File number: A/220-1/MKI/2025

Order No. 20/2025 of the Managing Director

on the Privacy and Data Security Policy

of Magyar Külügyi Intézet Nonprofit Zártkörűen Működő Részvénytársaság (Hungarian Institute of International Affairs Nonprofit Private Limited Company)

Name of the business entity:	Magyar Külügyi Intézet Nonprofit Zrt.
Registered office:	H-1016 Budapest, Bérc utca 13–15
Company registration number:	01-10-142325
Tax number:	32262535-2-41
Authorised representative:	Dorina Molnár, Managing Director
Effective from:	01/10/2025

MAGYAR KÜLÜGYI INTÉZET

Table of contents

Preamble

In compliance with its obligation under Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter: GDPR) and under Act CXII of 2011 on the Right of Informational Self-determination and on Freedom of Information (hereinafter: Privacy Act), for the protection of personal data processed by it Magyar Külügyi Intézet Nonprofit Zártkörűen Működő Részvénytársaság (Hungarian Institute of International Affairs Nonprofit Limited Liability Company, hereinafter: Company) has adopted the following Policy.

I. General provisions

1. Purpose and scope of the Policy

(1) The purpose of the Policy is to establish the lawful regime of measures and procedures for the protection of personal data of natural persons processed by the Company in the course of its activities and operations, and to ensure the application of the fundamental principles of data protection, the right to informational self-determination, the right to the protection of personal data and the requirements of data security.

(2) The personal scope of the Policy covers:

a) all organisational units of the Company, as well as natural persons engaged by the Company under an employment relationship, a contract of assignment or any other legal relationship for the performance of work who process personal data in the course of their work;

b) any natural person who uses the services, organisational units or infrastructure of the Company or who has or will have actual contact with the Company, whether for the purpose of establishing a legal relationship or otherwise;

c) persons who are not in a legal relationship with the Company as referred to in points (a)–(b), but whose personal data are processed by the Company by law;

d) employees of contracted partners engaged as data processors by the Company;

e) employees of service providers who have a partnership contract with the Company.

(3) The material scope of the Policy covers personal data processed by the Company for any purpose and all records of personal data held by the Company, regardless of the form in which they are presented.

(4) The scope of the Policy does not cover technical data protection related to information technology devices.

2. Definitions applied for the purposes of this Policy

(1) For the purposes of this Policy, the following definitions shall apply:

confidentiality breach: accidental or unauthorised disclosure of or access to personal data;
Personal identification data: Surname and forename, surname and forename at birth, sex, place and date of birth, mother's maiden name and forename, place of residence, habitual residence, identity card number (hereinafter: ID number) and personal identification number, taken together, or any of these, where they are or may be suitable to identify a natural person.
integrity incident: accidental or unlawful alteration of data.
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.
Recipient: A natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the data protection rules applicable to the purposes of the processing.
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.
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.
Supervisory authority: Hungarian National Authority for Data Protection and Freedom of Information (NAIH).
Mandatory processing: where processing is necessary as decreed by law or by a local authority based on authorisation conferred by law concerning specific data defined therein for the performance of a task carried out in the public interest.
Data erasure: Rendering data unrecognisable in such a way that they can no longer be restored.
Data transfer: Ensuring access to data for a third party.
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.
accessibility incident: accidental or unlawful destruction or loss of personal data.
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.
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. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data.

Processor: A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Data subject: a natural person identified or identifiable by reference to any information.

Controller: A natural or legal person, or organisation without legal personality which alone or jointly with others determines the purposes and means of the processing of data; makes and executes decisions concerning data processing (including the means used) or have it executed by a data processor.

Processing: Any operation or set of operations which is performed on personal data, irrespective of the procedure applied; thus, in particular, 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, prevention of further use, as well as taking photos, making audio or visual recordings, or recording, or providing access to, physical characteristics suitable for personal identification (such as fingerprints or palm prints, DNA samples or iris scans).

Sensitive data: Personal data revealing racial origin or nationality, political opinions and any affiliation with political parties, religious or philosophical beliefs or trade-union membership, personal data concerning sex life, or personal data concerning health, pathological addictions, or criminal record.

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. For the purposes of this Policy, all references to 'data' are to be understood as personal data.

A natural person shall be deemed identifiable if he or she 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 the natural person.

Types of personal data breaches:

- confidentiality breach: accidental or unauthorised disclosure of or access to personal data;
- accessibility incident: accidental or unlawful destruction or loss of personal data.
- integrity incident: accidental or unlawful alteration of data.

Restriction of processing: marking of stored personal data with the aim of limiting their processing in the future.

Data protection officer: the person responsible for the implementation and continuity of data protection as defined in this Policy.

Data protection: a set of technologies and organisational methods that facilitate the integrity, usability and confidentiality of the accumulated data sets.

Processing: all data processing operations performed by the processor acting on behalf of, or instructed by, the controller.
Data: information, communication, news or intelligence that is independent of the data carrier.

General principles of processing

As defined in the interpretative provisions of this Policy, 'data' should be understood as any information, communication, news or intelligence that is independent of the data carrier. The Company processes several types of data, including, but not limited to: personal data (relating to natural persons only), sensitive data (also relating to natural persons), data relating to legal persons, organisations, trade secrets, business data, data accessible on public interest grounds (with possible overlaps between different types of data).

Persons subject to the Company's Privacy Policy are bound by confidentiality not only with respect to personal data, but also with respect to all information/data obtained by them or of which they became aware at the COMPANY. Employees sign a statement of confidentiality in their employment contracts, while persons engaged under another legal relationship or another contractual relationship issue a statement in this regard in the instrument establishing the relationship.

Persons covered by this Policy may process personal data and any other data obtained at the Company strictly for the purposes for which they are collected and only to the extent necessary for the adequate performance of their duties.

In the course of their work, the Company's staff shall prevent unauthorised persons from viewing personal data and ensure that personal data are stored and located in such a manner that prevents the data from being available, accessed, altered or destroyed by unauthorised persons.

3. Controllers and processing

(1) All persons who have a legal relationship with the Company and who obtain personal data, or process such data based on his or her employment or position shall protect and safeguard such personal data, and make every effort to ensure that they are adequately protected.

(2) Data shall be protected from unauthorised access, alteration, transmission, public disclosure, erasure or destruction, damage or accidental loss, ensuring that stored data may not be corrupted and rendered inaccessible due to any changes in or modification of the technique applied.

(3) Persons who are in a legal relationship with the Company or who act on behalf of the Company shall treat as confidential any personal data that have come to their knowledge in connection with their legal relationship.

(4) Persons who act as controllers or carry out processing under a legal relationship with the Company shall be liable for any damage resulting from a breach of their data processing and data protection obligations.

(5) Where processing is to be carried out on behalf of the Company, the Company shall use only processors providing suitable safeguards to implement appropriate technical and organisational measures in such a manner that processing will meet the processing requirements and ensure the protection of the rights of the data subject.

(6) Processing by a processor shall be governed by a contract or other legal act that is binding on the processor with regard to the Company and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. The contract shall be concluded strictly in writing, stipulating the content prescribed by Article 28(3) of the GDPR; thus, in particular that the processor:

a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

c) takes all measures required to ensure the security of processing pursuant to Article 32 of the GDPR;

d) respects the conditions referred to in Article 28(2)–(4) of the GDPR for engaging another processor;

e) taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR;

f) assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR, in particular the notification of a personal data breach, the implementation of a data protection impact assessment and prior consultation, taking into account the nature of processing and the information available to the processor;

g) at the choice of the controller, deletes or returns all personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;

h) makes available to the controller all information necessary to demonstrate compliance with the above obligations and allows for and contributes to audits, including inspections, conducted by the controller or another auditor mandated by the controller. The processor shall immediately inform the controller if, in its opinion, an

instruction infringes the provisions of the GDPR or other Union or Member State data protection provisions.

(7) Organisations with commercial interests in the use of the personal data to be processed cannot be contracted for data processing.

(8) Where necessary, the controller and processor shall take further steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller.

(9) Transfers to third countries or international organisations may only take place if the conditions set out in Articles 44–50 of the GDPR are met, in particular, based on the adequacy decision of the European Commission, binding corporate rules, standard contractual clauses adopted by the European Commission or the explicit consent of the data subject. In all cases, the transfer of data shall be documented in writing.

Processing of personal data

The Company processes the following personal data in particular:

- employees' personal data;
- personal data of persons engaged under another legal relationship;
- personal data of business partners and representatives and contact persons of business partners who are not legal persons;
- personal data of managers and employees of the Company's contractors (including, but not limited to: security company, cleaning company, etc.);
- personal data of temporary visitors (e.g. guests, business/commercial visitors);
- personal data of applicants and notifiers contacting the Company in writing (e.g. parties requesting data of public interest, PR notifiers, etc.).

This Chapter applies to all processing by the Company involving the personal data mentioned above. It also covers all processing carried out in the context of the employment relationship: processing relating to an existing employment relationship, processing relating to an employment relationship that has been terminated, and processing prior to the establishment of the employment relationship.

Principles for the processing of personal data

In the course of processing, the Company shall respect the requirements of acting fairly and in good faith, in cooperation with the data subjects.
The Company shall exercise the rights and fulfil the obligations of data controller in accordance with their purpose.
The right to the protection of personal data is a fundamental right of natural persons enshrined in the Fundamental Law, which guarantees the data subjects' right to informational self-determination. This right may be restricted only in the cases set out in Section 10.28. The carrying out the tasks of the data controller subject to the personal scope of this Policy shall be responsible for the lawful processing of personal data of which he or she becomes aware in the course of his or her duties and responsibilities, and for the lawful exercise of access rights to the Company's records.

The Company applies the principles of 'data protection by design and by default' in its IT systems. Upon the introduction of a new IT system that entails the processing of personal data, appropriate technical and organisational measures shall be taken to ensure that the principle of data protection by design and by default is respected before the system is introduced. A data protection impact assessment shall be carried out before the introduction of an IT system that performs data processing operations if it is likely to present a high risk to the rights and freedoms of natural persons.

Personal data may be processed only for specified, explicit and legitimate purposes, where it is necessary for the exercise of certain rights and the performance of obligations. The purpose of processing shall be satisfied at all stages, and no processing may be carried out in a way that is incompatible with those purposes. The personal data processed must be essential for the purpose for which it was recorded, and it must be suitable to achieve that purpose. Personal data may be processed to the extent and for the duration necessary to achieve its purpose. Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject. Personal data shall be accurate and, where necessary, kept up to date; every reasonable step shall be taken to ensure that personal data that are inaccurate are erased or rectified without delay.

The processing of personal data should be avoided wherever possible; where the processing of personal data is unavoidable, the Company must at all times be able to demonstrate compliance with the principles set out in this section. Appropriate procedures shall be designed to ensure that the lawfulness of all data processing by the Company may be readily demonstrated.
Where personal data are processed by the Company or provided by another controller for the performance of the Company's tasks, using such data for private purposes or making them available to unauthorised persons are strictly prohibited.
If the Company no longer needs the personal data for the purposes of the processing or the processing is otherwise unlawful or is subsequently found to be unlawful, such data shall be erased. The purposes for which the data are processed shall be monitored regularly.
Erasure means the rendering of data unrecognisable so that it can no longer be restored. The facts relating to the erasure or cancellation of data shall be recorded in a protocol in accordance with Annex 4 to this Policy.

Where the Company makes the personal data processed by it available to a third party under a contractual agreement, it shall sign with such third party a declaration of confidentiality and an agreement on compliance with the data protection rules pertaining to data covered by this Policy or, where the third party performs data processing operations, the Company shall enter into a processing agreement with the third party.

Personal data processed by the Company and the legal basis for processing
The Company may process personal data lawfully on the following grounds only:
a) with the consent of the data subject;
b) processing is necessary for the Company's performance of a contract to which the natural person data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
c) as decreed by Union law, or by a local authority based on authorisation conferred by law in the manner and to the extent prescribed therein (in order to fulfil a legal obligation of the Company);
d) in order to protect the vital interests of the data subject or of another natural person;

e) processing is necessary for the performance of a public task or a task carried out in the public interest;

f) where the processing is necessary for the purposes of the legitimate interests pursued by the Company as controller or by a third party, provided that the resulting harm is proportionate to the legitimate interests of the controller or of the third party.

In the course of its processing operations, the Company shall ensure the protection of legally protected secrets and personal data.

The Company shall file the documents received by it in accordance with its current File Management Policy and the applicable legislation.

Where processing is based on consent, the Company shall be able to demonstrate that the data subject has consented to the processing of his or her personal data. To this end, the organisational unit which actually carries out the processing – or its designated or specified employee – shall safeguard the consent obtained from the data subject or the technical solution or certificate (log file) that clearly proves the fact of consent given and, if necessary, present it or make it available to the data protection officer.

Where data processing is mandatory, the purpose and the conditions of processing, the dataset to be processed and access to such data, as well as the duration of the proposed processing operation, and the name of the controller are generally specified by the legislation ordering the processing. Where the law provides for mandatory processing but does not specify the precise conditions, the personal data concerned should be processed in accordance with the principles set out in the Section entitled '*Principles of processing personal data,'* strictly limited to the scope necessary to comply with the legal obligations and for the shortest possible duration.

The processing of sensitive data (genetic, biometric or health data) is subject to the explicit, recorded consent of the data subject, unless the sensitive data have been disclosed by the customer or the notifier in a written submission or through one of the Company's electronic interfaces, or the processing of sensitive data is required by law. Their consent to the processing of such data to the extent necessary shall be deemed to be given at the time of such written submission; however, the data concerned may only be processed in relation to the matter to which the submission relates.

Sensitive data may also be processed in the following cases:

- where the processing is necessary to protect the vital interests of the data subject or of another natural person if the data subject is physically or legally incapable of giving consent;
- where the processing relates to personal data which are manifestly made public by the data subject;
- where the processing is necessary for the submission, enforcement or defence of legal claims.

If the Company carries out processing operations for a third party or a third party carries out processing operations for the Company involving personal data, prior to the commencement of processing the parties shall, in accordance with Article 28 of the GDPR and Section 25/D (1) of the Privacy Act, conclude a contract establishing their legal relationship, containing, in particular, the subject matter, duration and nature of the legal relationship for the processing, as well as the purpose of processing, the type of data processed, the categories of data subjects, the rights, obligations and responsibilities of the parties, and the guarantees set out in Article 28(3) of the GDPR.

Before the commencement of processing operations, the data subject shall be clearly and elaborately informed of all aspects concerning the processing of his or her personal data, in particular, the purpose for which his or her data are required and the legal basis, the person entitled to control the data and to carry out the processing, the duration of the proposed processing operation, whether the data subject's personal data are processed based on the consent of the data subject, and the persons to whom the data may be disclosed.

The information given to the data subject shall specify the purposes for which the personal data are processed clearly, accurately and precisely, in particular where the duration of the processing of personal data is defined, without determining a specific time limit, as the time needed to achieve the purposes of the processing.

Information shall also be provided on the data subject's rights and remedies. In the case of mandatory processing such information may be supplied by way of publishing reference to the legislation containing the information above.

The information must be provided in an understandable and easily accessible form, using clear and plain language. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from such other matters.

If the provision of personal information to the data subject proves impossible or would involve disproportionate costs, the obligation of information may be satisfied by the public disclosure of the following (including on the Company's official website):

- identity and contact details of the controller;
- contact details of the data protection officer(s);
- indication of the fact that data are being collected;
- scope of data subjects;
- purpose and legal basis for the collection of data;
- duration of processing;
- controllers to whom data may be disclosed to;
- rights and remedies available to the data subjects in connection with the processing.

Informing data subjects of the processing of personal data

The Company shall ensure that the data subjects are informed in a concise, transparent, intelligible and easily accessible form, in a clear and plain language (in writing, or orally upon request, after identification of the data subject) of the details of the processing (controller's data, purpose, legal basis, duration of the processing), the scope of the data processed, possible data transfers), their legal remedies in relation to the processing (including the relevant rules of jurisdiction), the contact details of the data protection officer and possible legal consequences (including the consequences of the data subject's failure to provide the data, possible withdrawal of consent).

If further processing of personal data becomes necessary for a purpose other than that for which the personal data were obtained, the data subject shall be informed of the different purpose and of all relevant facts concerning the processing prior to such further processing.

4. Consent of the data subject as the legal basis for processing

(1) Where the legal basis for processing is the consent of the data subject, the Company shall be able to demonstrate that the data subject has duly consented to the processing of his or her personal data.

(2) The consent of the data subject may be deemed a valid legal basis for processing if it is a 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. Silence, pre-ticked boxes or inactivity shall not constitute consent.

(3) In obtaining the data subject's consent, it should be ensured that he or she is given a real choice. Consent should not be regarded as freely given if the data subject is unable to refuse or withdraw consent without detriment or there is a clear imbalance between the data subject and the controller.

(4) Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations.

(5) Consent should not be regarded as freely given if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance.

(6) The controller is required to ensure that the data subject can withdraw consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent in the period prior to its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent. The Company keeps up-to-date records of the granting and withdrawal of consents.

(7) Where the controller obtains the data subject's consent through a written statement, the consent form must be clearly and unambiguously separated from the rest of the contract and must be drafted in clear and plain language by the controller.

5. Rights of the data subject and their enforcement

Under the GDPR, data subjects shall have the following rights:

- to request information at any time regarding the processing of his or her personal data, and has the right to access his or her personal data and to access information concerning the processing of such data;
- to request the rectification of his or her personal data, and to have incomplete personal data completed;
- to request the erasure, restriction or blocking of personal data, except for mandatory processing;
- to object to the processing of personal data; and
- have the right to data portability as set out in Section 10.25.

5.1 Obligation to provide prior information

(1) Where the personal data processed are collected by the Company from the data subject, at the time when the personal data are obtained, the data subject shall be informed of the identity and contact details of the controller and the controller's representative, the contact details of the Company's data protection officer, the purposes of the processing for which the personal data are intended as well as the legal basis for the processing, the legitimate interests pursued by the controller or by a third party where processing is based on legitimate interest, the recipients or categories of recipients of the personal data, the fact that the controller intends to transfer personal data to a third country or international organisation, the period for which the personal data will be stored, or the

criteria used to determine that period, the existence of the data subject's right to request from the Company access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability, the right to lodge a complaint with a supervisory authority, whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data, and the existence of automated decision-making, including profiling, where applicable. Information on the possibility of exercising the right to object shall be presented clearly and separately from any other information.

(2) The above information shall be provided:

a) to persons who enter into an employment, agency or other legal relationship for the performance of work with the Company, at the time of the establishment of the legal relationship, general information in accordance with the relevant Privacy Notice of the Company;

b) to applicants for employment with the Company, in accordance with the relevant Privacy Notice of the Company;

c) to persons who have a contractual relationship with the Company, in accordance with the content of the relevant Privacy Notice of the Company.

(3) The information referred to in sub-paragraph 2(a) shall be provided electronically by indicating the link to the relevant Privacy Notice or by incorporating it into the text of the contract, while the information referred to in sub-paragraph 2(c) shall be provided by indicating the link to the relevant Privacy Notice in the text of the contract.

(4) In order to ensure that applicants applying for a job at the Company are provided information on the processing of their personal data before submitting their application, in the call for applications the Company refers to the availability of the relevant information on the website.

(5) Where the personal data processed have not been obtained by the Company from the data subject, the Company shall provide the data subject with the necessary information within a reasonable period of time from the date of obtaining the personal data but no later than one month, or, if the personal data are used for the purpose of contacting the data subject, at least at the time of the first contact with the data subject or, if the data are likely to be communicated to another recipient, at the time of the first communication of the personal data at the latest. In this context, the data subject shall be informed of the identity and contact details of the Company and its representative, the contact details of the data protection officer, the purposes of the processing for which the personal data are intended as well as the legal basis for the processing, the categories of personal data concerned, the recipients or categories of the recipients of the personal data, the fact that the controller intends to transfer personal data to a recipient in a third country or international organisation, the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period, where the processing is based on the legitimate interest of the controller the legitimate interests pursued by the controller or by a third party, the existence of the

data subject's right to request from the Company access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability and, where the processing is based on consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal, the right to lodge a complaint with a supervisory authority, the source from which the personal data originate and, where applicable, whether the data came from publicly accessible sources, and the existence of automated decision-making, including profiling, where applicable.

(6) Under the dedicated 'Privacy Policy' tab, the Company shall publish on its website information related to its other activities that may involve personal data processing if such information is not covered in Section 22, in a concise, transparent, intelligible and easily accessible form, in clear and plain language, to ensure that data subjects are aware of it in advance.

(7) In the case of persons whose mother tongue is not Hungarian, the information shall also be provided in his or her language. In such a case, the Company will arrange for the translation of the information through its data protection officer.

(8) The Company shall communicate any rectification or erasure of personal data or restriction of processing to each recipient to whom it disclosed the personal data, unless this proves impossible or involves disproportionate effort.

(9) The data subject may submit his or her request by post (registered office: H-1016 Budapest, Bérc utca 13–15, postal address: H-1062 Budapest, Bajza utca 44, Baruch Palace), by electronic means (gdpr@hiia.hu) or in person at the registered office of the Company.

(10) The Company may not refuse to provide the data subject with information unless the GDPR or the law so permits. The grounds for refusing to disclose the information shall be communicated to the data subject.

(11) Information and communication shall be provided to the data subject free of charge, unless the data subject's request is manifestly unfounded or excessive, in particular because of its repetitive nature, in which case the Company may charge a reasonable fee taking into account the administrative costs, or refuse to act on the request.
The information under this Section need not be provided if
a) the data subject already has the information;
b) the provision of the information proves impossible or would involve a disproportionate effort; or
c) obtaining the data is required by law.

(12) Where the data subject has requested access to his or her personal data processed by the Company, the data processed and the relevant information shall be made available to the data subject as soon as possible. Where the data subject has made his or her request electronically, the information shall be provided in a widely used electronic format (e.g. pdf), in anonymised form; i.e. excluding the personal data of any person other than the data subject.

5.2 The data subject's right to information (right of access)

(1) At the request of the data subject – accepted after verification of his or her eligibility – the competent staff member responsible for processing or the data protection officer shall provide

information on the ongoing processing of the personal data of the data subject within no later than 1 month of receipt of the request.

(2) The data subject shall have access to the personal data and the following information:

a) purposes of processing;

b) the categories of personal data concerned;

c) the recipients or categories of recipients to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

f) the right to lodge a complaint with a supervisory authority;

g) where the personal data are not collected from the data subject, any available information as to their source;

h) the existence of automated decision-making, including profiling and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

(3) Access to personal data must be ensured in such a way that the data subject does not have access to the data of another person.

(4) The Company may restrict or deny the data subject's right of access in proportion to the purpose pursued, if such a measure is indispensable for:

a) the efficient and effective conduct of investigations or proceedings involving the Company, in particular criminal proceedings;

b) the efficient and effective prevention and prosecution of criminal offences;

c) the enforcement of penalties and measures against offenders;

d) the efficient and effective protection of public security;

e) safeguarding the external and internal security of the State efficiently and effectively, in particular, defence and national security; or

f) ensuring the protection of the fundamental rights of third parties.

(5) If the Company refuses or restricts the right of access of the data subject, it shall inform the data subject in writing without delay, provided that the purpose of the restriction or refusal is not jeopardised, stating the reasons for the measure. In the information, the Company shall specifically draw the attention of the data subject to the fact that he or she may also exercise his or her right of access with the assistance of the supervisory authority.

5.3 Right to rectification

If the personal data are deemed inaccurate and the accurate personal data are at the Company's disposal, the Company rectify or supplement the personal data without undue delay, at its own discretion or at the request of the data subject (free of charge), accepted after verification of his or her eligibility. Taking into account the purposes of the processing, the data subject shall also have the right to have incomplete personal data completed, including by means of providing a supplementary statement. The Company shall inform the organisations to which it normally transmits data of the rectification of the data.

5.4 Right to restriction of processing

(1) At the request of the data subject – accepted after verification of his or her eligibility – the competent staff member responsible for processing or the data protection officer shall restrict processing where one of the following applies:

a) the accuracy of the personal data is contested by the data subject, for a period enabling the competent staff member responsible for processing or the data protection officer to verify the accuracy of the personal data;

b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

c) the Company no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims; or

d) the data subject has objected to processing, pending the verification whether the legitimate grounds of the controller override those of the data subject.

(2) Where the processing is restricted as referred to above, such personal data, except for storage, may be processed only with the consent of the data subject or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or of an important public interest of the Union or of a Member State. During the restriction period, the restricted personal data may not be processed for the purpose(s) specified and shall be stored separately.

(3) The competent staff member responsible for processing or the data protection officer shall inform the data subject at whose request the processing has been restricted of the lifting of the restriction in advance.

(4) When data are rectified, restricted or erased, the data subject and all recipients to whom they were transmitted for processing shall be notified; at his or her request, the data subject shall be notified of such recipients. The notification shall not be required if it proves impossible or would involve a disproportionate effort.

5.5 Right to erasure ('right to be forgotten')

(1) At the request of the data subject – accepted after verification of his or her eligibility – the competent staff member responsible for processing or the data protection officer shall erase the data subject's personal data, or the scope of data specified by the data subject, where one of the following applies:

a) the data subject requests the erasure (unless this is precluded by a legal obligation);

b) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

b) the data subject withdraws the consent on which the processing is based and there is no other legal ground for the processing;

c) the data subject objects to the processing and there are no overriding legitimate grounds for the processing;

d) the personal data are incomplete or inaccurate and this cannot be lawfully rectified, unless the erasure is not precluded by a legal obligation;

e) the personal data have been unlawfully processed;

f) the personal data are no longer necessary in relation to the purposes for which they were processed or the statutory time limit for storage has expired (the requirement of erasure shall not apply to personal data recorded on a carrier that is to be deposited in archive under the legislation on the protection of archive materials.)

g) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the Company is subject;

h) the personal data have been collected in relation to the direct offer of information society services to children;

i) the erasure of the personal data has been ordered by a court or public authority.

(2) Where the Company has made the personal data public and is obliged, in accordance with the above, to erase the personal data, taking account of available technology and the cost of implementation, it shall take reasonable steps, including technical measures, to erase any links to, or copy or replication of, those personal data.

(3) The Company shall not erase personal data despite a legitimate request, to the extent that processing is necessary:

a) for exercising the right of freedom of expression and information;

b) for compliance with a legal obligation which requires processing by Union or Member State law to which the Company is subject;

c) for the performance of a task carried out in the public interest;

d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in so far as the erasure is likely to render impossible or seriously impair the achievement of the objectives of that processing;

e) for the establishment, exercise or defence of legal claims.

(4) The Company shall reject the data subject's request for erasure where erasure may not be requested in accordance with this Section or where the Company has an adequate legal basis for processing the personal data concerned by the erasure request even after the withdrawal of the data subject's consent (e.g. it has a statutory obligation to process the data concerned or processing is necessary for the performance of the contract concluded with the data subject).

5.6 Right to object

(1) Where the Company processes the data subject's data on the following legal bases:

a) processing is necessary for the performance of a task carried out in the public interest; or
b) the processing is necessary for the purposes of the legitimate interests pursued by the Company or by a third party,

the data subject may object to the processing of the personal data thus processed, including profiling that is based on the abovementioned provisions. In such a case the Company shall no longer process the personal data unless it demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

(2) Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to the processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

(3) In the event of objection, the Company shall investigate the cause of objection within the shortest possible time, adopt a decision as to merits and shall notify the data subject in writing of its decision within the statutory time limit. During the investigation, the processing of the personal data concerned by the objection shall be restricted.

(4) If, according to the findings of the Company the data subject's objection is justified, it shall terminate all processing operations (including data collection and transmission), and notify – to the extent it is possible – all recipients to whom any of these data had previously been transferred

concerning the objection and the ensuing measures, upon which these recipients shall also take measures regarding the enforcement of the objection.

(5) If the data subject does not agree with the Company's decision or if the Company fails to inform the data subject within the relevant time limit, the data subject may take the matter to court. Where the data subject objects to the processing of personal data that are (also) processed by the controller for direct marketing purposes, the personal data may no longer be processed for such purposes.

5.7 Right to a judicial remedy

In the event of a breach of his or her rights in relation to processing, through the staff member responsible for processing or directly, the data subject may contact the data protection officer, who shall investigate the complaint and, where it is well-founded, take action with the Company's Managing Director; otherwise the complaint shall be rejected. He or she will inform the complainant of the refusal in writing within 1 month of receipt of the request at the latest, stating the factual and legal grounds for the refusal. If the request is rejected, the complainant shall be informed of the possibility of judicial remedy and recourse to a supervisory body. The data protection officer is required to draw up a protocol for all rejected requests.

6. Security of processing

6.1 Data security rules

(1) The Company will ensure the safe handling and storage of data. To this end, it takes, monitors and, where necessary, develops the necessary technical and organisational measures, both for datasets stored via information technology devices and on traditional paper-based media. The Company shall ensure that the manner of maintaining the records and the content thereof comply with the legislation in effect.

Taking into account the state of science and technology, the costs of implementation and the nature, scope, context and purposes of processing as well as the potential risks involved, the Company shall ensure a level of security appropriate to the risk, including as appropriate the pseudonymisation and encryption of personal data.

The Company shall apply suitable measures to protect the data processed by it from unauthorised access, alteration, transmission, public disclosure, deletion or destruction, as well as damage and accidental loss, and ensure that the data stored cannot be corrupted or rendered inaccessible due to any changes in or modification of the applied technique.

The effectiveness of the technical and organisational measures adopted to ensure the security of data processing shall be monitored regularly and, if a deficiency is detected, measures shall be taken as soon as possible to remedy it.

The Company implements appropriate technical and organisational measures in order to ensure that processing is limited to personal data which are necessary for each specific purpose of the processing. This obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.

(2) In order to ensure data security, the Company assesses and records all data processing operations carried out by it. The registry is maintained by the data protection officer.

(3) Based on the records of data processing operations, the Company conducts a risk analysis, which is intended to assess which organisational unit carries out each processing operation under which conditions, and which risk factor may lead to what kind of personal data breach with what possible damage. The risk analysis shall be carried out based on data processing activity that has been actually performed. The purpose of the risk analysis is to define security rules and measures that effectively ensure the appropriate protection of personal data aligned with the Company's operations and activities.

(4) Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the Company shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the GDPR.

a) the pseudonymisation and encryption of personal data;

b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

(5) In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

(6) These measures are reviewed and updated as necessary by the data protection officer.

(7) The Company implements appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. This obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that, by default, personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

(8) A document containing personal data should not be left in a place accessible to a third party. Such documents also need to be stored securely in offices or staff rooms where third parties other than the authorised file managers may be present.

(9) In agreement with the data protection officer, the head of the data manager organisational unit shall decide on the security of the location and physical protection of the data carrier images and documentation.

(10) The environment of the data management system to be established at the organisational units shall be protected by the competent managers, taking into account local circumstances, including the prevention of data breaches.

(11) In order to prevent the loss of manually processed personal data, original documents shall only be released in the course of official administrative procedures, in particular judicial proceedings or investigative procedures. Prior to releasing the documents, a complete copy of the original shall be made for safekeeping at the competent organisational unit.

(12) In the event of the corruption or destruction of personal data, attempts shall be made to replace the corrupted data to the extent possible from other available data sources. Responsibility for replacing the corrupted data shall be taken by the head of the unit where the corruption occurred. The relevant operator who participated in the recording of the data shall be involved in the data replacement. The fact that the data have been replaced shall be indicated on the data concerned.

(13) In particular, the Company applies the following technical and organisational measures: regular password changes and the application of strong passwords, multi-factor authentication, regular backups, encrypted data transmission (TLS/SSL), annual review of access rights, storage of paper-based documents in a lockable cabinet.

6.2 Data protection officer

(1) The data protection officer is appointed by and reports to the Managing Director.

(2) The data protection officer may be an employer of the Company, or fulfil his or her tasks under a service contract. The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39 of the GDPR.

(3) After the appointment of the data protection officer, the Company shall publish his or her contact details, and communicate them to the supervisory authority.

(4) The data protection officer shall perform the tasks specified in the GDPR, and in this respect he or she shall cooperate closely with the Company's organisational units and the Managing Director.

(5) The data protection officer shall have, in particular, the following tasks:

a) to inform and advise at the Company the controller or the processor and the employees who carry out processing of their obligations pursuant to the GDPR and to other Union or Member State data protection provisions;

b) to monitor compliance with the GDPR, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

c) to provide advice where requested as regards the data protection impact assessment and monitor its performance;

d) to cooperate with the supervisory authority;

e) to act as the contact point for the supervisory authority on issues relating to processing, and to consult, where appropriate, with regard to any other matter;

f) to participate and assist in the decision-making process with regard to data processing and enforcing the rights of data subjects;

g) to investigate complaints conveyed to him or her and, if any unauthorised data processing operations are detected, call on the controller or processor concerned to discontinue such operations;

h) to organise training on the subject of data protection.

(6) The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

(7) The data protection officer shall provide professional advice on the following record-keeping obligations to be fulfilled by the Company:

a) the records of the processing activities carried out by the Company shall contain the name and contact details of the controller organisational unit and, where applicable, the name and contact details of the joint controller, the controller's representative and the data protection officer; the purposes of the processing; a description of the categories of data subjects and of the categories of personal data; the categories of recipients to whom the personal data have been or will be disclosed; where applicable, information on the transfer of personal data to a third country or an international organisation (including a description of the suitable safeguards); where possible, the envisaged time limits for erasure of the different categories of data; and, where possible, a general description of the technical and organisational security measures for data protection. Records shall be stored in written or electronic form and kept up to date.

b) with a view to verifying measures relating to personal data breaches and informing data subjects, the registry of personal data breaches detected at the Company shall contain the personal data affected, the scope and number of the data subjects involved, the date, time, circumstances and effects of the personal data breach, the measures taken to eliminate thereof, as well as other information required by law, as defined in Annex 2 to this Policy.

c) with a view to verifying legitimacy of data transfer and for the provision of information to the data subject, the Company shall maintain a data transfer registry, containing the date and time of the transmission, the legal basis of the transfer and the recipient, description of the personal data transmitted, and other information required by the relevant legislation on data processing, as defined in Annex 3 to this Policy.

(8) The data protection officer may get involved, properly and in a timely manner, in all issues which relate to the protection of personal data, and may have access to personal data and processing operations in carrying out his or her tasks.

(9) The data protection officer may not be instructed in the performance of his or her duties.

(10) He or she shall not be dismissed or penalised by the Company in relation to the performance of his or her tasks.

(11) Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under the GDPR.

(12) The data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law.

(13) The data protection officer may fulfil other tasks and duties. If the Company entrusts the data protection officer with other tasks, it shall ensure that no conflict of interest arises from such additional tasks.

6.3 Data protection impact assessment and prior consultation

(1) 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 Company 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.

(2) The Company shall seek the professional advice of the data protection officer when carrying out a data protection impact assessment.

(3) A data protection impact assessment shall in particular be required in the case of:

a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

b) processing on a large scale of special categories of personal data or of personal data relating to criminal convictions and offences; or

c) a systematic monitoring of a publicly accessible area on a large scale.

(4) The impact assessment shall contain at least:

a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;

b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

c) an assessment of the risks to the rights and freedoms of data subjects; and

d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR taking into account the rights and legitimate interests of data subjects and other persons concerned.

(5) The Company may seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.

(6) Where necessary, the Company shall carry out a review to assess if processing is performed in accordance with the previously conducted data protection impact assessment at least when there is a change of the risk represented by processing operations.

(7) The data protection officer shall consult the supervisory authority prior to processing where the data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk (prior consultation).

(8) The Company, through the Data Protection Officer, shall inform the supervisory authority in prior consultation with the supervisory authority:

a) where applicable, the respective responsibilities of the controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings;

b) the purposes and means of the intended processing;

c) the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to the GDPR;

d) the data protection impact assessment; and

e) any other information requested by the supervisory authority.

If, as a result of the prior consultation, the data protection authority finds that the envisaged processing would be in breach of the statutory principles of data protection, in particular if the identification of the risk or the envisaged measures to address it are inadequate, it shall provide written advice or exercise its other powers within 6 weeks (which may be extended by the data

protection authority for an additional month) of receipt of the request for consultation. The precise conditions of the envisaged processing shall be designed in consideration of the recommendations received in consultation with the data protection authority and in accordance with the advice given by the data protection authority.

6.4 Management of personal data breaches

(1) If any employee, agent or any other person authorised to act on behalf of the Company detects or becomes aware of a personal data breach at the Company, he or she shall notify the data protection officer immediately by completing the Personal Data Breach Notification Form presented in Annex 1 to this Policy.

(2) In the case of a personal data breach, the data protection officer shall without undue delay, not later than 72 hours after the personal data breach has been detected, report the personal data breach to the competent supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

(3) The notification to the supervisory authority shall at least:

a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

c) describe the likely consequences of the personal data breach;

d) describe the measures taken or proposed to be taken by the Company to remedy the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

(4) Where it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

(5) The data protection officer shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken.

(6) When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the Company shall communicate – primarily through the data protection officer – the personal data breach to the data subject without undue delay.

(7) The communication to the data subject shall describe in clear and plain language the nature of the personal data breach and contain at least the following information and measures:

a) the name and contact details of the data protection officer or other contact point where more information can be obtained;

b) the likely consequences of the personal data breach;

d) the measures taken or proposed to be taken by the Company to remedy the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

(8) The communication to the data subject shall not be required if any of the following conditions are met:

a) the Company has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;

b) the Company has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise;

c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

(9) Following the implementation of the measures taken in relation to the personal data breach, the Company shall assess the effectiveness of the measures and, if necessary, carry out a new risk analysis with respect to the data concerned.

7. Data transfer

(1) In all cases, data may be transferred only with the consent of the data subject or on the basis of a legal authorisation.

(2) Data may be transferred abroad in accordance with the provisions of Section 8 of the Privacy Act, and to third countries outside the borders of the European Union in accordance with Articles 44–46 of the GDPR.

(3) Within the Company's organisational system, personal data may be transferred, to the extent and for the period necessary for the performance of the task, to an organisational unit or person whose access to and processing of personal data are necessary for the performance of his or her task at the Company. Within the Company's organisation, personal data may only be transferred in accordance with the principles of purpose limitation and data minimisation, and access to the data may only be granted for an appropriate purpose. Within the Company's organisation, the requesting party may submit a request in writing to the competent data owner, concurrently informing the data owner's manager at the executive level, specifying the exact scope of the data requested and the purpose thereof.

(4) The Company may combine processing for different purposes only in accordance with legitimate purposes and where justified.

(5) A request for the transfer of personal data processed by the Company may only be fulfilled on the basis of a legal requirement or, in the absence thereof, only if the data subject gives his or her consent in a verifiable manner after having been informed in detail. In all other cases, the transfer shall be refused.

(6) In the case of data transfers abroad, the data exporter must specifically verify that the conditions for data transfers abroad set out in the GDPR are met. In this context, it should be assessed whether the transfer is made in accordance with a legal basis set out in the GDPR and whether an adequate level of data protection is ensured by the recipient controller. Where the transfer is to a Member State of the European Economic Area, the adequate level of protection of personal data needs not be assessed.

(7) Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if the conditions laid down in the GDPR are complied with both by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation.

(8) A transfer of personal data to a third country or an international organisation may take place where the European Commission has decided – and published in the Official Journal of the European Union and on the website thereof – that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection (adequacy decision). Such a transfer shall not require any specific authorisation.

(9) Unless provided otherwise by law, the Company may only transfer personal data if it is the controller of the data. Where another body is the controller, the data request shall be refused – unless provided otherwise by law – and the requesting party shall be informed of the body, where identifiable, from which he or she may request the data.

(10) In all cases, the transfer shall be documented in such a way that its lawfulness can be readily demonstrated (Annex 3 – on data transfers, Annex 3/A – on transfers based on a statutory requirement). The document drawn up on the transfer is also intended to inform the data subjects.

(11) If personal data are transferred as a postal consignment, it shall be sent in a sealed package.

(12) The Company undertakes to provide personal data for statistical purposes only in such a way that they may not be linked to the data subject.

II. Special provisions

1. Personal data processed manually

(1) In determining and applying the measures intended to ensure the security of processing, the Company shall take into account the current level of development of technology. Where alternate data processing solutions are available, the one selected shall ensure the highest level of protection of personal data, except where this would entail unreasonable hardship for the Company.

(2) To ensure the security of manually processed personal data, the following measures shall be taken:

a) archived documents shall be held in a lockable, dry room equipped with fire safety and property protection equipment;

b) only authorised staff members shall have access to documents processed actively on a continuous basis, and personnel, payroll and employment files shall be stored securely locked;

c) the documents related to processing carried out by the Company shall be archived regularly and the archived documents shall be sorted and filed in accordance with the Company's document management and scrapping policy and its filing plan, taking into account the provisions of Act LXVI of 1995 on Public Records, Public Archives, and the Protection of Private Archives and the provisions of Government Decree No. 335/2005 (XII. 29.) on the general document management requirements of public sector bodies.

(3) The rules for access to the keys of the premises or lockers concerned shall be established by the head of the Company's relevant organisational unit and shall be communicated to the data protection officer.

2. Personal data processed electronically

(1) If the Company processes personal data in an electronic system that may only be accessed by a registered, authorised person listed on the access list as a person with access rights, the authorised person shall log in to the system with a unique, secret password. The authorised person shall ensure, also with a view to avoiding personal data breaches, that the password is protected and shall log out of the system when the processing is completed. The unique password allocated to the authorised person may be revealed only to the IT staff responsible for the development and operation of the data management software and to the data protection officer, if it is necessary for the performance of their duties at the Company.

(2) The computers used for data processing may not be left unattended in a state suitable for data entry or retrieval.

(3) The Company may only use a data management system that is capable of registering access to the system, with the recorded data indicating at what time the data were recorded by whom.

III. Final provisions

(1) This Policy shall enter into effect on the date of signature and, subject to continuous review, it shall remain in effect until revoked. On the effective date of this Policy, the Privacy and Data Security Policy dated 06/09/2023 and all amendments thereto shall be repealed.

(2) The Finance Directorate shall ensure that this Policy and the annexes thereto are made available to the staff members covered by the personal scope of the Policy. The Policy shall be made available to the employees of the Company and to persons engaged by the Company under a contract of assignment at the Secretariat of the Managing Director, on the Company's electronic platform or via electronic means.

(3) Annexes to this Policy may be amended subject to the Managing Director's approval without the amendment of this Policy.

Budapest, 1 October 2025

Dorina Molnár
Managing Director

Annex 1/A – Personal Data Breach Notification Form

(Template)

MAGYAR KÜLÜGYI INTÉZET Nonprofit Zrt.
registered office: H-1016 Budapest, Bérc utca 13–15
company registration number: 01-10-142325

Unique file number:

I. Notifier of personal data breach

- name:
- position:
- workplace contact details:

II. Particulars of the personal data breach

- nature:
- assumed date, time and place:
- date/time and manner of detection:
- categories and approximate number of data subjects concerned:
- scope and approximate number of personal data concerned:
- perceived or potential consequences:
- measures taken or proposed to be taken to remedy the breach; persons who ordered and implemented the measure (by name and position):

III. The personal data breach is likely to result in a high risk to the rights and freedoms of natural persons: YES / NO

IV. Other comments:

Budapest, ... day …….. month 20…...

_____

Annex 1/B – Personal Data Breach Registry

(Template)

MAGYAR KÜLÜGYI INTÉZET Nonprofit Zrt.
registered office: H-1016 Budapest, Bérc utca 13–15
company registration number: 01-10-142325

Unique file number:

For compliance with Article 33(5) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Regulation (EC) No 95/46/EC (GDPR), and for the enforcement of accountability under Article 5(2) of the GDPR, Magyar Külügyi Intézet (Hungarian Institute of International Affairs) keeps the following registry of personal data breaches.

#	Date, place and time of the personal data breach	Number of data subjects involved in the personal data breach	Scope of the personal data concerned	It concerns data under Article 9 or Article 10 of the GDPR	Transfer to a third country	Circumstances of the personal data breach, other data prescribed by the legislation requiring the processing	Effects of the personal data breach	Measures taken to eliminate the data breach	Date of entry, name and signature of the recorder
1.									
2.									
3.									
4.									
5.									
6.									
7.									

Annex 1/C – Data transfer registry

(Template)

MAGYAR KÜLÜGYI INTÉZET Nonprofit Zrt.
registered office: H-1016 Budapest, Bérc utca 13–15
company registration number: 01-10-142325

For the verifiability of compliance with the requirements set out in Recital (111) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Regulation (EC) No 95/46/EC (GDPR), and for the enforcement of accountability under Article 5(2) of the GDPR, the Hungarian Institute of International Affairs keeps the following registry of data transfers.

#	Date of the transfer of personal data	Name of the reporting organisational unit	Legal basis and purpose of the transfer	Scope of personal data transferred	Recipient of the data transfer	Transfer to a third country	Other data prescribed by the legislation requiring the processing, additional comments	Date of entry, name and signature of the recorder
1.								
2.								
3.								
4.								
5.								
6.								
7.								

Annex 2 – Protocol on data transfer

PROTOCOL
on data transfer

I, the undersigned ..... (address/registered office, hereinafter: controller) hereby declare that MAGYAR KÜLÜGYI INTÉZET Nonprofit Zrt. (registered office: H-1016 Budapest, Bérc utca 13–15, company registration number: 01-10-142325) has transferred data to me for the purpose of processing as follows:

date of the transfer of personal data: ……..

legal basis for the transfer: ……..

recipient of data transfer: ……..

scope of the personal data transferred: ……..

other data prescribed by the legislation requiring the processing (where appropriate): ……..

data were transferred to a third country outside the EEA (hereinafter: 'abroad') (yes/no) (if data are transferred to a foreign country in respect of which the European Commission has not adopted an adequacy decision, safeguards provided by the recipient controller/processor or the number of the special authorisation issued by NAIH: ……

Where neither the Commission's adequacy decision nor appropriate safeguards are available, this Protocol shall be accompanied by the data subject's consent or by an indication of one of the grounds referred to in Article 49(1)(b) to (g) of Regulation (EU) 2016/679 of the European Parliament and of the Council (GDPR): ……..

The Controller hereby declares that it shall act in accordance with the provisions of Act CXII of 2011 on the Right of Informational Self-Determination and Freedom of Information, the GDPR and other applicable legal provisions.

Dated, ...

MAGYAR KÜLÜGYI INTÉZET Nonprofit Zrt.	recipient of the data transfer

Annex 3 – Protocol on data transfer based on a legal obligation

PROTOCOL
on data transfer based on a legal obligation

I, the undersigned ....., hereby declare that MAGYAR KÜLÜGYI INTÉZET Nonprofit Zrt. has carried out a data transfer for the purpose of compliance with its statutory reporting obligations as follows:

Date of the transfer of personal data: ……

Legal basis for the transfer: ……

Recipient of data transfer: ……

Scope of the personal data transferred: ……

Other data prescribed by the legislation requiring the processing (where appropriate): ……
Data were transferred abroad (yes/no)[1] ....

The letter containing the data transferred and the annex(es) thereto are attached.

Dated, ...

_____
MAGYAR KÜLÜGYI INTÉZET Nonprofit Zrt.

Annex 4 – Protocol on data erasure

PROTOCOL ON DATA ERASURE

Date: …….

Reasons for the erasure: data subject's request; withdrawal of consent; unlawful processing; expiry of the statutory storage period; storage is no longer necessary for the given purpose; other: ……..

Which data were erased? ……...……
……...…….....

How long had they been stored?
……...

From which registry were data erased? ……...…….

The erasure was performed by (IT specialist):
……..…….

Backups in which the erased data may be (are) included: …….
…….
.

Where personal data that have been made public, person to be notified of the erasure: ……
…….
.

Robinson list / restriction of processing: …….

IT specialist:	signature: ……. name:	data protection officer:	signature: ……. name:

Annex 5: Form for keeping a record of processing operations

FORM
for keeping a record of processing operations

Internal processing registration number (to be filled in by the data protection officer):
MKI - ☐☐☐☐☐☐☐☐ **-** ☐ **-** ☐

1. Name of processing operation: Click or tap here to enter text.
- purpose, function: Click or tap here to enter text.
- detailed description (including data flow) Click or tap here to enter text.
- legal basis: *Select an item.*
- responsible manager: Click or tap here to enter text.
Position: Click or tap here to enter text.
Contact details: Click or tap here to enter text.
Organisational unit: Click or tap here to enter text.
Exact address or website of the actual processing operation (if processing takes place on a website or in data centres other than those at HIIA's headquarters*):* Click or tap here to enter text.
Data availability (exact name of database and application): Click or tap here to enter text.
System administrator: Click or tap here to enter text.
General description of technical and organisational data security measures: Click or tap here to enter text.
IT security classification of data: Click or tap here to enter text.
Source of data: Click or tap here to enter text.
Scope of personal data processed: Click or tap here to enter text.
Scope of sensitive data (e.g. genetic, biometric, health) **processed:** Click or tap here to enter text.
Availability of Consent Form for sensitive data: Click or tap here to enter text.
Are data of minors (under 16 years of age) **/ vulnerable data subjects being processed?** Click or tap here to enter text.
Does the processing involve profiling? (If so, provide a brief description:) Click or tap here to enter text.
Duration of processing: (if possible, specific reference to legislation, the exact duration of processing is required, including the retention period and the time of erasure): Click or tap here to enter text.
Estimated number of data subjects: Click or tap here to enter text.
Scope of data subjects: Click or tap here to enter text.
Manner of notification of data subjects in the event of a breach: Click or tap here to enter text.
Availability of documentation where consent is given: Click or tap here to enter text.
Notification of data subjects of the processing (how and when): Click or tap here to enter text.

2. Processing (to be completed only if external processor is used)
Name of processor: Click or tap here to enter text.
address: Click or tap here to enter text.
Name of contact person: Click or tap here to enter text.
Phone number: Click or tap here to enter text.
E-mail address: Click or tap here to enter text.

Processing activity (e.g.: data recording, providing technical support, mailing,...): Click or tap here to enter text.
Place of processing (address or website): Click or tap here to enter text.
Processing technology (manual/electronic): Click or tap here to enter text.
Processing contract available at: Click or tap here to enter text.

3. Data transfer, regular data supply

To whom, for which body: Click or tap here to enter text.
Exact address of the recipient: Click or tap here to enter text.
Exact legal basis for the transfer (consent of the data subject, legislation, ...): Click or tap here to enter text.
Type of data transmitted: Click or tap here to enter text.
Which data are involved? Click or tap here to enter text.
Method of transmission: Click or tap here to enter text.
Date of transmission: Click or tap here to enter text.
Regularity of the transfer: Click or tap here to enter text.
Are data transferred abroad or to a third country outside the EEA? Click or tap here to enter text.
A description of the appropriate safeguards enabling the transfer of data: Click or tap here to enter text.

Envisaged date of the next review of processing: .....

Dated in Budapest, ...

_____ _____

head of the controller organisational unit | data protection officer