MILESTONE

INSTITUTE

MILESTONE INSTITUTE

DATA PROTECTION NOTICE

Updated 10 March 2025

CONTENT

1. Preamble **2**

Operation of the Institute and Purpose of the Notice 2

Identity of the Data Controller and Location of Data Processing 2

Our Principles of Data Processing 3

What Happens If You Do Not Provide Personal Data? 3

2. Definitions **4**

3. Purpose, Legal Basis, and Duration of Personal Data Processing **4**

3.1. Data Processing Related to the Adult Education Legal Relationship 5

3.2. Data Processing Related to Distance Learning 7

3.3. Data Processing Related to Video Recordings During Training 7

3.4. Data Processing Related to Room Rental 8

3.5. Fulfillment of Accounting Obligations, Processing of Billing Data 8

3.6. Data Processing Related to Website Visits 9

3.7. Data Processing Related to Enquiries Received Through the Website 9

3.8. Data Processing Related to the Newsletter Service 10

3.9. Data Processing Related to Market Research and Focus Group Research 10

3.10. Data Processing Related to Administration and Complaints 11

3.11. Data Processing Related to Employee Applications 11

3.12. Data Processing Related to Employment 12

[1] Fktv. Section 16 13

[2] Fktv. Section 21 (1) 13

4. How the Institute Protects Data **14**

5. Data Storage and Processing Systems Used **14**

6. Cookies **15**

7. What Should You Know About Our Direct Marketing and Newsletter Data Processing? **17**

8. Key Rights of the Data Subject in Relation to Data Processing **18**

Supplement No. 1 to the Privacy Policy **21**

1. Preamble

Operation of the Institute and Purpose of the Notice

Milestone Consulting Kft. (hereinafter: the Institute) carries out building management, educational content development, and research activities, primarily in support of structured scientific training and university admission preparation for talented students outside the formal education system. The purpose of the developed educational content and programs is to facilitate the identification and development of talented students, support their professional careers, and organize them into a community from which successful enterprises and social initiatives may emerge in the future. The mission of the Institute is to equip the next generation of the country's future leaders with the knowledge and intellectual community needed to responsibly utilize their opportunities through the developed educational content. In addition to the above, the Institute provides consulting and adult education services to corporate and higher education clients, the latter as a registered adult education institution.

The purpose of this notice, together with the terms of use of the Institute's website and the cookie policy, is to provide users with information regarding the processing and protection of their personal data. The Institute processes personal data in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council (April 27, 2016, hereinafter: GDPR) on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, as well as Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information (hereinafter: Infotv.).

Identity of the Data Controller and Location of Data Processing

Data Controller:	Milestone Consulting Ltd. / Milestone Consulting Kft.
Registered Address:	1077 Budapest, Wesselényi u 17.
Training Location:	1077 Budapest, Wesselényi u 17.
Tax Number:	22946632-2-42
Adult Education Registration Number:	B/2020/001976
Contact Information:	info@msinst.org, + 36 30 567 5499
Website:	www.milestone-institute.org
Representatives:	Péter Palasics, CEO; György Greskovits, CEO

Our Principles of Data Processing

The Institute follows the following main data processing principles:

- The Institute processes personal data lawfully and fairly, in a transparent manner for the data subject.
- The Institute collects personal data only for specified, explicit, and legitimate purposes and does not process them in a manner that is incompatible with these purposes.
- The personal data processed by the Institute are adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
- The Institute takes all reasonable measures to ensure that the processed personal data are accurate and up to date. The Institute erases or rectifies inaccurate personal data without delay.
- The Institute stores personal data in a form that permits identification of the data subject only for as long as necessary to achieve the purposes for which they are processed.
- The Institute processes personal data in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing, accidental loss, destruction, or damage, using appropriate technical and organizational measures.

The Institute processes your personal data...

- based on your prior informed and voluntary consent, only to the necessary extent and always for a specific purpose.
- In certain cases, the Institute processes and shares personal data based on legal requirements and mandatory obligations, including sharing data with Hungarian authorities (e.g. the National Vocational and Adult Education Office, and in the case of employees, the National Health Insurance Fund Manager (NEAK) and the National Tax and Customs Administration (NAV)).
- In certain other cases, the Institute processes personal data because it has a legitimate interest in doing so, or a third party has a legitimate interest (e.g. the operation, development, and security of our website).

Detailed information on the purpose, legal basis, and duration of personal data processing in various cases is provided in Chapter 3 of this Privacy Notice.

What Happens If You Do Not Provide Personal Data?

You are not obligated to provide personal data to the Institute. However, if you choose not to provide the required data, the Institute may not be able to process your request, application, or enrollment properly - or at all.

2. Definitions

For the purposes of this Privacy Notice:

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 one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person. (GDPR Article 4)

Processing: any operation or set of operations which is performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction. (GDPR Article 4)

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. (GDPR Article 4)

Processor: a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller. (GDPR Article 4)

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 authorized to process personal data. (GDPR Article 4)

Data subject's rights: the rights provided under Articles 12-22 of the GDPR, including the right to information, access, rectification, erasure, restriction of processing, objection, and data portability. (GDPR Article 4)

3. Purpose, Legal Basis, and Duration of Personal Data Processing

The Institute processes only those data for which the purpose of processing is defined, the legal basis is justified, and it retains such data only for the period specified in this Privacy Notice. If the training or service contract related to the activity is terminated, the personal data associated with that activity will also be deleted.

As an adult education provider operating under notification, in accordance with Act LXXVII of 2013 on Adult Education (hereinafter: Fktv.), the Institute's staff, in the course of performing their job duties or contractual assignments, may access and process the personal data of training participants only to the extent necessary for the administration of the training.

The Institute only transfers personal data to individuals who are in an employment relationship or other contractual relationship aimed at work performance with the Institute (e.g., service contracts), and only under a data processing agreement. If such a contract terminates, the data processing activities associated with it also cease.

If the list of data processors changes, the Institute will update this Privacy Notice accordingly and inform the affected individuals about the modifications.

To carry out its building management, training, consultancy, educational content development and related activities, the Institute collects and processes the following types of personal data, as detailed in the sections below.

3.1. Data Processing Related to the Adult Education Legal Relationship

In view of the adult education legal relationship established between the Institute, as an adult education provider, and the participant in the training program under the adult education contract, the Institute processes personal data for the purpose of successfully and effectively conducting the training specified in the contract.

Scope of Processed Data	The data specified in Section 16(a), (b), and (c) of the Fktv. [1], and Section 21(1) of the Fktv. [2]. Name (surname, given name) and signature of the training participant and their legal representative.
Source of Data	The data subject.
Purpose of Data Processing	Ensuring the successful and effective completion of training in accordance with Section 21(1) of the Fktv.
Legal Basis of Processing	Processing is based on compliance with a legal obligation pursuant to Article 6(1)(c) of the GDPR, as Sections 16(a)-(c) and 21 of the Fktv. require the Institute to process the above-mentioned personal data of training participants. Additionally, under Section 2:14 of the Civil Code (Ptk.), the legal declaration of an incapacitated minor is null and void, and their legal representative must act on their behalf. Furthermore, under Section 2:12 of the Civil Code (Ptk.), for a minor with limited legal capacity, their legal representative's consent is required for the validity of their training contract. Accordingly, the training contract includes the above-mentioned data of the legal representative.

Duration of Data Processing	Personal data processed under Section 16(a)-(c) of the Fktv. will be retained until the last day of the eighth year following its creation, as required by Section 16 of the Fktv.. Personal data processed under Section 21(1) of the Fktv. will be retained until the last day of the eighth year following the conclusion of the training contract, in accordance with Section 21(5) of the Fktv..
Data Processor	The data controller's contracted electronic storage service providers and customer relationship management system operators (currently: Google LLC, Salesforce Inc., MiniCRM Zrt.); the provider of the e-learning system used in training (Canvas – Instructure, Inc.); and instructors contracted by the Institute for the purpose of carrying out teaching activities as specified in their contracts. Milestone Consulting Kft. processes data for financial and accounting tasks related to application and training fees (supporting membership fees) and for general communication and administration with training participants.
Obligation to Provide Data	Under Section 15(1) of the Fktv., the Institute is required to provide the adult education administrative authority with the following data in the adult education data provision system: a) The name, type, location, duration (hours), start date, and - except for closed-system online training - the planned completion date of the training. b) The personal identification data, email address, and highest level of education of training participants. c) The training fee and its payer.
Data Transfer	Under Section 21(2) of the Fktv., the above data may be used for statistical purposes and transferred for statistical use in a non-identifiable form. Additionally, the data may be transferred to and used by the Hungarian Central Statistical Office for statistical purposes in an individually identifiable manner, free of charge.

3.2. Data Processing Related to Distance Learning

Scope of Processed Data	The image, voice, and other personal data perceivable via an online connection, as well as the environment of the training participant.
Source of Data	The data subject.
Purpose of Data Processing	Conducting distance learning as part of the successful and effective completion of training, in accordance with Section 21(1) of the Fktv.
Legal Basis of Processing	Processing is based on compliance with a legal obligation pursuant to Article 6(1)(c) of the GDPR, as data processing is necessary for the implementation of the provisions set out in Sections 16(a)-(c) and 21 of the Fktv.
Duration of Data Processing	For the duration of the training, with the condition that the training may not be recorded.
Data Processor	The data controller's contracted electronic storage service providers and remote communication service providers (at time of issuance: Google LLC, Teachable Inc.).

3.3. Data Processing Related to Video Recordings During Training

Scope of Processed Data	The image, voice, other personal data, and surroundings of the training participant.
Source of Data	The data subject.
Purpose of Data Processing	During training, images and video recordings of participants may occasionally be made to support their development.
Legal Basis of Processing	Voluntary consent (Article 6(1)(a) GDPR).
Duration of Data Processing	Until consent is withdrawn.
Data Processor	The data controller's contracted electronic storage service providers and remote communication partners (at time of issuance: Google LLC, Teachable Inc.).

3.4. Data Processing Related to Room Rental

Scope of Processed Data	Full name, email address, phone number, mailing address. Other personal messages.
Source of Data	The data subject.
Purpose of Data Processing	Understanding the needs of the room renter and managing administrative tasks related to providing the requested service.
Legal Basis of Processing	Voluntary consent (Article 6(1)(a) GDPR).
Duration of Data Processing	Until consent is withdrawn.
Data Processor	The data controller's contracted electronic storage service providers and other systems used for data processing (at time of issuance: Google LLC; Salesforce, Inc.; DocuSign Inc., MiniCRM Zrt.).

3.5. Fulfillment of Accounting Obligations, Processing of Billing Data

Scope of Processed Data	In the case of room rental, the data of the user of the service, in the case of training, the participant or for participants under the age of 18 – in accordance with Sections 2:12 and 2:14 of the Civil Code (Ptk.) – the billing name (surname and first name) and billing address of their legal representative, the amount of the application or training fee, the method of payment, the transaction identifier, and information regarding which application period the application fee pertains to, as well as which training program the training fee applies to.
Source of Data	The data subject.
Purpose of Data Processing	Issuance of invoices in connection with the rental of rooms or payment of the training fee, fulfillment of the Institute's accounting obligations, specifically the retention of accounting documents supporting bookkeeping records, in accordance with the statutory obligation defined in the 2000 Act C on Accounting.

Legal Basis of Processing	Fulfillment of a legal obligation pursuant to Article 6(1)(c) of the GDPR, in accordance with Section 169(2) of the 2000 Act C on Accounting.
Duration of Data Processing	Compliance with the statutory obligation to retain accounting documents, i.e., as specified in Section 169(2) of the 2000 Act C on Accounting, for 8 years.
Data Processor	The data controller's contracted electronic storage service providers and customer relationship management system operators (as of the date of this notice: Google LLC; Salesforce, Inc., MiniCRM Zrt.).

3.6. Data Processing Related to Website Visits

Scope of Processed Data	Visitor's IP address, date and time of visit. Data on visited subpages. Type of operating system and browser used.
Source of Data	The data subject.
Purpose of Data Processing	Ensuring the proper functioning of the website. Monitoring and improving services. Identifying malicious visitors attacking the website. Measuring website traffic. Statistical purposes.
Legal Basis of Processing	The Institute's legitimate interest (Article 6(f) GDPR).
Duration of Data Processing	12 months.
Data Processor	—

More detailed information about the use of cookies can be found below, in Section 6.

3.7. Data Processing Related to Enquiries Received Through the Website

Scope of Processed Data	Full name, email address, phone number, mailing address. Other personal messages.
Source of Data	The data subject.

Purpose of Data Processing	Understanding the visitor's request and responding to the inquiry.
Legal Basis of Processing	Voluntary consent (Article 6(1)(a) GDPR).
Duration of Data Processing	Duration of Data Processing Until consent is withdrawn.
Data Processor	—

3.8. Data Processing Related to the Newsletter Service

Scope of Processed Data	Full name, email address, phone number.
Source of Data	The data subject.
Purpose of Data Processing	Communication, market research, focus group research.
Legal Basis of Processing	Voluntary consent (Article 6(1)(a) GDPR).
Duration of Data Processing	Until consent is withdrawn (i.e., until unsubscribing from the newsletter).
Data Processor	The data controller's contracted electronic storage service providers and customer relationship management system operators (at time of issuance: Google LLC; Salesforce, Inc., MiniCRM Zrt.).

More detailed information about our direct marketing and newsletter-related data processing can be found below, in Section 7.

3.9. Data Processing Related to Market Research and Focus Group Research

Scope of Processed Data	Gender, age. Data contained in responses to specific questionnaires.
Source of Data	The data subject.
Purpose of Data Processing	Conducting surveys and research tailored to client needs by forwarding aggregated, anonymized data.

Legal Basis of Processing	Voluntary consent (Article 6(1)(a) GDPR).
Duration of Data Processing	For the duration of the external contract.
Data Processor	The data controller's contracted electronic storage service providers and customer relationship management system operators (at time of issuance: Google LLC; Salesforce, Inc., MiniCRM Zrt.).

3.10. Data Processing Related to Administration and Complaints

Scope of Processed Data	Full name, email address, phone number, mailing address. Other personal messages.
Source of Data	The data subject.
Purpose of Data Processing	Responding to feedback and complaints.
Legal Basis of Processing	The Institute's legal obligation (Article 6(1)(c) GDPR).
Duration of Data Processing	5 years.
Data Processor	The data controller's contracted electronic storage service providers and other systems used for data processing (at time of issuance: Google LLC; Salesforce, Inc.; DocuSign Inc., MiniCRM Zrt.).

3.11. Data Processing Related to Employee Applications

Scope of Processed Data	Applicant's identification and contact details (name, residence, place of stay, mailing address, email address, phone number). Data necessary for recruitment (personal data voluntarily provided in the CV, educational background, degrees / qualifications / certifications, name of the institution issuing the qualification). Personal identification data and other identifiers (current and birth name, nationality, mother's maiden name, place and date of birth, social security number, tax identification number, educational background, qualifications, name and serial number of the qualification certificate, number of children).

Source of Data	The data subject.
Purpose of Data Processing	Processing job applications. Recruitment and communication.
Legal Basis of Processing	Voluntary consent (Article 6(1)(a) GDPR).
Duration of Data Processing	Until the recruitment process is completed; thereafter, for 2 years if voluntary consent is given.
Data Processor	The data controller's contracted electronic storage service providers and customer relationship management system operators (at time of issuance: Google LLC; Salesforce, Inc., MiniCRM Zrt.). Milestone Consulting Kft. for managing job applications.

3.12. Data Processing Related to Employment

Scope of Processed Data	Employment details (start date of employment, duration of employment contract, employee's salary, job title, probation period, FEOR code, weekly working hours, full-time or part-time employment status, work schedule, salary payment method, any additional 36-hour employment, long-term job seeker status, sick leave dates, vacation dates, overtime details). Financial identification data (bank name, bank account number, private pension fund membership, pension fund name, date of enrollment, private pension fund ID number, wage garnishments, pensioner status, expected annual pension amount). Other financial data (taxes and contributions related to the employee's salary).
Source of Data	The data subject.
Purpose of Data Processing	Performing services specified in the employment contract between the employee and the Institute, including its annexes.
Legal Basis of Processing	Performance of a contract (Article 6(1)(b) GDPR).
Duration of Data Processing	For the duration of the contract and for 5 years to comply with tax obligations, as well as for any additional period required by applicable legal provisions.
Data Processor	The data controller's contracted electronic storage service providers and customer relationship management system

	operators (at time of issuance: Google LLC; Salesforce, Inc., MiniCRM Zrt.); the data controller's payroll service provider (at time of issuance: Summa-Profit Kft.) for financial and accounting tasks.

[1] Fktv. Section 16

The adult education provider must record, register, and retain the following documents for a period ending on the last day of the eighth year following their creation, in order to ensure the exercise of the supervisory powers of the adult education administrative authority:

a) attendance sheets signed by the training participant for contact hours requiring personal attendance, as well as documents verifying attendance and the completion of training activities for contact hours not requiring personal attendance and for non-contact sessions;

b) the personal data of the training participant processed under Section 21(1), along with the original documents or certified copies (authenticated by the adult education provider) proving the conditions necessary for commencing and participating in education and training, as well as documents verifying the entry competence assessment and prior knowledge assessment,

c) the adult education contract, the training programme, and the documents verifying the implementation of the training in accordance with the training programme.

[2] Fktv. Section 21 (1)

The adult education provider processes the following data for the purpose of conducting the training programme and for fulfilling the reporting and data provision obligations to the authority, as required by the authority under Section 1(2) and (2a):

a) the personal data of the training participant:
   - aa) natural personal identification data and, in connection with the issuance of the educational identification number, the educational identification number itself,
   - ab) email address and
   - ac) data regarding the highest level of education attained.

b) the training-related data of the training participant:
   - ba) data concerning the highest level of education attained, vocational qualification, professional qualification, and foreign language proficiency,
   - bb) data concerning entry into the training programme, completion of the training programme, or—if the training programme is not completed—withdrawal from the programme,
   - bc) data concerning evaluation and grading during the training programme,

bd) data related to payment obligations associated with the training programme and any training loans utilised.

4. How the Institute Protects Data

The Institute takes all necessary steps to ensure that your data is processed securely and in accordance with data protection regulations.

The Institute does not retain your personal data for longer than necessary in relation to the original purposes for which it was collected. Your data is only transferred within the contractual and legal frameworks specified, and in the case of our data processors, we ensure through contractual terms that they do not process your personal data for purposes contrary to your consent.

You voluntarily provide your personal data during registration or when communicating with the Institute. Therefore, we ask you to pay special attention to the accuracy, correctness, and truthfulness of the data you provide, as you are responsible for them. Incorrect, inaccurate, or incomplete data may prevent you from using our services.

If you provide personal data that does not belong to you but to another person, we assume that you have the necessary authorisation to do so.

In the event of the use of misleading personal data, or if any of our visitors commits a criminal offence against us or attacks the Institute's system, we will retain the visitor's data for the purpose of establishing civil liability or conducting criminal proceedings.

The employees and contributors involved in the Institute's data processing and/or data handling are entitled to access your personal data to a predetermined extent, subject to confidentiality obligations.

We protect your personal data with appropriate technical and other measures to ensure data security and availability, as well as to protect it from unauthorised access, modification, damage, disclosure, or any other unauthorised use.

As part of our organisational measures, we control physical access to our buildings, provide continuous training to our employees, and store paper-based documents securely. As part of our technical measures, we use encryption, password protection, and antivirus software.

However, please note that data transmission over the internet cannot be considered fully secure. While the Institute does everything possible to make processes as secure as possible, we cannot assume full responsibility for data transmission via our website. However, once data is received by the Institute, we comply with strict regulations to ensure the security of your data and to prevent unauthorised access.

5. Data Storage and Processing Systems Used

The Institute stores data on various cloud-based platforms and does not operate its own servers. The Institute's internal regulations govern proper data management and access, ensuring that only employees with the appropriate authorisation can access the data necessary for their work.

The Institute may also transfer data abroad. The cloud-based services detailed below do not always have storage locations in Hungary. All systems used by the Institute either operate on servers located within the European Union or have special agreements with the relevant authorities to certify the security of data storage outside the EU.

By submitting your personal data, you accept that its transfer, storage, and processing may take place outside the European Economic Area (EEA).

If we use external service providers for data processing on our behalf, we only transfer the personal information necessary for the provision of the service, and we enter into a contract ensuring that the provider complies with the Institute's data protection and information security requirements. These data are processed in compliance with legal regulations and are only disclosed to third parties with your consent or where the Institute is legally or legally obliged to do so.

The court, the prosecutor's office, and other authorities (e.g. the police, the tax authority, the National Authority for Data Protection and Freedom of Information) may contact the Institute to request information, disclose data, or provide documents. In such cases, we must comply with our data disclosure obligations, but only to the extent strictly necessary to fulfil the purpose of the request. Affected individuals will be informed accordingly.

The Institute uses the following systems for data storage and processing:

- Salesforce, Salesforce Inc., San Francisco, California, USA
- Google (Apps, Mailing, etc.), Google LLC, Mountain View, California, USA
- Canvas, Instructure, Inc., Salt Lake City, Utah, USA
- MiniCRM, MiniCRM Zrt., Budapest, Hungary

The data processing carried out by these systems is subject to their own privacy policies. For more information, please refer to the privacy policies and data processing practices available on the respective third-party websites.

Our website may contain links to other websites that are not owned by the Institute. While we strive to display reliable sources, we do not accept responsibility for data collected by websites not operated by the Institute, including how they use, store, or disclose such data.

6. Cookies

Our website uses cookies to ensure its efficient operation. Additionally, we record and store IP addresses to provide you with an even more personalised service.

What are cookies, and how do we manage them?

Cookies are small data files (hereinafter referred to as cookies) that are placed on your computer when you use our website. These are saved and stored by your internet browser. The most commonly used internet browsers (Chrome, Firefox, etc.) generally accept and enable cookies by default, but you can modify your browser settings to reject or disable them. You can also delete stored cookies from your computer. More detailed information on managing cookies can be found in the “Help” section of your browser.

Some cookies do not require your prior consent. A short notification about these is provided when you first visit our website. These include authentication cookies, multimedia player cookies, load-balancing cookies, session cookies that assist with user interface customisation, and user-centric security cookies.

For cookies that require consent, the Institute notifies you upon your first visit and requests your approval, provided that data processing begins upon accessing the website.

The Institute does not use or permit any cookies that allow third parties to collect data without your consent.

Accepting cookies is not mandatory. However, the Institute does not take responsibility for any potential malfunctioning of the website if cookies are disabled.

What types of cookies do we use?

Type	**Name**	**Consent**	**Description**	**Purpose**	**Validity**
System cookies	__cfduid; wordpress_google _apps_login; wordpress_test _cookie	No	Session cookie for web application firewall, preventing cross-referencing abuse	Ensuring website functionality	Until the end of the browser session
Analytical cookies	_ga; _gid; _gat	Yes	Used by Google Analytics to distinguish between users and sessions	Statistical analytics	Determined by third party

Remarketing cookies	_fbp; _fr	Yes	Used by Facebook Pixel to identify users	Targeting Facebook ads	Determined by third party

Further information on data protection can be found here and here.

7. What Should You Know About Our Direct Marketing and Newsletter Data Processing?

During registration, or later by modifying your stored personal data on the newsletter and/or direct marketing registration interface (i.e., by clearly expressing your intention to give consent), you may grant your consent for us to use your personal data for marketing purposes. In this case, until consent is withdrawn, we will process your data for direct marketing and/or newsletter purposes and send you advertisements, other mailings, informational materials, and offers, as well as forward you our newsletter (Grtv. Section 6).

The Institute maintains records of the following types of registrations:

Type of Registration	Legal Basis	Description of Activity and Purpose of Registration	Duration
General newsletter for visitors subscribing via the website.	Voluntary consent (GDPR Article 6(a))	Subscription to the newsletter as a website visitor, in order to receive the latest news about the Institute.	Until unsubscribed
Newsletter for interested training participants who have subscribed.	Voluntary consent (GDPR Article 6(a))	Subscription to the newsletter as an interested training participant, in order to receive updates related to the topics for which they subscribed.	Until unsubscribed
Emails for current training participants.	Performance of a contract (GDPR Article 6(b))	The Institute may send emails to all training participants to inform them about programme-related tasks, opportunities, and general news.	Duration of the contract

Emails for the Institute's employees.	Performance of a contract (GDPR Article 6(b))	The Institute may send emails to all employees (including contract staff) to inform them about work-related tasks, opportunities, and general news.	Duration of the contract

If you have registered as a website visitor or a prospective training participant, you may give your consent for direct marketing and the newsletter either jointly or separately, and you may withdraw such consent(s) at any time, free of charge.

The deletion of a registration is in all cases considered a withdrawal of consent. However, the withdrawal of consent for direct marketing and/or newsletter-related data processing is not interpreted as a withdrawal of consent for data processing related to our website. Each consent is granted for a specific purpose; for example, registering on the website and subscribing to the newsletter are two separate purposes, managed in two separate databases, and are not linked.

For technical reasons, we commit to processing the withdrawal or cancellation of individual consents within 15 working days.

As a current training participant or employee of the Institute, you gave your consent upon signing your contract or agreement for the Institute to send you emails at any time. This consent cannot be withdrawn before the end of the contract or agreement; however, once the contract or agreement is terminated, the Institute's right to contact you automatically ceases.

8. Key Rights of the Data Subject in Relation to Data Processing

The data subject may, at any time, in relation to data processing:

- Request information about data processing,
- Request access to the data processed about them,
- Request rectification of inaccurate data or completion of incomplete data,
- Request the erasure of data processed based on their consent,
- Object to the processing of their data,
- Request the restriction of data processing.

Upon request for information, the data subject—unless restricted for legally defined reasons—has the right to know whether their personal data is being processed by the Institute and to receive information regarding:

- The purpose of processing their data,

- The legal basis for the Institute's data processing,
- The duration for which the Institute processes their data,
- The specific data processed by the Institute and to receive a copy of them,
- The recipients or categories of recipients of their personal data,
- Any transfers to third countries or international organisations,
- The source of the data, if not collected directly from the data subject,
- The characteristics of automated decision-making, if applied by the data controller,
- The data subject's rights related to data processing,
- The available legal remedies.

The Institute responds to requests for information and access within a maximum of one month. If the data subject requests additional copies of their processed personal data, the Institute may charge a reasonable fee based on administrative costs.

When requesting the rectification (modification) of data, the data subject must prove the accuracy of the new data and confirm that they are authorised to request the modification. The Institute can only evaluate whether the new data is valid and if the previous data should be corrected based on this proof.

If it is unclear whether the processed data is accurate or correct, the Institute will not rectify the data but will instead mark it, indicating that it has been contested by the data subject but is not necessarily incorrect. Once the authenticity of the request has been verified, the Institute rectifies the inaccurate personal data or completes the requested data without undue delay. The Institute notifies the data subject of the rectification or marking of the data.

The data subject may request the erasure or blocking of their data, meaning that the Institute is obliged to delete the data subject's personal data without undue delay if:

- The processing of personal data was unlawful,
- The personal data is no longer necessary for the purpose for which it was processed,
- The data was processed based on consent, and the data subject has withdrawn their consent, and no other legal basis justifies further processing,
- A legal regulation requires the Institute to delete the data, and this obligation has not yet been fulfilled.

The data subject may request the restriction of data processing, which the data controller must comply with if any of the following conditions apply:

- The data subject disputes the accuracy of the personal data. In this case, restriction applies for the period necessary for the data controller to verify the accuracy of the personal data.
- The data processing is unlawful, but the data subject objects to the erasure of the data and instead requests restriction of its use.

- The data controller no longer needs the personal data for processing, but the data subject requires it for the establishment, exercise, or defence of legal claims.
- The data subject has objected to the processing of their data. In this case, the restriction applies until it is determined whether the data controller's legitimate grounds override the data subject's legitimate interests.

If data is subject to restriction, such personal data - except for storage - may 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 European Union or a Member State.

The Institute will notify the data subject in advance before lifting the restriction on processing. The data subject has the right to object at any time, on grounds relating to their particular situation, to the processing of their personal data under Article 6(1)(f) of the GDPR.

In such cases, the Institute may no longer process the personal data, unless it demonstrates compelling legitimate grounds for processing that override the interests, rights, and freedoms of the data subject, or if processing is necessary for the establishment, exercise, or defence of legal claims.

If the data subject believes that the data processing violates the GDPR or the Infotv. (Hungarian data protection law), or they object to how the Institute processes their personal data, they are advised to first contact the Institute with their complaint. All complaints will be investigated.

If, despite filing a complaint, the data subject remains dissatisfied with how the Institute handles their data, or if they wish to escalate their concerns directly to an authority, they may lodge a complaint with the National Authority for Data Protection and Freedom of Information (NAIH) (address: 1055 Budapest, Falk Miksa utca 9-11., postal address: 1363 Budapest, Pf. 9., email: ugyfelszolgalat@naih.hu, website: www.naih.hu).

The data subject also has the right to take legal action to protect their data. The court will proceed with the case as a priority. The data subject is free to choose whether to submit their claim to the court (http://birosag.hu/torvenyszekek) competent for their place of residence (permanent address) or place of stay (temporary address). Find your local court: http://birosag.hu/ugyfelkapcsolati-portal/birosag-kereso.

9. Other Provisions

The Institute reserves the right to unilaterally modify this Privacy Policy at any time at its sole discretion. In justified cases, we will notify you of such changes via email.

Detailed information about the modifications can be found on the updated website of Milestone Institute. We recommend that you check this Policy each time you visit the website to see if any changes have been made to sections that are important to you.

Budapest, 10 April 2025

Péter Palasics
CEO
Milestone Consulting Ltd.

Supplement No. 1 to the Privacy Policy

The Institute is responsible for the education and supervision of persons under the age of eighteen, and the best interests of children must be given paramount protection. This requires the Institute to verify the moral integrity of all its employees and contractors who have direct contact with children. The Institute applies the analogy of Section 44/A of the currently effective Labour Code to its contracted personnel as well. (For full references to the relevant legislation, please see the Hungarian version of this policy available on our website.)

For employees:

1. The Institute may not establish an employment relationship with any person who:

a) is listed in the criminal records under:

aa) offences under Act IV of 1978 on the Criminal Code, applicable until 30 June 2013, including: murder, assisting in suicide, violation of personal liberty, human trafficking, altering family status, endangering minors, violent sexual offences, indecency, corruption of minors, abuse of prohibited pornographic material, facilitating prostitution, drug abuse, among others.

ab) offences under Act C of 2012 on the Criminal Code, including: recruitment for illegal activities, murder, assisting in suicide, prohibited use of the human body, drug trafficking, drug possession, inducing addiction, abuse of performance-enhancing substances, kidnapping, human trafficking, forced labour, violation of personal liberty, sexual coercion, sexual violence, sexual abuse, pandering, facilitating prostitution, exploitation of child prostitution, child pornography, indecent exposure, endangering minors, and child labour, among others.

b) is subject to criminal proceedings for any of the offences listed in point (a).

c) is prohibited from engaging in the profession under Section 52(3) of the Criminal Code.

d) is under compulsory medical treatment due to the commission of any of the offences listed in point (a).

2. A person may not be employed if they have been convicted of an intentional criminal offence listed in point (1a) and sentenced to:

a) imprisonment:

aa) less than five years – ineligible for eight years from the date of rehabilitation.

ab) five years or more – ineligible for ten years from the date of rehabilitation.

b) community service or a fine – ineligible for three years from the date of rehabilitation.

c) suspended imprisonment – ineligible for five years from the date of rehabilitation.

3. Verification of compliance with points (1) and (2) must be provided by the applicant:

a) Before the employment relationship is established, or

b) During the employment relationship, if requested in writing by the employer, within fifteen working days of such request. If it is not possible for reasons beyond the employee's control, the verification must be provided immediately upon resolution of such reasons.

4. If the employee provides proof of compliance with points (1) and (2), the employer must reimburse the administrative service fee paid for obtaining the official certificate from the Criminal Records Office.

5. Consequences of Non-Compliance:

a) If the employee fails to provide verification from the Criminal Records Office, or

b) If any of the exclusionary conditions become known to the employer,

then Section 29(1) of the Labour Code shall apply accordingly.

6. For the purpose of verifying compliance with points (1) and (2), the employer processes the personal data of:

a) Job applicants,

b) Employees

as contained in the official certificate issued by the Criminal Records Office.

7. Personal data obtained under points (1)–(3) shall be processed until the date of the employment decision or, in the case of employment, until the termination of the employment relationship.

For Contracted Personnel:

The Institute only requires the contracted individual contributor to present their criminal record certificate but does not make a copy of it. A copy of an official criminal record certificate does not constitute legally valid proof that it is an authentic copy of an official public document. Therefore, a copy is not suitable for verifying the authenticity of the data contained in the certificate. Under current legal provisions, only the presentation of the original document is legally compliant, whereas making copies would violate the principle of purpose limitation under the General Data Protection Regulation (GDPR).

Before establishing the contractual relationship, the Institute's authorised representative verifies the criminal record certificate to ensure that there are no entries contradicting the Child Protection Policy.

Once this verification is completed - if the reviewer is not the authorised signatory - they inform the signatory that there is no integrity-related obstacle to concluding the contract. The Institute does not make any records regarding the content of the criminal record certificate. If the notification is made in writing, it must be deleted immediately after the contract is signed or if the contract is not concluded.