

Document title

# **ANTI-MONEY LAUNDERING AND SANCTIONS POLICY**

Document type

POLICY

Version number

Version Number: 6.0

Date

17-08-2023

Number of pages

21 pages

All proprietary rights and interest in or connected with this publication shall vest in Euronext. No part of it may be redistributed or reproduced in any form without the prior written permission of Euronext.

Euronext refers to Euronext N.V. and its affiliates. Information regarding trademarks and intellectual property rights of Euronext is located at [www.euronext.com/terms-use](http://www.euronext.com/terms-use).

© 2022, Euronext N.V. - All rights reserved.

## DOCUMENT SUMMARY

<b>Document type</b>	Policy	
<b>Purpose of the document</b>	Prevent and detect money laundering, terrorist financing and violations of sanctions programs.	
<b>Target Audience</b>	All staff	
<b>Classification</b>	Public	
<b>RACI</b>	<b>Responsible / Document owner</b>	Euronext N.V. Managing Board
	<b>Accountable</b>	Group Compliance
	<b>Consulted</b>	Local Compliance officers, Legal
	<b>Informed</b>	All staff
<b>Reference to related documentation</b>	Euronext Code of business conduct and ethics The Euronext Anti-Money Laundering and Sanctions Guidance The Whistleblower Policy; The Anti- Bribery Policy;	
<b>Regulations linked to this document</b>	Directive EU 2015-849 (4th EU AML Directive) and Directive EU 2018-843 (5th EU AML Directive)	

## VERSION CONTROL

REVISION NO./ VERSION NO.	DATE	AUTHOR	APPROVAL	CHANGE DESCRIPTION
5.0	27-12-2021	Compliance department	Euronext N.V. Managing Board	Annual policy update 2021
6.0	17-08-2023	Compliance department	Euronext N.V. Managing Board	Update 2023

## CONTENTS

<b>1. OBJECTIVES, OWNERSHIP AND GOVERNANCE.....</b>	<b>4</b>
1.1 Objectives .....	4
1.2 Scope and ownership .....	5
1.3 Governance .....	5
<b>2. DETAILED REQUIREMENTS .....</b>	<b>7</b>
2.1 Global legal framework for AML and Sanctions .....	7
2.2 Definition of money laundering .....	7
2.3 General principles.....	8
2.3.1 Criminal offences related to money laundering and terrorist financing.....	8
2.3.2 Sanctions program .....	8
<b>3. AML AND SANCTIONS COMPLIANCE PROGRAM.....</b>	<b>10</b>
3.1 Elements of an AML and Sanctions Compliance Program - Summary .....	10
3.2 Roles and responsibilities.....	10
3.3 Detailed elements of our AML and Sanctions Compliance Program .....	12
3.3.1 Risk based and appropriate approach.....	12
3.3.2 Employee awareness and training .....	13
3.3.3 Customer due diligence.....	14
3.3.4 Screening for sanctions and PEPs .....	15
3.3.5 Appointment of a Money Laundering Reporting Officer.....	16
3.3.6 Retention of records.....	16
3.3.7 Monitoring transactions.....	17
3.3.8 Reporting obligations.....	18
3.3.9 Independent audit.....	18
3.4 Request for information from relevant authorities such as regulators .....	18

---

# 1. OBJECTIVES, OWNERSHIP AND GOVERNANCE

---

## 1.1 OBJECTIVES

### **Background**

The Euronext Anti-Money Laundering (AML) and Sanctions Policy is designed to ensure compliance with EU AML Directives and Regulations applicable to an operator of regulated markets, trading venues, investment firms, central securities depositories (CSDs) and for Central Counterparties (CCPs). It includes the need to have in place appropriate systems and controls to identify and mitigate the risk of Euronext being used to facilitate money laundering, other financial crime and terrorist financing and to avoid sanction violations. Anti-money laundering laws are primarily aimed at banks and financial institutions that carry out specified banking activities. Euronext is not a bank; however it still has an important role to play as a market operator, as a CSD and CCP.

### **Objectives**

The purpose of the Euronext Anti-Money Laundering (AML) and Sanctions Policy (the "Policy") is to clearly set out the high level AML requirements that apply to Euronext. Additional detail can be found in the separate Anti-Money Laundering and Sanctions Guidance, as well as relevant guidances and procedures applicable to specific companies of the Group.

### **The AML and Sanctions Policy – Minimum standards**

- Establishing and maintaining a Risk Based Approach towards assessing and managing the money laundering and terrorist financing risks to Euronext;
- Establishing and maintaining Risk-based customer due diligence, identification, verification and know your customer (KYC) procedures, including enhanced due diligence for those customers presenting higher risk, such as Politically Exposed Persons (PEPs);
- The appointment of a Money Laundering Reporting Officer (MLRO);
- Procedures for reporting suspicious activity internally and to the relevant law enforcement authorities as appropriate;
- The maintenance of appropriate records for the minimum prescribed periods; and
- Screening, training and awareness for relevant employees.

### **The role of a Euronext employee in preventing money laundering and sanctions violations**

To protect yourself and Euronext, and to avoid being implicated in money laundering or violation of sanctions programs, you must:

- Understand the risk of Euronext being used to facilitate money laundering;
- Follow the Initial and Ongoing Customer Due Diligence requirements as required including the screening of customers;
- Not assist any person to obtain, conceal, retain or invest any assets if it is (or should be) known or suspected that they are the proceeds of any criminal conduct;
- Report any suspicion or knowledge of money laundering to the Money Laundering Reporting Officer ('MLRO');
- Not "tip-off" any person that a potential case of money laundering has been reported or is being investigated, (whether they are the subject of a suspicion, or anybody else), and

- Forward all inquiries from relevant authorities such as regulators to Compliance, who will coordinate the response.

---

## 1.2 SCOPE AND OWNERSHIP

### **Scope**

This Policy applies to Euronext N.V. and its majority owned subsidiaries (collectively referred to as the “**Company**” or, “Euronext”) and to all Euronext employees including consultants (among which interns and temporary staff) and agents (collectively “You” or, “**Employees**”).

Following a risk based approach, Euronext must implement measures to mitigate risks related to money laundering, terrorism financing and sanctions programs. Residual risks may remain for certain customer types, products or jurisdictions where we conduct business. The Managing Board should agree with concerned business units to what extent residual risks are acceptable.

This Policy should be read in conjunction with other Euronext policies such as:

- the Code of Business Conduct and Ethics;
- the Whistleblower Policy;
- the Anti- Bribery Policy;

### **Ownership**

Owner of this policy is the Euronext N.V. Managing Board. The Compliance department monitors the AML and sanctions Policy, provides training to Employees, works with the business areas to identify areas of particular risk in order to put in place appropriate procedures and mitigate controls and update this Policy and the Guidance when necessary. Compliance is also responsible for securing the proper approval from the Managing Board for such updates.

---

## 1.3 GOVERNANCE

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

No specific responsibilities for the Euronext N.V. Supervisory Board in connection with this policy.

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

The Euronext N.V. Managing Board has overall responsibility for the AML and Sanctions framework. This includes approving or rejecting high risk customers and setting boundaries on risk appetite, and approval of policy updates. The day-to-day responsibility for implementation, management and maintenance is delegated to Compliance.

### **Reporting on this policy**

In the event that an employee becomes aware of facts and circumstances that may indicate potential money laundering or terrorist financing, these matters must be promptly reported to the MLRO. Following the report, the MLRO and Compliance Department will consider the circumstances and decide whether an alert should be made to the relevant authorities and/or the Managing Board. Breaches of this policy should be reported to Compliance. Compliance will report breaches to Managing board.

**Stakeholders' responsibilities**

Responsibilities of stakeholders are detailed under "Objectives" above and in section 3.2 "Roles and Responsibilities" below.

---

## 2. DETAILED REQUIREMENTS

---

### 2.1 GLOBAL LEGAL FRAMEWORK FOR AML AND SANCTIONS

Anti-Money Laundering laws and regulations are directed at protecting the integrity, stability and confidence of the financial system against its use for financial crime, money laundering and terrorist financing. AML laws are concerned with the source of money to prevent the proceeds of crime from being concealed or disguised so as to appear legitimate, thereby preventing the "laundering" of "dirty money". Combatting the financing of terrorism is more concerned with the destination of funds, including legitimate funds being made available to, or for the benefit of, sanctioned countries, organizations and persons including terrorists.

Sanctions programs are employed for a variety of reasons including Diplomatic, Criminal Enforcement, Economic, Humanitarian, and National Security.

---

### 2.2 DEFINITION OF MONEY LAUNDERING

**"Money laundering"** is generally defined as engaging in acts designed to conceal or disguise the origins of proceeds derived from criminal origins to appear as though they are from a legitimate source. These illegal sources may include proceeds from drug trafficking, embezzlement, bribery, organized crime, or insider trading. Money laundering is not limited to cash transactions, but also includes non-cash transactions such as wire transfers and foreign exchange. Money laundering usually consists of three fundamental stages: placement, layering and integration.

- **Placement.** Cash first enters the financial system at the placement stage, where cash from criminal proceeds is deposited into a bank or other depository institution, or converted into negotiable instruments, such as money orders or travellers' checks. It can also occur when illegal funds are used to purchase real estate, stocks, bonds, or business assets. To disguise criminal activity, cash sometimes is also routed through a "front" operation business, for example, a cheque cashing service.
- **Layering.** This stage refers to the creation of complex or multiple layers of transactions that are intended to break the audit trail from the illegal source. The funds can be transferred or moved into other accounts, financial institutions, shell companies, or disguised as the proceeds of legitimate business. Sometimes, layering is accomplished by transferring funds to countries that have strict bank secrecy laws, for example, the Cayman Islands, the Bahamas and Panama. These secrecy laws and the high daily volume of wire transfers can make it difficult for law enforcement agencies to trace these transactions. Once deposited in a foreign bank, the funds can be moved through accounts of "shell" corporations that exist solely for laundering purposes.
- **Integration.** At this stage, the layered funds that are no longer traceable to their criminal origin are moved into the financial system. The money is therefore re-introduced into the economy and may be used to purchase legitimate assets or to fund other criminal activities or legitimate businesses. Examples include making loan repayments, creating a new business with the laundered money and mixing laundered money with income from other legitimate income or assets.

Additionally Money Laundering includes:

- handling the benefit of acquisitive crimes such as theft, fraud and tax evasion;
- handling stolen goods; and
- being directly involved with any criminal or terrorist property, or entering into arrangements to facilitate the laundering of criminal or terrorist property.

---

## 2.3 GENERAL PRINCIPLES

---

### 2.3.1 Criminal offences related to money laundering and terrorist financing

The broad groups of criminal offences related to money laundering and terrorist financing are:

- knowingly assisting (in a number of specified ways) in concealing, or entering into arrangements for the acquisition, use, and/or possession of, criminal property;
- providing or collecting funds, by any means, directly or indirectly, with the intention that they be used, or in the knowledge that they are to be used, in full or in part, to commit, or to contribute to the commission of, any acts of terrorism, including public provocation, recruitment, training and travelling in relation to acts of terrorism;
- failing to report knowledge, suspicion, or where there are reasonable grounds for knowing or suspecting, that another person is engaged in money laundering or terrorist financing; and
- tipping off, or prejudicing an investigation.

It is also a separate offence not to establish adequate and appropriate policies and procedures to forestall and prevent money laundering and terrorist financing (regardless of whether it actually takes place or not).

---

### 2.3.2 Sanctions program

Sanctions are imposed by the EU, the United Nations and governments and include a range of financial or trading restrictions, such as freezes on the assets of and travel restrictions on nominated individuals, bans on financing of state-owned enterprises, prohibitions on the supply of technical, financial and other assistance and outright prohibitions on trade. In its business activities, the Company has due regard to relevant applicable sanction programs.

#### EU Sanctions

The EU imposes sanctions within the framework of the Common Foreign and Security Policy, either on an autonomous EU-basis, typically imposed through Council Regulations that have immediate legal effect in member states, or by implementing binding resolutions of the United Nations Security Council. Sanctions imposed by the EU may target governments of third countries or non-member state entities and individuals, such as terrorist groups and individual terrorists. The EU maintains and publishes lists of targeted countries, entities, groups or individuals (EU Sanctions Lists). New kind of sanctions may prohibit any type of financing or funding of entities under sanctions, including entities that are listed on regulated markets in the EU.

Sanctions requirements imposed by the EU have to be followed by all persons and entities doing business in the EU, including nationals of non-EU countries, and also by EU nationals

and entities incorporated or constituted under the law of an EU member state when doing business outside the EU.

For more information about these sanctions, see the following European Commission website: [http://ec.europa.eu/external\\_relations/cfsp/sanctions/index\\_en.htm](http://ec.europa.eu/external_relations/cfsp/sanctions/index_en.htm)

### **US Sanctions**

In the US, the Office of Foreign Asset Control of the US Treasury Department ("OFAC") administers and enforces US-based economic and trade sanctions programs against targeted foreign countries, terrorists, international narcotics traffickers and those engaged in activities related to the proliferation of weapons of mass destruction and other threats to the national security, foreign policy or economy of the US. These sanctions programs are based on US foreign policy and national security goals, as well as on United Nations and other international mandates.

OFAC also publishes a list of individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries. Additionally, OFAC lists individuals, groups and entities, such as terrorists and narcotics traffickers, designated under programs that are not country-specific. Collectively, such individuals and companies are called Specially Designated Nationals ("SDNs") (US Sanction lists). New kind of sanctions prohibit any type of financing or funding of entities under sanctions, including entities that are listed on regulated markets in the EU. OFAC maintains and publishes lists of these targeted countries, entities, groups or individuals, referred to generally as sanctions and SDNs lists. A US person is prohibited by OFAC from engaging in a wide range of transactions with any individual, group, entity or country on these lists. For more information about these sanctions, see the following US Treasury Department website: <http://www.ustreas.gov/offices/enforcement/ofac/>

The Company screens against OFAC sanctions lists and has due regard to any linkages with this. Such linkages will be considered as a risk factor in determining the appropriate level of customer due diligence to be applied and the Company will not undertake any business activities that are not allowed under OFAC sanctions.

---

### 3. AML AND SANCTIONS COMPLIANCE PROGRAM

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

---

#### 3.1 ELEMENTS OF AN AML AND SANCTIONS COMPLIANCE PROGRAM - SUMMARY

Euronext's AML Compliance program is risk based and proportionate. It contains the following elements:

- **Employee Awareness and Training.** The AML Compliance program should ensure that Employees are aware of and understand the AML Compliance program and their personal responsibilities.
- **Know Your Customer Procedure.** Procedures must be in place to ensure that Know Your Customer ("KYC") due diligence is performed for Customers. The risk based approach includes enhanced procedure where risk increasing factors are identified on product, customer or country.
- **Screening for Sanctions.** Procedures must be in place to ensure screening against lists of sanctions and politically exposed persons (PEPs).
- **Appointing Officers.** The Company has appointed Money Laundering Reporting officers or Anti- Money Laundering Compliance Officers "MLROs".
- **Retention of Records.** Complete and accurate records of the KYC due diligence process and screening for sanctions must be retained and kept retrievable during the relationship with the Customer as required by local law. Depending on and if allowed by local legislation, records must be kept from seven to ten years from the date when the relationship with the Customer ends.
- **Monitoring Company's Transactions/ trading.** A monitoring program must be implemented for suspicious transactions/ trades where money laundering/ terrorist financing is a risk or is suspected.
- **Reporting Obligations.** Procedures must be implemented to ensure that the relevant authorities are informed in a timely fashion if money laundering/ terrorist financing is suspected.

---

#### 3.2 ROLES AND RESPONSIBILITIES

Each Employee has a role to play in achieving a successful AML and Sanctions Compliance program, which can be summarized as follows:

- Managing Board has overall responsibility for the AML and Sanctions framework.
- All Employees are responsible for reading and getting familiar with the AML and Sanctions Policy.
- Employees of certain Euronext business areas are identified and trained by the Compliance department to perform due diligence and screening procedures for third parties, or government officials or entities with which those Euronext businesses conduct business. The Anti-Money Laundering and Sanctions Guidance (the 'Guidance') outlines the risk-based procedures that these business areas should adhere to.
- The Compliance department monitors the AML Policy, provides training to Employees, works with the business areas to identify areas of particular risk in order to put in place appropriate procedures and mitigate controls and update this Policy and the Guidance when necessary.

- Internal Audit performs an independent opinion on effectiveness of the AML framework.

Staff	Responsibility
Managing Board <sup>1</sup>	Has overall responsibility for the AML and Sanctions framework. This includes approving or rejecting high risk customers and setting boundaries on risk appetite.
Group Compliance	Reviews the AML and sanctions framework and prepares updates to this Policy and the Guidance when necessary and provides training to employees. As a second line of defense, Compliance can monitor customer files on quality, risk rating and completeness, provides guidance to business operations on issues with customer files and gives advice to the Managing Board and business areas on high risk customers/factors.
Member Compliance / Surveillance / Operations	Performs transaction/trade monitoring.
MLRO and deputies	Reports to regulators or Financial Intelligence Units (FIUs) in applicable cases.
Management of designated Euronext business units (see the Guidance for further details)	Contributes to AML and sanctions awareness of their teams and designates team members that are responsible for performing CDD and screening. Implements AML and sanctions procedures within their business units.
Employees of designated Euronext business units (see the Guidance for further details)	Perform the risk based customer due diligence procedures as outlined in the Guidance. They are responsible for risk rating their customers, and maintaining a paper trail and the quality of customer files and act as contact point for customers in relation to KYC procedures. High risk factors identified require advice from Compliance (evidenced).
All staff	Must familiarize themselves with this Policy and understand the risk of Euronext being used to facilitate money laundering. Also they must report to the MLRO or Compliance if in the exercise of their functions they have any suspicion or knowledge of money laundering or violations of sanction programs.

<sup>1</sup> The Board of Directors of Euronext VPS and the Board of Directors of Oslo Børs ASA (or delegated to Oslo Børs Listing Committee) approves or rejects high risk customers and sets boundaries on risk appetite for the respective regulated entity.

---

### 3.3 DETAILED ELEMENTS OF OUR AML AND SANCTIONS COMPLIANCE PROGRAM

---

#### 3.3.1 Risk based and appropriate approach

To know your customers and performing customer due diligence (CDD) is an important part of the process to prevent and detect money laundering, terrorist financing and violations of sanctions programs. CDD procedures must be carried out on a risk sensitive basis. Euronext's risk-based approach is established through:

- Appropriate governance
- Identifying and assessing the risks Euronext faces
- Managing and mitigating those risks through:
  - This Policy
  - The guidance
  - Training and awareness
  - Establishing CDD and sanctions screening procedures
  - Including specific AML and sanctions provisions in application forms, agreements and contracts
- Monitoring and improving the effectiveness of Euronext's procedures, controls and documentation.

In assessing the risks for Euronext in relation to money laundering and sanctions programs, it is necessary to consider:

- Applicable regulation
- Customer and geographical risk factors
- Products, services and / or delivery channels

It is important to note that in its business activity of operating markets, CSDs, and CCP, Euronext does not carry on the credit institution activities that are typically considered as activities carrying a higher risk of getting involved in money laundering. For example, Euronext does not:

- operate retail or individual customer accounts, nor accept any such customer deposits or securities, except through account operators that are responsible for the KYC/AML according to applicable law
- offer any consumer or mortgage lending
- offer payment services
- trade in financial instruments for its own account or on behalf of customers.

#### Risk overview per business unit

The main products and services offered by Euronext fall into the following business units:

- Listings
- Trading / Membership
- Market Data and Indices
- Post Trade (CSD services and clearing)
- Market Solutions

- Corporate services
- Investment firm

A detailed risk assessment for all these business units is included in the Guidance. This risk assessment for Listings distinguishes different product lines where particular attention is given to listings on the Euronext Growth and Access markets and listings on the regulated market and the MTFs operated by Euronext Dublin. The guidance also outlines the risk based CDD and screening procedures that these business units must adhere to.

**A summary of the risk assessment for the business units has been taken out of this public version of the Anti-money laundering and Sanctions Policy as it contains sensitive business information.**

---

### 3.3.2 Employee awareness and training

All Employees must understand and be familiar with this AML and Sanctions Policy. Certain business areas, dependent on their function and location, will also receive targeted, in-person training from Compliance<sup>2</sup> on a risk assessed basis. In addition, assigned Employees in charge of the KYC due diligence process will receive training on the process and the use of tools necessary in performing their duties. Dates and names of those in attendance at the training will be recorded, with training materials and records kept for the mandatory retention period as required. The training will cover, at a minimum, factors that Employees who handle or supervise the handling of transactions that may involve suspicious activity should be made aware of.

These are the following:

- Their responsibilities under applicable AML laws, as well as their responsibilities under this Policy, including the responsibility for obtaining sufficient evidence of customer identity for KYC due diligence and recognizing and reporting suspicious activity.
- Red flags and signs of money laundering that arise during the course of the Employee's activities.
- The identity and responsibilities of the MLRO and Compliance.
- The potential effect and consequences of non-Compliance with applicable AML laws and sanctions programs, including disciplinary, civil and criminal penalties.
- The Company's record retention policy in relation to the AML Policy.

The Company, in conjunction with the MLRO, will review its businesses to see if certain Employees, depending on the business in which they are involved, may need to receive further or more specific training, which will be recorded and retained in the same manner as the Company-wide AML Policy training.

***All Employees must be familiar with this AML and Sanctions Policy.  
Employees who are assigned to perform KYC due diligence and sanctions screening  
will be given further specified training by Compliance<sup>3</sup>.***

---

<sup>2</sup> In coordination with local relevant department for local requirements

<sup>3</sup> In coordination with local relevant department for local requirements

### 3.3.3 Customer due diligence

CDD must take place on a risk sensitive basis before the establishment of a business relationship or the carrying out of a new transaction. Accordingly, certain businesses must assign employees to perform the CDD process. Employees responsible for performing the due diligence process must recognize that different business partners pose different risks and trigger different requirements depending on a number of varied factors. The Guidance outlines the standard KYC due diligence measures including the development of Risk Categories to be used in determining the appropriate steps to be taken.

#### **Initial CDD at onboarding of customers**

##### **Standard CDD shall comprise identifying and verifying the customer's identity:**

- Identifying the customer and, as applicable, its CEO, main directors, partners, and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source.
- Identifying the beneficial owner and taking reasonable measures to verify that person's identity so that Euronext is satisfied that it knows who the beneficial owner is, including, as regards legal persons, trusts, companies, foundations and similar legal arrangements, taking reasonable measures to understand the ownership and control structure of the customer.
- Assessing and, as appropriate, obtaining information on the purpose and intended nature of the business relationship.
- Conducting ongoing monitoring of the business relationship including appropriate scrutiny of transactions undertaken throughout the course of that relationship.

**Enhanced CDD** is applied in case where high(er) risk indicators are found during the customer identification process. Enhanced CDD contains additional measures to mitigate the risks identified. All high risk files should be sent to Compliance for advice. Compliance may decide to escalate a case to the Management Board.

Examples of high risk indicators:

- Countries with low AML regulation, a high level of corruption or political instability and countries that are subject of EU or OFAC sanctions programs.
- Politically Exposed Persons (PEPs) as senior management, a director or Beneficial Owner (natural person) involved.
- Complicated company structures using foundations, trusts or a fund as holding company (i.e. risk of hiding ultimate beneficial owners).
- Companies, senior management, directors or Beneficial Owners generate alerts in the screening tool (criminal activity/ sanction lists).

**Simplified CDD** can be applied when products, services and / or delivery channels and the characteristics of the customers imply a (very) low risk in relation to money laundering and sanctions programs. Low risk customers are regulated financial institutions in the EU, government bodies, and companies with full regulated market listings in the EU or the US.

#### **Ongoing monitoring**

As part of the KYC due diligence process, the Customer's information must be kept updated and screened in accordance with the risk profile determined by the business throughout the

duration of its relationship with the Company so that it reflects relevant changes in, for example, a significant change in the type of business activity or a change in the ownership structure. This is an important step in the KYC due diligence process and is described further in the Guidance.

**Employees who are assigned to perform KYC due diligence must read, understand and follow the Guidance in performing the due diligence.**

---

### 3.3.4 Screening for sanctions and PEPs

Prior to entering into a business relationship with a new customer, the Company must screen against OFAC and EU sanctions lists, as well as PEPs lists, to determine whether the Customer appears on any of these lists, or is a resident of or organized in the targeted countries on the lists maintained by EU or OFAC.

Employees should act with caution on any indication that there is a risk of violating a sanctions program and should not approve, give advice, or otherwise participate in any meeting, transaction, or business activity when confronted with an actual or potential sanctions issue. In performing the KYC process, relevant business units of Euronext, following a risk based approach, must identify and verify whether the customer (the entity) or its senior management, directors or ultimate beneficial owner are on a sanction list. If a potential or existing business partner is identified as being on a sanctions list, this must be reported promptly to Compliance<sup>4</sup>. The onboarding process or business with the (prospective) customer must be put on hold until further notice/advice from Compliance.

**Politically Exposed Person or PEPs** are natural persons who are or have been entrusted with prominent public functions whether this be domestic prominent public functions, prominent public functions in a foreign country, and/or prominent public functions in an international organisation. This would include, for example, senior politicians, senior government, judicial or military officials or senior executives of state-owned corporations, and immediate family members, or persons known to be close associates, of such persons.

Business relationships with PEPs may change the risk rating of a customer due to the possibility that individuals who hold such positions may misuse their power and influence for personal gain or for the personal gain of family and close associates. Such individuals may also use their families or close associates to conceal funds or assets that have been misappropriated as a result of abuse of their official position or resulting from bribery and corruption. In addition, they may also seek to use their power and influence to gain representation with access to, or control of, legal entities for similar purposes.

In performing the KYC process, relevant business units of Euronext, following a risk based approach must identify and verify whether the customer has senior management, directors or ultimate beneficial owners that are PEPs.

If a potential or existing customer is identified as a PEP:

---

<sup>4</sup> Where applicable, escalations are directed to the relevant department in charge of such assessment, with the involvement of Compliance. Regarding Euronext Dublin escalations will go to the local Head of Regulation and the local MLRO as well as to the Compliance department.

- this must be escalated to Compliance<sup>5</sup> for assessment (where the presence of such gives rise to additional risk for the Company) and senior management approval may be obtained for establishing or continuing the business relationships with the PEP;
- take adequate measures as appropriate to establish the source of wealth and source of funds that are involved in business relationships or transactions with such persons;
- conduct enhanced, ongoing monitoring of those business relationships.

PEPs should be treated as such until at least 12 months after they cease to be a PEP.

Identifying and reporting such instances will alert the Company of the need for further investigation before proceeding with the transaction; it does not automatically mean that a transaction should not proceed.

**Employees who are assigned to screen for sanctions and PEPs must read, understand and follow the Guidance in performing the screening.**

---

### 3.3.5 Appointment of a Money Laundering Reporting Officer

The Company has appointed a Group MLRO and where relevant local MLROs. The duties of the Company's MLROs together with the Compliance Department include the monitoring this AML Policy and any enhanced procedures that have been developed for a business line that conducts activities in a high risk environment (as defined by virtue of its location or business type). The MLROs and Compliance are also responsible for providing training for Employees, as well as ensuring proper AML record keeping in accordance with regulatory requirements. The Company's MLRO's contact details can be found on the Company's internal website/ Compliance page or, ask the Compliance department or your local Compliance officer.

**All Employees must be aware of the identity of their MLRO. If you have any questions, contact Compliance<sup>6</sup>.**

---

### 3.3.6 Retention of records

If a Business Partner comes under investigation, the Company must be able to provide an audit trail of the processes undertaken pursuant to this AML Policy. The MLRO must retain, or cause to be retained, the following:

- Records in relation to the identity of the Business Partner obtained in the KYC due diligence process, including a copy of the evidence of identity obtained or a record of where a copy of the evidence of identity can be obtained.
- A record containing details of every transaction or a record of where a copy of every transaction can be obtained that is carried out by the Company with the Business Partner.
- Records of action taken or reports made with respect to the internal and external reporting of suspicious activities.

---

<sup>5</sup> Where applicable, escalations are directed to the relevant department in charge of such assessment, with the involvement of Compliance

<sup>6</sup> Where applicable, other departments may be involved, such as legal department

- Records of the dates of and topics covered by AML training.
- Copies of any reports generated by the MLRO with respect to any exemptions from or any waivers of any of the AML Policy requirements.
- Other books and records as required by applicable law and regulation.

Complete and accurate records must be retained and kept retrievable during the relationship with the Business Partner as required by local law. The records must be kept at least seven years from the date when the relationship with the Business Partner ends if allowed by domestic law.

Records that relate to current investigations, or activities that have been disclosed to the authorities, should be retained pending agreement by the authorities that records may be destroyed.

**All Employees must retain records and reports produced pursuant to the AML Compliance program, as required.**

### 3.3.7 Monitoring transactions

AML laws require financial institutions to monitor, investigate and report transactions of a suspicious nature to the relevant authorities (e.g. a national Financial Intelligence Unit (FIU) or Tracfin). Accordingly, financial institutions must have appropriate and risk-sensitive procedures in place that provide for the identification and scrutiny of transactions that may be related to money laundering, for example, transactions that do not match the business partner's profile, transactions involving suspicious countries, or unusual patterns of transactions occur. However, this mainly applies to the typical activities of financial institutions when dealing with customers: opening an account, accepting assets of the customer and carrying out financial transactions for such customer. Euronext does not carry out such activities for its customers, except through account operators that are responsible for the KYC/AML according to applicable law.

Euronext does perform Post Trade Surveillance activities, which are primarily aimed at detecting possible market abuse. This monitoring is performed every day and relates to t+ 1 market activity of Members. The monitoring is automated and alerts are analyzed by Member Compliance/ Surveillance / Operations. Some of the monitoring scenarios are catering for Money Laundering related activity, such as Wash trades and Money passing. Alerts can also trigger an incident driven review of a listed company or Member, based on the indicators found. Member Compliance has a procedure for treating the alerts, and this procedure<sup>7</sup> forms part of the AML framework.

**Employees who are assigned to perform due diligence and screening procedures must read, understand and follow the Guidance to effectively monitor for the Company's AML risk. In addition, Employees who work in certain businesses that may be subject to AML risk as identified by Compliance will assist in identifying specific risks and monitoring controls.**

<sup>7</sup> Member Compliance manual.

---

### 3.3.8 Reporting obligations

In the event that an Employee becomes aware of facts and circumstances that may indicate potential money laundering or terrorist financing, these matters must be promptly reported to the MLRO. Failure to do so will be a breach of this Policy, and could result in disciplinary action being taken by either Euronext or the relevant authorities. Employees must not disclose to any other person including the customer concerned (tipping off), except as may be required by law or regulation or in connection with an internal review by the Company (on a need to know basis), that a potential case of money laundering has been reported or is being investigated. For examples of Red Flags that may indicate money laundering or terrorist financing, see the Guidance.

Following the report, the MLRO and Compliance Department<sup>8</sup> will consider the circumstances and decide whether an alert should be made to the relevant authorities. Where the Company knows, suspects, or has reasonable grounds to suspect that money laundering or terrorist financing is being or has been committed or attempted, it will promptly make the report.

The MLRO / Compliance Department may report and/or escalate any suspicions of money laundering to members of the Managing Board.

**All Employees must report promptly to their MLRO and Compliance when they become aware of facts and circumstances that may indicate potential money laundering or terrorist financing.**

---

### 3.3.9 Independent audit

The Company may periodically conduct an independent audit of the AML Compliance program to evaluate the adequacy and effectiveness of the Company's system of internal controls and Compliance with the requirements of this AML Policy and, accordingly, AML laws. Such an audit may be performed by the Euronext Internal Audit department or by an independent third party.

---

## 3.4 REQUEST FOR INFORMATION FROM RELEVANT AUTHORITIES SUCH AS REGULATORS

The Company and Employees may receive a request from relevant authorities to communicate about suspected money laundering and terrorist financing. Employees and the Company may not disclose to any person the fact that a relevant authority has requested information except to the extent necessary to comply with such a request.

**All Employees must forward all inquiries from a relevant authority to Compliance , who will coordinate the response. Employees must not disclose the request to any**

---

<sup>8</sup> Where applicable, other departments may be involved, such as legal department

**person except to the extent necessary to comply with the request of the relevant authority.**