Whistleblowing Policy & Process

Banqup Group

Date: 26.01.2026

Table of Contents

Introduction

Banqup 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.

Section 1. Legal framework

This policy is built upon the principles outlined in Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law.

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.

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.

Section 2. Who is protected by this policy

Whistleblowers who have obtained information about violations in a professional context, including, at least, the following persons:

- Persons with worker status ;
- Persons with self-employed status (e.g. freelancers, consultants);
- Shareholders and members of the company's administrative, management or supervisory body, including non-executive members;
- Volunteers and paid or unpaid trainees;
- Any person working under the supervision and direction of contractors, subcontractors and suppliers;
- Reporters whose employment relationship has ended since the report was made;
- Whistleblowers whose employment relationship has not yet commenced (in cases where information about violations has been obtained during the recruitment process or other pre-contractual negotiations);
- Facilitators;
- Third parties who are linked to the whistleblowers and who are at risk of retaliation in a professional context (colleagues or relatives);
- Legal entities belonging to the whistleblowers or for which they work, or with which they are connected in a professional context.

Section 3. Protection of the whistleblower

1. 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.

As well as being protected by confidentiality, whistleblowers have the option of making an anonymous report and not disclosing their identity throughout the procedure. 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. If the whistleblower acts anonymously, the protection will continue to apply in the event that his identity is subsequently revealed

2. 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 suffer from retaliation 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.

The prohibition of retaliation also includes threats of retaliation and attempts to take reprisals including in particular in the form of:

- Suspension, lay-off, dismissal or equivalent measures;
- Demotion or withholding of promotion;
- Transfer of duties, change of location of place of work, reduction in wages, change in working hours;
- Withholding of training;
- A negative performance assessment or employment reference;
- Imposition or administering of any disciplinary measure, reprimand or other penalty, including a financial penalty;
- Coercion, intimidation, harassment or ostracism;
- Discrimination, disadvantageous or unfair treatment;
- Failure to convert a temporary employment contract into a permanent one, where the worker had legitimate expectations that he or she would be offered permanent employment;
- Failure to renew, or early termination of, a temporary employment contract;
- Harm, including to the person's reputation, particularly in social media, or financial loss, including loss of business and loss of income;
- Blacklisting on the basis of a sector or industry-wide informal or formal agreement, which may entail that the person will not, in the future, find employment in the sector or industry;
- Early termination or cancellation of a contract for goods or services;
- Cancellation of a licence or permit;
- Psychiatric or medical referrals.

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

Section 4. 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
- …

The whistleblower does not need to have hard evidence before reporting a disclosure: having reasonable suspicion of misconduct or unethical behavior is enough ("Suspected Breach"). 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. You can always contact compliance@banqup.com if you are unsure.

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.

Where the report contains unfounded or opportunistic allegations, or where the whistleblower makes a report with the sole intention of defaming or causing harm to others, Banqup may take appropriate disciplinary and/or legal action against the Whistleblower.

Section 5. 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@banqup.com.

Section 6. How to make a disclosure

Banquo recognises the importance of both internal and external reporting channels. While individuals are encouraged to use internal channels in the first instance, the company recognises that external reporting may be necessary in certain circumstances. The internal reporting process is seen as the preferred route for dealing quickly with issues within the organisation, facilitating the adoption of solutions internally and promoting transparency and trust between stakeholders.

1. Reporting through whistleblowing tool

To ensure confidentiality, the Group strongly encourages to report disclosures using the IntegrityLog whistleblowing tool. This centralized 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 organization which we carefully selected and ensures that disclosures are at all times treated in a confidential manner.

For a more detailed process, please consult Annex 1.

2. 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@banqup.com.

3. 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 local competent authorities.

4. Reporting through public disclosure

Public disclosure is the act of making information available in the public sphere (via journalists, platforms, social networks, etc.).

- It is the last resort (after an internal and/or external alert)
- in the event of imminent danger to the public interest
- with a risk of reprisals
- with little chances of success by other means.

The whistleblower has the choice of taking the course of action he or she deems most appropriate, but public disclosure is the most damaging to the company's reputation. This is why it must ensure that these conditions are met.

Section 7. 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 our privacy notice.

Annex 1. Reporting process

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

STEP 1. Identification

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.

STEP 2. Thick the right alert category

In the next phase you will be asked to select the type of wrongdoing. There is an explanation of each alert category when you click on the information buttons.

STEP 3. Details of the wrongdoing

Finally you will be asked to give more details about the case, including the country and the date of the incident. If you opt to do so, you can upload a file or make a voice recording 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.

STEP 4. Automatic notification from the tool

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.

STEP 5. First screening

A first screening of the disclosure made in the whistleblowing tool will be done by the Group's Internal Auditor and the Principal Compliance Officer. 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 Principal Compliance Officer 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 Principal Compliance Officer.

STEP 6. Acknowledgement of receipt

Within a period of maximum seven (7) working days[1], 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.

STEP 7. Investigation

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.

STEP 8. Information during the investigation

[1] With the exception of Lithuania, where the period for acknowledgment is 2 working days.

The whistleblower will in any case be informed about the proceedings of the investigation within three (3) months[2] as of the date on which the Investigation Team has been appointed to the case. The organisation is not obliged to deal with the alert within this time limit but only to inform you of the actions planned or already taken to assess the reality of your alert (for example: initiation of an internal investigation) and to remedy the situation reported

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.

[2] With the exception of Lithuania, within 10 working days from the confirmation of the receipt, we will inform the person about the progress of the information submitted or eventually the refusal to investigate this information.