

## PRIVACY NOTICE

on data management of CCTV surveillance systems

The **Central European Academy of the University of Miskolc** (hereafter: **Data Controller**) hereby informs the Data Subjects **about the processing of their personal data in connection with the use of CCTV surveillance at the Data Controller's headquarters** (1122 Budapest, Városmajor utca 12-14.), in accordance with Regulation 2016/679 of the European Parliament and of the Council (hereinafter: **GDPR**) and in accordance with the provisions of Act CXII of 2011 on the Right of Informational Self-Determination and Freedom of Information.

This Privacy Notice is permanently available in printed form at the Data Controller's headquarters and on its website(<https://centraleuropeanacademy.hu/dokumentum/>).

### **I. The Data Controller and its Data Protection Officer**

#### **Data Controller:**

#### **Central European Academy of the University of Miskolc**

Seat: H-1122 Budapest, Városmajor utca 12-14.  
Registration number: Education Authority FNYF/419-4/2023  
Tax identification number: 19359711-1-43  
Statistical number: 19359711-7220-599-01

Data Protection Officer of the Data Controller:

#### **Réti, Várszegi and Partners Law Firm**

Responsible employee: Dr. András Csenterics, lawyer, data protection and data security lawyer  
Address: 1055 Budapest, Bajcsy-Zsilinszky út 78.  
Email address: [hu.central.european.academy@pwc.com](mailto:hu.central.european.academy@pwc.com)

**If you wish to exercise your rights in relation to data protection, you can contact the Data Controller using the contact details above.**

**II. Scope of personal data processed by the Data Controller, purpose, legal basis and duration of processing**

Scope of processed data	Purpose of data processing	Legal basis of data processing	Duration of data processing
<p>The image of the Data Subjects in the field of view of the CCTV cameras installed at the Data Controller's seat and the data (location, time) that can be inferred from the recording data</p> <p>The CCTV cameras do not record sound and do not have smart features (e.g. face recognition)</p>	<p>Protection of persons, property and trade secrets and confidential information at the Data Controller's seat</p>	<p>Article 6(1)(f) GDPR: the legitimate interest of the Data Controller in the protection of property and persons, the protection of business secrets and confidential information and, where justified, the investigation of events recorded by the CCTV</p>	<p>30 days</p>
<p>The above-mentioned personal data, if their retention is necessary for the purposes of legal claims</p>	<p>Ensuring that the Data Controller has sufficient evidence to pursue and defend its legal position in the case of legal claims, and to take appropriate legal actions in relation to the events recorded by the CCTV</p>	<p>Article 6(1)(f) GDPR: the legitimate interest of the Data Controller in being in possession of the relevant evidence in the event of legal proceedings</p>	<p>Until the end of the applicable legal claim period: 5 years for civil claims, 3 years for labour claims</p> <p>In the case of any official or judicial proceedings in which the use of the CCTV footage is indispensable, until the final conclusion of the relevant proceedings</p>

### **III. Recipients of personal data**

The Data Controller stores the CCTV footage on its own server, does not use external service providers, does not transfer the recordings to other organisations, and does not make them available (not including ad hoc data transfers based on a request from an authority, if the Data Controller is under an explicit legal obligation to transfer the data). Access to the footage within the Data Controller's organisation is strictly limited.

### **IV. Automated decision-making, profiling**

The Data Controller does not carry out any automated decision-making or profiling in relation to the data processed in accordance with this Privacy Notice. This means that it does not use the footage for any analysis of the Data Subject, nor does it use the footage to make any automatic (no human intervention) decisions about the Data Subject.

### **V. Rights of the Data Subject**

**In all cases, the rights referred to in this point may be exercised by using the contact details provided in point I. All questions, complaints and requests will be investigated individually and answered within one month of receipt at the latest.** If necessary, taking into account the complexity of the request and the number of requests, this deadline may be extended by two months. In such a case, we will inform the Data Subject of the extension of the deadline within one month of receipt of the request, stating the reasons for the delay.

The Data Subject has the following rights in relation to the processing of data under point II:

#### **a) Right to access:**

The Data Subject shall have the right at any time to obtain information on whether and how his/her personal data are processed by the Data Controller, including the purposes of the processing, the recipients to whom the data have been disclosed or the source from which the data were obtained by the Data Controller, the retention period, his/her rights in relation to the processing and, in the case of transfers to third countries or international organisations, information on the safeguards relating thereto. In exercising the right to access, the Data Subject also has the right to request a copy of the data. Where the Data Subject's right of access adversely affects the rights and freedoms of others, in particular the business secrets or intellectual property of others, the Data Controller shall have the right to refuse to comply with the Data Subject's request to the extent necessary and proportionate.

**b) Right to rectification**

The Data Subject shall have the right to request the Data Controller to correct inaccurate personal data relating to him/her. Depending on the purpose of the processing, the Data Subject has the right to request that incomplete personal data be completed, including by means of a supplementary declaration. If there is doubt about the corrected data, the Data Controller may request the Data Subject to provide the Data Controller with evidence of the corrected data in an appropriate manner, in particular by means of a document.

**c) The right to erasure ("right to be forgotten")**

Where the Data Subject requests the erasure of some or all of his/her personal data, the Data Controller shall erase them without undue delay where

- the Data Controller no longer needs the personal data for the purposes for which it was collected or otherwise processed;
- the Data Subject has objected to the processing and there is no overriding legitimate ground for the processing;
- the personal data have been unlawfully processed by the Data Controller, or
- the erasure of personal data is necessary to comply with a legal obligation.

The Data Controller is not always obliged to delete personal data, in particular if the processing is necessary for the establishment, exercise or defence of legal claims.

**d) Right to restriction of data processing**

Restriction of data processing means that during the period of restriction, the Data Controller will only store the data and will not perform any other operation on them.

The Data Subject may request the restriction of the processing of his/her personal data in the following cases:

- the Data Subject contests the accuracy of the personal data - in this case, the restriction applies for the period of time that allows the Data Controller to verify the accuracy of the personal data;
- the processing is unlawful, but the Data Subject opposes the erasure of the data and instead requests the restriction of their use;
- the Data Controller no longer needs the personal data for the purposes of processing, but the data subject requires them for the establishment, exercise or defence of legal claims; or
- the Data Subject has objected to the processing - in which case the restriction applies for the period until the Data Controller has dealt with the objection.

**e) Right to objection**

**The Data Subject has the right to object to the processing. The Data Controller is not obliged to uphold the objection if the Data Controller proves that**

- **data processing is justified by compelling legitimate grounds which override the interests, rights and freedoms of the Data Subject, or**
- **the processing relates to the establishment, exercise or defence of legal claims by the Data Controller.**

**f) Right to lodge a complaint with a supervisory authority, judicial redress**

If the Data Subject believes that his/her personal data have been misused, he/she can also contact the data protection authority and lodge a complaint, in particular in the Member State of his/her habitual residence, place of work or place of the alleged breach.

**In Hungary, you can contact the National Authority for Data Protection and Freedom of Information (NAIH):** address: H-1055, Hungary, Budapest, Falk Miksa utca 9-11.; postal address: 1363 Budapest, Pf.: 9.; phone: +36-1 391-1400; fax: +36-1 391-1410; e-mail: [ugyfelszolgalat@naih.hu](mailto:ugyfelszolgalat@naih.hu); website: <http://naih.hu/>).

Irrespective of their right to lodge a complaint, Data Subjects may also take legal action in the event of a breach of their rights in relation to the processing of their personal data. The Data Subject also has the right to take legal action against a legally binding decision of the supervisory authority. The Data Subject also has the right to judicial remedy if the supervisory authority does not deal with the complaint or does not inform the Data Subject within three months of the procedural developments or the outcome of the complaint.

This Privacy Notice is effective from 01 April 2026.

*Barzó Tímea*

Dr. Heiner Dr. Barzó Tímea Tünde  
Director-General



