Document title

WHISTLEBLOWER POLICY

Document type

POLICY

Version number

Version Number: 5.0

Date

21-02-2024

Number of pages

14 pages

DOCUMENT SUMMARY

Document type		Policy
Purpose of the document		Enable employees and third parties to report Alleged breaches, ensure that proper reporting channels and procedures for internal reporting and follow up are established and ensure that employees and third parties who report Alleged breaches in good faith are free to do so without fear of retaliation.
Target Audience		Employees and identified third parties
Classification		Public
RACI	**Responsible / Document owner**	Compliance department
	Accountable	Managing Board of Euronext N.V.
	Consulted	Supervisory Board of Euronext NV, Audit Committee of Euronext NV, General Counsel
	Informed	All staff, public document available on Euronext website
Reference to related documentation		Euronext Whistleblowing Procedure Euronext Code of Business Conduct and Ethics Euronext Anti-money laundering and Sanctions Policy Euronext Data Privacy Policy
Regulations linked to this document		EU Directive 2019/1937 (EU Whistleblowing Directive) and relevant local implementation thereof within countries where Euronext has relevant presence (an overview is included in an Appendix to the Whistleblowing Procedure). The 5th Anti-Money Laundering (AML) Directive (EU) 2018/843 "AML directive" General Data Protection Regulation (EU) 2016/679 "GDPR"

VERSION CONTROL

REVISION NO./ VERSION NO.	DATE	AUTHOR	APPROVAL	CHANGE DESCRIPTION
3.0	27-12-2021	Compliance department	Euronext N.V. Managing Board	Annual policy update 2021
4.0	17-08-2023	Compliance department	Euronext N.V. Managing Board	Update 2023
5.0	21-02-2024	Compliance Department	Euronext N.V. Managing Board and local Boards where necessary	Updates due to local implementation of EU Whistleblowing Directive

CONTENTS

1. OBJECTIVES, OWNERSHIP AND GOVERNANCE 5
1.1 Background 5
1.2 Objectives 5
1.3 Scope and ownership 5
1.4 Governance 6
2. DETAILED DESCRIPTION 7
2.1 Reportable breaches under this policy 7
2.2 The reporting person: non-retaliation 7
2.3 The reported person 8
2.4 Measures for protection of confidentiality 8
2.5 Reporting channels 9
2.5.1 Internal reporting channels 9
2.6 General obligations of persons having received a reported Alleged Breach 10
2.7 External reporting 10
3. TREATMENT OF REPORTED ALLEGED BREACHES 11
3.1 Breaches related to accounting and auditing matters 11
3.2 Breaches reported to the manager of an employee 11
3.3 Reported breaches received by the Compliance department 11
3.4 Reported breaches received by the Chairman of the Supervisory Board 12
4. REPORTING AND RETENTION OF ALLEGED BREACHES AND INVESTIGATION FILES 13
5. ANONYMOUS REPORTS 14

1. OBJECTIVES, OWNERSHIP AND GOVERNANCE

1.1 BACKGROUND

Euronext NV. and its subsidiaries (collectively, the "Company") are committed to comply with all applicable laws, regulations and Company Policies and believe that the ability of Employees and relevant Third Parties (as defined in this document, and together "Reporter") to report a breach or suspected breach of any law, regulations, or Company Policies is a vital component to achieve this goal.
As a result, the Company has established this Policy to enable Reporters to report an Alleged Breach (as defined in this document) in good-faith.
The Company does not tolerate any form of threat, retaliation or other action against Employees or Third Parties who have reported Alleged Breaches in good faith.

Employees and Third Parties who have acquired information on Alleged Breaches in a work related context may report these using the reporting channels made available to them as described in section 2.5 of this Policy.

Reports on Alleged Breaches will be treated in accordance with this Policy.

Questions regarding the Policy should be addressed to the Compliance Department.
You may also contact the Compliance department in confidence, should you have any question or should you need any advice or information on making a whistleblower report – via email to compliance@euronext.com or directly to your local Compliance contact.

1.2 OBJECTIVES

Objectives

With this Policy, Euronext intends to comply with any applicable local legislation regarding the protection of whistleblowers and define high standards of protection and safeguards for any Alleged Breaches reported in good faith.
This Policy enables Employees and Third Parties to report Alleged Breaches, ensures that proper reporting channels and procedures for internal reporting and follow up are established and that Employees and Third Parties who report Alleged Breaches in good faith are free to do so without fear of retaliation.
The Policy defines the rights and obligations of Employees and Third Parties when reporting an Alleged Breach.
This Policy is supplemented by a Euronext Whistleblowing Procedure that further details the treatment of reports.

1.3 SCOPE AND OWNERSHIP

Scope

This Policy applies to any person working at the Company, including full time and part time employees, temporary staff, consultants and self-employed staff, trainees, interns, volunteers agents, members of the Managing Board and Supervisory Board of Euronext, of the local boards and supervisory bodies of its subsidiaries ("Employees").

Shareholders, former Employees, job applicants or persons working for the Company's contractors, subcontractors and suppliers ("Third Parties") may make a report in good faith relating to Alleged Breaches they have identified in a work related context with the Company or in case of job applicants during the recruitment / pre-contractual negotiation process.

This Policy applies to a report made in good faith by any Reporter concerning an Alleged Breach.

Ownership

Ownership of this policy is the Euronext N.V. Managing Board. Compliance is responsible for maintaining the policy and related documentation. The policy should be reviewed at least on an annual basis, and updated based on requirements from the Euronext group.
Compliance is also responsible for securing the proper approval from the Managing Board and the local boards, in case such approval is required, in cooperation with local staff.

1.4 GOVERNANCE

Responsibility and tasks of the Supervisory Board in connection with this policy

If an Alleged Breach relates to a member of the Managing Board or a member of the Supervisory Board it may be reported directly to the Chairman of the Supervisory Board and will be investigated by the Supervisory Board (and in case of an Alleged Breach of a member of the Supervisory Board, by the Supervisory Board excluding that Member[1]). Alleged Breaches regarding accounting and auditing matters will be investigated under the direction and oversight of the Company's Audit Committee.

Responsibility and tasks of the Managing Board in connection with this policy

The Euronext N.V. Managing Board has overall responsibility for the whistleblowing framework. This includes ensuring non-retaliation and approval of policy updates. The day-to-day responsibility for implementation, management and maintenance is delegated to Compliance .

Responsibility of the Compliance Department

Save for reports investigated by the Supervisory Board and for specific designated local officers[2], the Compliance Department has been designated for the following up and investigation of reports on Alleged Breaches made under this Policy.

Reporting on this policy

Employees and Third Parties can report an Alleged Breach via the relevant channels described in this Policy.

The Compliance department[3] will prepare for the Audit Committee, and for local Boards or committees if required, an annual summary of reported Alleged Breaches, unresolved breaches and breaches resolved during the year. The summary will be accompanied by reports regarding completed investigations. For Italian subsidiaries, the summary also includes the correct functioning of the IT internal reporting channels.

[1] For Euronext subsidiaries, violations of a member of a local management or supervisory boards shall be reported to Compliance using one of the reporting channels included in 2.5.

[2] For Euronext Italian subsidiaries, under applicable local law a designated Whistleblowing responsible shall be appointed by the local Boards who will be in charge of specific activities (i.e. leading the investigation, reporting to Board and 231 Supervisory Body, if applicable, etc.).

[3] For Euronext Italian subsidiaries the designated Whistleblowing responsible, under applicable local law, will report to the local Boards.

2. DETAILED DESCRIPTION

2.1 REPORTABLE BREACHES UNDER THIS POLICY

Employees and Third Parties are expected to report Alleged Breaches they have information on.

A reportable breach under this Policy ("Alleged Breach") is an actual or potential breach, including reasonable suspicions about a breach, or an attempt to conceal an actual or potential breach related to:

- Failure to comply with applicable laws, rules and regulations, or legal obligations;
- Violations of the Company's Code of Business Conduct and Ethics and other Company policies;
- Accounting or auditing matters;
- Criminal offences or criminal activities;
- Conduct that may be corrupt, dishonest or fraudulent[4];
- Affecting the public interest by posing an unacceptable risk to the life, health or safety of people or to the environment;
- Any other conduct that may have a detrimental effect on the financial situation, integrity or reputation of the Company.

If under applicable local law, reporting a concern which is not covered by the definition of Alleged Breach falls under local law on the protection of a whistleblower, e.g. a report concerning misconduct within the workplace (like for instance harassment, discrimination or bullying) that affects the public interest, e.g. because the misconduct affects multiple persons, there is a pattern or structural character or the conduct is serious and extensive, such reporting will be likewise subject to this Policy and the rules established herein.

2.2 THE REPORTING PERSON: NON-RETALIATION

A Reporter who reports an Alleged Breach in accordance with this Policy and in good faith shall be protected and shall in no way be put at a disadvantage by the Company as a result of the report.

A report is considered made in good faith when the Reporter has reasonable grounds to believe that the information reported is true at the time the report is made.

Any form of retaliation, including attempts or threats of retaliation, against a Reporter who made a report in good faith under this Policy is prohibited. This includes, for example, 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

[4] Belgian law specifically mentions tax fraud and social fraud. Social fraud includes all breaches under the Belgian social penal code and all breaches of the stature of independent workers.

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; psychiatric or medical referrals.

The Company will protect in the same way a Reporter who has made a report directly to the competent authority or by way of public disclosure, provided that the report has been made in good faith and in accordance with applicable law.

Retaliation against a Reporter who has reported an Alleged Breach in conformity with this Policy or who participates in any investigation with respect to a reported Alleged Breach shall be considered as a serious violation of this Policy. Any act that aims at preventing in any way a Reporter from submitting a report or to contribute to an investigation following a report shall be also considered as a serious violation of this Policy.

If retaliation does occur it must be reported to the Compliance department. The violator may be subject to Company-imposed sanctions, including dismissal for cause.

The protection against retaliation described in this paragraph also applies to any facilitators, i.e. any person who assists the Reporter in a confidential manner (for example confidential advisors, trade union representatives), to persons connected with the Reporter, such as colleagues or relatives of the Reporter, legal entities that the Reporter owns, works for or are otherwise connected to the Reporter in a work related context, and to the officers in the Company who conduct the investigation or receive a report on an Alleged Breach.

2.3 THE REPORTED PERSON

In case of a reported person, i.e. a person to whom the Alleged Breach is attributed, this person will be informed by the Compliance department that a report of an Alleged Breach has been filed, unless the Compliance department determines that specific circumstances apply or this would compromise the anonymity of the Reporter. The reported person will be given an opportunity to defend him or herself

2.4 MEASURES FOR PROTECTION OF CONFIDENTIALITY

The measures for the protection of Reporters shall apply to the Employees and other reporting persons as mentioned in scope for this Policy. Reporting persons shall qualify for protection provided that:

- they had reasonable grounds to believe that the information on breaches reported was true at the time of reporting and that such information fell within the scope of whistleblower reporting,
- they reported either internally or externally or made a public disclosure;
- they reported or publicly disclosed information on breaches anonymously, but who are subsequently identified and suffer retaliation.

All reports of Alleged Breaches shall be dealt with in a confidential manner by all persons that are involved in the treatment of a report. The Company will take appropriate steps to keep the identity of Reporters confidential.

The identity of the **Reporter** cannot be disclosed other than to staff authorised to receive or follow up on the report, unless (1) the Reporter expressly consents to a wider disclosure or (2) the Company is under a legal obligation to disclose their identify in the context of judicial proceedings or to competent authorities.

The identity of the **reported** person cannot be disclosed other than to staff authorised to receive or follow up on the report, except to the authorities once the report has been considered well-founded.

In order not to jeopardize investigations, the Reporter is expected to keep the fact they have reported an Alleged Breach, the nature of the Alleged Breach and the identity of those involved, confidential.

2.5 REPORTING CHANNELS

In order to facilitate the treatment of reports, it is important that the Reporter reports Alleged Breaches at the right level. The following alternatives apply:

1. Through internal reporting channels[5]

    Level I: Report to the management of the employee

    Level II: Report to the Compliance Department

    Level III: Report to the Chairman of the Supervisory Board

    Level IV: Reporting through external advisor supporting anonymous reporting

2. Through external reporting channel

3. Through public disclosure

Reporting persons shall report information on breaches using the external reporting channels and public publications, after having first reported through internal reporting channels, or by directly reporting through external reporting channels in the circumstances permitted by local laws.

2.5.1 Internal reporting channels

Reporting to the Compliance department – Alleged Breaches may be reported to the Compliance Department via the following channels:

- Via email to the following email address: wb@euronext.com
- Via phone – by calling your (local) compliance contact or the Group Head of Compliance.
- In person – by requesting an interview with your (local) compliance contact or with the Group Head of Compliance

Should the Alleged Breach concern the Compliance Department, the Employee may report any Alleged Breach to the Group General Counsel.

Reporting to the Chairman of the Supervisory Board - Alleged Breaches relating to a member of the Managing Board of Euronext N.V. may also be reported directly to the Chairman

[5] For Euronext Italian subsidiaries the internal reporting channels must address the reports to the Whistleblowing responsible appointed by the local Boards of Directors (as specified in the footnote 2). The Whistleblowing responsible will be involved in the investigation of the report and in the related activities as detailed in the following sections of the Policy even if the report is initially addressed to other people.

of the Supervisory Board of Euronext NV. Reporters can reach out to the Corporate Secretary in case they wish to report directly to the Chairman of the Supervisory Board.

Reporting via Ethics Point - Alleged Breaches may be reported via the following third-party website: www.ethicspoint.com which also offers the possibility to make a report anonymously. Reports via Ethics Point may be done:

- In writing – by filling in the web based form in Ethics Point
- By phone – via the toll free numbers that you can find on the Ethics Point website.

Reporting to the manager - Finally, the Employee may feel more comfortable and choose to report an Alleged Breach directly to their manager in their day to day activities. A manager receiving a report under this Policy shall forward any such report received without delay to the Compliance Department for investigation.

Third Parties who have acquired information on an Alleged Breach in a work related context may report their concern to the Compliance Department via wb@euronext.com or at www.ethicspoint.com. Reports on Alleged breaches submitted by such Third Parties will be treated in accordance with this Policy.

After the receipt of a report of an Alleged breach, a confirmation of acknowledgement of the report will be sent to the Reporter within 5 days, and feedback on the report will be provided within three months following the confirmation of acknowledgement.

2.6 GENERAL OBLIGATIONS OF PERSONS HAVING RECEIVED A REPORTED ALLEGED BREACH

Persons who have received a reported Alleged Breach are expected to handle all matters related to that Alleged Breach promptly, seriously and confidentially.

If the Reporter has reported an Alleged Breach using an inappropriate channel, the person who has received the report is expected to forward the Alleged Breach to the appropriate recipient and via the appropriate channel identified in the previous section.

2.7 EXTERNAL REPORTING

Reporters are encouraged to first report any Alleged Breach noticed in the context of Euronext activities internally, unless the person believes that the report may not be effectively dealt with internally or there is a risk of retaliation.

Nonetheless, nothing in this Policy is aimed to prevent direct reporting to the competent authorities designated under applicable law or reporting publicly (i.e. external reporting) and a Reporter who in good faith chooses to make such external reporting in the circumstances permitted by local laws will be protected in accordance with this Policy (see sections 2.2) and shall not suffer any form of retaliation.

3. TREATMENT OF REPORTED ALLEGED BREACHES

Below is described how reported breaches must be treated by persons who receive the report. The Whistleblowing Procedure provides further details[6].

3.1 BREACHES RELATED TO ACCOUNTING AND AUDITING MATTERS

Examples of Alleged Breaches that can be considered as related to accounting and auditing matters are:

- fraud or error in the preparation, evaluation, review or audit of any financial statement of the Company;
- fraud or error in the recording and maintaining of financial records of the Company;
- deficiencies in or non-compliance with the Company's internal accounting controls;
- misrepresentation or false statement to or by a senior officer or accountant regarding a matter contained in the financial records, financial reports or audit reports of the Company;
- deviation from full and fair reporting of the Company's financial condition;
- bribery of public agents, officials or any other person;
- theft or fraud against Euronext.

Upon receipt of an Alleged Breach regarding accounting and auditing matters, the Compliance Department will investigate the breach under the direction and oversight of the Company's Audit Committee.[7] Without prejudice to the provisions of section 2.4, confidentiality will be maintained to the extent possible, consistent with the need to conduct an adequate investigation or to take legal action. Prompt and appropriate corrective action will be taken through the Company's Audit Committee as warranted by any investigation.

3.2 BREACHES REPORTED TO THE MANAGER OF AN EMPLOYEE

Regardless of the nature of a reported Alleged Breach, the manager of the Employee who has been notified of an Alleged Breach by that Employee must promptly inform the Compliance Department of the content of the report on the Alleged Breach.

3.3 REPORTED BREACHES RECEIVED BY THE COMPLIANCE DEPARTMENT

Upon receipt, a reported Alleged Breach will be examined promptly by the Compliance Department to determine whether it actually meets the provisions of this Policy and should be

[6] For Euronext Italian subsidiaries the Whistleblowing responsible shall be involved in the investigation of the report and in the related activities, even if the report is initially addressed to other people, unless it relates to a Legislative Decree n. 231/01 crime that should be addressed by him/her to the competent 231/01 Supervisory Body.

[7] For Italian entities in the Euronext Group which have appointed a Supervisory Body ('Organismo di Vigilanza' / ODV) applies that if an Alleged Breach refers to a crime covered by Italian Legislative Degree n. 231/01, the Alleged Breach must be presented to the Supervisory Body of the Italian entity concerned and the breach will be investigated under the direction and oversight of that Supervisory Body.

investigated. The Compliance Department will assess the risk linked with the report. High risk reports will trigger an information of the Head of Risk and Compliance who may decide to inform the Managing Board. The risk assessment will be described in an internal procedure. Without prejudice to the provisions of section 2.4, the Compliance department may involve officers and staff of the Company as well as external advisors or institutions. If the Alleged Breach relates to a member of the Managing Board, the Compliance department will inform the Chairman of the Supervisory Board.

3.4 REPORTED BREACHES RECEIVED BY THE CHAIRMAN OF THE SUPERVISORY BOARD

If the Chairman of the Supervisory Board receives a report, he/she shall review and discuss the report with the other members of the Supervisory Board (in case of an Alleged Breach by a member of the Supervisory Board excluding that Member) and/or the Compliance department and the Company's Audit Committee (if the Alleged Breach relates to accounting and auditing Matters) and will determine whether it meets the provisions of this Policy and it should be investigated. The Supervisory Board will follow up on the report in accordance with this Policy and with the Whistleblowing Procedure and may involve other officers and staff of the Company as well as external advisors or institutions where necessary, without prejudice to the provisions of section 2.4.

If the Alleged Breach does not relate to a Managing Board member, the Chairman of the Supervisory Board will submit the report to the Compliance department who will inform the reporting person about the follow up.

4. REPORTING AND RETENTION OF ALLEGED BREACHES AND INVESTIGATION FILES

The Compliance department will maintain a register of all reported Alleged Breaches, tracking their receipt, investigation and resolution[8].

Personal data that is not relevant to the processing of a specific report shall not be collected, or, if collected unintentionally, shall be deleted immediately.

If the reported Alleged Breach is considered out of scope of this Whistleblower Policy by the recipient, the personal data in the report must be deleted immediately and the report may be archived following anonymization.

If the reported Alleged Breach is determined to be unfounded, the personal data contained in that reported Alleged Breach will be destroyed within two months after the investigation has been finished.

If the reported Alleged Breach is founded but not directly substantiated, but could be in case of a pattern of similar reports, the personal data contained in that report may be kept but will be destroyed within six months after the investigation has been finished and no pattern has been determined.

If the reported Alleged Breach is substantiated, the personal data will be destroyed once associated disciplinary or judicial proceedings have finished (unless the personal data is archived to mitigate against potential liabilities).

In certain jurisdictions, different retention periods apply in accordance with local laws. In such jurisdictions, the local retention period will apply[9].

Each Reported person (person to whom the Alleged Breach is attributed), as well as each Reporter, has the right:

- to access his or her personal data;
- to request, to rectify the data if the information is inaccurate or incomplete; and
- to object to their data being processed subject to having legitimate grounds to do so.

The Compliance department will prepare an annual summary of reported Alleged Breaches, unresolved breaches and breaches resolved during the year, which will be forwarded to the Company's Audit Committee and, to local Boards or committees if required. The summary will be accompanied by reports regarding completed investigations. Both the annual summary and the reports shall be in anonymous form and shall not carry any details that might lead to the identification of the Reporter or reported person.

---

[8] Note that the Compliance department will not determine nor decide on any disciplinary actions towards Reported persons in case such actions are part of the resolution of a reported Alleged Breach.

[9] For group entities located in Italy, local law limits the max period of retention of a received report to 5 years or 10 years following the communication of the finalised investigation, depending on specific local legislation.

For group entities located in Portugal, a received report (whether it is deemed founded or unfounded must be kept for a period of 5 year or longer, in case of ongoing proceedings, for the duration of such proceedings.

For group entities located in Denmark and Norway Personal data shall be deleted after five (5) years following finalised investigation. For CSD related purposes the report will be saved for ten (10) years.

5. ANONYMOUS REPORTS

The Company encourages Reporters to report Alleged Breaches promptly and where possible directly the Compliance Department, the Chairman of the Supervisory Board if the Alleged Breach relates to the members of the Managing Board, or to their management. However, if the reporting person believes that it is not feasible to report the Alleged Breach while mentioning their name, he/she may report the Alleged Breach using the third-party confidential reporting system called EthicsPoint, which includes a website www.ethicspoint.com through which Reporters can make reports, including in an anonymous manner.

Reporters can also call EthicsPoint toll free. Designated toll-free numbers depending on geographic locations are listed on the EthicsPoint website. EthicsPoint administers the technical aspects of the reporting system and ensures that it does so while preserving complete confidentiality.

EthicsPoint will forward the report as an anonymous report to the Compliance department which will deal with it like with any other report.

However the anonymous Reporter should realise that an anonymous reported Alleged Breach could hinder or complicate investigations and further communication between who reports the Alleged Breach and the Compliance department and even prevent appropriate actions from being taken.