



Multitude Group's Whistleblowing Policy

Last updated on December 20, 2023

Approved and enacted by Multitude Group's Board of Directors on December 22, 2023

The purpose of this Whistleblowing Policy (hereinafter "Policy") is to encourage Multitude Group's (hereinafter together with its affiliates and subsidiaries "Group", "we", "us" or "our"), employees and other persons, as determined below, to report about improper practices such as illegal activity occurring within the Group, to provide a clear framework for such reporting, to regulate the investigations of the reports and to provide protection framework for the reporting persons.

This Policy is applicable to all Group's affiliates and subsidiaries, except for Multitude Bank plc, which has its own whistleblowing policy established, and to all its current, former, and prospective employees at all levels, shareholders, board members, including non-executive members, trainees, volunteers, agency workers, self-employed persons, and contractors as well as persons working under the supervision of our contractors, subcontractors, and suppliers.

The person who exposes improper practices such as serious misconduct, dishonest or illegal activity within the Group is considered as a "Whistleblower", hereinafter also referred to as a "Reporting Person". Whistleblowing is therefore the disclosure by a Reporting Person of information regarding improper practices within the Group.

Improper practices may include, but are not limited to:

- a criminal offence, miscarriage of justice, corrupt practice, bribery, or an unethical act that has occurred or is likely to occur or to have occurred;
- a violation or suspected violation of law¹ or a failure to comply with laws or regulations;
- deliberate concealment of any of the above noted matters;
- human rights violations.

1. Internal Reporting

The Group has in place an appropriate internal framework to report improper practices. For this purpose, the Group has appointed its Group Head of Legal and Compliance as the Whistleblowing Reporting Officer, to receive and deal with such internal disclosures.

The Group ensures that the person appointed to receive and investigate the reports has sound judgement, investigation skills, integrity, sound communication skills, diplomacy, and objectivity.

¹The violations of law could be anything from the following areas of law of European Union or members states:

- public procurement;
- financial services, products and markets, and prevention of money laundering and terrorist financing;
- product safety and compliance;
- transport safety;
- protection of the environment;
- radiation protection and nuclear safety;
- food and feed safety, animal health and welfare;
- public health;
- consumer protection;
- protection of privacy and personal data, and security of network and information systems;
- breaches affecting the financial interests of the Union;
- infringements or breaches of the internal market of the Union.



1.1. Reporting procedure

All good faith concerns or reports regarding any improper practices can be reported in the following manner:

- submitting directly by hand or by e-mail address whistleblower@multitude.com to the Whistleblowing Reporting Officer;
- if the report concerns the Whistleblowing Reporting Officer, the report must be directly handed over or sent to the Chairperson of the Audit Committee.

The reporting email channel is operated in a secure manner that ensures that the confidentiality of the identity of the Reporting Person and any third party mentioned in the report is protected and prevents access thereto by non-authorized staff members. These reports shall be accessible only by the Whistleblowing Reporting Officer, or by the Chairperson of the Audit Committee as the case may be, and by a minimum number of named persons the access of whom is necessary for the appropriate processing of the report in a secure manner.

When raising concerns or filing a report, the reasons supporting the belief that an improper practice has occurred, is occurring or is likely to occur should be explained with sufficient clarity to comprehend and solve the alleged problem. Ideally, disclosures should be presented using the form provided in Appendix I, however, you may also submit your concerns in a format that is most convenient for you.

If the Reporting Person would like to discuss the matter with the Whistleblowing Reporting Officer, or with the Chairperson of the Audit Committee as the case may be, the reporting person should indicate this in his or her submission and include contact details at which he or she may be contacted.

1.2. Investigation procedures

The Whistleblowing Reporting Officer will be in charge of investigating and handling all concerns and reports submitted under this Policy. At her/his discretion, (s)he shall advise the Company's CEO, or the Board of Directors of the concerns and reports received. The Whistleblowing Reporting Officer may retain, at the Company's expense, external legal counsel, or other advisor to assist in conducting the investigation.

In the event that a disclosure under this section leads to the detection of an improper practice which constitutes a crime under any applicable law, the Whistleblowing Reporting Offices may refer the report received to the police for investigation thereof, however, should the subject matter of the report have been rectified no provision of any law shall be interpreted as imposing an obligation on the Whistleblowing Reporting Officer to report a such matter.

Individuals who are accused of violations, if their name is disclosed, will be provided an opportunity to respond to the concern or report and demonstrate that the concern or reporting is false.

The Whistleblowing Reporting Officer shall investigate the report impartially and in confidentiality. The investigation process will be carried out with the level of care and speed appropriate to the case being investigated.

The Whistleblowing Reporting Officer shall confirm to the Reporting Person the receipt of the report within 7 (seven) days from the receipt of the report.



1.3. Investigation outcomes and follow-up

At the outcome of the investigation, the Whistleblowing Reporting Officer will draft a report. If substantiated, the violation will be qualified in the report and the matter will be resolved through appropriate corrective measures as recommended by the Whistleblowing Reporting Officer or, where applicable, as decided by the police or other relevant authority.

Corrective actions by the Group, if deemed necessary, may include clarification of a Group's policy, additional training, disciplinary action against a director or employee or termination of service or employment. Such sanctions will be implemented by the Group's department of Human Resources in co-operation with the Head of Legal and Compliance or by the Board of Directors.

The reporting person shall be informed within a reasonable timeframe but not later than within 3 (three) months from the receipt of the report, about the action envisaged or taken as a follow-up to the report and the grounds for the choice of that follow-up. Where the appropriate follow-up is still being determined, the Reporting Person shall be informed about this and about any further feedback that may be expected.

1.4. Confidentiality and protection measures

All disclosures that are made in good faith, and where the Whistleblower reasonably believes the information to be true, qualify to be treated as "protected disclosures". A protected disclosure affords the Whistleblower protection against detrimental action, including but not limited to any form of retaliation and/or discrimination, and against revealing the identity of the said Whistleblower, which can only be revealed with the written consent of the Whistleblower or if required under any applicable laws. This includes the safety of any information that could identify directly or indirectly the Whistleblower. The Group shall do its utmost to protect the identity of the Whistleblower and keep it confidential regardless of which reporting channel is used.

Except as otherwise provided by applicable Slovakian law, the Group does not undertake any obligation to investigate anonymous reports received. Notwithstanding the foregoing, in compliance with the Slovakian Act No. 189/2019 Coll. (the Amendment Act), which, among others, amends Act No. 54/2019 Coll. on the Protection of Whistleblowers (the Whistleblower Act), the Group will investigate anonymous reports originating from Slovakia.

An anonymous disclosure shall not be treated as a protected disclosure, but it may still be processed, exclusively based on our discernment, and considered in determining whether an improper practice has occurred. However, if the information provided in the report enables us to conclude the identity of the anonymous Whistleblower, the protected disclosure shall be applicable to such disclosure as well.

1.5. False reports

False or malicious reports must not be made knowingly, and any person who makes such a claim is not protected under this Policy. If a person is found to have made such a report in bad faith, it will be considered serious misconduct, and this person may be liable for disciplinary proceedings.

1.6. Data protection and record keeping

All personal data obtained by the recipient of the report through a submission (including data related to the Reporting Person and any accused persons) will be processed on confidential basis



and in accordance with the applicable data protection laws, including the General Data Protection Regulation (EU) 2016/679 and other applicable and relevant Data Protection Acts.

In the case where a concern or report of a violation leads to an investigation, or it is established that false or malicious report was made knowingly, the data relating to that report will be retained for as long as is necessary and proportionate to comply with the requirements of the applicable relevant law. In the case where a concern or report of a violation is found to be uncorroborated or unnecessary, data relating to that respective report or concern will be deleted, at the latest, within 3 (three) months following the day when it was realized that there was no violation.

Every data subject identified in a whistleblowing database is entitled to data subject's legal rights under applicable data protection laws such as a right to access, rectification and erasure. To make such a request, please contact our Data Protection Officer by e-mail dpo@multitude.com. Please note that any such communication must be in writing. In your request, please make clear what specific personal information you would like to have accessed, rectified, or deleted.

However, your above-mentioned rights may be restricted in accordance with applicable laws if the use of these rights could hamper the investigation of the suspected violations. In the event that we cannot provide you with access to, or rectification or deletion of your personal information, we will endeavor to inform you of the reasons why, subject to any legal or regulatory restrictions.

We will not discriminate against you for exercising any of your rights described in this Policy.

2. External Reporting

It is hoped that these guidelines will provide the assurance needed to raise whistleblowing issues within the Group and the Group strongly encourages the Reporting Person to first use reporting through internal reporting channels before reporting through external reporting channels, where the breach can be addressed effectively internally. However, nothing in this Policy should be construed to restrict any person from making an external report in accordance with any applicable law or regulation and the Group accepts that there may be circumstances where a person may feel it is more appropriate to make the disclosure to an external competent authority. In the event of an external disclosure the relevant authority will carry out investigations as necessary and to the procedures and processes set out by them.

The contact details of local external competent Whistleblowing authorities can be found on the following webpage <https://www.mofo.com/gdpr-european-privacy/whistleblowing/whistleblowing-authorities>.

3. Revisions of Policy

This Policy has been compiled by the Group Legal & Compliance function and approved and enacted by the Group's Board of Directors. This Policy is reviewed on a regular basis and may be revised as necessary and appropriate to reflect the dynamics of the Group and its environment. Changes will be made following the approval of the Board of Directors and will be communicated as and when the revisions are brought into effect.

Should you have any inquiries about this Policy, including processing of your personal data, please contact us at whistleblower@multitude.com.



APPENDIX I - WHISTLEBLOWING INTERNAL DISCLOSURE FORM

The completed form must be submitted directly and exclusively to the Whistleblowing Reporting Officer either by hand or using the email address whistleblower@multitude.com.

WHISTLEBLOWER'S CONTACT INFORMATION

This section may be left blank if the whistleblower wishes to remain anonymous.

Anonymous disclosures are not considered as protected disclosures.

NAME AND SURNAME:

POSITION AND ROLE:

CONTACT NUMBER:

E-MAIL ADDRESS:

SUSPECT'S INFORMATION

NAME:

POSITION AND ROLE:

CONTACT NUMBER:

E-MAIL ADDRESS:

WITNESS(ES) INFORMATION (if any)

If there are more than three witnesses, give their details on as many pages as necessary.

NAME:

DESIGNATION:

POSITION AND ROLE:

CONTACT NUMBER:

E-MAIL ADDRESS:

NAME:

DESIGNATION:



POSITION AND ROLE:
CONTACT NUMBER:
E-MAIL ADDRESS:

NAME:
DESIGNATION:
POSITION AND ROLE:
CONTACT NUMBER:
E-MAIL ADDRESS:

DISCLOSURE OF IMPROPER PRACTICE

Briefly describe the improper practice and how you came to know about it. Specify what, who, when, where and how. If there is more than one allegation, number each allegation and use as many pages as necessary.

1. Describe the improper practice.
2. Who committed the improper practice?
3. When did it happen and when did you notice it?
4. Where did it happen?
5. Is there any evidence that you can provide?

YOU SHOULD NOT attempt to obtain evidence for which you do not have a right of access since whistleblowers are ‘disclosing parties’ and **NOT** ‘investigators’.

6. Other persons involved other than the suspect(s) stated above:
7. Any other details or information which would assist in the investigation:
8. Additional comments:

Date:

Signature:
(optional)