CENTRAL EUROPEAN ACADEMY

Data Protection and Data Security Policy

Effective: March 1, 2025.
Version: 2.0

Version		Name	Provisions affected by the amendment	Date
1.0	Created by:	Dr. Beraczkai Dávid	-	May 31, 2023.
2.0	Created by:	Réti, Várszegi és Társai Ügyvédi Iroda (PwC Legal) Dr. Csenterics András lawyer	drafting new rules	December 10, 2024.
2.0	Reviewed by:	dr. Osváth Ildikó Legal Director, Central European Academy	-	February 12, 2025.
2.0	Approved by:	Dr. Heinerné Prof. Dr. Barzó Tímea Tünde Director General, Central European Academy	-	February 14, 2025.

1. GENERAL PROVISIONS AND PURPOSE OF THE POLICY

1.1. The **Central European Academy** (registered office: 1122 Budapest, Városmajor utca 12-14., registration number at Oktatási Hivatal (Educational Authority): FNYF/419-4/2023, tax number: 19359711-1-43), as data controller (**"Data Controller"**), establishes the following Data Protection and Data Security Policy (hereinafter referred to as "**Policy**") based on *Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data* (General Data Protection Regulation, hereinafter referred to as "**GDPR**") and *Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information* (hereinafter referred to "**Infotv.**") to regulate its internal processes and procedures related to data processing and to ensure legality.

1.2 This Policy serves to facilitate the Data Controller's compliance with data protection laws. The purpose of the Policy is to establish uniform rules for all data processing activities conducted by the Data Controller and to set forth requirements that ensure the continuous legality of the Data Controller's data processing operations. Another goal is to increase data protection awareness within the Data Controller's organization and to minimize the risks and violations arising from human error.

1.3 Considering the above, this Policy particularly covers the following areas:

- Enforcement of data processing principles as per Article 5 of the GDPR;
- Correct determination of legal bases and purposes of data processing;
- Ensuring the exercise of data subjects' rights;
- procedure for processing special categories of data;
- data transfers;
- legal relationships with data processors;
- legitimate interests balancing tests and data protection impact assessments;
- management of personal data breaches;
- technical background of data processing.

1.4 However, the Policy does not aim to inform any group of data subjects, nor does it aim to replace any legitimate interest test or impact assessment documentation. These functions are fulfilled by other data protection-related documents of the Data Controller.

1.5 The personal scope of the Policy extends to all individuals who, based on their employment, data processor-, and/or contractual relationship with the Data Controller, have access to or come into possession of personal data processed by the Data Controller (hereinafter collectively referred to as „**employees**"). The Data Controller recognizes that one of the most significant risks in any data processing is the human factor. Therefore, the Data Controller places great importance on ensuring that all employees who come into contact with personal data processed by the Data Controller are aware of the basic rules of data protection and data security.

1.6 Familiarity with and adherence to the Policy is mandatory for all employees of the Data Controller.

1.7 This Policy is classified as an internal document of the Data Controller, and it is forbidden to disclose it to the public or share it in any way outside the scope of individuals to whom it applies.

1.8 In case an employee of the Data Controller violates the Policy and causes damage, they are liable for the damage according to the rules applicable to breaches of obligations arising from their employment.

1.9 If a person in another legal relationship with the Data Controller violates the Policy and causes damage, *the rules on liability for damage in Act V of 2013 on the Civil Code* (hereinafter: „**Civil Code**"), as well as other liability rules contained in the contract with the Data Controller, apply.

1.10 The material scope of the Policy extends to all processes at the Data Controller where personal data, as defined in Article 4 (1) of the GDPR, is processed.

1.11 The interpretation, application, and execution of the provisions in this Policy are governed by the GDPR and the provisions of the Infotv.

1.12 If it is not clear whether certain data qualifies as personal data or special categories of personal data, it should be treated as if it possesses such a quality/characteristic until an internal decision is made on the matter. The classification of data as personal data or special categories of personal data is decided by the Director General of the Data Controller, considering the opinion and recommendation of the employee responsible for data protection compliance and the data protection officer.

2. INTERPRETATIVE PROVISIONS

- **Data Subject**: an identified or identifiable natural person;
- **Personal Data:** any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
- **Data processing:** any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
- **Profiling:** any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;
- **Pseudonymization:** processing personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;
- **Filing system:** any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;
- **Controller:** the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;
- **Processor:** a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

- **Third party:** a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;
- **Consent of the data subject:** any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;
- **Personal data breach:** a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;
- **Data processing:** performing technical tasks related to data processing operations, regardless of the method and tool used for executing the operations, as well as the location of the application, provided that the technical task is performed on the data;
- **Data Transfer:** making data available to a specified third party;
- **Anonymization:** rendering data unrecognizable in such a way that its restoration is no longer possible;
- **NAIH**: National Authority for Data Protection and Freedom of Information

3. PRINCIPLES OF DATA PROCESSING CONDUCTED BY THE DATA CONTROLLER

3.1. The Data Controller organizes all its data processing activities according to the principles set out in the GDPR, acting as follows:

3.1.1. **Lawfulness, Fairness and Transparency [GDPR Article 5 (1) point a)]:** The Data Controller processes personal data lawfully and fairly, in a transparent manner for the data subject, primarily by publishing and continuously making available the data processing information document prepared for the specific data processing activities. The Data Controller maintains a dedicated contact point for data subjects, responding to all data subject inquiries, complaints, and comments within the GDPR deadlines in a personalized manner.

3.1.2. **Purpose limitation [GDPR Article 5(1)(b)]:** The Data Controller collects personal data only for specified, explicit, and legitimate purposes and does not process them in a manner that is incompatible with those purposes. The Data Controller defines only those purposes that are relevant and sufficiently specific for its operations. The Data Controller does not process personal data for future, uncertain, or insufficiently defined purposes. Once the purpose of data processing is fulfilled and no legal obligation requires further processing, or it is not necessary or lawful for another data processing purpose, the Data Controller deletes the personal data.

3.1.3. **Data minimisation [GDPR Article 5(1)(c)]:** The personal data processed by the Data Controller must be adequate and relevant from the perspective of the purposes of data processing and must be limited to what is necessary.

3.1.4. **Accuracy [GDPR Article 5(1)(d)]:** The personal data processed by the Data Controller must be accurate and, where necessary, kept up to date; the Data Controller must take every reasonable step to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay. However, the Data Controller conducts several data processing activities where rectification is not possible without the proactive behaviour of the data subject, as the Data Controller would not otherwise be aware of the data change (e.g., change of contact person in a contractual relationship), or

the rectification of the data is conceptually excluded (e.g., already recorded security camera footage). The Data Controller draws the attention of data subjects to this aspect in the relevant data processing information.

3.1.5. **Storage limitation [GDPR Article 5(1)(e)]:** The Data Controller stores personal data in a form that permits identification of data subjects only for as long as necessary for the purposes for which the personal data are processed. However, the Data Controller may retain personal data beyond the original purpose of data processing to comply with a legal obligation (e.g., retention of former employees' data for five years after reaching the retirement age based on the Pension Act) or if a legitimate interest can be demonstrated on the part of the Data Controller that lawfully allows for a longer retention period (e.g., retention of certain personal data for the five-year civil law limitation period for use in potential legal disputes). The Data Controller always considers the circumstances justifying the longer retention as a new, separate data processing purpose and adjusts its data processing information accordingly.

3.1.6. **Integrity and Confidentiality [GDPR Article 5(1)(f)]:** The Data Controller processes personal data in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical and organizational measures. This includes physical security and the supporting camera system, keeping the Data Controller's IT infrastructure up to date, employing suppliers with adequate IT and data protection legal preparedness and infrastructure, and engaging professional legal services for daily data protection legal support.

3.1.7. **Accountability [GDPR Article 5(2)]**: The Data Controller designs and implements its data processing activities in a way that it can demonstrate compliance with data protection principles at any time. The primary tool for this is the Data Controller's existing and up-to-date data protection documentation.

4. RIGHTS OF THE DATA SUBJECTS AND THEIR ENFORCEMENT

4.1. During data processing, the Data Controller ensures the exercise of the following GDPR rights for the data subjects, depending on the legal basis:

	Applied Legal Basis (GDPR Article 6(1))				
Data Subject Right	a) consent	b) contract	c) legal obligation	d) vital interest	f) legitimate interest
information	yes	yes	yes	yes	yes
access	yes	yes	yes	yes	yes
rectification	yes	yes	yes	yes	yes
erasure	yes	yes	yes	yes	yes
withdrawal	yes	no	no	no	no
restriction	yes	yes	yes	yes	yes
objection	no	no	no	no	yes
data portability	yes	yes	no	no	no

4.2. Right to information

4.2.1. If the Data Controller obtains personal data directly from the data subject, it informs the data subject at the time of data collection about the following:

a) the exact name and contact details of the Data Controller;
b) the contact details of the Data Controller's data protection officer,
c) the purpose of data processing;
d) the legal basis for data processing;
e) if the data processing is based on the legitimate interests of the Data Controller or a third party, the legitimate interest of the Data Controller or the third party;
f) if the Data Controller transfers personal data to a third party during data processing, the recipients of the personal data or the categories of recipients;
g) the duration of personal data storage or, if this is not possible, the criteria for determining this duration;
h) the data subject's right to request access to, rectification, erasure, or restriction of processing of personal data concerning them, and to object to the processing of such personal data, as well as the right to data portability;
i) the rules for exercising the right to withdraw consent if the legal basis for data processing is the data subject's consent [GDPR Article 6(1)(a)] or the legal basis specified in GDPR Article 9(2)(a);
j) the right to lodge a complaint with the NAIH;
k) whether the provision of personal data is a statutory or contractual requirement or a requirement necessary to enter into a contract, and whether the data subject is obliged to provide the personal data and the possible consequences of failure to provide such data;
l) The existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject..

4.2.2. If the data controller does not obtain the personal data directly from the data subject, they will inform the data subject about the following:

a) the exact name and contact details of the Data Controller;
b) the contact details of the Data Protection Officer;
c) the purpose of the intended processing of personal data, as well as the legal basis for processing;
d) the categories of personal data processed;
e) the source of the personal data;
f) if the collection of data from a third source is required by law, the specific legal provision;
g) the time of obtaining the personal data by the Data Controller;
h) if the personal data is necessary for a case conducted by the Data Controller, the specific case number or other identifier;;
i) whether the personal data originates from a publicly accessible source;
j) the recipients of personal data, or the categories of recipients, if applicable;
k) the duration of storage of personal data, or if this is not possible, the criteria for determining this duration;
l) if the data processing is based on Article 6(1)(f), the legitimate interests of the Data Controller or a third party;
m) the data subject's right to request access to, rectification, erasure, or restriction of processing of personal data concerning them, and to object to the processing of such personal data, as well as the right to data portability;

n) in the case of data processing based on Article 6(1)(a) or Article 9(2)(a), the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
o) the right to lodge a complaint with the NAIH;
p) the existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

4.2.3. If the Data Controller does not obtain the data directly from the data subject during data processing, the data subject will be informed at the following time:

- within a reasonable period after obtaining the personal data, but at least within one month;
- if the Data Controller uses the personal data for the purpose of contacting or communicating with the data subject, upon the first contact with the data subject, or
- if the Data Controller is expected to disclose the data to another recipient, no later than the first time of such disclosure.

4.2.4. If the Data Controller does not obtain the personal data directly from the data subject, there is no requirement to inform the data subject if

- the data subject already possesses the aforementioned information;
- providing the information proves impossible or would involve disproportionately great effort;
- the acquisition or disclosure of data is expressly mandated by the applicable EU or current Hungarian law to which the Data Controller, which also includes provisions for appropriate measures to protect the legitimate interests of the data subject, or
- personal data must remain confidential under a professional secrecy obligation prescribed by EU or current Hungarian law.

4.2.5. The Data Controller primarily provides information to the data subjects through its data processing information notices. These notices are prepared by the Data Controller whenever it is required to inform the subject about data processing. The rules for the publication of the notice:

a) in every case, the information must be made available to the data subject before data processing begins, or, if this is impossible, it must be provided to the data subject at the earliest possible time;
b) in every process where data is collected on paper, the relevant information must be accessible at the place of data collection;
c) in every process where data is collected via a technical device, the information must be accessible through the technical device;
d) in every instance where the data subject consents to data processing through implied conduct, the information and process description must be accessible at the place or platform where the implied conduct is performed, allowing the data subject to consent with full awareness;
e) if it can be assumed that the data subject will initiate the data processing themselves, the information and process descriptions of these data processing must be available on the Data Controller's website for the data subject's prior information;
f) the information and process descriptions must be published in such a way that the Data Controller can always prove that the data subject could get informed of them before the start of data processing, especially in the case

of online data collection, a so-called "check box" must be used to obtain the declaration from the data subject that they have understood and accepted the rules of data processing.

4.3. Right of access:

4.3.1. If the data subject wishes to exercise their right of access according to Article 15 of the GDPR, the Data Controller will inform the data subject of the following:

a) the purpose(s) of the data processing;
b) the categories of personal data concerned;
c) the recipients or categories of recipients to whom or with whom the personal data have been or will be disclosed, including recipients in third countries and international organizations;
d) the envisaged period of the storage of personal data, or if this is not possible, the criteria for determining that period;
e) the right of the data subject to request from the controller rectification, erasure, or restriction of processing of personal data concerning them, and the right to object to such data processing;
f) the right to lodge a complaint with the NAIH;
g) if the personal data is not collected from the data subject, all available information regarding their source;
h) the existence of automated decision-making, including profiling, along with a brief, understandable description of how automated decision-making and profiling are conducted based on what data and parameters are concerned, the results produced (e.g., the outcome of a software evaluation of a job application or the content of a customized newsletter sent to the user based on their activity on the organization's website), what methodology is used to produce them, and the understandable information about what significance such data processing has for the data subject and what expected consequences it entails.

4.3.2. The data subject is also entitled to have the Data Controller provide them with a copy of the personal data undergoing processing. The Data Controller may charge a reasonable fee for any additional copies requested by the data subject. If the data subject submitted their request electronically, the information must be provided in a widely used electronic format, unless the data subject requests otherwise.

4.3.3. The right to request a copy, however, must not adversely affect the rights and freedoms of others.

4.4. Right to rectification:

4.4.1. The data subject has the right to obtain from the Data Controller without undue delay the rectification of inaccurate personal data concerning them. or request their completion.

4.4.2. If the data subject requests the rectification of their personal data and the personal data to be rectified is not available, the Data Controller shall request the data subject to provide the missing data.

4.4.3. If the data subject requests the rectification of their personal data and the personal data is available, the Data Controller will correct the personal data and simultaneously notify the data subject in writing about the fact and date of the completed rectification.

4.4.4. If the data subject requests the rectification of personal data in relation to a data processing operation where rectification is technically impossible (e.g., recorded camera footage), the Data Controller will inform the data subject accordingly.

4.5. Right to erasure („Right to be forgotten"):

4.5.1. The data subject has the right to obtain from the Data Controller the erasure of personal data concerning them without undue delay, and the Data Controller is obliged to delete that personal data if any of the following reasons exist:

a) the personal data is no longer needed for the purpose for which the Data Controller collected or otherwise processed it;
b) the data subject withdraws their consent on which the processing is legally based, and there is no other basis for the processing;
c) the data subject objects to the processing and there is no overriding legitimate ground for processing;
d) the Data Controller processed the personal data unlawfully;
e) the personal data must be erased to comply with a legal obligation in EU or Hungarian law applicable to the Data Controller;
f) personal data was collected in relation to the offer of information society services referred to in Article 8(1) of the GDPR.

4.5.2. If the Data Controller has made the personal data public and the personal data are no longer needed for the purpose for which it was collected or otherwise processed, the Data Controller is obligated to erase them.

4.5.3. Personal data cannot be erased even at the request of the data subject in cases of data processing specified in Article 17(3) of the GDPR.

4.5.4. The Data Controller erases personal data in such a way that it can no longer be restored.

4.5.5. If personal data cannot be erased from the data carrier containing the personal data, the Data Controller is obliged to destroy the aforementioned data carrier.

4.5.6. If the data subject wishes to have such personal data erased, where the absence of the data would make it impossible to maintain the legal relationship between the data subject and the Data Controller, the Data Controller informs the data subject of this circumstance before the erasure. If the data subject maintains their request for erasure, it is carried out. The request for erasure is considered maintained if the data subject does not withdraw their request within 5 days from the receipt of the notification.

4.6. Right to restriction of processing:

4.6.1. The data subject has the right to request the restriction of the processing of their personal data. In this case, the Data Controller will mark the personal data concerned, which, except for storage, can only be processed with the data subject's consent, or for the establishment, exercise, or defense of legal claims, or for the protection of the rights of another natural or legal person, or for important public interest of the EU or of a Member State.

4.6.2. The Data Controller will restrict data processing at the request of the data subject if at least one of the following conditions is met:

a) the data subject disputes the accuracy of the personal data, in which case the restriction applies for a period enabling the Data Controller to verify the accuracy of the personal data;
b) the processing is unlawful, and the data subject opposes the erasure of the data and requests the restriction of their use instead;

c) the Data Controller no longer needs the personal data for processing purposes, but the data subject requires them for the establishment, exercise or defence of legal claims, or

d) the data subject has objected to the processing, in which case the restriction applies until it is determined whether the Data Controller's legitimate grounds override those of the data subject.

4.6.3. If the restriction of processing is lifted by the Data Controller, the Data Controller informs the data subject in writing about the lifting of the restriction at least three (3) working days before its execution.

4.6.4. The Data Controller informs all recipients of any correction, erasure, or restriction of data processing with whom the personal data has been shared, except if this proves impossible or requires disproportionate effort. Upon the request of the data subject, the Data Controller informs the data subject about these recipients.

4.7. Right to object:

4.7.1. The data subject has the right to object at any time, on grounds relating to their particular situation, to the processing of their personal data based on the legitimate interests of the Data Controller or a third party.

4.7.2. In the event of an objection by the data subject, the Data Controller examines whether there are compelling legitimate grounds for the processing that override the interests, rights, and freedoms of the data subject, or that relate to the establishment, exercise, or defence of legal claims.

4.7.3. If the Data Controller determines during its investigation that the data processing is not justified by compelling legitimate reasons that override the interests, rights, and freedoms of the data subject, or that relate to the establishment, exercise, or defence of legal claims, the personal data concerned by the objection will be erased.

4.7.4. In connection with the investigation mentioned in the previous two points, the burden of proof lies with the Data Controller.

4.8. Right to data portability:

4.8.1. If the processing is based on the data subject's consent or the performance of a contract to which the data subject is a party, the data subject has the right to receive the personal data they have provided to the Data Controller in a structured, commonly used, and machine-readable format, and has the right to transmit those data to another data controller without hindrance from the Data Controller, where it is technically feasible.

4.8.2. The Data Controller primarily ensures compliance with the above by fulfilling requests in *.xml, .csv, .txt, .xls .pdf* or *.doc* file formats, depending on the nature of the personal data concerned.

4.8.3. This right does not apply to the data subject if it would adversely affect the rights and freedoms of others.

4.9. Right to withdraw consent:

4.9.1. If the legal basis for data processing is the consent of the data subject, the data subject has the right to withdraw their consent at any time. Withdrawal of consent does not affect the legality of data processing based on consent prior to its withdrawal. The data subject must be informed of this before giving consent. The withdrawal of consent must be as easy to perform as giving it was.

4.9.2. If the data subject withdraws consent given to the Data Controller for the processing of their personal data, the Data Controller may not be able to fully or partially provide the requested services or maintain the legal relationship with the data subject. The Data Controller will inform the data subject of this fact. If the data subject maintains their request to withdraw consent despite this information, the Data Controller will erase the personal data processed based on the consent, unless it is entitled to process the data on another legal basis. It is considered to be a request to maintain the withdrawal of consent if the data subject does not withdraw their request within 5 days of receiving the information.

4.10. Right to appeal to supervisory authority and courts

4.10.1. The data subject may lodge a complaint with the NAIH regarding the Data Controller's data processing procedures based on Article 77(1) of the GDPR.

4.10.2. Under Article 79(1) of the GDPR, the data subject may seek judicial remedy for a violation of their rights related to the Data Controller's data processing procedures before the competent court („Törvényszék"; Regional Court) based on their place of residence or habitual residence.

4.11. Exercise of data subject rights

4.11.1. For data subjects to exercise their rights guaranteed by the GDPR, the Data Controller sets out the obligations and procedural rules related to the exercise of data subject rights in this section.

4.11.2. The Data Controller strives to ensure that the information provided to the data subject is concise, transparent, intelligible, easily accessible, clear, and plain.

4.11.3. The Data Controller provides information to the data subject in writing, including in electronic form, as a general rule.

4.11.4. The data subject may exercise their rights under the GDPR in writing, including electronically (via email or contact form on the website), or orally.

4.11.5. The Data Controller provides information to the data subject only if an authorized employee of the Data Controller has verified the identity of the data subject.

4.11.6. Verification of the data subject's identity includes:

a) in the case of an oral request: if the data subject proves their identity by presenting a document suitable for identity verification under current Hungarian law, or a document suitable for identity verification under European Union law;

b) in the case of an electronically submitted request: if the request comes from an email address associated with the data subject and already known to the Data Controller;

c) in the case of a request submitted in writing by other means: the request itself contains the personal identification data of the data subject already known to the Data Controller;

d) The request of the data subject arrives through a secure channel provided by the Data Controller, usable after proper identification.

4.11.7. The Data Controller, during the providing of information referred to in the previous point, does not accept any form of identification conducted via telephone.

4.11.8. If identification is not verified as described above, the Data Controller rejects the data subject's exercise of rights request and informs the data subject how they can exercise their rights in accordance with the Policy.

4.11.9. The Data Controller informs the data subject in writing of the measures taken regarding their request to exercise rights within one month of receiving the request.

4.11.10. Receipt is considered to occur when the request is:

a) made orally, in person, to the Data Controller's designated representative following identity verification;
b) The written request arrives at the Data Controller's contact address.

4.11.11. The one-month deadline may be extended by the Data Controller by a maximum of two additional months if the complexity of the request or the number of requests currently being processed justifies it.

4.11.12. The Data Controller informs the data subject of the extension of the deadline and the reasons behind the delay within one month of receiving the request.

4.11.13. If the Data Controller does not act on the data subject's request, the data subject may exercise their right to legal remedy against the Data Controller.

4.11.14. The Data Controller carries out the measures requested by the data subject free of charge. However, if the data subject's request is manifestly unfounded or excessive, particularly due to its repetitive nature, the Data Controller may charge a fee for the administrative costs of providing the information or fulfilling the request or may refuse to act on the request. A written record must be made of the reasons for considering the request manifestly unfounded or excessive.

4.11.15. The fulfilment of data subject rights is the responsibility of the Data Controller's legal director or an operational employee designated by them. The heads of the relevant departments and the Data Controller's data protection officer are obliged to cooperate in fulfilling data subject rights.

4.11.16. The department/organizational unit with relevant data for fulfilling data subject rights must provide all information and data in writing to fulfil the request in cooperation with the data protection officer.

4.11.17. If the data subject's request necessitates changes to the Data Controller's internal data processing procedures/records, the employee responsible for data protection compliance (see point 5.2.1) must carry out this task with the involvement or through the data protection officer.

4.11.18. Fulfilling the data subject's request under GDPR, as well as providing information to the data subject, is not possible without the prior involvement of the data protection officer.

5. THE DATA CONTROLLER'S DATA PROTECTION FRAMEWORK

5.1. The Data Controller has contracted the law firm Réti, Várszegi and Partners for carrying out the tasks of the data protection officer. The law firm has a team of experts specifically dedicated to the matters of the Data Controller, possessing expertise in all legal areas relevant to the Data Controller's data protection compliance (such as data protection and data security law, labour law, IT contract law, procurement law, intellectual property law). Several lawyers from the firm are continuously available for consultation to the Data Controller, and the coordination of the activities provided is managed by the law firm member responsible for the legal services provided to the Data Controller.

5.2. The Data Controller's data protection system is structured as follows:

5.2.1. The Data Controller's Director General appoints the person responsible for data protection compliance within the organizational system of the Data Controller ("person responsible for data protection compliance");

5.2.2. Leaders of specific operational areas/organizational units of the Data Controller ("Heads of Organizational Units") are in direct contact with both the person responsible for data protection compliance and the data protection officer;

5.2.3. The heads of organizational units or the person responsible for data protection compliance notify the data protection officer of all matters and questions with data

protection relevance (especially regarding changes affecting existing data processing or any new process involving data processing) and seek their opinion;

5.2.4. Communication with the data protection officer is conducted via telephone and email;

5.2.5. Following consultation with the data protection officer, the Director General of the Data Controller makes decisions on further steps, and the data protection officer begins to establish data protection compliance. This primarily involves preparing documentation, modifying existing documentation, preparing summaries for the operational and contact staff coordinating the steps, and providing targeted training and consultation for the staff involved in the process, as well as making further recommendations if necessary;

5.2.6. In line with the principle of data protection by design and data protection by default, actual data processing only begins after the steps outlined in the previous points have been verifiably completed;

5.2.7. Depending on the case, considering the severity of the relevant risks or the urgency of the matter, the data protection officer consults directly with the Director General of the Data Controller about the necessary measures.

5.3. The Data Controller's Director General primarily oversees all data processing activities. Within the internal organizational structure of the Data Controller, the person responsible for data protection compliance and the legal director assist in this task, along with the external data protection officer.

5.4. To ensure the predictability of work, the data protection officer prepares an annual audit plan, which is documented in writing. This takes into account which data processing activities of the Data Controller are of the greatest significance, either due to the nature of the data processed or the number of data subjects. During the audit plan, the data protection officer identifies potential risks requiring action, practices needing correction, and provides training to the staff involved in the process if necessary.

5.5. In the case of tasks falling into priority category 1 or 2 as per the following point, the data protection officer immediately suspends activities as per the annual inspection plan and promptly focuses available resources on the priority tasks.

5.6. During their activities, the data protection officer categorizes relevant events into the following priority categories:

- Priority category 1:
  - management of personal data breaches;
  - responding to complaints, questions and inquiries from data subjects;
  - responding to inquiries from the NAIH;
  - cases requiring immediate and urgent instructions to any of the data processors.
- Priority category 2: Urgent, ad-hoc projects requiring immediate action, such as introducing a new function on the website, new data processing related to regular events, steps related to the introduction of an operational process, the use of a new data processor, or changes in existing data processing.;
- 3rd priority category: Long-term tasks defined in the annual audit plan, such as the conceptual preparation of a planned data processing, preparation of related documentation, conducting data protection impact assessments, reviewing previously prepared documentation, etc. Additionally, any event falling into the 1st or 2nd priority categories may result in tasks falling into the 3rd priority category (e.g., addressing a systemic deficiency identified based on a data subject's complaint through internal training).

5.7. The foundation of the Data Controller's data protection system is the daily work of those employees who access and work with personal data in the process. The employees ensure that unauthorized persons cannot view the personal data processed by the Data Controller or perform any other unauthorized operations on it.

5.8. The Data Controller publishes the contact details of the data protection officer in all its data processing information documents and notifies the NAIH about the data protection officer.

5.9. The Data Controller ensures that the email address specifically for receiving complaints related to data protection (adatvedelem@centraleuropeanacademy.hu) automatically forwards incoming complaints to the email address dedicated to the data protection officer (hu_central_european_academy@pwc.com). In this way, it is ensured that the data protection officer is promptly informed of any subject communication requiring their action.

5.10. The Data Controller provides the data protection officer with the necessary resources to perform their tasks and pays them a fee based on the service contract. It also ensures that the data protection officer enjoys complete independence in forming their professional opinion as guaranteed by *Act LXXVIII of 2017 on attorneys at law*, considering that the data protection officer performs their tasks as a law firm.

5.11. The main data protection-related duties of the Data Controller's Director General:

5.11.1. responsible for ensuring the conditions necessary for the exercise of data subjects' rights as defined in the GDPR;

5.11.2. responsible for ensuring the personal, material, and technical conditions necessary for the protection of personal data processed by the Data Controller;

5.11.3. responsible for addressing any deficiencies or legal violations potentially uncovered during data processing-related audits, initiating and conducting procedures necessary for establishing personal responsibility;

5.11.4. oversees the activities of the data protection officer;

5.11.5. may order an investigation;

5.11.6. approves and announces the internal rules related to data protection of the Data Controller;

5.11.7. appoints the person responsible for the data protection compliance of the Data Controller.

5.12. Data protection-related responsibilities of the heads of organizational units:

5.12.1. responsible for data protection compliance of the processes under their control;

5.12.2. consult with the data protection officer or the person responsible for data protection compliance;

5.12.3. report any personal data breaches, other data protection violations, or suspicions thereof immediately to the data protection officer or the person responsible for data protection compliance;

5.12.4. if data processing activities in their area expand or existing processes change, they immediately inform the data protection officer or the person responsible for data protection compliance to coordinate the necessary steps.

5.13. The person responsible for data protection compliance is responsible for the following tasks:

5.13.1. overseeing the data processing activities conducted by the Controller;

5.13.2. initiating consultations with the data protection officer before starting any activities involving the processing of personal data or in the event of changes of such activities;

5.13.3. if necessary, consulting with the Director General of the Data Controller on matters related to personal data processing;

5.13.4. informs the Director General of the Data Controller of any known data processing-related violations, breaches, incidents, or suspicions thereof immediately, precisely meaning immediately after detection;
5.13.5. participates in and oversees information security, data security checks, and related audits;
5.13.6. notifies the data protection officer of received notifications, data subject complaints, and the exercise of rights, and provides the data protection officer with the information/documents requested to respond to/fulfil notifications, data subject complaints, and the exercise of rights;
5.13.7. participates in the further development and operation of procedures for managing personal data breaches;
5.13.8. maintains contact with external authorities and organizations on data protection issues, provides them with necessary information, and cooperates with the authorities and organizations conducting investigations in case of external audits;
5.13.9. manages and, with the involvement of the data protection officer, keeps the data protection and personal data breach registers up to date.

5.14. If the completion of a task defined in the previous section involves multiple persons responsible for data protection compliance, the Director General may designate a specific person among them to be responsible for completing the task or specify the tasks to be performed by the designated person. In the absence of a designation, persons responsible for data protection compliance are collectively required to take action to fulfil tasks within their scope of authority.

5.15. In addition to the tasks outlined in Article 39 of the GDPR, the data protection officer performs the following duties:
5.15.1. conducting necessary consultations with the Data Controller's person responsible for data protection compliance, legal director, and Director General on all data protection-related matters;
5.15.2. monitoring the Data Controller's data processing operations;
5.15.3. examining data protection compliance in all operations involving data processing, preparing the relevant documentation, and reviewing existing documentation;
5.15.4. developing substantial content when responding to data subject complaints and inquiries;
5.15.5. conducting legitimate interests balancing tests, data protection impact assessments and procedures in case of personal data breaches;
5.15.6. executing the annual audit plan;
5.15.7. providing data protection and data security training for employees if needed or requested;
5.15.8. examination of the data protection aspects of contractual relationships established with individual contractual partners, ensuring legality, including in particular the preparation of data processing agreements and conducting consultations with partners;

5.16. Any circumstances indicating that a person in a contractual relationship with the Data Controller is not complying with the legal provisions related to data processing must be immediately reported to the director-general. In such cases, the performance of the contract must be suspended until the legality of the data processing is restored, in such a way that employees, partners, and data subjects do not suffer damage, or the reduction in the level of services provided by the Data Controller is as minimally perceptible to them as possible.

5.17. All employees of the Data Controller must adhere to the following practical rules regarding the processing of personal data:

5.17.1. during work, only personal data that is absolutely necessary for that purpose can be processed and transferred, and it is the responsibility of the head of the organizational unit performing the task to design the workflows accordingly (avoiding unnecessary data collection or „stockpiling of data");

5.17.2. When granting IT permissions, it must be ensured that only the person who needs the data for their work and only for as long as necessary has access to personal data;

5.17.3. paper-based documents containing personal data can only be forwarded in a sealed envelope or in a sealed device suitable for document transfer;

5.17.4. documents containing a large amount of personal data, special categories of personal data, or personal data of minors must not be forwarded via email. If an employee needs to send such a document, record, etc. to another person electronically, the sender is obliged to upload it to the Data Controller's own file server or another secure storage and send the method of access (link) to the document, and additionally arrange for specific access rights to be granted to the person authorized to access personal or sensitive data;

5.17.5. documents containing personal data may only be stored on shared drives used by organizational units if it is ensured that only authorized persons can access them. In the case of shared drives, the leader of the organizational unit responsible for the drive is accountable for the obligations stated in this section.

5.17.6. employees are required to promptly report any violation of data processing rules to the Director General or the person responsible for data protection compliance upon detection.

6. LAWFULNESS OF DATA PROCESSING, POSSIBLE LEGAL BASES

6.1. The Data Controller processes personal data solely based on one of the legal grounds specified in Article 6 of the GDPR - and in the case of special categories of personal data, considering the exceptions outlined in Article 9 (2). The Data Controller determines the legal basis for data processing before commencing any data processing, considering the nature of the data, the nature of the intended data processing, and the characteristics of the data subjects, while also adhering to the guidelines of the European Data Protection Board (EDPB) and the NAIH.

6.2. The Data Controller processes personal data solely on one of the following legal bases:

6.2.1. the **explicit and voluntary consent of the data subject**: this legal basis is primarily applied by the Data Controller in cases where data processing is not strictly necessary (such as the use of certain optional cookies running on the website, or when requesting certain preferences related to events). In the context of processing employee data, the Data Controller only conducts data processing based on employee consent in unique cases and with special care, provided that voluntariness can be ensured without doubt, considering the characteristics of the employment relationship;

6.2.2. the **performance or preparation of a contract concluded with the data subject**: the Data Controller primarily processes the personal data of employees and natural person partners of the Data Controller based on this legal basis. When determining the contractual legal basis, the Data Controller adheres to the decision of NAIH/2020/5552, which states that the contractual legal basis cannot be broadly applied to every data processing related in some way to the contract. Therefore, the Data Controller only processes the data of the data subjects on a contractual basis when the data processing is directly necessary for the performance and

preparation of the contract. The enforcement of any legal claims arising from the contract is managed by the Data Controller as a separate data processing purpose and is associated with a different legal basis (legitimate interest);

6.2.3. **fulfilment of legal obligation applicable to the Data Controller**: the Data Controller primarily processes data on this legal basis to fulfil its obligations under labour and tax law, as well as accounting and public procurement regulations (for example: mandatory storing of workplace accident reports and accounting documents). In most cases, the Data Controller's employees or contractual partners are also considered data subjects in these data processes;

6.2.4. the **vital interest(s) of the data subject or another natural person**: the Data Controller generally does not process data on this legal basis, however, its application cannot be excluded due to the nature of the exception;

6.2.5. the **performance of a task carried out in the public interest or in the exercise official authority vested in the data controller**: the Data Controller qualifies as a public authority, thus it processes personal data that are necessary for the performance of tasks within its public duties based on this legal ground;

6.2.6. the **legitimate interest(s) of the data controller or a third party**: the Data Controller applies the legitimate interest legal basis for processing certain personal data of employees, visitors to the Data Controller's events and contractual partners. The Data Controller's legitimate interest as a legal basis is particularly important because there are situations involving data processing where consent—due to lack of voluntariness—cannot be applied, there is no explicit legal obligation for data processing, and no contractual relationship exists that could serve as a basis for data processing (since the contract is not concluded with the data subject themself but with an organization). In these cases, the Data Controller typically processes data based on legitimate interest.

6.3. The Data Controller processes personal data only if, in addition to the legal bases defined above, the following conditions are also met:

6.3.1. the need for personal data processing has been reported to the Director General;

6.3.2. if **necessary, concerning the data processing, the data protection risk analysis, legitimate interests balancing test or data protection impact assessment has been completed** – and if based on the data protection impact assessment, the data processing likely involves high risk even in light of the measures taken to mitigate the risk, consultation with the supervisory authority (NAIH) has occurred, and the NAIH has not prohibited the data processing, and the conditions prescribed by it have been fulfilled by the Data Controller;

6.3.3. the data processing has been recorded in the internal data protection register.

6.4. The Data Controller processes special categories of personal data only in the following cases of exceptions under Article 9 (2) of the GDPR:

6.4.1. with data subject's explicit consent according to Article 9 (2) point a) of the GDPR;

6.4.2. if data processing is necessary to fulfil the obligations arising from employment law regulations applying to the Data Controller under GDPR Article 9(2)(b);

6.4.3. if data processing is necessary for occupational health purposes to assess the employee's capacity to work under GDPR Article 9(2)(h);

6.4.4. if data processing is necessary for the establishment, exercise or defense of legal claims under GDPR Article 9(2)(f).

6.5. Access to special categories of personal data is granted exclusively to the Director General, the employee responsible for the task of processing special data (and their substitute employee), as well as the person responsible for data protection compliance

and the data protection officer. Access to other persons can only be provided in particularly justified cases.

6.6. If the legal basis for data processing is Article 6(1)(a) and it involves processing personal data of a minor as data subject, consent must be given by the minor's legal representative to the Data Controller.

6.7. The Data Controller ensures that only data necessary for achieving the specific data processing purpose are processed.

7. LEGITIMATE INTERESTS BALANCING TEST WHEN APPLYING LEGITIMATE INTEREST AS A LEGAL BASIS

7.1. If the Data Controller intends to carry out data processing based on the legal basis of legitimate interest under GDPR Article 6(1)(f), a legitimate interests balancing test must be conducted.

7.2. The legitimate interests balancing test primarily includes:

7.2.1. identification of personal data to be processed;

7.2.2. presentation of the Data Controller;

7.2.3. presentation of the legitimate interest(s);

7.2.4. determination of the purpose of data processing;

7.2.5. examination of whether data processing is absolutely necessary for the enforcement of the identified legitimate interest;

7.2.6. if data processing is necessary for the enforcement of the legitimate interest, examination of whether it can be enforced by another process that does not, or to a lesser extent, affects the privacy of the data subject compared the planned data processing;

7.2.7. if the legitimate interest cannot be enforced by another process as described in the previous point, examination of the extent to which the data subject's interests and fundamental rights are restricted or infringed by the data processing;

7.2.8. comparison of the legitimate interest and the restriction of fundamental rights of the data subject;

7.2.9. examination of alternative legal bases;

7.2.10. presentation of the guarantee measures applied by the Data Controller in connection with data processing;

7.2.11. result of the legitimate interests balancing test, final conclusion (whether data processing can be carried out on the basis of legitimate interest or not);

7.2.12. date of the conducting the legitimate interests balancing test.

7.3. For data processing activities that are logically closely related or occur in different but interconnected stages of a process, the interests balancing test can be performed in a single document (one test).

7.4. If, as a result of the legitimate interests balancing test, the Data Controller determines that the interests and fundamental rights of the data subject take precedence over the legitimate interest affected by the data processing, then the given data processing cannot be applied.

7.5. The legitimate interests balancing test is reviewed out of turn by the data protection officer in every case where the Data Controller plans a change that justifies this in the relevant data processing. Even in the absence of such circumstances, it is necessary to review the interests balancing tests at least annually.

7.6. The Data Controller does not make the legitimate interests balancing test available to the data subjects. The legitimate interests balancing test is considered a document constituting business secret of the Data Controller, and only the Data Controller's person

responsible for data protection compliance, the data protection officer, the legal director, the Director General and persons authorized by the Director General have access to it.

8. DATA PROTECTION IMPACT ASSESSMENT

8.1. If the Data Controller intends to introduce a new data processing operation, it is required by this section to examine whether a data protection impact assessment is necessary before starting the data processing.

8.2. The Data Controller conducts a data protection impact assessment in the following cases:

8.2.1. if the type of data processing, particularly one involving new technologies, is likely to involve a high risk to the rights and freedoms of natural persons, considering its nature, scope, circumstances and purposes;

8.2.2. if the data processing involves a significant amount of sensitive data;

8.2.3. the planned data processing, in terms of its characteristics, appears on the impact assessment list published by the NAIH

8.3. Similar types of data processing operations that pose similar high risks can be assessed within the framework of a single impact assessment.

8.4. The data protection impact assessment should primarily cover:

8.4.1. the systematic description of the planned data processing operation and the explanation of the purposes of the data processing;

8.4.2. the necessity and proportionality examination of the data processing operations in view of the purposes of data processing;

8.4.3. the examination of risks to the rights and freedoms of the data subjects;

8.4.4. the presentation of measures aimed at managing the risks, and

8.4.5. any other relevant circumstances depending on the case.

8.5. The data protection impact assessment is carried out by the data protection officer, who closely collaborates with the person responsible for the Data Controller's data protection compliance, and if necessary, with other employees.

8.6. If the data protection impact assessment determines that the data processing may still pose a high risk to the data subjects in the absence of measures to mitigate the risk, the director-general is obliged to initiate a consultation with the NAIH before processing personal data. The data protection officer must be involved in the consultation, who will review the risk analysis and the data protection impact assessment based on the results of the measures implemented according to the consultation's findings.

9. RECIPIENTS OF PERSONAL DATA, DATA TRANSFERS

9.1. The Data Controller may also transfer the personal data it processes to other persons outside the organization of the Data Controller.

9.2. In performing its data processing tasks, the Data Controller may involve data processors to carry out data processing operations.

9.3. The Data Controller only engages data processors for any of its data processing activities that provide adequate guarantees for compliance with the GDPR requirements and ensure the protection of the data subjects' rights through appropriate technical and organizational measures.

9.4. The Data Controller enters into a written data processing agreement with each of its data processors, which contains the content elements specified in Article 28 of the GDPR. These content elements are determined considering the specifics of the parties' cooperation. Additional liability rules, penalties or other provisions that encourage the data processor to

perform the contract in accordance with the GDPR rules may be included in the data processing agreement.

9.5. The data processing agreement can only be concluded with the involvement of the data protection officer in every case. Before entering into the data protection agreement, the person responsible for the Data Controller's data protection compliance must inform the data protection officer of all relevant circumstances of the planned cooperation.

9.6. The Data Controller enforces at least the following data security requirements against data processors:

9.6.1. in the absence of the data controller's instructions, no part or fragment of personal data processed by the data processor may be published, made available, or disclosed in any way to a third party;

9.6.2. the data processor ensures that those involved in data processing sign a confidentiality agreement, provided that they are not subject to confidentiality obligations stipulated by the Labor Code;

9.6.3. the Data Processor grants access to personal data exclusively to those employees who need it for performing data processing activities;

9.6.4. the Data Processor ensures that the employee conducting data processing at the Data Controller's headquarters leaves the room where data processing takes place during the day in such a way that the entrusted data carriers are secured, or the room is locked;

9.6.5. every operation performed on the data is logged in a traceable manner;

9.6.6. to ensure the security of data stored on computers, the Data Processor protects the data and avoids data loss through backups and archiving;

9.6.7. the server room must be located in a physically protected room equipped with air conditioning and a fire alarm system;

9.6.8. only a limited number of individuals are allowed to enter the server room;

9.6.9. if a person needs to enter the server room to perform activities while not being authorized to enter or not being an employee of the data processor, they must always be accompanied by someone who has the authorization to enter the server room.

9.7. Personal data can be transferred to a third country (i.e., outside the European Economic Area) only based on Articles 45, 46, and 48-49 of the GDPR.

9.8. In the case of transferring personal data to a third country, the Data Controller primarily examines whether the European Commission has an adopted adequacy decision for the respective country (available at: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en?prefLang=hu). If so, the transfer of personal data is based on the adequacy decision.

9.9. In case data is transferred to a country for which there is no adequacy decision, the transfer can only take place with appropriate safeguards. Appropriate safeguards are considered met if

9.9.1. the data transfer is based on and compliant with the standard data protection clauses adopted by the European Commission, or

9.9.2. if the transfer is based on a code of conduct or certification mechanism accepted in the European Union, with the third-country recipient making a binding and enforceable commitment to apply the code of conduct and/or certification mechanism and the safeguards therein.

9.10. The person responsible for data protection compliance maintains a registry of providers offering appropriate safeguards.

9.11. In the case of data transfer to a third country, the Data Controller is obliged to consult with the data protection officer.
9.12. If the data transfer to the third country is not possible as described above, the transfer can only occur in cases permitted under Article 49 of the GDPR.

10. PERSONAL DATA BREACHES

10.1. Every employee of the Data Controller is required to report any personal data breach they become aware of without delay – but no later than within 12 hours – to the head of their organizational unit, who will immediately inform the person responsible for data protection compliance, the data protection officer, and the Director General about the data breach and its circumstances.
10.2. If the personal data breach affects the IT system, the Data Controller's IT staff must also be immediately notified in writing so that the data breach can be investigated and assessed from an IT perspective.
10.3. Upon receiving the report, the data protection officer, involving the relevant organizational units and the person responsible for data protection compliance, immediately begins investigating and assessing the personal data breach. All involved organizational units must cooperate with the data protection officer in the investigation and assessment.
10.4. The data protection officer, if necessary, may request further information about the breach from the employee who detected it or the leaders of the affected organizational units.
10.5. As far as possible, the data protection officer, in cooperation with the person responsible for data protection compliance, must uncover at least the following circumstances:
  10.5.1. the time of the personal data breach;
  10.5.2. the scope of data affected by the personal data breach;
  10.5.3. the range and number of data subjects affected by the personal data breach;
  10.5.4. circumstances leading to the personal data breach
10.6. The Data Controller classifies personal data breaches into three categories:
  10.6.1. **1. Category**: a breach likely not posing a risk to the rights and freedoms of individuals;
  10.6.2. **2. Category**: a breach likely posing a low or average risk to the rights and freedoms of individuals;
  10.6.3. **3. Category**: a breach likely posing a high risk to the rights and freedoms of individuals.
10.7. The Data Controller categorizes the personal data breach by evaluating the following aspects:
  10.7.1. the nature of the breach (confidentiality breach, data integrity breach, accessibility data breach);
  10.7.2. the nature or type of affected personal data (personal data / special category of personal data/ criminal data);
  10.7.3. the sensitivity of personal data (child, vulnerable person);
  10.7.4. the amount of personal data;
  10.7.5. the number and categories of data subject individuals;
  10.7.6. the identifiability of the data subject natural persons;
  10.7.7. the likelihood and severity of consequences for the natural person;
  10.7.8. the legal basis for the data processing in question;
  10.7.9. the nature and type of data processing;
  10.7.10. any potential adverse legal consequences on the data subjects.
10.8. Upon becoming aware of the personal data breach, the data protection officer promptly performs the categorization of the breach as described above, taking into account all known

circumstances of the breach, summarizes his findings in an internal memo, and immediately sends it to the person responsible for data protection compliance and the Director General.

10.9. If the breach is classified into category 2 or 3, the Data Controller must report the personal data breach to the NAIH within 72 hours of becoming aware of it, with the assistance of the data protection officer. If only part of the information required for the report is available at the time of reporting, the Data Controller will still make the report, providing the missing information afterwards when it becomes available to the NAIH (phased reporting).

10.10. If the personal data breach is classified into category 3, the Data Controller, following the completion of the risk assessment, immediately informs the data subjects affected by the breach in writing, electronically or by mail, with the mandatory content set out in the GDPR.

10.11. The information provided to the affected data subjects must not be combined with any other communication (e.g., newsletters), and its content and presentation must clearly indicate that it pertains to a personal data breach.

10.12. Based on the conclusions drawn from the personal data breach, the data protection officer makes recommendations to the Director General for corrective and/or preventive measures to prevent similar data breaches. The Director General decides on the implementation of these measures.

10.13. Access to information related to personal data breaches is only granted to the data protection officer, the Director General, and the person responsible for data protection compliance.

10.14. The Data Controller, with the assistance of the data protection officer, maintains a registry of personal data breaches.

10.15. The registry includes:

10.15.1. the scope of the personal data affected;

10.15.2. the scope and number of data subjects affected by the personal data breach;

10.15.3. the timing, circumstances, and effects of the personal data breach;

10.15.4. the measures taken to mitigate the situation;

10.15.5. the corrective-preventive measures introduced as a result of the investigation of the personal data breach;

10.15.6. an explanation of the decisions made by the Data Controller in response to the personal data breach.

11. THE TECHNICAL BACKGROUND AND RECORDS OF DATA PROCESSING ACTIVITIES

11.1. The Data Controller implements appropriate technical and organizational measures, taking into account the state of the art in science and technology, implementation costs, the nature, scope, circumstances, and purposes of data processing, as well as the varying likelihood and severity of risks to the rights and freedoms of natural persons, to ensure a level of data security appropriate to the degree of risk, which may include, among other things, when applicable:

11.1.1. the pseudonymization and encryption of personal data;

11.1.2. ensuring the continuous confidentiality, integrity, availability, and resilience of systems and services used for processing personal data;

11.1.3. in the event of a physical or technical incident, the ability to restore timely access to and availability of personal data;

11.1.4. procedures for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of data processing.

11.2. The Data Controller is obliged to consult with the data protection officer and IT staff when implementing or modifying technical and organizational measures. Following consultation with the data protection officer and IT staff, the Data Controller's Director General decides on the introduction or modification of the technical measure.

11.3. Paper-based documents containing personal data can only be stored in the manner and devices specified in the document management policy and can only be taken out from the Data Controller's headquarters with the Director General's permission.

11.4. Personal data stored electronically or documents containing personal data may only be processed on password-protected computers. The transfer of such documents or databases to external storage or email systems, or their use or opening on devices potentially accessible by third parties, may only occur with the permission of the Director General.

11.5. Security solutions must be installed on computers that meet IT security requirements in relation to the objective of data processing and its nature. Specific requirements should be determined based on the results of data protection risk analysis or impact assessment as necessary.

11.6. Efforts must be made to ensure that electronic documents or databases containing special categories of personal data are stored and processed exclusively on the Data Controller's own devices.

11.7. Backups of documents or databases containing personal data (or backups containing such documents or databases) may only be stored in an environment that supports data processing guarantees at a high level and does not pose a risk to data security, even with appropriate encryption.

11.8. To erase data on a case-by-case basis, prior approval from the Director General must be obtained, except for those automated data erasures that involve electronic databases or documents, and for which the erasure protocol has already been approved by the Director General. Before approving the erasure, the Director General is required to consult with the data protection officer.

11.9. When erasing personal data, the following procedures should be followed:

11.9.1. the paper-based document containing personal data must be completely destroyed (e.g., with a shredder), or, if complete destruction of the document is not justified, the erasure must be ensured by rendering the personal data unreadable, in such a way that any electronic copies of the document are also erased or replaced with the unreadable version.

11.9.2. The electronic document containing personal data must be completely erased, or if complete erasure is not justified, the data to be deleted must be removed in such a way that the version of the electronic document containing personal data cannot be restored.

11.10. Electronic documents and databases must also be erased from backups, or a recovery protocol must be ensured that does not restore the questionable files, and access to the contents of the backups (even for third parties, such as those performing administrative tasks) is not allowed.

11.11. The employee directly processing the data is responsible for erasing the data, if instructed to do so.

11.12. The Data Controller's person responsible for data protection compliance – with the involvement of the data protection officer – compiles the records of data protection in accordance with Article 30 of the GDPR. If there is any change in data processing, the person responsible for data protection compliance is required – with the involvement of the data protection officer – to update the records. The person responsible for data protection compliance – with the involvement of the data protection officer – is required to review the records annually.

12. MISCELLANEOUS PROVISIONS

12.1. Statements and instructions related to data processing must be made in writing. If the circumstances of the case justify urgent verbal communication, the statements and instructions related to it must be promptly documented in writing after the circumstances necessitating the verbal communication have ceased. Communication via email within the Data Controller's organization, as well as between the Data Controller and the data protection officer, is considered written if it is available in an unaltered form traceable for the necessary period.

12.2. Employees of the Data Controller are individually and directly responsible for complying with data protection rules. Employees performing work under a legal relationship different from employment are fully liable for damages related to data processing, including fines imposed by authorities, compensation paid to the data subject, and reputational losses. Employees are liable for damages according to *Section 179 of Act I of 2012 on the Labor Code*, in line with point 1.8 of this Policy.

12.3. This Policy shall be reviewed if necessary, but at least annually, according to the annual review plan prepared by the data protection officer.

12.4. The present Policy shall enter into force on 1 March 2025, at the same time the Policy in force as of 31 May 2023, file number KEA/349-1/2023, shall be repealed.

Dated: Budapest, February 28, 2025

Dr. Heinerné Dr. Barzó Tímea
Tünde Director General