WHISTLEBLOWER POLICY

EXECUTIVE SUMMARY

Euronext NV. is committed to comply with all applicable laws and regulations and believes that the ability of Employees to report a suspected breach is a vital component to achieve this goal. As a result, Euronext NV. has established procedures to enable Employees to report alleged breaches of a general, operational and financial nature. Euronext NV. ensures that Employees who report alleged breaches in good faith are free to do so without fear of retaliation.

Employees can report alleged breaches:

- **directly to their management**
- **to the Compliance department**
- **to the Chairman of the Supervisory Board under specific circumstances.**

Alternatively, Employees can also report an alleged breach via the following third-party website: www.ethicspoint.com which provides the ability to report anonymously alleged breaches.

Breaches that pertain to accounting and auditing matters will be investigated by Internal Audit under the direction and oversight of the Euronext NV. Audit Committee.

This Policy is global and applies to all Euronext NV. Employees.

For more information about this policy, please contact your local compliance officer or send an email to: compliance@euronext.com

1. INTRODUCTION

Euronext NV. and its subsidiaries (collectively, the "Company") are committed to comply with all applicable securities laws, regulations and Company Policies and believes that the ability of Employees to report a breach or suspected breach of any law, regulations, or Company Policies (an " alleged breach") is a vital component to achieve this goal. As a result, the Company has established the following procedures to enable Employees to report an alleged breach in good-faith. The Company does not tolerate any form of threat, retaliation or other action against Employees who have reported alleged breaches in good faith.

This Policy applies to all Employees of the Company including consultants (among which interns and temporary staff) and agents (collectively "You" or, "**Employees"**), and does not supersede other existing information reporting channels in effect within the Company or otherwise restrict the ability of Employees to make reports direct to the competent regulatory authorities in their jurisdiction where applicable[1].

The Whistleblower Policy contains the rights and obligations Employees have to respect when they want to report an alleged breach. 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 regarding a potential report or on the status of whistleblower – via email to compliance@euronext.com or directly to your local Compliance contact.

This Policy is supplemented by a Euronext Whistleblowing Procedure that further details the treatment of reports. The Policy and the Procedure may be amended periodically.

2. BREACHES THAT MUST BE REPORTED UNDER THIS POLICY

Employees with good faith concerns are expected to report all alleged breaches of applicable laws, regulations and Company Policies regarding accounting or audit irregularities or which may affect the public interest by posing an unacceptable risk to the life, health or safety of people or the environment. If allowed by local legislation, Employees with good faith concerns may also report other alleged breaches under this whistleblowing policy.

3. THE REPORTING PERSON: NON-RETALIATION

Employees who report an alleged breach in accordance with this Policy will be protected and shall in no way be put at a disadvantage by the Company as a result of the report: Employees cannot be subject to termination, direct or indirect disciplinary or discriminatory sanctions following a report conducted in good faith and in accordance with the Policy. Retaliation against an employee that has reported an alleged breach

[1] Within Euronext Dublin, a person appointed to perform a pre-approval controlled function ("**PCF**") is required under Section 38 Central Bank (Supervision & Enforcement) Act 2013 to disclose to the Central Bank of Ireland information pertaining to a breach of, or offence under, financial services legislation.

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 an employee to submit a report or to contribute to an investigation following a report shall be also considered as a serious violation of this Policy as well as national laws .

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.

In order not to jeopardize investigations, the reporting person is expected to keep the fact he/she has reported an alleged breach, the nature of the alleged breach and the identity of those involved, confidential.

After the receipt of a report of an alleged breach, a confirmation of acknowledgement of the report will be sent to the reporting person within 5 days.

4. THE REPORTED PERSON

In case of a reported person, he or she will – unless the Compliance department determines that specific circumstances apply – be notified of the fact that a report of an alleged breach has been filed. The reported person will be given an opportunity to defend him or herself

5. CONFIDENTIALITY

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 employee who reports an alleged breach under this Policy confidential.

The identity of the **reporting** person cannot be disclosed, except to the authorities[2] with the person's consent.

The identity of the **reported** person cannot be disclosed, except to the authorities once the report has been considered well-founded. If such circumstances arise, the Company will do its best to inform the reported person that their identity is likely to be disclosed.

6. REPORTING PROCEDURE

In order to facilitate the treatment it is important that Employees report alleged breaches at the right level. The following alternatives apply:

Level I: Report to the management of the employee

Level II: Report to the Compliance Department: email wb@euronext.com or call your local Compliance contact.

Level III: Report to the Chairman of the Supervisory Board if the alleged breach relates to the members of the Managing Board.

[2] Competent state agencies as foreseen in local laws

The Chairman of the Supervisory Board can be reached via the Company Secretary.

7. 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 employee has reported the alleged breach at the wrong level, the person who has received it is expected to refer the alleged breach to the appropriate level.

8. 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.

8.1 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, or
- 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 Company will investigate the breach under the direction and oversight of the Company's Audit Committee. 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.

8.2 REPORTED BREACHES RECEIVED BY THE MANAGEMENT OF THE EMPLOYEE

Whatever could be the nature of the reported alleged breach, the manager of the employee who was notified of an alleged breach by that employee must inform the Compliance department of the content of the alleged breach and the follow-up actions taken to solve the issue and do so immediately if the alleged breach relates to:

- Conduct that may be corrupt, dishonest or fraudulent;
- (Suspected) criminal activity or violation of any applicable law or regulation and any Compliance policies;
- Abuse of authority, including instructions not to report breaches to higher management or to Compliance;
- Any other conduct that may have a detrimental effect on the financial situation or reputation of the Company;
- Accounting and auditing matters.

8.3 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 investigated. The Compliance officer receiving the report 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. 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.

8.4 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 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 may involve other officers and staff of the Company as well as external advisors or institutions where necessary.

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.

9. REPORTING AND RETENTION OF BREACHES AND INVESTIGATIONS

The Compliance department will maintain a log of all reported alleged breaches, tracking their receipt, investigation and resolution. 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 substantiated, the personal data will be destroyed once associated disciplinary or judicial proceedings have finished (unless the data is archived to mitigate against potential liabilities).

Each employee who is the subject to a reported alleged breach, as well as each employee who files the alleged breach, 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. The summary will be accompanied by reports regarding completed investigations.

10. ANONYMOUS REPORTS

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