Reference number: KEA/2025/1092

PRIVACY NOTICE

ON THE PROCESSING OF PERSONAL DATA OF NATURAL PERSONS WHO HAVE AN EMPLOYMENT RELATIONSHIP WITH THE CENTRAL EUROPEAN ACADEMY

The purpose of this notice is to provide you with detailed and clear information about how the Central European Academy processes your personal data as a data subject (hereinafter referred to as "**Data Subject**") in accordance with the General Data Protection Regulation of the European Union. The contact details for questions and complaints, a detailed description of data processing and the rights the Data Subject can exercise are the following:

1 DATA CONTROLLER, DATA PROTECTION OFFICER AND THEIR CONTACT DETAILS

Name of the Data Controller: **Central European Academy (Data Controller)**

Seat: 1122 Budapest, Városmajor utca 12-14.

Email: adatvedelem@centraleuropeanacademy.hu

Phone: +36 30 102 7401

Data Protection Officer of the Data Controller:

- Réti, Várszegi & Partners Law Firm, responsible employee: Dr. András Csenterics, attorney, data protection and data security lawyer
- Data Protection Officer postal address: 1055 Budapest, Bajcsy-Zsilinszky út 78.
- Please report your data protection complaints to the Data Protection Officer at the following email address: centraleuropeanacademy@pwc.com

2 SCOPE OF DATA PROCESSED BY THE DATA CONTROLLER, PURPOSE, LEGAL BASIS OF PROCESSING AND DURATION OF PROCESSING

Scope of processed data	Purpose of data processing	Legal basis of data processing	Duration of data processing
Data required for the establishment of an employment relationship or other legal relationship for the purpose of employment (e.g., employee's name, address, place and date of birth, mother's name, position, signature, etc.), as well as personal identification data related to the notification to the NAV, including tax identification number and social security number, and data on education, professional	Identification of the Data Subject, establishment of a legal relationship with the Data Subject, proof of the existence of the qualifications required for the given position Complying with tax and social security obligations	Preparing and fulfilling the agreement of the Data Subject Fulfilling legal obligations under tax and social security legislation, including in particular the obligations related to the notification pursuant to Section 16(1) of Act CL of 2017 and Annex 1, point 3 of the CL Act of 2017 and Section 66(2) of Act CXXII of 2019	Until 5 years after the retirement age applicable to the Data Subject, pursuant to Section 99/A (1) of Act LXXXI of 1997

Scope of processed data	Purpose of data processing	Legal basis of data processing	Duration of data processing
or qualifications, nationality			
Bank account number, name of the financial institution holding the account	Payment of wages and salaries (including allowances, fringe benefits and reimbursements) as well as other settlements arising from the employment relationship	Fulfilling the agreement of the Data Subject	If the bank account forms part of the accounting records, then it must be kept for 8 years in accordance with Section 169 (2) of Act C of 2000 In other cases, until the end of the period for enforcing labour law claims (3 years)
		Fulfilling legal obligations	
Data relating to the use and registration of work (mobile) phones, computers, laptops, tablets, external storage media, internet and email accounts, data recorded during the course of work or inspection (the identification data of the inspector and witnesses, detected infringement and its description)	Requesting, ensuring and registering the use of work (mobile) phones, computers, laptops, tablets, external storage media, internet and e-mail accounts in order to perform tasks and conduct official correspondence	Fulfilling the agreement of the Data Subject in relation to the request and registration of the work tool	Data recorded on work (mobile) phones, computers, tablets, external storage media: until the end of employment (except for official email accounts) Data concerning the use and other data concerning the possibility of enforcement: until the end of the applicable enforcement period (labour law: 3 years or civil law: 5 years) With regard to documents to invoicing, until the end of the tax retention period (end of the calendar year in which the tax return is due plus 5 years pursuant to Section 78(3) of Act CL of 2017) or accounting retention period (8 years pursuant to Section 169(2) of Act C of 2000)
	Employer control of the correct use of work tools where justified*(without control of private data)*[1]	Legitimate interest of the Data Controller in monitoring the Data Subject's proper use of the work tools *(without control of private data)*	
	Ensuring the Data Controller's business continuity (in the case of temporary maintenance of an official email account after termination of employment)	Legitimate interest of the Data Controller in ensuring business continuity (official email account)	

[1] The private use of work tools is permitted by the Data Controller. However, the Data Controller does not check the employee's private data when monitoring work tools and does not perform any processing activities on these data. When monitoring the employer's tools, the Data Controller shall act in accordance with the NAIH Resolution of 28 October 2016, in compliance with the principle of gradualness.

Scope of processed data	Purpose of data processing	Legal basis of data processing	Duration of data processing
			Contents of an official email account: until the last day of the month following the termination of the relationship with the Data Subject
Work related contact details, including the name, position, work email address, work (mobile) phone numbers of the Data Subject	Communicating on behalf of the Data Controller with third parties or within the organisation of the Data Controller and transmitting these data to the Data Controller's partners for the purpose of communication	Fulfilling the agreement of the Data Subject	Until the end of the applicable time limit for making a claim (labour law: 3 years or civil law: 5 years)
	Creating other business media (e.g. business cards)		
Data relating to the medical (work) fitness assessment: name of the Data Subject and result of the assessment (with categories o*fit, unfit, fit with limitations* without further details)	Ensuring healthy and safe working conditions	Taking into account the exceptions under Article 9(2)(b) and (h) of the GDPR: the Data Controller's legitimate interest in the protection of health and safety at work	Until the end of the period of enforcing labour law claims (3 years)
Data on the access card and data generated in the access control system in connection with its use (name, position, card number, card authorisation level, log data related to entry and exit)	Preparation of an access card for the Data Subject, protection of persons and property when entering, leaving or staying at the Data Controller's headquarters	The Data Controller's legitimate interest in controlling access to its territory, including the legitimate interest in the protection of persons and property	Log data will be deleted immediately upon termination of regular access (but no later than 6 months after the data were generated) Other data on the access card will be kept until the last day of the month following the month in which the legal relationship ends, or until the end of the legal claim period in case of a claim In case of temporary access, log data will be

Scope of processed data	Purpose of data processing	Legal basis of data processing	Duration of data processing
			deleted within 24 hours
Data on age and pension entitlement (number and date of the decision by the pension insurance administration to determine the pension)	Fulfilling employer's tasks to establish pension rights	Fulfilling the agreement of the Data Subject Fulfilling a legal obligation under Act LXXXI of 1997	Until 5 years after the employee reaches the retirement age pursuant to Section 99/A (1) of Act LXXXI of 1997
Data required for the registration of accidents at work (date, place, nature and circumstances of the accident; action taken; injured employee's name, position, social security number, mother's name, date and place of birth, sex, nationality, place of residence)	Recording and investigating accidents at work and fulfilling reporting obligations	Taking into account the exceptions under point 9(2)(b) and (h) of the GDPR – complying with the legal obligation under Section 64/A of Act XCIII of 1993	For 5 years from the date of registration pursuant to Section 64/A (4) of Act XCIII of 1993
Duration of incapacity to work, code, depending on the type of incapacity the data on dependants	Paying incapacity benefits	Taking into account the exception under point 9(2)(h) of the GDPR – complying with legal obligations under tax and social security legislation and Act LXXXI of 1997	Until 5 years after the employee reaches the retirement age pursuant to Section 99/A (1) of Act LXXXI of 1997
Contact details of the person(s) to be notified (name, address, telephone number and/or email address of the person(s) to be notified)	Ensuring that in the event of an emergency (i.e., accident at work), the person indicated by the Data Subject (e.g., family member) is notified	Protecting the vital interests of the Data Subject	Until the end of the legal relationship with the Data Subject
Data on previous employers, exit documents and social security record book issued by the previous employer, or, in the absence of these, personal data contained in the relevant employee declarations	Verification and provision of previous employment data for employment purposes	Fulfilling a legal obligation, including the legal obligation to retain data under Act LXXXI of 1997	Until 5 years after the retirement age applicable to the Data Subject, pursuant to Section 99/A (1) of Act LXXXI of 1997

Scope of processed data	Purpose of data processing	Legal basis of data processing	Duration of data processing
In connection with the request for additional leave, unpaid leave, sick leave, maternity/paternity leave, the data contained in the declaration of entitlement and supporting data, as well as data on the changed capacity to work (name of the requesting employee, data identifying the requesting employee and other necessary information i.e., date of birth of the child, the fact of the child's disability, the starting date and expected duration of the absence in case of sick leave, the reason for the absence in case of unpaid leave)	Ensuring the lawful granting and keeping records of the additional and unpaid leave, and ensuring that the benefits provided for in the various laws are paid and employment prohibitions are observed	Fulfillment of the legal obligation under Section 134 of the Labour Code with regard to leave records	Until 5 years from the termination of the legal relationship in case of the leave records Until 5 years after the retirement age of the Data Subject pursuant to Section 99/A (1) of Act LXXXI of 1997 in the case of the data processed in relation to the benefits to be provided
		The legitimate interest of the Data Controller in the lawful granting of additional leave and payment of certain benefits	
Payroll data (including allowances, fringe benefits and reimbursements i.e., cafeteria payments, as well as data on marital status and dependants, in order to determine eligibility for certain tax benefits and allowances): • absence period (date and type of leave); • data on incapacity for work and sick leave; • details and stats code of dependant	Payment, payroll accounting, checking entitlement to benefits, advancing and reimbursing employee expenses	Fulfilling the agreement of the Data Subject	Until 5 years after the retirement age applicable to the Data Subject, pursuant to Section 99/A (1) of Act LXXXI of 1997
	Meeting tax, accounting, social security and employer obligations under the Labour Code	Fulfillment of legal obligations pursuant to Section 29/F, 29/D, 29/C, 29/A of Act CXVII of 1995 on Personal Income Tax, Section 50 of Act CL of 2017 on the Rules of Taxation, Section 66 of Act CXXII of 2019 on Entitlements to Social Security Benefits and on Funding These Services, or other social security legislation	
Data relating to advances on wages and salaries	Recording of advances on wages and salaries owed to employees	Fulfilling the agreement of the Data Subject	Until the end of the period of enforcing labour law claims (3 years)

Scope of processed data	Purpose of data processing	Legal basis of data processing	Duration of data processing
Personal data relating to the foreign and domestic posting and the personal data necessary for the reimbursement of the costs related thereto (name of the employee, place and date of the posting, duration and other personal data necessary for the settlement of the claim)	Organising and managing business trips and ensuring the calculation of daily allowance for the period of the trip, cost accounting	Fulfilling the agreement of the Data Subject, where the travel is necessary for the performance of the Data Subject's obligations under the contract with the Data Controller	Until 5 years after the retirement age applicable to the Data Subject, pursuant to Section 99/A (1) of Act LXXXI of 1997
		Fulfilling legal obligations under Act CXVII of 1995 on Personal Income Tax with regard to the accounting of fuel costs	
		In other cases, the Data Controller's legitimate interest in the organisation of the trip and the settlement of related costs	
Working time registration data: • name and department of the Data Subject • indication of the period • the starting and finishing times (hours and minutes) of the working day, the number of working hours per day • dates and reasons for absences, leaves and standby periods	Payroll, monitoring compliance with working time, leave records, compliance with legal obligations	Fulfilling a legal obligation under Section 134 of the Labour Code	Until 5 years after the retirement age applicable to the Data Subject, pursuant to Section 99/A (1) of Act LXXXI of 1997
Information about any disciplinary action taken against the employee (warning, adverse legal consequence)	Taking action against the employee, keeping records	Fulfilling the agreement of the Data Subject	Until the end of the period of enforcing labour law claims (3 years)
The fact of termination of employment, the manner and reason for termination, the information on the exit documents, including information on the employee's final and deductible debts	Provision of the employer's accounts in the event of termination or cessation of employment, subsequent justification of the legitimate nature of the termination	Fulfilment of legal obligations under tax and social security legislation and Act LXXXI of 1997 on Social Security Pension Benefits, fulfilment of legal obligations under legislation on exit	Until 5 years after the retirement age applicable to the Data Subject, pursuant to Section 99/A (1) of Act LXXXI of 1997

Scope of processed data	Purpose of data processing	Legal basis of data processing	Duration of data processing
Data processed in connection with occupational and fire safety training (place, time, subject of the training, instructor, names Data Subjects who have completed the training, signatures)	Complying with legal obligations on occupational and fire training, ensuring the protection of persons and property	The Data Controller's legitimate interest in monitoring the conduct of and participation in mandatory occupational and fire safety training	Until the end of the period of enforcing civil law claims (5 years)
Performance appraisal data, evaluation of the work of the Data Subject	Performance appraisal of Data Subjects, performance incentives	Fulfilling the agreement of the Data Subject	Relevant legal claim period (until the end of the labour law claim period (3 years) or civil law claim period (5 years))
Private contact details (name, phone number, private email address of the data subject)	Ensuring prompt contact with the Data Subject in connection with his/her position or tasks laid down in the agency agreement, ordering extraordinary work or standby, sending payroll	The Data Controller's legitimate interest in being able to keep in contact with the Data Subject for the purposes of its continuous, operational and professional management	Until the Data Subject's agreement expires
Pregnancy data (including data on participation in human reproductive procedures and on high-risk pregnancies), in particular the expected date of delivery	Payment of pregnancy-related benefits, maternity/paternity leave	Taking into account the exceptions under point 9(2)(b) and (h) of the GDPR – the legal obligation under the Labour Code; the legal obligation under Act LXXXI of 1997 on Eligibility for Social Security Benefits and Private Pensions as well as the legal obligation under the relevant regulations	Until the end of the period of enforcing labour law claims (3 years)
	Taking into account employer obligations and employment prohibitions		
Information on debts covered by an enforceable decision	Deducting from wages or salaries	Fulfilling a legal obligation pursuant to Section 24 (2) and Section 75 of Act LIII of 1994 on Judicial Enforcement	Until the limitation period for enforcement claims (5 years)
Photographs and videos of Data Subject	Recording the operation of the Data Controller and its events, reporting on them on the Data Controller's online interfaces and in its publications	The Data Controller's legitimate interest in recording the events it organises and in teambuilding	Until consent is withdrawn

Scope of processed data	Purpose of data processing	Legal basis of data processing	Duration of data processing
Data relating to the registration and use of company car – employee's name, car's registration number, data from the employee's driving licence, data recorded by on-board GPS	Keeping records of the use of company cars, protecting assets and ensuring that the Data Controller only allows the use of company cars by its employees with a valid driving licence	The legitimate interest of the Data Controller in the registration of the use of company cars, the protection of property and the safeguarding of the right to assign the driving of company cars only to employees with a driving licence	Until the end of the employment claims period (3 years)
Data related to the use of the fuel card – company car registration number, name of the employee using the fuel card	Accounting for reimbursement of expenses, checking the use of fuel cards	Fulfilling the employment agreement Legitimate interest in checking the correct use of the fuel card	During the legal retention period for accounting records (8 years)
Personal data related to the use of the parking space (name of the employee, car registration number)	Providing parking lot	The Data Controller has a legitimate interest in the protection of property and in ensuring that the parking lot is used only by those persons who are entitled to use it.	Until the end of the employment claims period (3 years)
Data relating to the criminal record check of workers, for workers for whom it is necessary to check that they are not restricted or excluded from employment by law or by the employer in the position they are applying for (data contained in an Certificate of Good Conduct, proof of criminal record)	Ensuring the protection of property and that the Data Controller employs only persons who meet this condition in positions for which criminal records are required by law or the internal rules of the Data Controller	The legitimate interest of the Data Controller in checking the integrity of the employees assigned to the position	The Data Controller does not store or make a Certificate of Good Conduct, but only checks its content in order to verify the employee's clean criminal record
Personal data required for the fulfilment of the publication obligation pursuant to *Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information* ("**Information Act**") - according to the relevant parts of the general publication list in Annex 1 to this Act (such as: names, titles, contact details of	Fulfilling the publication obligation pursuant to Article 37 (1) (e) of the Information Act	Fulfilment of the legal obligation under Article 37 (1) (e) of the Information Act and Annex 1 of the Information Act	Until the end of the retention periods set out in Annex 1 of the Information Act depending on the type of data published.

Scope of processed data	Purpose of data processing	Legal basis of data processing	Duration of data processing
directors; name and contact details of the account manager; budget support; name of the editor-in-chief of the publications founded by the Data Controller)			
Personal data concerned by a public interest data request under the Data Protection Act and released by the Data Controller to the data requester: the name, scope of duties, job title, managerial mandate, other personal data related to the performance of public duties, or personal data the disclosure of which is required by law, of the person acting in the capacity of the Data Controller.	Fulfilling data requests in the public interest, ensuring compliance with the provisions of the Information Act	Fulfilment of the legal obligation pursuant to Article 26 (1) and (2) (e) of the Information Act	The Data Controller shall keep the personal data for one year from the date of execution or refusal of the public interest data request or, if the Data Controller does not respond to the data request within the time limit for execution of the data request, from the expiry of the time limit for execution, in order to be able to support its legal position in the event of legal claims (the Data Controller also states that it may keep the personal data for other purposes after the retention period)
Where the Data Subject creates and transfers an intellectual work to the Data Controller in performance of a contract with the Data Controller: the personal data content of the notification form as set out in Annex 2 to the Data Controller's Intellectual Property Policy for the Data Subject	Notification of intellectual works to the Data Controller and registration of intellectual works by the Data Controller	The legitimate interest of the Data Controller in keeping a register of intellectual property rights during the term of the employment contract with the Data Subject, and after the termination of the employment contract	For 5 years from the last use of the intellectual work by the Data Controller (e.g. its publication for scientific purposes)

In relation to the above processing, the Data Controller draws attention to the fact that the provision of data by the Data Subject which is **processed on the basis of a legal obligation or on the basis of the preparation or fulfilment of an agreement with the Data Controller,** is mandatory for the establishment of the legal relationship or for the fulfilment of certain obligations arising from the legal

relationship, without the provision of the necessary data the Data Controller is not able to fulfil its obligations undertaken in the legal relationship or required by law.

Regarding the legitimate interest of the Data Controller the Data Controller draws the attention of the Data Subject to the fact that he/she has the right to object to the data processing (for further rules, see point 6.5.). If the data processing is based on legitimate interest and the Data Subject does not provide the data, the failure to provide the data may, in justified cases, be an obstacle in maintaining the legal relationship between the parties.

In the case of processing based on consent the Data Subject shall have the right to refuse or withdraw his/her consent at any time by contacting the Data Controller at the contact details provided above. Withdrawal of consent does not affect the lawfulness of the processing prior to its withdrawal. Refusal or withdrawal of consent shall not have any adverse legal consequences for the Data Subject.

In connection with the above processing, the Data Controller draws your attention to the fact that in connection with most of the above-mentioned data categories, in addition to the above-mentioned processing purposes, processing for the purpose of legal claims may also arise, and the Data Controller has determined the retention periods in the above table with regard to this, the actual longest **retention period.** The legal basis for the processing for the purpose of legal claims is the legitimate interest of the Data Controller to have sufficient evidence to protect its interest in legal claims.

3 RECIPIENTS OF PERSONAL DATA, CATEGORIES OF RECIPIENTS

In some cases, the Data Controller transfers certain personal data to third parties, so-called recipients. These recipients are listed in the following points, with some recipients being considered as processors and others as independent controllers. Processors follow the instructions of the Data Controller and provide services to the Data Controller in connection with the technical process. Independent controllers, however, determine the purposes and means of the processing of personal data and are responsible for their own processing.

3.1 Name or category of data processor

The Data Controller does not use a data processor for the above processing.

3.2 Name or category of independent data controller

Banks
Insurance providers
Cafeteria providers
Auditor
Data subjects with a public interest
Occupational health service providers (occupational doctor)
Government agencies, courts and investigative authorities
National Tax and Customs Administration
Independent bailiffs
Voluntary insurance funds
Accommodation providers, travel agencies
Passenger transport companies (i.e., airlines, bus companies, train companies)

Social security institutions and health and safety authorities
Telecommunications companies providing company equipment
Legal representatives and law firms
Meta Platforms Technologies Ireland Limited (seat: MERRION ROAD, DUBLIN 4, D04 X2K5, IRELAND): operator of Facebook and Instagram
Google Ireland Limited (seat: Gordon House, Barrow Street, Dublin 4, Ireland): operator of Youtube

Google Ireland Limited acts as an independent data controller in the case of the content uploaded to YouTube. For further information on Google's data processing practices, please visit the following website: https://policies.google.com/privacy?hl=en

Meta acts as an independent data controller in the case of the content posted on the social networking sites Instagram and Facebook. For further information on Meta's data processing activities, please visit the following websites:

- Facebook: https://m.facebook.com/privacy/policy/version/20220104
- Instagram: https://help.instagram.com/155833707900388

In addition to the above, the Data Controller may receive certain information about the Data Subject from a third party rather than directly from the Data Subject. This will be done when the occupational health service provider sends the results of the occupational health assessment to the Data Controller or when a final court order is received. In any case, the Data Controller shall endeavour not to transfer personal data to or make personal data available to a recipient outside the European Economic Area (so-called third country). If this should nevertheless be necessary, the Data Controller shall ensure that an appropriate safeguard mechanism applicable to data transfers outside the European Economic Area is in place in relation to the transfer.

4 TREATMENT OF SENSITIVE DATA

The Data Controller also processes sensitive personal data (i.e., data relating to health condition) as explained in point 2.

The Data Controller is entitled to process these sensitive data

- partly based on Article 9(2)(h) of the GDPR, in view of the fact that the processing is necessary for occupational health purposes, to assess the employee's ability to work, to provide social care, subject to the obligation of professional confidentiality of the occupational health professional employed by the employer as a guarantee condition, based on the legislation applicable to the employment relationship (in particular the occupational health and safety regulations);
- partly based on Article 9(2)(b) of the GDPR, given that the processing is necessary for the fulfilment of its obligations arising from the legal provisions governing employment and social security and protection, to the extent permitted by law,
- based on Article 9(2)(f) of the GDPR in the context of the processing of sensitive data relating to legal claims, on the grounds that the processing is necessary for the establishment, exercise or defence of legal claims.

5 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 1. All questions, complaints and requests will be investigated individually and

answered within one month of receipt at the latest, in accordance with Article 12 of the GDPR. 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 may request from the Data Controller access to personal data concerning him/her, rectification, erasure, and in certain cases restriction of processing, object to the processing of personal data and the right to data portability. The Data Subject also has the right to lodge a complaint with a supervisory authority, the right to a judicial remedy and, in the case of processing based on consent, the right to withdraw consent at any time. These rights are explained in detail below.

5.1 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.

5.2 Right to rectification

The Data Controller shall correct or supplement personal data concerning the Data Subject at the Data Subject's request. 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.

5.3 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 processing was based on the Data Subject's consent, but the Data Subject has withdrawn that consent and there is no other legal basis for the processing;
- the processing was based on a legitimate interest of the Data Controller or a third party, but 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.

5.4 Right to restriction of data processing

Restriction of data 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.

5.5 Right to objection

Where the legal basis for the processing of data relating to the Data Subject is the legitimate interest of the Data Controller or a third party, the Data Subject shall have 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.

5.6 Right to data portability

The Data Subject shall have the right to request the Data Controller to provide personal data which he/she has provided to the Data Controller based on the consent or on a contractual legal basis and which are processed by the Data Controller by automated means (i.e., in a computer system), either in a structured format for the purpose of transfer to another controller or, if technically feasible, directly to another controller designated by the Data Subject upon his/her request. 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.

5.7 Right to complain, right to redress

If the Data Subject believes that the Data Controller's processing of personal data is in breach of applicable data protection laws, in particular GDPR, the Data Subject has the right to lodge a complaint with the competent data protection supervisory authority of the Member State where his/her habitual residence, place of work or place of the alleged infringement. In Hungary, you can contact the National Authority for Data Protection and Freedom of Information **(NAIH).** Contact details of the NAIH:

Website: http://naih.hu/
Address: 1055 Budapest, Falk Miksa utca 9-11
Postal address: 1363 Budapest, PO Box: 9.
Phone: +36-1-391-1400
Fax: +36-1-391-1410
Email: ugyfelszolgalat@naih.hu

Irrespective of his/her right to lodge a complaint, Data Subject can also go to court if this/her rights are infringed. 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.

6 AUTOMATED DECISION-MAKING, PROFILING

No automated decision-making or profiling is carried out in the course of the Data Controller's processing of the data subject.

7 INFORMATION TO OTHER DATA SUBJECTS

The Data Controller shall consider the Data Subject as the representative of the relative or third party in the case of providing personal data of relatives or other third parties, unless proven otherwise. In this regard, the Data Controller informs the Data Subject's relatives or third parties about the processing of their personal data through the Data Subject as representative in accordance with the provisions of this Privacy Notice.

8 DATA SECURITY

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 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.

* * *

Applicable from: 4 February 2025

Dr. Heinerné Dr. Barzó Tímea Tünde
Director-General