

DATA PROCESSING NOTICE

VERSION 1.0

EFFECTIVE FROM: 1 AUGUST 2026

The purpose of this data processing notice (hereinafter: Notice) is to set out the data processing activities arising in connection with the internal whistleblowing system established by Menton Human Expert Korlátolt Felelősségű Társaság (company registration number: 13 09 232782; tax number: 32506220-2-13; registered office: 2724 Újlengyel, Dózsa György utca 11.; hereinafter: Company or Data Controller) under Act XXV of 2023 on Complaints, Disclosures of Public Interest and Rules on Reporting Abuses, in accordance with the applicable legislation and professional guidelines.

I. Data Controller

Information on the Data Controller:

Name:	Menton Human Expert Korlátolt Felelősségű Társaság (Limited Liability Company)
Company registration number:	13 09 232782
Tax number:	32506220-2-13
Registered office:	2724 Újlengyel, Dózsa György utca 11.
E-mail:	eszter.miklos@mentonhumanexpert.hu
Telephone:	+36 70 682 9788

II. Basic principles

The handling of personal data in accordance with the applicable rules plays a particularly important role in the Data Controller's operations. The Data Controller is committed to processing the personal data it handles in compliance with data protection requirements and with due regard to the special importance of the right to privacy and the protection of personal data.

III. Applicable legislation

Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter: GDPR);

Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information (hereinafter: Privacy Act / Infotv.);

Act V of 2013 on the Civil Code (hereinafter: Civil Code / Ptk.);

Act XXV of 2023 on Complaints, Disclosures of Public Interest and Rules on Reporting Abuses.

IV. Definitions

Identifiable natural person: a natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Data subject: any natural person identified or identifiable on the basis of any information;

Personal data: any information relating to the data subject;

Special category data: all data belonging to the special categories of personal data, i.e. personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, as well as genetic data, biometric data processed for the purpose of uniquely identifying natural persons, data concerning health, and personal data concerning the sex life or sexual orientation of natural persons;

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;

Data Controller: the natural or legal person, public authority, agency or any 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 processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may also be provided for by Union or Member State law;

Joint controller: a controller who determines the purposes and means of the processing jointly with one or more other controllers;

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

Data transfer: making data available to a specified third party;

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

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;

EEA State: a Member State of the European Union and another state party to the Agreement on the European Economic Area, as well as a state whose national enjoys the same legal status as a national of a state party to the Agreement on the European Economic Area under an international treaty concluded between the European Union and its Member States and a state not party to the Agreement on the European Economic Area;

Third country: any state that is not an EEA State;

Internal whistleblowing system: the independent system established at the Data Controller for this purpose, intended for making reports and complaints under the Complaints Act and the rules established by the Data Controller;

Whistleblower protection attorney: the attorney entrusted with receiving and handling reports related to the Data Controller's activities and with investigating information on unlawful or allegedly unlawful acts or omissions or other abuses;

Whistleblower: a person who makes a report to the Data Controller through the internal whistleblowing system;

Report: information on an unlawful or allegedly unlawful act or omission, or other abuse;

Abuse: an act or omission that is unlawful, contrary to the Data Controller's code of conduct, or qualifies as other abuse under the Complaints Act.

V. Scope of data processing

1. Operation of the internal whistleblowing system

Legal basis for processing: Compliance with a legal obligation [Article 6(1)(c) GDPR]. In certain cases the whistleblower may share special category data, in which case the legal basis for processing is likewise a legal requirement [Article 9(1)(b) GDPR].

Purpose of processing: The purpose of the processing is for the Data Controller to receive and investigate reports and, where justified, to terminate or remedy the conduct that is the subject of the report.

Categories of data processed: Within the internal whistleblowing system, the personal data of (a) the whistleblower, (b) the person whose conduct or omission gave rise to the report, and (c) the person who may have material information about the content of the report, which are indispensable for investigating the report, may be processed solely for the purpose of investigating the report and remedying or terminating the conduct that is the subject of the report, and may be forwarded to the whistleblower protection attorney and any external organisation involved in the investigation.

Duration of processing: If the Data Controller decides to dispense with the investigation, the personal data processed shall be deleted without delay. If, following the investigation, the report proves unfounded or no further action is required, the Data Controller shall delete the personal data within 30 days of the report being made. If action is taken on the basis of the report, in particular but not exclusively where employment-law claims are enforced, the Data Controller shall process the data until the legal act becomes time-barred. Personal data not falling within the scope of the 'categories of data processed' shall be deleted by the Data Controller without delay.

VI. Processors, recipients and third countries

Data processed within the internal whistleblowing system may be transferred to a third country or international organisation only where the recipient of the transfer has given a legal commitment to comply with the rules laid down in the Act regarding the report, and with due regard to the provisions on the protection of personal data.

The whistleblower's personal data may only be disclosed to the body competent to conduct the proceedings initiated on the basis of the complaint or disclosure of public interest, if that body is entitled by law to process them, or if the whistleblower has consented to the transfer of his or her data. The whistleblower's personal data may not be made public without his or her consent.

If it becomes evident that the whistleblower communicated false data or information in bad faith, and circumstances indicating the commission of a criminal offence or a minor offence arise:

- his or her personal data must be handed over to the body or person entitled to conduct the proceedings;
- if it is reasonably likely that he or she caused unlawful damage or other infringement to another person, his or her personal data must be handed over, upon request, to the body or person entitled to initiate or conduct the proceedings.

No automated decision-making or profiling takes place during the data processing.

The Data Controller uses the following processor: Whistleblower protection attorney services: Dr. Zsófia Kanyok, sole practitioner attorney (1024 Budapest, Szilágyi Erzsébet fasor 13-15, 1st floor, door 2).

VII. Rights of data subjects

Right to withdraw consent

Where processing is based on consent, the data subject has the right to withdraw consent at any time. The withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal.

Right to request information

The data subject has the right to request information in writing from the Data Controller about the processing of his or her personal data. Within one month, the Data Controller shall inform the data subject in writing of the purpose and legal basis of each processing activity, the categories of data processed, the duration of processing, the source of the data, any data transfers, etc.

If the report concerns a natural person, the personal data of the whistleblower may not be disclosed to the person requesting information when that person exercises his or her rights of information and access under the personal data protection rules.

Right to rectification

The data subject has the right to request in writing that the Data Controller correct, supplement or amend personal data relating to him or her (e.g. in the event of erroneous data entry or a later change of data). The Data Controller shall inform the data subject in writing within one month that the correction, supplementation or amendment has been carried out.

Right to erasure

The data subject has the right to request in writing that the Data Controller erase personal data relating to him or her. Unless the Data Controller is obliged by law to retain the data, the Data Controller shall

erase the personal data specified in the request within 5 working days and shall inform the data subject thereof in writing.

Right to restriction of processing

The data subject has the right to request in writing that the Data Controller restrict the processing of personal data relating to him or her. Restriction (blocking) may take place, for example, where the data subject wishes to use the blocked personal data for legal proceedings before a court or authority. Except for storage, the Data Controller may process blocked personal data only with the data subject's consent, for the establishment, exercise or defence of legal claims, or for the protection of the rights of another natural or legal person; it must also clearly mark the fact of the blocking and keep the blocked personal data separate.

Right to data portability

The data subject has the right to request in writing that the Data Controller send him or her the personal data concerning him or her in a structured, commonly used, machine-readable format, and has the right to transmit those data to another controller without hindrance from the Data Controller.

The right to data portability may be exercised where:

- the processing is based on the data subject's consent, or the processing is necessary for the performance of a contract to which the data subject is a party (including where steps are taken at the data subject's request prior to entering into a contract); and
- the processing is carried out by automated means.

The data subject may request the direct transmission of his or her personal data between controllers, where technically feasible.

Right to object

The data subject has the right to object, on grounds relating to his or her particular situation, to the processing of personal data based on the legitimate interests of the Data Controller or a third party, including profiling based on those provisions. In this case the Data Controller may no longer process the personal data, unless it demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject, or which relate to the establishment, exercise or defence of legal claims.

Legal remedies in relation to data processing

The data subject is entitled to contact the Data Controller directly if he or she has any question about the processing of his or her personal data or wishes to exercise his or her data protection rights.

In the event of infringement of his or her data protection rights, the data subject may seek a legal remedy from the Hungarian National Authority for Data Protection and Freedom of Information (Nemzeti Adatvédelmi és Információszabadság Hatóság, NAIH; registered office: 1055 Budapest, Falk Miksa utca 9-11.; postal address: 1363 Budapest, P.O. Box 9; telephone: +36 (1) 391-1400; e-mail: ugyfelszolgalat@naih.hu).

If the processing of the data subject's personal data is unlawful, the data subject is entitled to bring a civil action against the Data Controller. The data subject may also bring the action before the regional court (törvényszék) competent for his or her place of residence (<https://birosag.hu/torvenyszekek>).

Budapest, 1 August 2026

Menton Human Expert Kft.
on behalf of
Roland Letenovics
Managing Director