

Whistleblowing Policy

Unifiedpost Group



Table of Contents

Introduction	4
Who is this policy intended for	4
Disclosures covered by the whistleblowing policy	4
Disclosures not covered by the whistleblowing policy	5
How to make a disclosure	5
Reporting through whistleblowing tool	5
Reporting through internal channels	6
Reporting through external channels	6
How are disclosures handled and investigated?	6
Protection of the whistleblower	7
Non-disclosure	7
Non-retaliation	7
Local legislation	7
Data Protection	7

Introduction

Unifiedpost Group SA, its subsidiaries and affiliates (the **Group** or **Company**) encourages a culture of openness that allows everyone to express any concerns about unlawful or unethical behaviour within the Group. In addition, as a listed company, the integrity of the Company's financial information and legal compliance is critical to the Company's success.

Misconduct or misbehaviour will only be reported if the people observing such behaviour feel safe in reporting the issue. Employees, customers and providers speaking up when observing (potential) misbehaviour is the most effective way for companies to discover unethical behaviour. Therefore, having a whistleblowing policy, ensuring confidentiality and protection of the whistleblower, is essential. If you observe misbehaviour or misconduct, you are encouraged to speak up. By doing so, you give our Company the opportunity to deal with the issue. Remaining silent about possible misconduct may worsen a situation and decrease trust.

The Board of Directors and the Management Team of the Group express their hope and expectation that all people involved will apply the whistleblowing policy in a sound and respectful way.

The Group reserves the right, at any time, to add provisions to this policy or to adapt it to possible changes in local legislation. If any provision of these rules were or should become invalid, this would not prevent the other rules from remaining in force.

Who is this policy intended for

This whistleblowing policy applies to all managers, directors, shareholders, (future, former and current) employees (including temporary staff and trainees) of the Group, as well as to all self-employed consultants (contractors and subcontractors), providers or customers and their employees working for or with the Group or taking services from the Group with relevant information on unethical or unlawful activities.

This policy does not affect the whistleblowing policies which are effective in the subsidiaries or affiliates ("Local policies") and complements these Local policies where relevant and applicable. In case of conflict between the Local policies and this policy, depending on the case and circumstances, the most stringent rules shall have priority. If any conflict arises between legal standards and this policy, we apply the more stringent standards.

Disclosures covered by the whistleblowing policy

The whistleblowing policy does not cover all types of wrongdoing which may occur. You can use the reporting system to report breaches of the Group's policies and/or violations of the laws and regulations of the European Union including the following matters:

- Financial services, products and markets, and prevention of money laundering and terrorist financing – this includes but is not limited to: consumer and investor protection, banking, investment funds and insurance;
- Product safety and compliance;
- Transport safety;
- Protection of the environment – this includes but is not limited to: criminal offences against the protection of the environment, rules on pollution or on the protection of biodiversity;
- Consumer protection – this includes but is not limited to: indication of prices, digital services or unfair commercial practises;
- Protection of privacy and personal data, and security of network and information systems (GDPR);

- Breaches affecting the EU's financial interests – this includes but is not limited to: fraud, bribery or corruption;
- Breaches relating to the (EU) internal market – this includes but is not limited to competition law or corporate tax law;
- Breaches relating to the Group's code of conduct; and
- Breaches relating to the Group's corporate governance charter
- the fight against tax fraud, tax evasion and social fraud
- ...

Disclosures not covered by the whistleblowing policy

For the avoidance of doubt, this policy does not apply to personal work-related concerns such as concerns or dissatisfaction with wages, workplace circumstances, interpersonal issues, psychosocial risks (such as harassment, violence, etc.) or performance evaluations. These kinds of matters must be reported through the regular internal channels, e.g. by contacting your manager, HR department, trust person and/or prevention advisor directly. If you are in doubt as to whether the disclosure you intend to make falls within the scope of this policy, please contact **compliance@unifiedpost.com**.

How to make a disclosure

The whistleblower does not need to have hard evidence before reporting a disclosure: having reasonable suspicion of misconduct or unethical behaviour is enough. Although you do not have to prove your allegations, they are more likely to be considered reasonable if you can back them up with some objective supporting information, such as emails, file notes or receipts.

Anyone filing a disclosure under this policy, must act in good faith and must have reasonable grounds for believing the information disclosed consists in a (potential) violation of the Group's policies and/or applicable legislation related to the topics listed above.

The whistleblower can choose at his/her sole discretion if he/she wants to be anonymous or not. It should be noted however, that it is of high importance to retrieve as much information as possible. Staying anonymous could have an impact on the quality and level of investigation of the case or can make further investigation impossible.

Reporting through whistleblowing tool

To ensure confidentiality, the Group strongly encourages to report disclosures using the IntegrityLog whistleblowing tool. This centralised whistleblowing tool allows the Group to gain insight on the number and type of disclosures and allows as such an objective reporting.

The whistleblowing tool is managed by an external and independent organisation which we carefully selected and ensures that disclosures are at all times treated in a confidential manner.

The whistleblowing tool can be accessed via a web portal through the following link:
unifiedpost.integrity.complylog.com.

Once you have logged into the tool, you will be asked whether you want to identify yourself or whether you want to submit the report anonymously. In the next phase you will be asked to select the type of wrongdoing. Finally you will be asked to give more details about the case, including the country of the incident. If you opt to do so, you can upload a file to support your report.

All feedback on these questions (and possible supporting documentation – where you select to do so) is of importance for the investigation.

Reporting through internal channels

If you would like to address the issue in person, having a discussion with your manager, HR manager or alternatively with our Group compliance office, remains possible at all times. This option is not available for our providers and customers. Please note that, if the intended disclosure is substantial and is deemed to fall within the scope of the policy, the person with whom you have spoken will request you to report the disclosure in the whistleblowing tool as well (for reasons of reporting and centralisation of disclosures, outlined above).

External individuals can consult with members of our Group compliance office, in case they suspect or have knowledge of misconduct or unethical behaviour. Their information will be processed in accordance with the confidentiality provisions included in this policy.

The Group compliance office can be contacted on the following email address: compliance@unifiedpost.com.

Reporting through external channels

The use of internal reporting channels before reporting through external reporting channels is encouraged. If you would have reasons to report externally, information regarding the procedures for reporting externally to competent authorities and, where relevant, to institutions, bodies, offices or agencies of the European Union, can be found through the relevant website(s).

How are disclosures handled and investigated?

All disclosures reported in the whistleblowing tool will be addressed by the Company in line with the following procedure:

When a disclosure is reported in the whistleblowing tool, the whistleblower will receive an immediate and automatic notification of the disclosure being recorded in the tool. This notification will be done via email. In order to maintain confidentiality, this notification will not contain any details of the report.

A first screening of the disclosures made in the whistleblowing tool will be done by the Group's Internal Auditor and the Head of Legal. They will check whether the reported disclosure falls within the scope of the policy and if so, they will forward it to and request the Investigation Team to convene and investigate the reported disclosure.

The Investigation Team is composed of the Group's Internal Auditor and of the Head of Legal and in addition, depending on the nature of the reported disclosure and department or business unit involved, the HR Group manager, business unit manager, CFO or CEO shall be part of the Investigation Team.

If a member of the Investigation Team has a conflict of interest, he/she will be excluded from further proceedings. If the reported case concerns the CEO, the case will be investigated by the Head of Legal.

Within a period of maximum seven (7) working days, the whistleblower will receive initial notification from the Investigation Team. In case the disclosure is deemed out of the scope of the policy, the whistleblower will be informed accordingly (within such a time frame) and will be encouraged to address the issue with his manager, HR manager, trust person or prevention advisor.

The Investigation Team will investigate the case in close dialogue with the whistleblower. If the whistleblower revealed its identity, communication with the Investigation Team can take place via phone, email, ... If the whistleblower issued the report anonymously, communication with the Investigation Team will take place through the secure post box in the whistleblowing tool.

The whistleblower will in any case be informed about the proceedings of the investigation within three (3) months as of the date on which the Investigation Team has been appointed to the case.

It should be noted that, in some instances, it may be necessary to include external consultants/auditors/lawyers in the investigation process. If a criminal offence has occurred, police authorities may be involved as well.

At some point in the investigation process, the reported person will be informed about the accusations. This notification will only be made when there is no risk that the reported person(s) can obstruct the investigation and/or the collection of evidence.

Protection of the whistleblower

Non-disclosure

The whistleblowing procedure will ensure as much as possible that the identity of the whistleblower will not be disclosed and that due to the investigation no link can be made to him or her. Throughout the process of the investigation and afterwards, all members of the Investigation Team are bound by confidentiality. However this effort of confidentiality may never prevent the Group from disclosing certain information retrieved throughout the investigations when obliged thereto by the law, especially when it is enforced by authorities mandated thereto. On a regular basis, all cases reported in the whistleblowing tool will be reported to the CEO and CFO.

Non-retaliation

Unless a whistleblower knowingly made a false allegation, provided false or misleading information in the course of the investigation, or otherwise acted in bad faith, the whistleblower may not be discharged, suspended, threatened, harassed, intimidated or retaliated against for making a disclosure in good faith or assisting in the handling or investigation of a disclosure under the whistleblowing policy. This non-retaliation principle also applies if the disclosure was eventually proven to be unfounded by the investigation.

Complaints of retaliation against a whistleblower are taken very seriously. All such complaints will be reviewed promptly and, where appropriate, investigated.

Local legislation

In addition to this policy, local legislation may give you further protection.

Data Protection

The whistleblowing tool is operated and maintained by InsiderLog AB ("InsiderLog"), a company located at Biblioteksgatan 29, 114 35, Stockholm, Sweden, affiliated company of Euronext Corporate Services and of the Euronext NV Group, Euronext N.V. being a Dutch company located at Beursplein 5, 1012 JW, Amsterdam, the Netherlands. InsiderLog cannot read the reports as they are encrypted with a key to which InsiderLog does not have access.

InsiderLog has taken the necessary technical and organisational measures to prevent personal data entered into the tool from being accidentally or unlawfully destroyed, lost or damaged and to prevent any unauthorised disclosure or misuse of the personal data.

Personal data, which are manifestly not relevant for the handling of a specific report shall not be collected or, if accidentally collected, shall be deleted without undue delay. For more information on how we would process personal data please visit <https://www.unifiedpost.com/en/privacy-cookie-policy>.