

Reference number: KEA/421-3/2024.

PRIVACY NOTICE

concerning the processing of personal data of job applicants

The **Central European Academy** (hereinafter: **The Data Controller**) provides the following information on the processing of personal data of persons who submit job applications to the Academy, in accordance with Regulation 2016/679 of the European Parliament and of the Council on the General Data Protection Regulation (hereinafter: **GDPR**) and the provisions of Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information (hereinafter: **Infotv.**).

Please read the Privacy Notice carefully.

This Privacy Notice is available on the website of the Data Controller (<https://centraleuropeancademy.hu/>), at its registered office indicated below and at the postal address of the Data Protection Officer. Data Subjects may access, view, print and save this privacy policy on the website, but they may not modify it, only the Data Controller may do so.

I. The Data Controller and its Data Protection Officer

Data Controller:

Central European Academy

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
E-mail address: adatvedelem@centraleuropeancademy.hu

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.
E-mail: hu_central_european_academy@pwc.com

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

The Data Controller processes the following personal data of job applicants as Data Subjects:

Scope of processed data	Purpose of data processing	Legal basis of data processing	Storage time
Contact details of the applicant (name, e-mail address, telephone number)	Identification, contact	The Data Controller's legitimate interest in being able to contact the applicant during the application process	Duration of the selection procedure
The information provided by the applicant in his/her CV, cover letter or application form, including details of studies, qualifications, training, professional experience	Assessment of the qualifications, training and experience required for the job in question	The Data Controller's legitimate interest in selecting the most suitable candidate for the job in question	Duration of the selection procedure
Data provided by the applicant during the selection procedure or during recruitment interviews or relevant to the assessment of the applicant	Assessment of the applicant's suitability in the selection procedure	The Data Controller's legitimate interest in selecting the most suitable candidate for the job in question	Duration of the selection procedure
Applicant's contact details as indicated above, the details provided in his/her CV, covering letter and application form, and the details provided during the selection procedure and interviews	Contacting the applicant in case of new vacancies (if he/she would not be recruited in the actual recruitment process)	Express consent of the applicant	For 12 months from the end of the recruitment process, unless the applicant withdraws his/her consent before the end of the 12 months, in which case until the consent is withdrawn.
All the personal data mentioned above	Presenting, enforcing and defending legal claims in the event of a dispute	The Data Controller's legitimate interest in having the appropriate evidence at its disposal in the event of legal claims or in being able to enforce its legal claims	In case of enforcement of claims arising from the selection procedure, until the end of the civil enforcement period (5 years)

Reference number: KEA/421-3/2024.

The Data Controller draws your attention to the fact that **if the applicant does not provide all the data strictly necessary for the assessment, the possible consequence of not providing the data may be exclusion from the selection procedure**, given that the Data Controller cannot assess the job application or not fully assess it without the data.

The Data Controller does not collect special categories of data during the selection (recruitment) process and explicitly warns applicants **not to provide any data in the special category of personal data** (i.e. data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, health data, and data concerning sexual life or sexual orientation) **during the recruitment process**.

III. Data Processors, other recipients of data flows, data from other sources

The Data Controller uses the following data processors for the processing of the data covered by this notice:

Data Processor	Purpose of data processing
H1 Systems Mérnöki Szolgáltatások Korlátolt Felelősségű Társaság (seat: H-1117 Budapest, Budafoki út 62.; company registration number: 01-09-469226)	Operation of the Data Controller's IT system

Apart from the above, the Data Controller does not use any other data processor.

The Data Controller will not transfer the data processed in accordance with this Privacy Notice to third parties. The Data Controller is also entitled and obliged however, to transmit to the competent authorities and courts any personal data at its disposal and stored by it in accordance with the law, which it is obliged to transmit by law or by a final and binding order of a public authority or court.

In some cases, the Data Controller uses the services of a recruitment agency on the basis of a contract to advertise job vacancies and to carry out certain stages of the selection procedure. In such a case, the recruitment agency contacts the applicant and transfers the personal data related to the application to the Data Controller, which means that the Data Controller does not obtain them directly from the applicant, but from the service provider.

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.

V. Protection of personal data

The Data Controller respects the rights of Data Subjects under the law and, in accordance with the principle of data security, designs and implements its data processing operations in a way that ensures the protection of the privacy of Data Subjects.

In order to ensure the security of personal data, the Data Controller i takes in particular the following measures:

- the personal data can only be accessed by those authorised to do so, they cannot be accessed by others and cannot be disclosed to others, the Data Controller has defined the scope of authorised persons based on which employees' daily work requires the knowledge of the data;
- staff carrying out data processing may leave the premises where data processing is taking place only by locking the data media entrusted to them or by closing the office;
- the computers used in the processing are the property of the Data Controller or over which the Data Controller has the right to exercise control in order to protect personal data against unauthorised or unlawful processing, accidental loss, destruction or damage;
- access to the data on the computer is only possible with valid, personal, identifiable access rights - at least with a user name and password - and the Data Controller ensures that passwords are changed regularly;
- virus protection of the information systems processing personal data is continuously ensured by the Data Controller;
- in the event of a physical or technical incident, the Data Controller ensures the ability to restore access to and availability of personal data in a timely manner;
- the Data Controller regularly reviews its data processing;
- the Data Controller has adopted an internal data protection and data security policy and regularly provides data protection and data security awareness training to staff working with personal data;
- the Data Controller employs a Data Protection Officer with appropriate market reputation and expertise.

VI. Rights of the applicant

The rights listed in this point may in any case be exercised by the Data Subject by sending a request to the contact details indicated in point 1. 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 a further 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.

a) Right to access

The Data Subject shall have the right to obtain from the Data Controller information as to whether or not his or her personal data are being processed and, if so, to request access to and a copy of his or her personal data.

Reference number: KEA/421-3/2024.

The Data Subject shall have the right to request further information on the processing, in particular on the purposes of the processing, the persons to whom the data have been disclosed, the source from which the data were obtained by the Data Controller, the rights associated with the processing or the storage period.

Where the applicant's right of access adversely affects the rights and freedoms of others, in particular the trade secrets or intellectual property of others, the Data Controller shall be entitled to refuse to comply with the applicant's request to the extent necessary and proportionate. For identification purposes, the Data Controller may request additional information from the Data Subject or charge a reasonable administrative fee if the Data Subject requests more than one copy of the above information.

b) Right to rectification

The Data Subject shall have the right to obtain from the Data Controller the rectification of inaccurate personal data relating to him or 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 applicant to provide the Data Controller with evidence of the corrected data in an appropriate manner, in particular by means of documents.

c) Right to erasure ("right to be forgotten")

The Data Subject shall have the right to request the erasure of his or her personal data by the Data Controller and the Data Controller shall be obliged to erase such personal data if:

- the Data Controller no longer needs the personal data for the purposes for which it was collected or otherwise processed;
 - the processing is based on the consent of the applicant, but the consent has been withdrawn by the applicant and there is no other legal basis for the processing;
 - the processing was based on the legitimate interests of the Controller or a third party, but the applicant has objected to the processing and there are no overriding legitimate grounds for the processing;
 - the personal data have been unlawfully processed by the Data Controller, or
 - the data is deleted to comply with a legal obligation.
- In case of erasure, the applicant will no longer be able to participate in the selection process.

d) Right to restriction of data processing

The Data Subject has the right to request the restriction of the processing of his or her personal data. Restriction of processing means that the Data Controller does not process the personal data concerned by the restriction, except for storage, or only to the extent that the applicant has consented or the processing is necessary for the establishment, exercise or defence of legal claims, the protection of the rights of another person or for important public interest. In the event of a request for restriction, the Data Controller shall identify the personal data concerned which it may process only for the purposes set out above.

Applicants may request the restriction of the processing of their personal data in the following cases:

Reference number: KEA/421-3/2024.

- the applicant contests the accuracy of the personal data - in this case, the limitation 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 applicant opposes the deletion 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 applicant requires them for the establishment, exercise or defence of legal claims; or
- the applicant has objected to the processing - in this case the restriction applies for the period of time until the Data Controller has dealt with the objection.

d) Right to objection

Where the legal basis for processing of data relating to the applicant is the legitimate interest of the Data Controller or a third party, the applicant has the right to object to the processing. The Data Controller is not obliged to uphold the objection if the Data Controller proves that

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

f) The right to data portability

The Data Subject has the right to receive his or her personal data processed on the basis of consent in a structured, commonly used, machine-readable format (i.e. digital format) and the right to request, where transfer is technically feasible, the transfer of such data to another controller without hindrance from the Data Controller. In cases where the exercise of the Data Subject's right to data portability would adversely affect the rights and freedoms of others, the Data Controller is entitled to refuse to comply with the Data Subject's request to the extent necessary.

g) Right to withdraw consent

Where the processing of personal data is based on consent, the Data Subject may withdraw his or her consent at any time in a statement submitted to the Data Controller without giving reasons. The withdrawal of consent does not affect the lawfulness of processing based on consent prior to its withdrawal.

If the Data Subject withdraws his or her consent to the processing of his or her personal data by the Data Controller, the Data Controller will no longer be able to contact him or her with new job offers. This does not, of course, prevent the Data Subject from applying for any job opportunities that may be advertised by the Data Controller in the future.

h) Right to lodge a complaint with a supervisory authority

If the Data Subject believes that his or her personal data have been misused, he or she can also contact the data protection authority and lodge a complaint, in particular in the Member State of his or 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; website: <http://naih.hu/>.

Reference number: KEA/421-3/2024.

Irrespective of their right to lodge a complaint, the applicant may also take legal action in the event of such a violation. The applicant also has the right to appeal against a legally binding decision of the supervisory authority. The applicant also has the right to a judicial remedy if the supervisory authority does not deal with the complaint or does not inform the applicant within three months of the procedural developments or the outcome of the complaint.

This Privacy Notice is effective from 16. 07. 2024.



Dr. Heinerné Dr. Barzó Tímea Tünde
Director General



