Internal directive on whistleblower protection
Whistleblowing policy

An internal reporting system has been implemented in BitElevate sro , which is an integral part of the internal control mechanisms and procedures serving to reduce and effectively manage risks. Effective from August 1, 2023, all obliged entities pursuant to Act No. 253/2008 Coll., on certain measures against the legalization of proceeds from crime and the financing of terrorism (" **AML Act** ") are required to implement an internal reporting system within the meaning of Act No. 171/2023 Coll., on the protection of whistleblowers (" **Whistleblower Protection Act** ").

This system allows all employees, including those performing activities for our company outside of a traditional employment relationship, to report the actions described below. In the following lines, we inform you about what types of actions can be reported, how the report can be made, and who you can contact if you have any questions.

1. PURPOSE AND LEGAL FRAMEWORK

This internal reporting system (hereinafter referred to as the " **System** ") establishes a comprehensive framework for safe, transparent and effective reporting of misconduct in the organization and ensures the highest standards of whistleblower protection in accordance with **Czech law** . The system is developed in accordance with Act No. 171/2023 Coll., on the Protection of Whistleblowers, and other applicable legal regulations of the Czech Republic.
The main objective of this System is to create a culture of integrity and transparency where all persons feel safe in reporting potential violations of the law, ethical standards or company policies without fear of retaliation. The System uses modern technological tools and best practices to ensure maximum efficiency and protection of all stakeholders.

---

2. SCOPE AND DEFINITIONS

2.1 Persons covered by the System

This System applies to **all employees** (full-time, part-time, DPP, DPČ), managers, suppliers, subcontractors , consultants, interns and any third parties who come into contact with the organization's activities.

2.2 Types of reports covered by the System

The system covers a wide range of misconduct , including but not limited to:

- Violations of laws, including criminal offenses
- Financial fraud, corrupt practices and money laundering
- Violation of the General Data Protection Regulation (GDPR)
- Discrimination, harassment and mobbing in the workplace
- Violation of occupational health and safety rules
- Cybersecurity threats and incidents
- Violation of environmental standards
- Any other serious violation of ethical standards or company policies

2.3 Key definitions

A whistleblower is a person who, in good faith, reports a potential violation of law or ethical standards through the channels established by this System. **A violation of law** is an act or omission that violates applicable law, internal guidelines, or ethical standards. **Retaliation** includes any negative action taken against a whistleblower as a result of their reporting, including dismissal, demotion, harassment, or other disadvantage.

---

3. CHANNELS FOR NOTIFICATION AND RECEIPT OF REPORTS

3.1 Available communication channels

The organization provides **multiple secure** reporting channels that ensure flexibility and accessibility for all whistleblowers:

Channel	Description	Availability
Email channel	truth @ mion .group served directly by the executive	24/7
Postal address	Chudenická 1059/30, Hostivar, 102 00 Prague 10	Continuously
Telephone line	Communicated to the whistleblower after assessing the seriousness of the complaint, not published due to harassing phone calls	According to schedule

3.2 Recommendations for anonymous reporting

For whistleblowers who prefer anonymity, we recommend creating a new email account exclusively for whistleblowing purposes with the following secure services:

- **E-Mail encryption** - provides end-to-end encryption for free, e.g. gmail
- **Seznam.cz** (www.seznam.cz) - Czech email service with advanced security features

These services ensure a high level of anonymity and protection of communications between the whistleblower and the organization, which is key to preventing potential retaliation.

3.3 Process of receiving and recording reports

Each report goes through a structured admission process . The organization **issues an acknowledgement of receipt within 7 calendar days** of receipt of the report, which is usually done automatically if the reporter's contact details are provided. All reports are registered in a secure system with a unique case identification number and the use of tamper-resistant technology to ensure integrity and traceability.

---

4. DETAILED INVESTIGATION AND RESOLUTION PROCESS

4.1 Initial assessment and decision to investigate

The Commission (composed of the Executive Director) will conduct **an initial assessment of the credibility and scope of the report within 14 calendar days** of its receipt. This assessment includes a preliminary analysis of the facts, an assessment of the seriousness and a determination of whether a formal investigation is warranted.

4.2 Formal investigations with defined deadlines

If the initial assessment justifies the initiation of an investigation, **the full investigation will commence and be completed within 3 months** , with an extension possible with prior notice to the whistleblower. The investigation will be conducted in accordance with the principles set out in the legal order, in particular the requirement to establish the state of the matter beyond reasonable doubt.

4.3 Involvement of external experts and independence of investigation

Complex or sensitive cases may involve independent experts , which ensures objectivity and expertise in the investigation. Like administrative bodies, the investigation commission takes care to exclude bias from those involved in the investigation.

4.4 Detailed investigation procedures

The procedure contains detailed procedures for receiving, investigating and resolving reported violations, including:

Structure of the investigation process

├─ Receipt and registration of reports (0-7 days)
├─ Initial assessment (8-21 days)
├─ Decision on formal investigation (day 22)
├─ Appointment of the investigation team (days 23-30)
├─ Evidence collection and interrogations (1-2 months)
├─ Analysis and evaluation (2.5-3 months)
├─ Final report and recommendations (3-3.5 months)
└─ Implementation of corrective measures (4 months)

The responsible persons in the investigation process include the executive, who will request the opinion of the cooperating law firm ModerniPravnik.cz, advokátní kancelář sro, if necessary, at least until the Company grows. In the future, it is expected that the position of Compliance will be filled Officer (overall management), investigation team (collection of evidence), legal department (assessment of legal aspects), HR department (personnel measures) and senior management (approval of serious measures), where these persons will subsequently form a commission.

---

5. COMMUNICATION WITH THE WHISTLEBLOWER AND TRANSPARENCY

5.1 Notification schedule for the whistleblower

The organization ensures **regular and transparent communication** with the whistleblower according to the following schedule:

1. **Confirmation of receipt** : Within 7 calendar days of receipt of the report
2. **Ongoing updates** : Regular information on the progress of the investigation
3. **Information on the outcome of the investigation** : **Within 30 days** of the conclusion of the investigation
4. **Implemented measures** : Information on corrective measures taken in accordance with legal restrictions

5.2 Methods of secure communication

Communication with the whistleblower takes place through **secure channels** , including encrypted two-way email communications and, upon request, face-to-face meetings in a neutral environment or

telephone consultations via a secure line. Telephone consultations are usually offered after assessing the seriousness of the complaint.

---

6. PROTECTION OF WHISTLERS AND PROHIBITION OF REPLIANCE

6.1 Absolute prohibition of reprisals

The organization **categorically prohibits any retaliation** against whistleblowers, including dismissal, termination of employment, demotion, reduction of salary, harassment, workplace mobbing or any other adverse action. This protection is in accordance with the prohibition of discrimination set forth in the Labor Code and other Czech laws.

6.2 Practical protective measures

Anonymization of whistleblowers is ensured through advanced technological solutions and **is not considered a violation of** the whistleblower's job duties. Whistleblowing **cannot lead to dismissal from employment** or other sanctions, which is in accordance with the restrictions on dismissal set out in the Labor Code.

The reversed burden of proof means that the organization must prove that any negative action is not related to whistleblowing . **The urgent response mechanism** provides emergency review and temporary protection in the event of a report of retaliation.

---

7. INFORMATION AND TRAINING OF EMPLOYEES

7.1 Systematic information on whistleblowing mechanisms

Information on the existence and functioning of whistleblowing mechanisms is provided through:

- **Annual email campaigns** : Detailed information is sent to all employees annually
- **Onboarding protocol** : The system is explained during the orientation of new employees and contractors.
- **Mandatory interactive training** : Annual training with practical case studies and updates on new risks.
- **FAQ and instructions** : Available on the organization's internal portal.

7.2 Evaluation of the effectiveness of information

Anonymous surveys to assess awareness and trust in the system are conducted twice a year, allowing for continuous improvement of employee awareness and trust in the whistleblowing system .

7.3 Specialized training for management

Management receives **specialized training** on how to avoid, recognize, and respond to potential retaliation against whistleblowers.

---

8. PERIODIC REVIEW AND EFFECTIVENESS ASSESSMENT METHODOLOGY

8.1 Review schedule and frequency

Regular reviews of the effectiveness of whistleblowing mechanisms are conducted **at least once every 12 months** , following significant events or legal/regulatory changes. Some aspects are

reviewed more frequently – for example, security systems quarterly and whistleblower satisfaction semi-annually.

8.2 Comprehensive evaluation methodology

The review methodology includes :

1. **Quantitative analysis**
    - Number of reports filed by category
    - Average case processing time
    - Percentage of cases resolved within the specified time limits
    - Statistics of anonymous vs. identified reports
2. **Qualitative assessment**
    - Anonymous Whistleblower Satisfaction Surveys – automatically set up and sent email sent after case closure
    - Evaluation of the effectiveness of protective measures
    - Assessing the organization's culture regarding integrity
3. **Benchmarking and comparative analysis**
    - Comparison with industry best practices
    - Analysis of trends in similar organizations
    - International standards and recommendations
4. **Technology and security audit**
    - Evaluation of the functionality of IT systems
    - Testing anonymization mechanisms
    - Cybersecurity of communication channels
5. **Legal compliance audit – upon request with legal representative**
    - Compliance with current Czech and EU legislation
    - Review of compliance with Act No. 171/2023 Coll.
    - Updates following case law

8.3 Implementation of improvements

Continuous improvement of the System is implemented based on the results of the review, stakeholder feedback and identified risks. All significant changes are communicated to stakeholders within 30 days of their approval.

---

9. ROLES AND RESPONSIBILITIES

9.1 Compliance Committee – until the team is expanded, it is formed by a commission

Responsibility	Description	Time limits
Receiving reports	Coordination of all reporting channels	Continuously
Initial assessment	Credibility and severity assessment	Within 14 days
Management of the investigation	Coordination of investigation teams	As needed

Responsibility	Description	Time limits
Communication with the whistleblower	Regular information about the progress	Continuously
Implementation of measures	Supervision of the implementation of corrective actions	Within 30 days of completion of investigation

9.2 Senior management and organizational responsibility

Senior management has overall responsibility for the operation of the whistleblowing system , including allocating resources, approving serious disciplinary measures, and creating a culture of integrity **.**

9.3 Obligations of all employees

All employees and third parties have **an obligation to report** serious misconduct, **cooperate** in investigations, **comply with** the principles of this System and **participate** in regular training, which corresponds to their general obligations set out in labor regulations.

---

10. SANCTIONS AND DISCIPLINARY MEASURES

10.1 Sanctions for Violation of the System

Violations of this System , in particular retaliation against whistleblowers, may lead to disciplinary action up to and including termination of employment or other relationship, financial sanctions in accordance with the employment contract or cooperation agreement (subcontractor) and, where applicable, criminal liability under applicable law. The Organization shall proceed in accordance with the provisions of the Labor Code on grounds for termination.

10.2 Protection against system abuse

Intentionally false or malicious reports may result in disciplinary action, but only after a thorough investigation and proof of malicious intent. The organization distinguishes between reports made in good faith that turn out to be unfounded and intentionally false allegations.

---

11. TECHNOLOGICAL SECURITY AND MODERN TOOLS

11.1 Advanced technological solution

The organization uses **state-of-the-art technology** to ensure the integrity and security of the whistleblowing process, including blockchain technology for an immutable record of reports, artificial intelligence to identify trends and systemic risks, end-to-end encryption of all communications, and multi -factor authentication for access to sensitive data.

11.2 Cybersecurity and data protection

All systems are protected according to the highest cybersecurity standards with regular security audits, geographically separated data backups, and continuous monitoring of security threats.

---

12. CONTACT INFORMATION AND RESOURCES

12.1 Key contacts

- **Compliance Officer** : truth@mion.group
- **Anonymous reporting** : [secure email, easy to create anonymously]

12.2 Recommended secure email services for anonymous reporting

- **E-Mail** : https://proton.me/mail (free end-to-end encryption), Gmail, etc.
- **Seznam.cz** : www.seznam.cz (Czech service with advanced security)

---

13. FINAL PROVISIONS

13.1 Effectiveness and updates

This System shall enter into force on the date of its approval by the statutory body of the organization and shall replace all previous versions of similar guidelines. The System shall be **regularly updated** in accordance with legal changes, technological developments and practical experience from its application.

In Prague, on 31 July 2025
Behind BitElevate Ltd. approved
executive OLE HENRIK BAUMGARTEN SKOGSTRØM