

WEBSITE DATA PROCESSING NOTICE (PRIVACY POLICY)

The website operated by Mr. László Perger (hereinafter: *Business*) fulfils its obligation to provide prior information to data subjects regarding the processing of their personal data, as prescribed by REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (the “Regulation” or “GDPR”), by publishing this privacy notice. Under the relevant provisions of the Regulation, all information addressed to data subjects must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

I. IDENTIFICATION OF THE CONTROLLER

The Business informs the data subject that, in relation to the processing of personal data, it qualifies as the **data controller**.

OPERATOR OF THE WEBSITE: Károly Dörömbözy
TELEPHONE: 06203344910
DATA PROTECTION OFFICER: Károly Dörömbözy
LEGAL REPRESENTATIVE: Károly Dörömbözy
E-MAIL: info@safe4you.hu
WEBSITE: <https://l4y.hu>

Personal data may be accessed by the employees of the Business who have access rights linked to the given purpose of processing, and by those persons and organisations performing data processing activities for the Business on the basis of service contracts, to the extent determined by the Business and only to the extent necessary for the performance of their activities.

II. IDENTIFICATION OF THE DATA PROCESSOR(S)

1. Within the scope of personal data processed by the Business on the basis of the voluntary consent of the data subject, the Business engages an external data processor for the purpose of operating and maintaining its website.

OPERATOR OF THE WEBSITE: Károly Dörömbözy
TELEPHONE: 062033449410
DATA PROTECTION OFFICER: Károly Dörömbözy
LEGAL REPRESENTATIVE: Károly Dörömbözy
E-MAIL: info@safe4you.hu
WEBSITE: <https://l4y.hu>
ACTIVITY: E-learning training

III. DEFINITIONS

1. **“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;
2. **“processing”**: any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

3. **“restriction of processing”**: the marking of stored personal data with the aim of limiting their processing in the future;
4. **“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;
5. **“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;
6. **“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;
7. **“controller”**: the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;
8. **“processor”**: a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
9. **“recipient”**: a natural or legal person, public authority, agency or another body, to which or to whom 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 applicable data protection rules according to the purposes of the processing;
10. **“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;
11. **“data subject’s consent”**: 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;
12. **“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;
13. **“undertaking”**: a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity.

IV. LEGAL BASIS OF DATA PROCESSING

1. Consent of the data subject

1. The lawfulness of processing of personal data must be based on the consent of the data subject, or on another lawful basis established by law.
2. Where processing is based on the data subject's consent, the data subject may give consent to the processing of his or her personal data in the following forms:
 - a) in writing, in the form of a declaration granting consent to the processing of personal data;
 - b) electronically, by an explicit action performed on the Business's website, such as ticking a checkbox, or by making technical settings in connection with the use of information society services, or by any other statement or conduct which clearly indicates, in that context, the data subject's acceptance of the proposed processing of his or her personal data.
3. Silence, pre-ticked boxes or inactivity shall therefore not constitute consent.
4. Consent shall cover all processing activities carried out for the same purpose or purposes.
5. If the processing serves multiple purposes, consent must be given for all of those purposes. If the data subject gives consent following an electronic request, the request must be clear and concise and must not unnecessarily disrupt the use of the service for which consent is sought.
6. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. The data subject must be informed of this before consent is given. It must be as easy to withdraw as to give consent.

2. Performance of a contract

1. Processing shall be lawful if it 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.
2. The conclusion of a contract may not be made conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

3. Compliance with a legal obligation to which the controller is subject, or protection of vital interests of the data subject or another natural person

1. Where processing is based on compliance with a legal obligation, the legal basis of processing is determined by law; therefore, the data subject's consent is not required for processing his or her personal data.
2. The controller must inform the data subject of the purpose, legal basis and duration of the processing, the identity of the controller, as well as the data subject's rights and the available legal remedies.
3. On the basis of a legal obligation, the controller shall be entitled to process those categories of data that are necessary for the fulfilment of such obligation, even after the data subject has withdrawn his or her consent.

4. Performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, or for the purposes of the legitimate interests pursued by the controller or by a third party

1. The legitimate interests of the controller – including a controller to whom personal data may be disclosed – or of a third party may constitute a legal basis for processing, provided that the interests or fundamental rights and freedoms of the data subject do not override such interests, taking into consideration the data subject’s reasonable expectations based on his or her relationship with the controller. Such legitimate interest may exist, for example, where there is a relevant and appropriate relationship between the data subject and the controller, such as where the data subject is a client of the controller or is in the service of the controller.
2. In order to determine whether a legitimate interest exists, it is necessary to carefully examine, among other things, whether the data subject, at the time and in the context of the collection of the personal data, can reasonably expect processing for that purpose.
3. The data subject’s interests and fundamental rights may override the interest of the controller where personal data are processed in circumstances in which data subjects do not reasonably expect further processing.

V. RIGHTS OF THE DATA SUBJECT IN CONNECTION WITH THE PROCESSING OF HIS OR HER PERSONAL DATA

1. The Business provides the following brief information on the data subject’s rights:

The data subject has the right:

- a) to be informed prior to the start of processing;
- b) to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and to the following information;
- c) to obtain restriction of processing, and to receive notification from the controller when such restriction has been put in place;
- d) to data portability;
- e) to object where his or her personal data are processed for reasons of public interest or on the basis of the controller’s legitimate interest;
- f) not to be subject to automated decision-making, including profiling;
- g) to lodge a complaint with a supervisory authority. The data subject may exercise this right through the following contact details:
National Authority for Data Protection and Freedom of Information
Address: 1125 Budapest, Szilágyi Erzsébet fasor 22/c.
Telephone: +36 (1) 391-1400; Fax: +36 (1) 391-1410
Website: <http://www.naih.hu>
E-mail: ugyfelszolgalat@naih.hu
- h) to an effective judicial remedy against a supervisory authority;
- i) to an effective judicial remedy against the controller or the processor;
- j) to be informed about a personal data breach.

Data processors:

Data processing activity:

Hosting service provider: Sybell Informatika Kft.

Address: 1158 Budapest, Késmárk u. 7/B

Telephone: +36-1-707-6726

Website: <https://sybell.hu>

Information: hello@sybell.hu

2. Detailed information on the rights of the data subject

Right to be informed

1. The data subject has the right to receive information about the processing of his or her personal data before the processing activity begins.
2. Information to be provided where personal data are collected from the data subject:
 - a. the identity and contact details of the controller and, where applicable, of the controller's representative;
 - b. the contact details of the data protection officer, where applicable;
 - c. the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
 - d. where processing is based on point (f) of Article 6(1) of the Regulation, the legitimate interests pursued by the controller or by a third party;
 - e. the recipients or categories of recipients of the personal data, if any;
 - f.
 - g. where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or, in the case of transfers referred to in Article 46 or 47, or in the second subparagraph of Article 49(1) of the Regulation, the reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available.
3. In addition to the information referred to in paragraph (1), in order to ensure fair and transparent processing, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information:
 - a. the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
 - b. the existence of the data subject's right to request from the controller access to and rectification or restriction of processing of personal data concerning him or her and to object to processing, as well as the right to data portability;
 - c. where processing is based on point (a) of Article 6(1) of the Regulation or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
 - d. the right to lodge a complaint with a supervisory authority;
 - e. 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;
 - f. the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4)

of the Regulation 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.

4. Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:

- a. the identity and contact details of the controller and, where applicable, of the controller's representative;
- b. the contact details of the data protection officer, where applicable;
- c. the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- d. the categories of personal data concerned;
- e. the recipients or categories of recipients of the personal data, if any;
- f. where applicable, that the controller intends to transfer personal data to a recipient in a third country or an international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46, Article 47 or the second subparagraph of Article 49(1) of the Regulation, the reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available.

5. In addition to the information referred to in paragraph (1), the controller shall provide the data subject with the following additional information necessary to ensure fair and transparent processing:

- a. the period for which the personal data will be stored, or, if that is not possible, the criteria used to determine that period;
- b. where processing is based on point (f) of Article 6(1) of the Regulation, the legitimate interests pursued by the controller or by a third party;
- c. the existence of the right of the data subject to request from the controller access to and rectification or restriction of processing of personal data concerning him or her and to object to processing as well as the right to data portability;
- d. where processing is based on point (a) of Article 6(1) or point (a) of Article 9(2) of the Regulation, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- e. the right to lodge a complaint with a supervisory authority;
- f. from which source the personal data originate, and if applicable, whether they came from publicly accessible sources; and
- g. the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) of the Regulation 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.

6. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall, prior to that further processing, provide the data subject with information on that other purpose and with any relevant further information referred to in paragraph (5).

7. Paragraphs (1)–(3) shall not apply where and insofar as:

- a. the data subject already has the information;
- b. the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) of the Regulation, or in so far as the

obligation referred to in paragraph (1) of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;

c. obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or

d. where personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.

Right of access by the data subject

1. The data subject has the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed and, where that is the case, access to the personal data and the following information:

a. the purposes of the 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 of the data subject to request from the controller rectification or restriction of processing of personal data concerning him or her and 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, referred to in Article 22(1) and (4) of the Regulation and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing.

2. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards relating to the transfer pursuant to Article 46 of the Regulation.

3. The controller shall provide a copy of the personal data undergoing processing to the data subject. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, the information shall be provided in a commonly used electronic form, unless otherwise requested by the data subject.

Right to rectification and erasure

Right to rectification

1. The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject has the right to have incomplete personal data completed, including by means of providing a supplementary statement.

Right to erasure (“right to be forgotten”)

1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay, and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:
 - a. 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 consent on which the processing is based according to point (a) of Article 6(1) or point (a) of Article 9(2) of the Regulation, and where there is no other legal ground for the processing;
 - c. the data subject objects to the processing pursuant to Article 21(1) of the Regulation and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2) (processing for direct marketing purposes);
 - d. the personal data have been unlawfully processed;
 - e. the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
 - f. the personal data have been collected in relation to the offer of information society services referred to in Article 8(1) of the Regulation.
2. Where the controller has made the personal data public and is obliged to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.
3. Paragraphs (1) and (2) shall not apply 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 controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
 - c. for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) and Article 9(3) of the Regulation;
 - d. for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) of the Regulation, in so far as the right referred to in paragraph (1) is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
 - e. for the establishment, exercise or defence of legal claims.

Right to restriction of processing

1. The data subject has the right to obtain from the controller restriction of processing where one of the following applies:
 - a. the accuracy of the personal data is contested by the data subject; in this case, restriction shall apply for a period enabling the controller 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 controller 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 pursuant to Article 21(1) of the Regulation; in this case, restriction applies pending verification whether the legitimate grounds of the controller override those of the data subject.

2. Where processing has been restricted under paragraph (1), such personal data shall, with the exception of storage, only be processed with the data subject's consent, or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.
3. The controller shall inform the data subject who has obtained restriction of processing before the restriction is lifted.

Notification obligation regarding rectification or erasure of personal data or restriction of processing

1. The controller shall communicate any rectification or erasure of personal data or restriction of processing to each recipient to whom or to which the personal data have been disclosed, unless this proves impossible or involves disproportionate effort.
2. The controller shall inform the data subject about those recipients if the data subject requests it.

Right to data portability

1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:
 - a. the processing is based on consent pursuant to point (a) of Article 6(1) of the Regulation or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and
 - b. the processing is carried out by automated means.
2. In exercising his or her right to data portability under paragraph (1), the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.
3. The exercise of the right referred to in paragraph (1) shall be without prejudice to Article 17 of the Regulation. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
4. The right referred to in paragraph (1) shall not adversely affect the rights and freedoms of others.

Right to object

1. The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her carried out in the public interest or in the exercise of official authority vested in the controller, or necessary for the purposes of the legitimate interests pursued by the controller or by a third party (processing based on points (e) or (f) of Article 6(1) of the Regulation), including profiling based on those provisions. In such case, the controller shall no longer process the personal

data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or which are related to 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 at any time to object to 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.
3. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.
4. The data subject must be explicitly informed of the right referred to in paragraphs (1) and (2) at the latest at the time of the first communication with the data subject and the information shall be presented clearly and separately from any other information.
5. In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using technical specifications.
6. Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1) of the Regulation, the data subject shall have the right, on grounds relating to his or her particular situation, to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

Right not to be subject to automated decision-making

1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.
2. Paragraph (1) shall not apply if the decision:
 - a. is necessary for entering into, or performance of, a contract between the data subject and the controller;
 - b. is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
 - c. is based on the data subject's explicit consent.
3. In the cases referred to in points (a) and (c) of paragraph (2), the controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.
4. Decisions referred to in paragraph (2) shall not be based on special categories of personal data referred to in Article 9(1) of the Regulation, unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

Right to lodge a complaint and to an effective remedy

Right to lodge a complaint with a supervisory authority

1. Pursuant to Article 77 of the Regulation, the data subject has the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement, if the data subject considers that the processing of personal data relating to him or her infringes the Regulation.
2. The data subject may exercise the right to lodge a complaint using the following contact details:

National Authority for Data Protection and Freedom of Information

Address: 1125 Budapest, Szilágyi Erzsébet fasor 22/c

Telephone: +36 (1) 391-1400; Fax: +36 (1) 391-1410

Website: <http://www.naih.hu>

E-mail: ugyfelszolgalat@naih.hu

3. The supervisory authority with which the complaint has been lodged shall inform the complainant of the progress and the outcome of the complaint, including the possibility of a judicial remedy pursuant to Article 78 of the Regulation.

Right to an effective judicial remedy against a supervisory authority

1. Without prejudice to any other administrative or non-judicial remedy, each natural and legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.
2. Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to an effective judicial remedy where the competent supervisory authority does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint lodged pursuant to Article 77 of the Regulation.
3. Proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established.
4. Where proceedings are brought against a decision of a supervisory authority which was preceded by an opinion or a decision of the European Data Protection Board under the consistency mechanism, the supervisory authority shall forward that opinion or decision to the court.

Right to an effective judicial remedy against a controller or processor

1. Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77 of the Regulation, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under the Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with the Regulation.
2. Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers.

Restrictions

1. Union or Member State law to which the controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12–22 and 34, as well as the corresponding provisions of Article 5, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:

- a. national security;
- b. defence;
- c. public security;
- d. the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;
- e. other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters, public health and social security;
- f. the protection of judicial independence and judicial proceedings;
- g. the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;
- h. monitoring, inspection or regulatory functions connected, even occasionally, to the exercise of official authority in the cases referred to in points (a)–(e) and (g);
- i. the protection of the data subject or the rights and freedoms of others;
- j. the enforcement of civil law claims.

2. Legislative measures referred to in paragraph (1) shall include specific provisions, where relevant, at least as to:

- a. the purposes of the processing or categories of processing;
- b. the categories of personal data;
- c. the scope of the restrictions introduced;
- d. the safeguards to prevent abuse or unlawful access or transfer;
- e. the specification of the controller or categories of controllers;
- f. the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing;
- g. the risks to the rights and freedoms of data subjects; and
- h. the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.

Information to be provided in the event of a personal data breach

1. Where a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.
2. The communication to the data subject referred to in paragraph (1) shall describe in clear and plain language the nature of the personal data breach and contain at least the following information:

- the name and contact details of the data protection officer or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach;

– a description of the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

3. The communication to the data subject referred to in paragraph (1) shall not be required if any of the following conditions are met:

a. the controller 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 controller 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.

4. If the data subject has not yet been informed of the personal data breach, the supervisory authority, having considered the likelihood of the breach resulting in a high risk, may require the controller to communicate the breach to the data subject or may decide that any of the conditions referred to in paragraph (3) is met.

VI. PROCEDURE TO BE FOLLOWED IN THE EVENT OF A REQUEST BY THE DATA SUBJECT

1. The Business facilitates the exercise of the data subject's rights and may not refuse to act on the data subject's request to exercise his or her rights set out in this privacy notice, unless it demonstrates that it is not in a position to identify the data subject.

2. The Business shall provide information on action taken on a request under this Section to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay.

3. Where the data subject makes the request by electronic means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

4. If the Business does not act on the data subject's request, the Business shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

5. The Business shall provide the following information and take the following measures free of charge for the data subject: confirmation of whether or not personal data are being processed, access to the processed data, rectification, completion or erasure of data, restriction of processing, data portability, objection to processing, as well as information in relation to a personal data breach.

6. Where the data subject's requests are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may, taking into account the

administrative costs of providing the information or communication or taking the action requested, charge a fee of HUF 5,000 or refuse to act on the request.

7. The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.
8. Without prejudice to Article 11 of the Regulation, where the controller has reasonable doubts concerning the identity of the natural person making a request referred to in Articles 15–21 of the Regulation, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

IX. PROCEDURE TO BE FOLLOWED IN THE EVENT OF A PERSONAL DATA BREACH

1. Under the Regulation, a personal data breach is 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.
2. A personal data breach includes, for example, the loss or theft of a device containing personal data (laptop, mobile phone), the loss or unavailability of the decryption key to an encrypted file, infection by ransomware that makes the data processed by the controller inaccessible until a ransom is paid, an attack on the IT system, an erroneously sent e-mail containing personal data, or the disclosure of a mailing list.
3. In the event of the detection of a personal data breach, the representative of the Business shall immediately carry out an investigation to identify the personal data breach and determine its possible consequences. The necessary steps shall be taken to eliminate or mitigate the damage.
4. The controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of the personal data breach, notify it 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 is not made within 72 hours, it shall be accompanied by reasons for the delay.
5. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.
6. The notification referred to in paragraph (3) 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 controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
7. Where, and insofar as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

8. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with Article 33 of the Regulation.

VI. DATA PROCESSING IN CONNECTION WITH THE WEBSITE

Information relating to visitors to the Business's website

1. When visiting the Business's website, one or more cookies – small data files that the server sends to the browser and that the browser returns to the server with each request – are placed on the visitor's computer. Through these cookies, the browser of the visitor can be individually identified, provided the visitor has given his or her express (active) consent to this by continuing to browse the website after having been given clear and comprehensive information.
2. Cookies operate solely for the purpose of improving user experience and automating the login process. Cookies used on the website do not store information that enables personal identification; therefore, the Business does not carry out personal data processing in this context.

Data processing in connection with direct marketing activities

1. The legal basis of the Business's processing of personal data for direct marketing purposes is the explicit and unambiguous consent of the data subject. The data subject gives this prior, explicit consent via the Business's website by ticking the checkbox next to the text relating to consent for direct marketing after having read the information on data processing.
2. The data subject may also give consent on paper by completing the data sheet attached to this policy as Annex 2.
3. Scope of data subjects: any natural person who gives clear and explicit consent to the Business to process his or her personal data for direct marketing purposes.
4. Purposes of data processing: sending advertisements and offers relating to the provision of services and the sale of products, information on promotions, by electronic or postal means.
5. Recipients of personal data: the manager of the Business and those employees who perform customer service and marketing tasks by virtue of their job duties.
6. Categories of personal data processed: name, address, telephone number, e-mail address.
7. Duration of data processing: until the data subject withdraws consent to the processing of personal data for direct marketing purposes.

VII. DATA PROCESSING RELATING TO THE PERFORMANCE OF CONTRACTS

1. The Business processes the personal data of natural persons contracting with it – customers, buyers, suppliers, employees – in connection with contractual relationships. The data subjects shall be informed about the processing of their personal data.
2. Scope of data subjects: all natural persons who, based on a contract concluded with the Business, use e-learning training or request services related to training under a separate agreement.

3. Legal basis for processing is the performance of a contract; the purpose of processing is the provision of training, for which the collection of certain data is necessary.
4. Recipients of personal data: the manager of the Business and those employees and data processors who perform customer service and accounting tasks by virtue of their job duties.
5. Categories of personal data processed: name, address, telephone number, e-mail address, tax number, and information relating to work activities.
6. Duration of data processing: 20 years following the termination of the contractual relationship.

VIII. PROVISIONS ON DATA SECURITY

1. The Business may process personal data only in accordance with the activities set out in this policy and in line with the purposes of processing.
2. The Business shall ensure the security of the data and undertakes to take all technical and organisational measures that are essential to enforce the rules on data security, data protection and confidentiality, and to establish procedural rules required for the application of those laws.
3. The Business shall protect the data with appropriate measures against unauthorised access, alteration, transmission, disclosure, deletion or destruction, as well as against accidental destruction or damage and loss of accessibility resulting from changes in the technology used.
4. The technical and organisational measures to be implemented by the Business for data security are set out in the Business's data protection policy.
5. When determining and implementing the security measures, the Business shall take into account the current level of technological development; where there are several possible solutions, the Business shall choose the one that ensures the higher level of protection of personal data, unless this would cause disproportionate difficulty.

IX. RULES RELATING TO DATA PROCESSING CARRIED OUT BY A PROCESSOR

1. General rules on data processing by a processor

1. The rights and obligations of the processor with regard to the processing of personal data shall be determined by law and by the controller within the framework of specific laws governing data processing.
2. The Business declares that, in the course of its activity as a processor, it is not entitled to make substantive decisions regarding data processing; it may process personal data of which it becomes aware only in accordance with the instructions of the controller; it may not process personal data for its own purposes, and it shall store and retain the personal data in accordance with the controller's instructions.
3. The Business is responsible for the lawfulness of instructions given to the processor concerning data processing operations.
4. It is the obligation of the Business to provide information to data subjects regarding the identity of the processor and the location of processing.

5. The Business does not authorise the processor to engage another processor.
6. The contract for data processing must be concluded in writing. A processor may not be engaged if it is interested in business activities using the personal data to be processed.

Dated,