CENTRAL EUROPEAN ACADEMY
Privacy and Data Security Regulations

1. General provisions

1.1. The **Central European Academy** (registered office: H-1122 Budapest, Városmajor utca 12-14., registration number: Oktatási Hivatal FNYF/419-4/2023, tax ID number: 19359711-1-43, statistical ID number: 19359711-7220-599-01, hereafter referred to as: Data controller) as data controller, pursuant to the regulations of 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, hereafter as: **GDPR**), and with Act CXII of 2011 on the right to information self-determination and the freedom on information (hereinafter as: **Infotv**.) hereby issues the present Privacy and Data Security Regulations (hereinafter as: **Regulations**).

1.2 The purpose of the present Regulations is to specify the legal order of the keeping of records during and regarding the processing of personal data by the Data controller, moreover, to ensure the upkeep of the constitutional principles of data protection, information self-determination and data security, as well as to prevent unauthorized access, alteration or publication of data, and to specify the information and data that Data controller processes regarding natural persons, and the purposes for which they may use said data. It is also the purpose of the present Regulations to set out the internal procedures of Data controller regarding the processing of personal data in connection with their activities.

In the interpretation, facilitation and execution of the Regulations, the applicable legal framework shall be observed in all cases, especially:

- 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),
- Act CXII of 2011 on the right to information self-determination and the freedom on information;

The regulations of the laws in force shall be applicable to any and all activities regarding the processing of personal data.

1.3 Designation of the Data controller:

1.3.1. Name of data controller: **Central European Academy / Közép-európai Akadémia**

1.3.2. Registered seat of data controller: H-1122 Budapest, Városmajor utca 12-14.

1.4 If the personal nature, or the special personal nature of data cannot be decided on, then until the internal decision is made on its nature, they shall be construed as having this quality. Regarding data being considered personal data or special personal data, the chief executive officer of the Data controller shall decide.

1.5 In the processing of personal data, all activities shall be conducted in compliance with the applicable legal provisions and the present Regulations, with the activities:

a) only entailing the processing of personal data where it is necessary for the achievement of a given goal, and only for the time and scope that is necessary;
b) not endangering the security of personal data or the rights and freedoms of the data subject natural persons;
c) being risk-assessed with a marked priority on data security, and with all data protection impact assessments focussing on the largest potential adverse outcomes, with all assessments being kept from under-evaluating risks.

1.6 The present Regulations shall pertain to all employees of Data controller, and to all personnel involved in the execution of their activities, including subcontractors and contractual partners.

1.7 In case of every relevant contract being made, Data controller shall ensure that the contracting partner is aware of the provisions of these Regulations and the applicable legal regulations.

2. Terms

- **Personal data:** any information relating to an identified or identifiable natural person (hereinafter referred to as: Data subject); an identifiable person meaning one who can be identified directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. Personal data is e. g. name, telephone number, bank account number, residency data, e-mail address, IP address etc.;

- **Data processing:** any operation or set of operations performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

- **Restriction of data processing:** the marking of stored personal data for the restriction of their use and processing in future;

- **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;

- **Pseudonymisation:** the processing of 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;

- **Data controller:** the natural or legal person, government body, agency or any other organisation, which determines the purposes and means of the data processing either solely or jointly with others; if the purposes and means of the data processing is regulated by EU or state laws, such EU or state laws may set out the data processor to be appointed, or may set out the specific aspects per which the data processor is to be appointed;

- **Data processor:** a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

- **Employee:** a person engaged in a labour agreement or civil agreement aimed at the provision of labour;

- **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;

- **Processing by a processor:** the carrying out of technical tasks pertaining to data processing, regardless of the location, or the means or instruments used to carry out said tasks, given that the technical tasks are carried out regarding the data;

- **Data forwarding:** the making available of the personal data to a given third party;

- **Data erasure:** rendering the data unrecognisable in a way that ensures that recovery of the data is impossible;

- **Minor:** a natural person not over the age of 18;

- **Legally incapacitated minor:** a minor not over the age of 14;

- **Minor of limited capacity:** a minor who is over the age of 14 and is not legally incapacitated.

- **High volume of personal data:** a volume of personal data specified by a large number of data subjects, or the volume of processed data, or the types of data processed, or the geographical scope of processing, but at least 50 instances of personal data.

3. Privacy principles

3.1. Lawfulness, fairness and transparency: personal data shall be processed by the Data controller lawfully, fairly and in a transparent manner in relation to the data subject.

3.2. Purpose limitation: personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

3.3. Data minimisation: Data controller shall ensure that data processing is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

3.4. Accuracy: data processed by Data controller shall be kept accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

3.5. Storage limitation: personal data processed by Data controller shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with GDPR Article 89 (1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject.

3.6. Integrity and confidentiality: personal data processed by Data controller shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

3.7. Data security: Data processor shall plan and execute data processing tasks in a way that ensures the safety of the privacy of the data subjects as per the legal provisions that apply to data processing. Data processor shall ensure the safety of the personal data processed by them either as data controller or data processor, and shall carry out the technical and organisational measures, and set out the rules that are necessary for compliance with the legal provisions that apply, as well as the present Regulations.

3.8. Transparency: The controller shall take appropriate measures to provide any information relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language. This principle pertains especially to the data subjects being informed on who the data controller is, and what the purpose of data processing is, in order to ensure transparency of processing, and to make data subjects aware of their rights to request affirmation and information on their data being processed. Natural persons are to be informed on the risks, rules, guarantees, and rights related to their data being processed, and on how they may exercise their rights.

3.9. Fair and transparent data processing: the data subject shall gain information on the fact and the purpose of data processing. Data controller shall provide the data subject with information required to establish a fair and transparent data processing environment, noting the specific criteria and context of the data processing. The data subject shall be informed on any potential profiling and its ramifications. If personal data is collected from the data subject, they shall be informed on whether the provision of data is mandatory, and on what the lack of data provision shall entail.

3.10. Documentation: all activities regarding the data storage units containing personal data processed by Data controller shall be documented in order to make the route and location of all storage able to be pinpointed.

3.11. Responsibility: All employees involved in the processing of personal data are required to know and to comply with the provisions of privacy law regulations and those of these Regulations. Violators of privacy regulations shall bear legal liability as set out in the applicable legal regulations.

4. Rights of data subjects and the exercising thereof

4.1. Pursuant to the data protection legislation in place, the data subject is entitled to:

a) request access to their personal data,
b) request corrections regarding their personal data,
c) request deletion of their personal data,
d) request the restriction of their personal data,
e) object to the processing of their personal data,
f) request the porting of their personal data,
g) revoke their consent regarding data processing,
h) file a complaint regarding any grievances.

4.2. Right of access:

The data subject is entitled to receive feedback from the data controller on whether their personal data is being processed or not, and if so, to request access to their personal data.

The data subject is entitled to request copies of their personal data being processed. For the purposes of identification, the data controller may request additional information from the subject, and – with the exception of the first copy being handed out – to charge any warranted administrative fees that further copies may entail.

4.3. Right of correction:

The data subject is entitled to request any of their erroneous personal data to be rectified by the data controller. Based on the given data processing purpose, the data subject may be entitled to request incomplete personal data to be amended.

4.4. Right of deletion („right to be forgotten"):
The data subject is entitled to request the data controller to delete their personal data, and the data controller shall delete these if any of the following criteria are met:

a) the personal data are no longer needed for the purpose for which the Data controller collected them or processed them otherwise;
b) the data subject revokes their consent per Article 6 (1) a) or Article 9 (2) a) and no other legal grounds for data processing apply;
c) the data subject objects per GDPR Article 21 (1) to their data being processed, and no other, prevailing grounds apply to the data processing, or if the data subject objects pursuant to Article 21 (2);
d) personal data were processed unlawfully;
e) personal data is to be deleted as fulfilment of legal obligations as regulated either by EU law or one of the member states' laws;
f) the collection of personal data was conducted in connection to information society services as referenced under Article 8 (1) of GDPR.

4.5. Right of restriction:
The data subject is entitled to request the restriction of their personal data. In this case, the data controller shall mark the affected personal data, which, other than their storage, shall only be processed per the data subject's consent, or for filing or pursuing lawful interest, protection of rights, or for public interest as regulated either by EU law or one of the member states' laws.

4.6. Right to objection:
The data subject is entitled to object at any time, for any reasons of their own, to the processing of their personal data per Article 6 (1) e) or f) of the general data protection regulation, including the profiling based on said regulations, and to request that the data controller no longer process their personal data.

4.7. Right to data portability:
The data subject is entitled to request that their given personal data be provided to them in an articulated, widely recognised, computer readable format (i.e. digital format) from the data processor, and is entitled moreover – where technically possible – to request these data to be forwarded to another data controller without the Data controller hindering this.

4.8. Right to revoke consent:
Where the processing of User's personal data is conducted per their consent, User may revoke their consent at any time, with revocation having to be made as accessible as consent giving is. Revocation of consent does not affect the legality of consent-based data processing conducted prior to the revocation of consent.

If User revokes their consent given to the Data controller, the services provided by the Data controller may partially or wholly be unavailable to be provided.

5. Criteria regarding personal data being processed

5.1. Personal data may only be processed upon the joint meeting of the circumstances below:

a) its **legal grounds meet a point of GDPR Article 6 (1)**:
aa) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

ab) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
ac) processing is necessary for compliance with a legal obligation to which the controller is subject;
ad) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
ae) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
af) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

b) the intent regarding personal data processing has been announced to the director;

c) where necessary, **a data protection risk assessment, and where necessary, a data protection impact assessment has been made** – and if there are residual risks identified per the data protection impact assessment even after the mitigating measures have been taken into account, then if the NAIH has been consulted, and they have not forbidden the data processing, or if the measures prescribed by them have been carried out;

d) the data processing has been recored in the internal data processing register.

5.2. Special personal data may only be processed in case all criteria under point 5.1. have been met, and if the data processing is in line with both one of the points of GDPR Article 6 (1) and Article 9 (2).

5.3. In case the legal grounds of the data processing is Article 6 (1) a), then – with the exception under 5.4. herein – regarding legally incapacitated minors, only their legal guardian may give Data controller their consent, and in case of minors of limited capacity, the approval of the legal guardian must be sought.

5.4. Where point (a) of Article 6 (1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.

5.5. In cases of all data processing where the purposes and means of the data processing are not decided on by Data controller alone, the data processing requires Data processor to enter into an agreement per Article 26 with the joint data controllers, with the director being entitled to sign said agreement.

5.6. All current data processing of the Data controller is stated under Annex 1 to these Regulations.

5.7. The employee responsible for data protection shall be responsible for the following:

a) preparation of risk assessment required for data protection impact assessments, as well as the impact assessments per the applicable methodology;
b) making of recommendations regarding risk and impact assessments on:
   - restrictions (e. g. personnel, time) on access,
   - rules of data forwarding (to whom, for what purpose, per what conditions);
   - on miscellaneous technical and organisational measures (e. g. on the location of data storage, password practices, or the restriction of access to the Data controller's offices).
c) preparation of recommendations regarding the director's decisions on the necessity, purpose and timeframe of data processing;
d) routine monitoring of data processing regimes;
e) proper documentation of circumstances corroborating the lawfulness of data processing (especially consent and risk assessment);

f) if external personnel are to be involved in the data processing, they shall signal this to the director;
g) informing the data subjects of the data processing.

Regarding the recommendations per a) and b) above, the director shall decide based on the risk assessment and impact assessment results.

5.8. If the fulfilment of the tasks specified in 5.7. above pertain to more than one employee, the director may specify the employee responsible for the given tasks and may allocate certain tasks to certain employees. In absence of such specification or allocation, the employees shall be jointly responsible for the tasks.

5.9. Regarding legal grounds of data processing, only such circumstances may be specified which satisfy the legal requirements, and which are in direct connection with Data controller's activities and are either necessary or reasonable.

5.10. The scope of processed data shall be specified as is minimally necessary, safe and responsible in view of Data controller's activities.

5.11. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

5.12. The risk assessment, and – where reasonable (if the data processing is likely to result in a high risk to the rights and freedoms of natural persons) the data protection impact assessment shall be prepared by the employee responsible for data protection by the deadline specified by the director.

5.13. The controller shall consult the supervisory authority (NAIH) prior to processing where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk. The consultation shall include the employee responsible for data protection, who, per the results of the consultation, shall reassess the risk assessment and the data protection impact assessment.

5.14. The risk assessments and the data protection impact assessments shall be saved electronically by the employee responsible for data protection and sent to the director electronically. The risk assessments and the data protection impact assessments may only be accessed by the employee who prepared them (or who took over their position), by the employee responsible for data protection, and the director.

5.15. The data of the internal data protection records shall be maintained by the employee responsible for data protection, per the risk assessments and data protection impact assessments. The records shall be checked by the director when needed, but at least once a year.

6. Practical regulations of data processing

6.1. Personal data may only be processed in complete compliance with the legal regulations that apply, and with the Regulations issued by the director. All circumstances or facts that signal that an entity in a legal agreement with the Data controller is not in compliance with data protection regulations must be forwarded to the director. In any such case, the fulfilment of the agreement shall be ceased in a way that results in no damage to employees, partners and data subjects, or to keep any adverse circumstances to the minimum extent.

6.2. Employees in contact with data subjects must ascertain that:
- personal data are provided by the data subjects themselves and that they consent to their data being processed;
- or these are provided by a contractual partner of Data controller, whereby the legality of the data processing is provided for by the agreement between them (wherein the Data controller and the partner are joint data controllers);
- or where an agreement is made in which the data subject is a contracting party.

6.3. All employees of the Data controller shall comply with the following rules:
a) during work, only the expressly necessary personal data are to be processed, forwarded, with the given organisational section's leader being responsible for the establishment of work procedures in compliance with the above;
b) in allotting IT access credentials, only those may access personal data, and only for a time that is expressly necessary for work to be performed adequately;
c) paper documents containing personal data may only be forwarded in sealed envelopes, or in closed instruments suited for document forwarding;
d) large amounts of personal data, special personal data or personal data of minors may not be forwarded via e-mail. If any such data is to be forwarded by an employee to a third party, these shall be uploaded to a secure fileserver of Data controller, or a similar and suitable server, with the access link being sent and with the access control being ensured;
e) personal data may only be stored on shared drives if it is ensured that these may only be accessed by those entitled to do so; with the given organisational section's leader being responsible for the establishment of work procedures in compliance with the above.

6.4. If the personal data are not collected from the data subjects, the employee responsible for data protection shall prepare an information notice per Article 14 of GDPR for the data subjects, in which the following are stated:
a) the Data controller and their contact information,
b) the contact details of the employee responsible for data protection,
c) the planned purposes for which data are processed, and the legal grounds thereof,
d) the categories of processed data,
e) the recipients of personal data (e. g. to whom the data is forwarded)
f) where applicable, whether the data are planned to be forwarded by the Data controller to third parties, and per what guarantees this shall take place (6.17-6.20),
g) storage timeframes of personal data
h) the rights of data subjects on restriction, amendment, erasure, access, objection, and data portability,
i) the right to revoke consent at any time, which shall not affect the lawfulness of processing prior to revocation,
j) the right to file a complaint with the supervisory authority,
k) the source of personal data processed.

6.5. The employee responsible for data protection:
a) shall take part in the evaluation of the methodology adopted by the Data controller (incident, risk, and impact assessment), and shall assist in the development of said methodology, its documentation, and the fulfilment of connected tasks;
b) shall give advice to the director and other employees regarding their obligations per GDPR and other EU or national data protection regulations;
c) shall monitor compliance with GDPR, other EU or national data protection regulations and Data controller's internal data protection regulations, including the allocation of tasks;
d) shall take part and coordinate the awareness training of employees engaged in data processing tasks;
e) shall take part in and monitor the information security and data security audits;
f) shall cooperate with the data protection authority;

g) shall take the risks pertaining to the data processing activities into account, as well as the type, scope, circumstances, and purposes of data processing;
h) shall investigate the complaints sent to them, and in case of unauthorised data processing, shall call Data controller to cease processing said data;
i) shall take part in the development and operation of data breach mitigation measures;
j) shall keep contact with external authorities and organisations regarding data protection matters, shall provide them with the necessary information, and in case of external audits, shall cooperate with the auditing authorities or organisations;
k) shall keep and maintain the data breach records.

The employee responsible for data protection may not be ordered with regard to their data protection tasks, and, in this quality, is subordinate to the director directly, and shall report to them directly.

6.6. Should any employee gain knowledge of any breach of data protection regulations, they shall then report to the director or the employee responsible for data protection. Based on the reports, the director shall audit the data protection practices involved, or shall have them audited, and shall take the appropriate measures based on the findings in order to provide for data processing that is in compliance with the rights and freedoms of data subjects.

6.7. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:
- the pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

6.8. The Data controller's employee responsible for data protection shall manage all data subject requests (especially the declarations per Chapter III of GDPR regarding rectification, erasure, and requests regarding information), and – within no more than 3 days from the date of receipt of the request – shall:
a) prepare a written response to be sent by the director, with adequate reasoning, if the request cannot be fulfilled; or
b) carry out the required action – with the notification of the director – and notify the data subject and any other concerned parties to whom the data had been communicated prior to rectification.

6.8.1. The data subject shall be notified of the fulfilment or lack thereof (with reasoning as to the cause, along with information regarding appeal rights to NAIH or a competent court) shall be sent within no more than a month from the receipt of the request. This deadline may be extended in appropriate cases (due to a large number of subjects or an unusual complexity of the matter), with the data subject having to be notified thereof within the one-month deadline.

6.8.2. If, due to the request, data processing is to be modified, or data is to be deleted, the employee responsible for data protection shall amend the necessary changes in the internal records. Regarding the amendment or deletion, all concerned data subjects shall be notified, along with all recipients to whom the data had been communicated.

6.8.3. Management of the data subjects shall be conducted free of charge. Where requests are manifestly unfounded or excessive, in particular because of their repetitive character, the Data controller may charge a reasonable fee based on administrative costs (e. g. cost of copies or data storage) or refuse to act on the request. A written record shall be made demonstrating the manifestly unfounded or excessive character of the request.

6.9. Personal data shall be deleted if:

a) the timeframe of data processing has passed, or if the processing of the data has become otherwise unnecessary or unfounded,
b) the data subject requests,
c) if the Data controller is compelled by law or a final court or authority decision.

No data may be deleted that may be required for the fulfilment of Data controller's legal obligations. Before deletion, the prior approval of either the director or the employee responsible for data protection must be sought, not including cases of automatic deletion regarding electronic databases, or cases where a deletion routine has been previously approved by the director.

6.10. Deletion of personal data shall be conducted in a way that makes reading of the deleted data impossible. In this regard:

a) paper documents containing personal data:
   - shall be destroyed, (e. g. with a shredder), or
   - if destruction is not warranted, then by rendering the personal data unreadable

   with the electronic copies thereof being either destroyed or the personal data rendered unreadable as well;
b) paper documents containing personal data:
   - shall be destroyed, or
   - if destruction is not warranted, then by removing the personal data from them

   in a way that ensures that the version containing the personal data cannot be restored.

Electronic documents and databases are also to be deleted from the recovery backups, or a recovery protocol is to be adopted whereby the given files are not reinstated upon recovery, and the contents of the deleted files cannot be accessed from the backups (not even by third parties with administrative access rights).

6.11. Regarding the deletion of data, the employee processing the given data directly shall be responsible.

6.12. All employees are required to report any and all data breaches or incidents without delay, but no later than 12 hours after having gained knowledge to both the director and the employee responsible for data protection.

6.13. Data breaches shall be investigated without delay by the employee designated by the director, with the pertaining risks being evaluated and the employee responsible for data protection being involved. The results of the risk assessment are to be brought to the attention of the director.

The risk assessments shall be saved electronically by the employee responsible for data protection and sent to the director electronically. The risk assessments may only be accessed by the employee who prepared them (or who took over their position), by the employee responsible for data protection, and the director.

6.14. Based on the findings of the risk assessment, the director – after having consulted with the employee responsible for data protection – shall carry out the necessary measures in order to prevent further incidents or breaches.

The taken measures are to be communicated to the employee responsible for data protection, and, if needed, to other employees, or to third parties in contract with the Data controller. Such communications are to be avoided if these are likely to result in further data protection incidents.

6.15. Breaches constituting a risk to the rights and freedoms of data subjects shall – by approval of the director – reported to the NAIH by the employee responsible for data protection pursuant to Article 33 of GDPR within 72 hours of the breach or the recognition thereof, with the contents of the report being prepared by the employee designated by the director. If the breach constitutes a high probability level of risk to the rights and freedoms of data subjects, the employee designated by the director shall also prepare a notice informing the data subjects without delay, which is to be approved by the director.

6.16. Data controller shall keep a record of data protection breaches per Article 33 (5) of GDPR, which shall be drawn up by the employee responsible for data protection. The records shall show all incidents, even those which don't entail the necessity of having to notify the NAIH or the data subjects.

6.17. Personal data may only be forwarded to third party (non-EU) countries per articles 45, 46 and 48-49 of GDPR.

6.18. Personal data may freely be forwarded to EEA countries and to countries approved by the Commission. Pursuant to Article 45 of GDPR, these are: Andorra, Argentina, South Korea, United Kingdom, Faroe Islands, Guernsey, Israel, Jersey, Japan, Canada, Isle of Man, Switzerland, Uruguay, and New Zealand.

6.19. In all cases where data is to be forwarded to countries outside of those specified under 6.18., it must be ascertained that the given data controller has provided adequate guarantees per Article 46 of GDPR, whereby it is proven that:

- they observe binding corporate regulations, or
- they observe general data protection regulation approved by the Commission, or
- they have undertaken to comply with a code of conduct accepted in the EU, or one that has been audited by a mechanism approved by the EU.

The employee responsible for data protection shall keep records of service providers providing such guarantees.

6.20. If data forwarding is not possible under Articles 45-46 of GDPR, data forwarding may only take place pursuant to Article 49.

7. Processing of special personal data

7.1. Special personal data may only be accessed by the director, the employee directly involved in their processing, the employee substituting them, and to the employee responsible for data protection. Any other employee or external, contractually engaged persons may only be provided access in cases where it is especially warranted.

7.2. In cases where special personal data are concerned, risks may not be excluded neither in the data protection impact assessment, nor in cases of breaches, and these may not be regarded as being free of probable risks.

7.3. In cases where special personal data are concerned, the adopting of adequate technical and organisational measures may not be excluded.

8. Technical background of data processing

8.1. Paper documents containing personal data may only be kept per the record keeping regulations issued by the Data controller, and such may only be removed from the premises of Data controller per the prior approval of the director.

8.2. Personal data or documents containing personal data that are stored electronically may only kept on computers that are password protected. Such documents or databases may not be forwarded to external hard drives or exchange servers, and may not be used, opened or stored on devices that may be accessed by unauthorized third parties.

8.3. Regarding computers as per 8.2., such security measures are to be installed that ensure a level of security proportionate to the subject of the given data processing and the nature thereof. The exact requirements are to be specified pursuant to the data protection risk assessment, or, where necessary, the data protection impact assessment.

8.4. Where possible, electronic documents or databases containing special personal data shall only be stored and processed on Data controller's own devices, with the provisions of 8.2. being applicable.

8.5. Backups of documents or databases containing personal data (or backups containing such files) may only be stored per an adequate level of encryption, and in such an environment that promotes the upkeep of data protection guarantees to a high level, moreover which do not pose a risk to the safety of data.

9. Miscellaneous provisions

9.1. Declarations and orders regarding data protection shall be done in writing. Should the circumstances of a given situation call for prompt verbal communication, then after the circumstances having passed, these declarations and orders are to be duly recorded in writing. E-mails, text messages and other various messaging applications shall be considered as written communications within the context of Data controller's internal communication as long as these messages are able to be reconstructed according to their original contents.

9.2. During activities related to data protection, the highest possible level of compliance with the present Regulations and all applicable legislation must be able to be proven, especially:

a) data subjects' consent to data processing,
b) data subjects' consent to data processing regarding special personal data,
c) the fulfilment of data subjects' requests regarding deletion, rectification, restriction,
d) data subjects' notification regarding breaches,
e) data forwarding to third party countries,
f) in cases of data processing done pursuant to lawful interests, the necessary assessments.

In the above cases, the necessary documentation proving legality cannot be waived, not even in circumstances where haste is warranted. The online systems' operational background must be created in a way that afford the above needs being met – e. g. whereby the consent given by a data subject is able to be identified precisely.

9.3. Fulfilment from third parties cannot be accepted if it contains personal data, the lawful processing of which by Data controller cannot be guaranteed; this provision must be included in all contractual agreements.

9.4. Regarding any breach of data protection regulations, the employees and contractual partners of Data controller shall be responsible singularly and directly. Regarding damages incurred by breaches of data protection (e. g. authority penalties, reparations, reputational losses and

unrealised income) the latter shall bear complete liability. Employees shall be responsible per 179. § of Act I of 2012 on the Labour Code.

9.5. The present Regulations are to be reviewed by the director where necessary, but at least every two years.

9.6. The present Regulations shall enter into force on 31 May 2023.

Budapest, 31 May 2023.

_____

Dr. Heinerné Dr. Barzó Tímea Tünde (signed)
general-director

Annexes:
Annex 1 – The presently conducted data processing of Data controller

ANNEX 1
The presently conducted data processing of Data controller

1. Obligatory workplace data processing

1.1. Data processing use case: processing of Data controller's employees' data regarding the establishment, fulfilment, and termination of labour agreements, moreover regarding the exercising of rights and obligations pursuant to said labour agreements.

1.2. Source of data: Given by the data subject employee directly.

1.3. Types of data processed: Per the present data processing, Data controller processes the following personal data:
- Name
- Mother's maiden name
- Address
- Tax ID number
- Bank account number
- Photocopies of personal ID documents (tax ID, residency ID, personal ID)
- Photocopies of documents proving academic record

1.4. Purpose of data processing: Data controller processes the personal data per 1.3. above for the following purposes:
- Establishment, fulfilment, and amendment of labour relations (reporting of labour relations to NAV, accounting, filing tax and dues reports)

1.5. Legal basis of data processing: Data controller processes the personal data under 1.3. per Article 6 (1) c) of GDPR, with the bank account information being processed per Article 6 (1) b).

1.6. Location of data processing: The registered seat and the proprietary server of Data controller.

1.7. Timeframe of data processing: Data controller processes the personal data under 1.3. until the expected retirement of the employee, whereas the bank account data is processed until the fulfilment of all payment obligations after the labour agreement had been terminated.

1.8. Data forwarding: Data controller does not forward the personal data under point 1.3. hereto.

2. Data processing regarding delegation

2.1. Data processing use case: Data processing regarding delegations of Data controller's employees and persons in agreements with Data controller regarding the provision of work services.

2.2. Source of data: Given by the data subject employee directly.

2.3. Types of data processed: Per the present data processing, Data controller processes the following personal data:
- Name
- Destination
- Timeframe of delegation

2.4. Purpose of data processing: Data controller processes the personal data per 2.3. above for the following purposes:
- Record keeping regarding delegations;
- Calculation of daily wages.

2.5. Legal basis of data processing: Data controller processes the personal data under 2.3. per Article 6 (1) c) of GDPR.

2.6. Location of data processing: The registered seat and the proprietary server of Data controller.

2.7. Timeframe of data processing: Data controller processes the personal data under 2.3. for no more than 15 years after the labour/work agreement having been terminated.

2.8. Data forwarding: Data controller does not forward the personal data under point 2.3. hereto.

3. Data processing regarding employees' travel arrangements

3.1. Data processing use case: Data processing regarding the arrangement of employees' travel and team-building trips (events).

3.2. Source of data: Given by the data subject employee directly.

3.3. Types of data processed: Per the present data processing, Data controller processes the following personal data:
- Name
- Date and place of birth
- Personal ID or passport number

3.4. Purpose of data processing: Data controller processes the personal data per 3.3. above for the following purposes:
- Economic arrangement of travel;
- In cases of team-building trips and events, the economic and effective arrangement thereof for the convenience of the employees.

3.5. Legal basis of data processing: Data controller processes the personal data under 2.3. per Article 6 (1) b) of GDPR.

3.6. Location of data processing: The registered seat and the proprietary server of Data controller.

3.7. Timeframe of data processing: Data controller processes the personal data under 3.3. until the conclusion of the team-building event or trip.

3.8. Data forwarding: Data controller shall forward the personal data per 3.3. for the purpose of arranging and securing travel and events for the employees, to the lodging and transport services' providers.

4. Data processing detailed in separate policies

Regarding the

a) **data processing conducted in relation to personal data of contractual partners of Data controller as well as their liaisons;**
b) **data processing conducted in relation to personal data of persons registering to and attending the public events organised by Data controller;**
c) **data processing conducted in relation to personal data of prospective contractual partners contacting Data controller via the country referrer network;**
d) **data processing conducted in relation to mailing honorary copies of the books and other print products;**
e) **data processing conducted in relation to job applicants;**
f) **data processing conducted in relation to personal data of persons recorded by the CCTV operated by Data controller in their offices; and**
g) **data processing conducted in relation to the website of Data controller,**

Data controller informs data subject of the details of the above data processing activities in separate privacy policies made available on the website of Data controller and at their registered office.

*****