

## 1. Introduction

### WHISTLEBLOWING POLICY

#### I. GENERAL SECTION

**MTDM Management Ltd.** (hereinafter referred to as the "Company") shall establish a whistleblowing system to report information on unlawful or suspected unlawful acts, omission or other abuses, as well as violations of the rules of conduct established by its internal regulations, in compliance with its obligation under Article 18 (1) and (2) of Act XXV of 2023 on Complaints, Public Interest Notifications and Reporting of Abuses (hereinafter referred to as the "Complaints Act"). In the context of the use and operation of this whistleblowing system, it shall adopt the following rules (hereinafter referred to as 'the Rules') in order to establish internal procedures and rules in this respect.

## 2. Purpose and scope of the Policy

### 2.1. Purpose of the Policy

2.1.1. The purpose of this Policy to create an abuse reporting system for the reporting of Abuses related the operations of the Company, which complies with the provisions of the Complaints Act, while respecting the provisions of Act I of 2012 on the Labor Code (hereinafter: the Labor Code), and which facilitates the elimination of the Abuse, while protecting the Whistleblowers.

2.1.2. In this Policy, the Company establishes the procedures for the effective investigation of Reports, the measures to be followed to protect the personal data of the Reporting Party and the persons concerned by the Report, with the aim of setting out its whistleblower protection system in a clear and comprehensible manner.

### 2.2. Definitions of terms

2.2.1. *Employment relationship*: any legal relationship in which the Employee performs an activity for and under the direction of the Employer for remuneration or as a self-employed person.

2.2.2. *Employer*: the party that employs a natural person under an employment contract.

2.2.3. *Employee*: a natural person who performs an activity for and under the direction of the Employer within the framework of an employment contract for remuneration or who performs an activity on his/her own account.

2.2.4. *Complaint*: A request for redress of a violation of an individual right or interest that is not subject to any other procedure, particularly judicial or administrative. A complaint may also include a proposal.

2.2.5. *Public interest notification*: draws attention to a circumstance the remedying or removal of which is in the interest of the community or society as a whole. A Public Interest Notification may also contain a proposal.

2.2.6. *Notification*: a verbal or written communication containing a complaint or a Public Interest Notification that is made by a Reporting Party to a recipient in the whistleblowing system.

2.2.7. *Misconduct*: any act or omission that is contrary to the law applicable to the Company and its Employees, the Company's internal regulations, including in particular the principles and requirements set out in Section 3 of this Policy.

2.2.8. *Reporting Party*: the person who makes a Notification in the whistleblowing system.

2.2.9. *Reported Party*: The natural or legal person who is the subject of the Notification.

### 2.3. Scope of the Rules

2.3.1. This Policy applies to the officers of the Company and all its Employees, regardless of the nature of their employment relationship (hereinafter collectively referred to as Employees), as well as to all those who are entitled to report any misconduct in the course of the Company's operations pursuant to the Complaints Act and Section 6.1 of this Policy.

2.3.2. The scope of the Policy does not cover the receipt and investigation of Complaints or Public Interest Notifications in relation to the content of which another body designated by law is entitled and obliged to act (e.g. police, court in the case of a criminal offences).

## II. CIRCUMSTANCES GIVING RISE TO ABUSE NOTIFICATION

### 3. General principles

3.1. Employees of the Company shall perform their duties with due care, diligence, skill, and responsibility, in compliance with applicable laws, employer instructions, and professional standards. In this regard, employees must refrain from any actions or behavior that violate applicable laws or the Company's internal policies and regulations.

Employees are expected to contribute to the efficient and appropriate operation of the Company, support the achievement of its economic objectives, and uphold its good reputation.

3.2. Employees must maintain the confidentiality of all professional, business, personal, and other sensitive information they become aware of in the course of their work. Unless duly authorized, employees shall not disclose such information to the public or third parties, except when disclosure is required by law or professional duty.

3.3. Employees are required to collaborate with colleagues, foster positive working relationships, and treat one another with mutual respect. They should provide reasonable assistance to their colleagues within the limits of their knowledge and experience.

3.4. Employees must refrain from discrimination between colleagues throughout their stay at the workplace. In particular, the prohibition of discrimination should apply to workers in managerial positions when determining terms and conditions of employment, promotion, benefits and compensation and disciplinary measures and establishing liability. Employees must at all times respect the human dignity and personal rights of others.

3.5. Persons employed by the Company must comply with the standards of conduct set out in the Company's internal rules.

### 4. Subject of the Notification

- 4.1. The internal whistleblowing system allows for the reporting of illegal or suspected illegal acts or omissions, or other information about abuse.

### **III. THE COMPANY'S WHISTLEBLOWER PROTECTION SYSTEM**

- 5.1. The internal whistleblowing system shall be established and operated by the Company on its own, without the involvement of any external contributors. The Company shall appoint **Ildikó Tauszné Szimrók, HR Officer** (hereinafter referred to as the "Designated Person") to operate the Internal Whistleblowing System. The Company shall appoint **Tímea Birszki, HR Director** (hereinafter referred to as the "Deputy Designated Person") to replace the Designated Person (in case the Designated Person is unable to act or is involved in the Misconduct). The Designated Person and the Deputy Designated Person shall not be instructed or influenced in any way by the Employer in the performance of these duties (where not expressly provided otherwise in the Policy, the Designated Person shall include the Deputy Designated Person).
- 5.2. The framework for the operation of the internal whistleblowing system is set out in this Policy. Within the framework of the Code, the Designated Person shall independently determine the method of investigation, the persons to be interviewed where necessary and the means of evidence to be used. For the conduct of investigations, the Company shall provide a separate room where the technical conditions for the interview are adequate, and the privacy of the persons involved can be fully ensured.

### **IV. THE PERSONS ENTITLED TO MAKE THE NOTIFICATION**

- 6.1. Who is eligible to notify:

The following Parties are eligible to submit notifications in the whistleblowing system:

- a) an Employee employed by the Employer,
  - b) an Employee whose employment relationship with the Employer has ended,
  - c) a person who wishes to establish an employment relationship with the Employer and for whom the procedure for establishing such a relationship has started.
- 6.2. Additionally, the below Parties may submit notifications to the internal whistleblowing system
    - a) self-employed persons, sole proprietorships if the sole proprietorship has a contractual relationship with the Employer,
    - b) a person who holds an ownership interest in the Employer and a person who is a member of the Employer's administrative, management or supervisory body, including a non-executive director,
    - c) any contractor, subcontractor, supplier or person under the supervision and control of a delegate, who has initiated a procedure for establishing a contractual relationship with the Employer, or who is or was in a contractual relationship with the Employer,
    - d) trainees and volunteers working for the Employer,
    - e) persons who wish to enter into a legal or contractual relationship with the Employer under (a), (b) or (d), and for whom the procedure for the establishment of such a legal or contractual relationship has been initiated, and
    - f) person who ceased to have a legal or contractual relationship with the Employer under (a), (b) or (d).

## **7. Data provided by and the processing of personal data relating to Data Subjects**

- 7.1. Personal data of the notifier shall not be disclosed without his/her consent. The notifier may specifically request the disclosure of his/her personal data (name and identification data) when making his/her notification.

If the Notifier is a legal person, the Notifier must provide its registered office and the name of the legal representative of the legal person making the Notification.

- 7.2. The information on the processing of personal data relating to the Notifiers and other persons concerned by the Notification is set out in the "*Data Management Policy*", which is set out as Annex 1 to this Policy.

## V. THE APPLICATION

### 8. The ways to report

- 8.1. Notifications may be made in the following ways
- a) orally: in person at the Company, 1139 Budapest, Teve u. 33-41 C. building 1, 1139 Budapest, every week on Wednesday between 9.00 and 17.00 or, in justified cases, at a previously agreed time with the person designated to handle the Notification.
  - b) in writing: by sending an e-mail [toszimrok.ildi@metrodom.hu](mailto:toszimrok.ildi@metrodom.hu).
- 8.2. In the case of a Notification made orally, the designated person shall draw up a written record of the Notification with the content specified in Item 9. The content of the record may be inspected by the notifier before signing it, and he/she may make additions or suggestions to its content.
- 8.3. The operator of the internal whistleblowing system must take a full and accurate record of the oral Notification when preparing the written record.
- 8.4. In the case of an oral report, the whistleblower should be made aware of the consequences of making a report in bad faith, the procedural rules governing the investigation of the Notification and that his/her identity, if s/he provides the information necessary to establish it, will be treated confidentially at all stages of the investigation.
- 8.5. In order to facilitate the submission of a written Notification, a sample "*Notification Form*" is published as Annex 2 to these Policy, which contains the content requirements for an effective, investigable Notification. The use of the template is not mandatory, the Company intends to publish it to facilitate the effectiveness of the internal whistleblowing system. The designated person will acknowledge receipt of the written report within 8 days. The acknowledgement shall include general information to the Whistleblower on the procedural and data handling rules under the Complaints Act and this Policy. The designated person shall comply with the information set out in this point by providing the present Policy.

### 9. Content of the Notification

- 9.1. If the Notifier does not provide his/her name and contact details when making the Notification, he/she acknowledges that the examination of his/her Notification may be disregarded.

In the Notification, the Notifier is required to state the grounds for his/her right to make a Notification (e.g. employment).

- 9.2. In the Notification, the Whistleblower must describe in sufficient detail the circumstances of the Misconduct or Harm that he/she has experienced and on which the Notification is based, in order to investigate and take the necessary action.

Typically, the following information should be provided by the notifier:

- a) which organizational unit and who has committed the Misconduct;
- b) in what ways was the Misconduct manifested;
- c) if known, the information necessary to identify the perpetrator of the Misconduct;
- d) when the Misconduct happened.
- e) whether the Misconduct is still ongoing.

If there is a history of the Notification (e.g. the Reporting Party has previously reported the abuse), this fact must also be stated in the Report.

- 9.3. In the event that the Whistleblower has any documents or other evidence in support of his/her report of the Misconduct, he/she is encouraged to attach them in order to ensure the effectiveness of the investigation.
- 9.4. When making a Notification, the Reporting Party must declare that the Notification is made in good faith and the circumstances of which s/he has knowledge or reasonable grounds to believe are true.

## **VI. THE PROCEDURE OF THE INVESTIGATION**

### **10. Effectuating or denying an investigation**

- 10.1. On the basis of the Notification, the investigation may be waived in the following cases:
  - a) the Notification was made by an unidentified Notifier,
  - b) the Notification was not made by a person authorized to do so under Item 6 of this Policy,
  - c) a repeated Notification by the same Notifier with the same content as the previous Notification, or
  - d) the harm to the public interest or to an overriding private interest would not be proportionate to the restriction of the rights of the natural or legal person concerned by the notification resulting from the investigation of the notification.
- 10.2. If none of the cases set out in clause 10.1 applies, the designated person on behalf of the Company will effectuate the investigation on the basis of the Notification.

### **11. Examination of the Notification**

- 11.1. If the stipulations of Item 10.1 are not applicable and the Notification can be examined, the Designated Person shall investigate the facts contained in the Notification within the shortest time allowed by the circumstances, but not later than 30 days from the date of receipt of the Notification.
- 11.2. The above time limit may be extended in particularly justified cases, subject to simultaneous notification sent to the notifier. In this case, the notifier shall be informed of the expected date of the investigation and the reasons for the extension. The time limit for investigating the notification and informing notifier thereof shall not exceed 3 months in the case of an extension.
- 11.3. The investigation of the Notification shall include an assessment of the relevance of the circumstances set out in it and the measures that are appropriate to remedy the Misconduct.
- 11.4. If the report justifies the initiation of criminal proceedings, arrangements must be made to report the matter. The proceeding may be initiated by the Designated Person or by the Chief Executive upon the information received from the Deputy Designated Person. If the Chief Executive is involved in the act to which the proceeding relates, the decision to file the report shall be made by the Company's supreme body.
- 11.5. The person concerned by the Notification shall be informed in detail of the Notification at the start of the investigation, as set out in Chapter V. The person concerned by the notification may be omitted from the information if immediate information would frustrate the investigation of the notification. In this case, the information shall be provided at a later stage.

- 11.6. The Company shall ensure that the person concerned by the Notification may, at any time during the entire procedure initiated on the basis of the Notification, express his/her views on the Notification, including through his/her legal representative, and provide evidence in support of his/her views.
- 11.7. In all cases, the Company will act fairly, impartially and independently, in accordance with the requirements of equal treatment and the presumption of innocence, when investigating the Notification.

## **12. Means of investigation**

- 12.1. The investigation of a complaint must primarily be based on an assessment of the allegations made by the Reporting Party and the evidence they provide. If necessary, the Designated Person may interview the individuals concerned by the Notification or any witnesses. Statements from these individuals and witnesses shall be given voluntarily and shall not be obtained through coercion or under the threat of legal consequences
- 12.2. If the investigation requires company data that the Designated Person does not have, the competent supervisor or head of department must provide it.
- 12.3. All data and information obtained by the Designated Person during the investigation is strictly proprietary. The Designated Person may use the data and information only for the purpose of the investigation and may not share it with anyone else. The contents of the means of investigation may be shared with the parties to the investigation (data subject, witnesses, senior employees or officials) only to the extent necessary to ensure the effectiveness of the investigation.
- 12.4. If the investigative means available to the Designated Person do not reveal the facts of the case, the whistleblower must be informed immediately and advised to contact competent public authorities or a court if s/he maintains the allegations in his or her complaint.

## **13. Document management**

- 13.1. In the whistleblowing system, all written, printed or electronically stored documents, records, minutes, recordings and actions related to the Notification are considered as documents.
- 13.2. The whistleblowing system shall implement a separate document management system, separate from the Company's document management system. The filing, copying and safekeeping of documents shall be carried out exclusively by the Designated Person, who shall not be replaced in this capacity by any other person.
- 13.3. The documents must be kept in sealed envelopes, separated by filing date and by Notification, and the envelopes must be kept in a locked cabinet. Only the Designated Person shall have access to the filing cabinet.
- 13.4. The files relating to the Notification must be kept for five years after the investigation is closed. Thereafter they shall be destroyed and a record made thereof.

## **VII. MEASURES**

- 14.1. The investigation of the report shall include an assessment of the relevance of the circumstances set out in the report and the taking of measures appropriate to remedy the unlawful act or omission or the Misconduct.
- 14.2. If, on the basis of the investigation, the Designated Person finds that the Notification is unfounded and no further action is required, the Designated Person shall close the procedure on behalf of the Company.
- 14.3. If the investigation of the conduct described in the Notification justifies the initiation of criminal proceedings, the Company will, on the recommendation of the Designated Person, take steps to

file a report, in accordance with the relevant procedural rules.

- 14.4. If the conduct described in the Report does not justify a criminal prosecution, but the Designated Person finds during the investigation that it is contrary to the law or the Company's internal rules, s/he will submit a proposal for action to the competent employer' representative or the Company's supreme body.

The competent body shall establish the responsibility of the person(s) who committed the Misconduct.

The Company, as the employer, is entitled to take employer action against such person(s) in accordance with the provisions of the Labor Code and the employment contract. If the action is justified against a person in a position of authority, the senior officer is entitled to take the action. The supreme body shall be entitled to take action against a senior officer.

- 14.5. Following the investigation of the Notification, the Company shall inform the Reporting Party in writing (by post or e-mail) of the outcome of the investigation and the measures taken by the Company.

### **VIII. FINAL PROVISIONS**

These Policy and the provisions contained herein shall enter into force on 01.11.2023 and shall remain in force indefinitely. Amendments to the Policy shall take effect from the date of publication of the amendments.

The provisions of this Policy shall be interpreted in accordance with the provisions of the Complaints Act and the Labor Code.

Annexes:

1. *Annex 1 - Information Notice on Data Management*
2. *Annex 1 - Declaration form*

## I. Annex No.

### DATA PROCESSING NOTICE

#### I. Introduction

This Privacy Notice (the "Notice") is an annex to the Whistleblowing Policy. The Notice applies only to the processing of whistleblowing data.

The purpose of this Notice is to provide you with information about, among other things, who and what personal data we process in connection with misconduct notifications, for what purposes, on what legal basis and for how long, and to provide you with information about the data management principles and the data subjects' rights of enforcement and redress in relation to data management.

The security and proper handling of your personal data is of the utmost importance to us, so please read this Notice carefully and thoroughly. If you have any questions or comments about what is written here, please do not hesitate to contact us [szimrok.ildi@metrodom.hu](mailto:szimrok.ildi@metrodom.hu) and our colleagues will be happy to assist you.

#### II. Definitions of terms used in the Privacy Notice

1. **Personal Data:** any information relating to a Data Subject on the basis of which the Data Subject can be identified or identifiable. An identifiable natural person is one who can be identified directly or indirectly, in particular by reference to an identifier such as a name, 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. The Controller will indicate in Chapter V of this Notice precisely which personal data it processes about the Data Subject.
2. **Data processing:** any operation or set of operations which is performed upon data, regardless of the procedure used, in particular the collection, recording, organization, storage, alteration, use, searching, disclosure, transmission, matching or combination, classifying, erasure and destruction, as well as the prevention of further use of the data.
3. **Data Controller:** a 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. Our company is considered to be a controller in the context of the notification of misconduct. Details of the Data Controller are set out in Chapter III.
4. **Data Subject:** an identified or identifiable natural person, including, but not limited to, the Data.
5. **GDPR:** 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 (General Data Protection Regulation).

#### III. The Data Controller and its representative, Data Protection Officer

Contact details of the Data Controller:

- Company name: MTDM Management Üzletviteli Szolgáltató Korlátolt Felelősségű Társaság
- Registered office and mailing address: 1139 Budapest, Teve utca 33-41. building C. Door 1.
- Company registration number: 01-09-957503
- E-mail: [szimrok.ildi@metrodom.hu](mailto:szimrok.ildi@metrodom.hu)

Name and contact details of the Data Controller's representative:

- Name: Tamás Kricsfalussy Managing Director
- for correspondence: 1139 Budapest, Teve utca 33-41.

building C. Door 1 Data Protection Officer of the Data Controller:



- Name: Szabó, Kocsis and Hunya Law Office
- Registered office and mailing address: 1095 Budapest, Mester utca 83/A. IX. em. 4. a.
- E-mail: [szkiroda@szkiroda.hu](mailto:szkiroda@szkiroda.hu)
- Phone number: +36-1-878-0802

#### **IV. Principles of data management**

The following is a summary of the data processing principles that the Data Controller will fully enforce throughout the entire period of data processing in accordance with Article 5 of the GDPR.

1. **Lawfulness, fairness and transparency:** the processing of the Data Subject's personal data shall be carried out exclusively in a lawful, fair manner and transparent manner for the Data Subject. The processing of personal data under this Notice and the provision of personal data is based on law. The Data Controller shall make the current text of this Notice available free of charge, without obligations, on a continuous basis, as well as the Whistleblowing Policy.
2. **Purpose limitation:** the Data Controller processes personal data only for the explicit and legitimate purposes stated in the Notice, which are specified by law. The Data Controller shall not process personal data in a way incompatible with the purpose of the processing.
3. **Storage limitation:** the processing of the Data Subject's personal data is carried out for the time necessary to achieve the purpose of the processing.
4. **Accuracy:** the controller shall ensure that the personal data it processes is accurate and up to date; it shall take all reasonable steps to ensure that inaccurate personal data is corrected. Data subjects are requested to notify the Controller of changes to their personal data.
5. **Data minimization:** the Data Controller aims to process only the most necessary and relevant personal data. The Data Controller will only process data in the context of misconduct reporting that are genuinely necessary for the purpose of the processing. If certain data is unnecessary for the purpose, it will delete the data without delay.
6. **Integrity and Confidentiality:** the Data Controller shall ensure adequate security of personal data and protection against unauthorized or unlawful processing, accidental loss, destruction or damage by applying appropriate technical or organizational measures. The Data Controller shall, inter alia, ensure that the documents relating to the notifications are kept separately for each notification in a locked envelope in a locked cabinet, in order of date of receipt, and that only the designated person has access to them. Further provisions on the protection of personal data are set out, inter alia, in the Whistleblowing Policy.

#### **V. Data processing in relation to whistleblowing**

The Data Controller processes personal data in the course of investigating notifications of misconduct. The data handling rules are also governed by the Whistleblowing Policy.

- Purpose of processing: to investigate a report of misconduct, to investigate the notification and to remedy or stop the conduct that is the subject of the report.
- Those affected:
  - Reporting Party
  - Party reported in the Notification
  - Other persons involved in the proceedings e.g. witnesses or persons with information about the case
- Personal data:

- Name and, if necessary, other personal data necessary to identify the person (e.g. address, mother's name), contact details (telephone number / e-mail address).
- In case of a written notification, the e-mail address of the notifier from which the notification is sent.
- In the case of an oral report, signature on the record.
- Content of the notification and related documents.
- If the data subject is not an employee of the Data Controller, the name of the company that employs him or her.

Consequences of not providing the data: if the notifier does not provide personal data, the notification may be handled anonymously, or the Data Controller may decide not to examine the notification. If the data of the reported party concerned by the notification are not provided to the Data Controller, the Data Controller may not be able to effectively investigate the notification and take the necessary measures.

- Legal basis for processing: performance of a legal obligation [Article 6(1)(c) GDPR] - the Law 2023 on complaints, whistleblowing and reporting of misconduct. Act XXV, Chapter II.
- Duration of data management: the Data Controller shall keep the data and documents related to the Notification for five years after the investigation is closed.
- Data source: the data subject directly (the notifier) in the case of data of the notifier, and the notifier in the case of data of the person concerned by the notification.
- No automated decision-making or profiling shall take place.
- Access to data, data transmission:  
The Data Controller shall ensure that the personal data of the Reporting Party who discloses his/her identity and of the reported party concerned by the notification cannot be disclosed to persons other than those entitled to have that information. The persons investigating the notification may, pending the conclusion of the investigation or the initiation of formal prosecution as a result of the investigation, share information about the content of the notification and the person concerned, in addition to informing the person concerned, with other departments or staff of the Data Controller to the extent strictly necessary for the conduct of the investigation.

The Data Controller has set up and operates the whistleblowing system on its own, independently, without the involvement of any external parties, and does not employ any data processor.

Personal data relating to a notification may be transferred to the body competent to conduct the procedure initiated on the basis of the notification, if that body is entitled to process the data by law or if the data subject has consented to the transfer. If criminal proceedings are justified on the basis of the notification, arrangements shall be made to bring a complaint.

No data is transferred to third countries or international organizations.

## **VI. Enforcement and redress**

### **Rules on the exercise of rights of access:**

The Data Controller shall provide the requested information without undue delay, but at the latest within one month of the request for information. If necessary, taking into account the complexity of the request and the number of requests, this time limit may be extended by a period of additional two months. The Data Controller shall inform the Data Subject of the extension of the time limit, stating the reasons for the delay, within one month of receipt of the request.

If the Data Controller does not take action on the request of the Data Subject, the Data Controller shall inform the Data Subject without delay, but at the latest within one month of receipt of the request, of the reasons for the failure to act and of the possibility for the Data Subject to lodge a complaint with the Authority and exercise his or her

right to judicial remedy. If the Data Controller has reasonable doubts about the identity of the person making the request, it may also request the submission of additional information necessary to confirm the identity.

### **Communication with the Data Controller:**

The communication between the Data Subject and the Data Controller takes place by e-mail or by post. The e-mail address, postal address and seat of the Data Controller for this purpose are the ones provided under Item I. Introduction of the present policy

#### **1. Right of access:**

The Data Subject shall have the right to obtain feedback from the Controller at any time as to whether or not their personal data are being processed and, if the processing is ongoing, the Data Subject shall have the right of access to the personal data processed to the following extent.

In the context of access, the information provided by the Data Controller in relation to data management may include in particular:

- a) the source of the personal data processed,
- b) the purpose and legal basis of the processing,
- c) the scope of the personal data processed,
- d) in the case of transfers of personal data processed, recipients of the transfers,
- e) the period for which the personal data processed are kept and the criteria for determining that period,
- f) the rights of the data subject under the Information Act and the GDPR, and how to exercise them,
- g) the circumstances in which a personal data breach occurred in the context of the processing of the data subject's personal data, the effects of the personal data breach and the measures taken to address them,
- h) the right to lodge a complaint with a supervisory authority.

If the notification concerns a natural person, in exercising their right of information and access under the provisions on the protection of personal data, the personal data of the notifier shall not be disclosed to the person requesting the information.

#### **2. Correction:**

The Data Subject shall notify the Data Controller in writing of any changes to their personal data. If the Data Subject fails to notify the Data Controller of a change in their personal data without delay, the Data Subject shall bear the consequences thereof. If the personal data provided is inaccurate but the accurate personal data is available to the Data Controller, the Data Controller shall automatically correct the personal data.

#### **3. Data deletion:**

The Data Subject shall have the right to obtain from the Data Controller, upon their request, the deletion of personal data relating to them without undue delay, and the Data Controller shall be obliged to delete personal data relating to the Data Subject without undue delay, in particular where one of the following grounds applies:

- a) the personal data are no longer necessary for the purposes for which they were collected or otherwise processed;
- b) the Data Subject withdraws their consent to the processing and there is no other legal basis for the processing (the withdrawal does not retroactively affect the lawfulness of the processing);
- c) the Data Subject objects to processing based on legitimate interests;
- d) the personal data were unlawfully processed by the Controller;
- e) the personal data must be deleted in order to comply with a legal obligation under EU or Member State law to which the controller is subject;
- f) the personal data collected in connection with the provision of information society services referred to in Article 8(1) of the GDPR.

Even in the above cases, the Controller is not obliged to delete the personal data processed, if the processing is necessary:

- a) to exercise the right to freedom of expression and information;
- b) to comply with an obligation under EU or Member State law that requires the controller to process personal data or in the public interest;

- c) for statistical or archiving purposes, or for scientific or historical research purposes, where deletion would be unlikely to make such processing possible or would seriously undermine it;
- d) on grounds of public interest in the field of public health pursuant to Article 9(2)(h) and (i) and Article 9(3) of the GDPR;
- e) to bring, enforce or defend legal claims.

**4. Right to restriction of processing:**

The Data Subject shall have the right to obtain from the Data Controller, at his or her request, the restriction of processing if one of the following conditions is met.

- a) the Data Subject contests the accuracy of his or her personal data, in which case the restriction applies for the period of time necessary to allow the Controller to verify the accuracy of the personal data;
- b) the processing is unlawful and the Data Subject opposes the deletion of the personal data and requests instead the restriction of their use;
- c) the Controller no longer needs the personal data to fulfil the purpose of the processing, but the Data Subject requires them for the establishment, exercise or protection of legal claims;
- d) the Data Subject has objected to the processing, in which case the restriction shall apply for the period until it is established whether the legitimate grounds of the Controller prevail over the legitimate grounds of the Data Subject.

Where processing is restricted as described above, such personal data may be processed, except for storage, only with the consent of the Data Subject or for the establishment, exercise or protection of legal claims or the protection of the rights of another natural or legal person, or for important public interests. If the restriction of processing is lifted, the Data Subject who has requested the restriction shall be informed in advance by the Controller of that fact.

**5. Initiation of proceedings by the Authority:**

The Data Subject may lodge a complaint with the National Authority for Data Protection and Freedom of Information (hereinafter: the Authority), in order to initiate an investigation on the grounds that a breach of rights has occurred or is imminent in relation to the processing of their personal data. The Authority's investigation is free of charge and the costs of the investigation are advanced and borne by the Authority. No person shall suffer prejudice as a result of having made a notification to the Authority.

Authority contact details: address: 1055 Budapest, Falk Miska u. 9-11.; e-mail: [ugyfelszolgalat@naih.hu](mailto:ugyfelszolgalat@naih.hu); website: <http://naih.hu>; telephone: +36 (1) 391-1400.

**6. Enforcement before the courts:**

The Data Subject may take the Data Controller to court in the event of a breach of their rights, and the court shall have jurisdiction to hear the case. As a general rule, the competent court is the court in the place where the Controller has its registered office, but the lawsuit may also be brought, at the Data Subject's discretion, before the court of the Data Subject's registered address or place of residence. The jurisdiction of the court can be checked by using the "Court Search" application on the website [www.birosag.hu](http://www.birosag.hu). The tribunal will adjudicate the case on a priority basis.

**7. Compensation:**

Any person who has suffered damage as a result of a breach of data protection legislation is entitled to compensation from the Data Controller for the damage suffered.

The Data Controller is liable for any damage caused by processing in breach of data protection legislation.

The Data Controller shall be exempt from liability if it proves that it is not in any way responsible for the event resulting in the damage.

## **VII. Data security**

The Data Controller shall ensure the security of data processing and shall take the necessary and appropriate technical and organizational measures to this end. It shall ensure the confidentiality (e.g., unauthorized access), integrity (alteration, modification, deletion), availability (accessibility, retrievability) of personal data.

In its data management and related organizational activities, the Data Controller shall take into account the current state of science and technological development. It shall endeavor to use the most secure technology possible to maintain data security and to guarantee data security appropriate to the level of risk, in order to protect the rights and freedoms of natural persons.

#### **VIII. Other provisions**

The Data Controller reserves the right to unilaterally amend this Policy at any time, but the Data Controller will always publish the current Notice.

Budapest, 31.10.2023.

**2. Annex No.**

**REPORTING MISCONDUCT  
(FORM)**

**I. DETAILS OF THE NOTIFIER:**

Name: .....  
address: ..... telephone  
number: ..... E-mail:  
.....

**II. THE DATE AND CIRCUMSTANCES OF THE MISCONDUCT REPORTED:**

.....  
.....  
.....  
.....

**III. THE SUBJECT OF THE NOTIFICATION**

- corruption
- money laundering
- crime against property
- physical or mental integrity or invasion of privacy
- other crimes/offences specified in the Penal Code
- breach of data protection rules
- discrimination
- harassment
- improper or wasteful use of assets owned or held by the Company
- other unethical behavior towards colleagues, partners or third parties
- other misconduct that may damage the reputation of the Company

*(please mark the category of misconduct with an X)*

**IV. A DETAILED DESCRIPTION OF THE ABUSE**

.....  
.....  
.....  
.....  
.....  
.....  
.....  
.....  
.....  
.....  
.....

**V. EVIDENCE, DOCUMENTS SUPPORTING THE MISCONDUCT**

.....  
.....  
.....  
.....

**VI. OTHER COMMENTS**

.....  
.....  
.....  
.....

**VII. STATEMENTS**

By making this notification I declare that

- I submit the Notification in good faith, of circumstances of which I have knowledge or at least reasonable grounds to believe that they are true
- I have read the Company's whistleblowing policy.

Date: ....., ..... year ..... month .....day

.....  
(signature)