is only possible with your prior express consent.

4.4. The Data Controller does not verify the personal information you provide. The authenticity of the data given is your sole responsibility. When submitting your e-mail address, you also assume liability for being the sole user of the e-mail address provided. With respect to this liability, any entry from an e-mail address will be attributed solely to you as the person who registered the e-mail address.

5. THE DURATION OF THE DATA PROCESSING

The duration of the data processing is at most 30 years (counted from submitting the institutional final report by the entitled Higher Education Institution), in accordance with Point 8. of the Privacy Policy¹ on the central application platform <https://ceepus.info>.

¹ <https://ceepus.info/default.aspx?CMSPage=95>

6. SCOPE OF PERSONS WITH ACCESS TO THE DATA, DATA TRANSFER AND DATA PROCESSING

6.1. It is primarily the Data Controller and its internal staff who are entitled to have access to the data in order to accomplish their employment duties.

Besides the Data Controller, the following entitled persons are allowed to access your data:

- The entitled Hungarian Higher Education Institution where you apply. The entitled Higher Education Institution ensures that it processes your data in accordance with the applicable regulations and its internal rules. The Institution may request other data in addition to the personal data referred to in Point 3.

Primarily, the following persons have access to your data at the Institution:

- local coordinator of the CEEPUS network,
- CEEPUS institutional coordinator (IRO),
- colleagues of the finance department responsible for scholarship payment in the case of incoming mobilities.
- Colleagues of the foreign Higher Education Institution responsible for CEEPUS.
- National CEEPUS Offices of your sending and host countries.
- Overall coordinator of the CEEPUS network.
- Central CEEPUS Office.
- Developers who manage the CEEPUS Software.

6.2. The Data Controller may use a Data Processor to operate the IT system.

Name of the Data Processor:

CEEPUS Generalsekretariat (Central CEEPUS Office)
Albertgasse 35 A-1080 Wien, Ausztria

The Central CEEPUS Office is responsible for the central coordination of the CEEPUS Programme including the operation of the online application platform: <https://ceepus.info>.

7. THE RIGHTS AND RECOURSE TO LAW AVAILABLE TO THE PERSONS CONCERNED

7.1. You are entitled at any time to request information about your personal data managed by the Data Controller and may modify such data at any time by sending an e-mail request addressed to the contact details provided in Point 7.3.

7.2. At your request, the Data Controller must provide you with information regarding your personal data it manages, the data processed by the data processor entrusted by it, the source of such data, the purpose, legal basis and duration of the data management, the data processor's name, address and activities in connection with the handling of the data, the circumstances and effects of the data protection incident, the measures taken to remedy the incident, and – in the case of transmission of the personal data – the legal basis and the recipient of the data transfer. The service provider must provide the requested information in writing within 30 days of the submission of the request.

The Data Controller – through its data protection officer – keeps a record to supervise and keep you informed of any measures taken in connection with the data protection incident including the scope of personal data concerned, the scope and number of persons affected by the data protection incident, the date, circumstances and effects of the data protection incident and the measures implemented in order to remedy the incident, as well as any other data specified in the laws governing the management of data.

7.3. You can exercise your rights via the following contact details:

E-mail address: adatvedelem@tpf.hu

You may contact the Data Controller's data protection officer with any questions or observations regarding the processing of data via the contact details provided in Point 7.3.

7.4. You are entitled at any time to request the correction or erasure of any incorrectly recorded data. The Data Controller corrects or erases the data within one month of the receipt of the request at the adatvedelem@tpf.hu email address.

If the Service Provider refuses to comply with the Concerned Person's request for correction or erasure, it must justify in writing the factual and legal grounds for such refusal of the cancellation within one month of receipt of the request.

7.5. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation 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 withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;
- c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);
- d) the personal data have been unlawfully processed;
- e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
- f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

7.6. In case of complaint, you may apply to the National Privacy and Information Authority (1125 Budapest, Erzsébet Szilágyi fasor 22 / c, www.naih.hu).

7.7. If you have provided third-party data for the use of the service, the Data Controller is entitled to seek damages from you. In such cases, the Data Controller must provide all available assistance to the competent authorities for the purpose of establishing the identity of the infringing person.

8. OTHER PROVISIONS

8.1. In all cases where the Data Controller intends to use the data provided for purposes other than the purpose of the original data collection, it will notify and obtain from you your prior express consent, and will provide you the opportunity to prohibit such use.

8.2. The Data Controller undertakes to ensure the security of the data, to implement technical measures to ensure the protection of the recorded, stored or managed data, and to do everything in its power to prevent the destruction, unauthorized use and unauthorized alteration of the data. The Data Controller also undertakes to call on any third party to whom the data may be transferred or handed over to comply with these obligations.

8.3. The Data Controller reserves the right to unilaterally modify the rules and information on its website regarding the management of data.