



# ANTI-MONEY LAUNDERING POLICY

---

EURICOM S.p.A.

Sommario


DEFINITIONS ..... 3

INTRODUCTION ..... 4

FIELD OF APPLICATION..... 4

REGULATORY FRAMEWORK..... 4

CONTROL SYSTEMS ..... 4

RED FLAGS  ..... 5

In exceptional cases, in the presence of anomaly indicators, the CEO may decide whether to  
authorise the transaction with the customer..... 6

DIFFUSION AND TRAINING ..... 6

INFRINGEMENTS OF THE AML POLICY AND REPORTS OF SUSPICIOUS TRANSACTIONS ..... 6

DISCIPLINARY SYSTEM..... 6

APPROVAL OF THIS DOCUMENT AND SUBSEQUENT UPDATES..... 7

## DEFINITIONS

In this document the following terms have the meanings shown below:

- **“Recipients”**: all subjects who work in the name and on behalf of Euricom Group. All the following fall under the definition of Recipients: Employees, Board Members, Supervisory Bodies, Suppliers, Consultants, Professionals, Partners, Customers, and Subsidiaries of Euricom S.p.A., etc.
- **“Euricom S.p.A.”** or **“Group Leader”**: parent company of Euricom Group.
- **“Terrorism financing”**: activities carried out to find money or other support, even material, in favour of terrorist organisations that threaten national and supranational security.
- **“Group”** or **“Euricom Group”**: the corporate group Euricom Group S.p.A. is the parent company of.
- **“Suspicious transactions”**: transactions performed or attempted by the customer apparently aimed at carrying out money laundering or terrorist financing operations.
- **“PEP”**: politically exposed persons.
- **“Red Flags”**: warning signs, suspicious indicators to pay attention to.
- **“Money laundering”**: action aimed at hiding or disguising the origin of the proceeds of a criminal activity. For example, these earnings may arise from non-legitimate activities such as: drug trafficking, embezzlement, extortion, bribery, fraud or other crimes. Money laundering is the main source of terrorism financing.
- **“Third Parties”**: natural or legal persons, other than Employees who have *business* relationships with the Company. Third Parties means Suppliers, Consultants, Professionals, Mediators, Partners, Trading Partners, Customers, etc.
- **“UIF”**: The Italian Financial Intelligence Unit (UIF) was established at the Bank of Italy by Italian Legislative Decree No. 231/2007, in accordance with the international rules and criteria envisaging the presence of a Financial Intelligence Unit in each State with complete operational and administrative autonomy, and responsible for combating money laundering and terrorist financing. It is the authority responsible for acquiring financial flows and related information concerning possible money laundering activities and terrorist financing mainly through suspicious transaction reports transmitted by financial intermediaries, professionals and other operators; the unit then carries out financial analysis of this information, drawing on the available sources of intelligence and using the powers at its disposal, and assesses its relevance for possible transmission to investigative bodies and cooperation with the judicial authorities, to develop any countermeasures.

## INTRODUCTION

Euricom Group is committed to preventing its business from being used to facilitate financial crimes, including money laundering and terrorism financing in a context of widespread globalisation of terrorist organisations and the development of technological innovations (such as virtual currencies). The Group has voluntarily adopted this Policy to protect itself, its directors and its employees, as far as possible, from being used to favour money laundering, financing criminal and terrorist organisations and other financial crimes.

This Policy aims to strengthen Recipients' awareness of rules and behaviour that must be complied with by providing a framework useful for identifying, reviewing and achieving objectives on anti-money laundering matters defined in accordance with the same Policy.

## FIELD OF APPLICATION

This Policy applies to all subjects that operate in the name and on behalf of Euricom Group. The following are among these: Employees, Board Members, Members of the Supervisory Bodies, Third Parties the Companies in the Group and Employees of individual local entities. Hereafter also "Recipients".

## REGULATORY FRAMEWORK

The Group undertakes to comply with the laws, rules, regulations and conventions relating to anti-money laundering (hereinafter the "AML Rules"), such as:

- *Proceeds of Crime Act (POCA) 2002* from the United Kingdom;
- European Union directives on money laundering and implementing legislation of member States;
- Italian Legislative Decree No. 231/2007 and subsequent and related provisions (e.g., Italian Legislative Decree No. 90/2017);
- GAFI-FATF recommendations;
- any other Law, regulation and ordinance relating to money laundering or the proceeds deriving from criminal activities;

In this context Euricom Group deemed it appropriate to implement a prevention system regarding anti-money laundering which includes:

- drawing up this *Policy*, with principles and rules of conduct overseeing the commission of acts of money laundering or terrorism financing approved by Euricom S.p.A. Board of Directors;
- risk analysis and assessment of the possibility of acts of money laundering and/or terrorism financing, corruption carried out by individual Companies in the Group according to the AML Rules;
- providing information and training activities for Employees, aimed at spreading Euricom Group culture as well as the AML Rules;
- implementing reporting procedures and tools (*whistleblowing*) that are easy to access and comply with the AML Rules;
- periodic monitoring of money laundering risks, as well as verification of the effectiveness and adequacy of this document.

## CONTROL SYSTEMS

To counteract, or at least reduce the risk of incurring an infringement of the AML Rules, Euricom Group has defined a precise control system.

### CUSTOMER IDENTIFICATION

When establishing a business relationship with a new Customer, the counterparty must be identified and the beneficial ownership of the legal person verified (threshold of beneficial ownership of 25%) to identify and report the risk of criminal infiltration within the corporate structure.

In detail, it is necessary to collect information on:

- identification of the counterparty and beneficial owner;
- reports of prejudicial events;
- method of payment.

Among the checks to be implemented, Euricom Group proposes to adopt a strengthened due diligence measure to also consider the possible registration of the counterparty's country of residence on the *lists of foreign countries with deficiencies in money laundering and terrorist financing enforcement measures*<sup>1</sup>, so-called *black lists* (a list of countries at a high risk of money laundering and terrorism financing) with the aim of collecting more information on the origin of funds and the Customer's financial situation.

Finally, Euricom Group undertakes to verify whether the beneficial owner holds public office in areas included in the notion of PEP, to whom there is significant exposure to the risk of corruption.

All the checks indicated in this paragraph can be collected also using databases.

The final decision of whether to proceed the payment transaction alerted as having risk of facilitate financial crimes shall be finally approved by CCO of each company.

### FINANCIAL FLOW MANAGEMENT

As part of existing commercial relationships with Customers, within which the Customer expresses the need to make payments through third parties/natural persons it is necessary to obtain a communication on the Customer's headed paper indicating the name/company name of the third party, the country of origin of the electronic payment (bank transfer) and the type of relationship that exists between the third party and the Customer. In these cases, the Group must monitor the number of transactions carried out by third parties/natural persons relating to a single customer (or multiple customers) and the number of third parties used by the Customer in the reference period.

With reference to large cash transactions equal to or greater than the limit value dictated by legislation in force at the time, the Group undertakes to ensure compliance with the limit on the use of cash and ensure that all transfers above the limit are traceable, or are carried out exclusively through financial institutions, electronic money institutions and payment institutions. Further, in the event of payments received from third parties, the connection with the contractor and with the beneficial owner will be verified.

### RED FLAGS

Euricom Group recommends to Employees and individuals who operate in the name and on behalf of one of the Companies in the Group to pay attention to the following red flags (anomaly indicators):

- The Customer appears uncooperative and does not provide the requested information;

---

<sup>1</sup> Please see the link <https://www.fatf-gafi.org/en/topics/high-risk-and-other-monitored-jurisdictions.html>

- The Customer provides suspicious information to be investigated internally;
- The Customer tries to convince the Group Employee not to carry out the activities foreseen to identify the Customer;
- The Customer requests to be exempt from the control process implemented by Euricom Group;
- Payments are made via cheques, postal orders or cashier's checks withdrawn from the account of the entity that made the purchase;
- Using alternative corporate means (or shell companies) to obscure ownership, source of funds, or the countries involved;
- Using third parties/natural persons to protect the identity of sanctioned persons and/or PEP to hide the origin or ownership of the funds;
- Using shell companies to make international bank transfers, often in jurisdictions other than that of the customer company.

In exceptional cases, in the presence of anomaly indicators, the CEO may decide whether to authorise the transaction with the customer.

### **DIFFUSION AND TRAINING**

Euricom Group promotes the diffusion of this Policy, making it accessible and understandable to all Recipients as well as all Companies that are part of the Group. This Policy is published on the official Euricom S.p.A. website and shared with all Companies in the Group.

Furthermore, specific training and communications activities must be provided for the Employees in the Companies in the Group with the aim of ensuring effective knowledge of the contents of this Policy, of Policies implemented at local level as well as applicable regulations.

### **INFRINGEMENTS OF THE AML POLICY AND REPORTS OF SUSPICIOUS TRANSACTIONS**

Failure to comply with this Policy or knowledge or the suspicion of activities of money laundering and terrorist financing, in progress, completed or attempted, must be reported by the Recipients if they become aware of any, using the *whistleblowing* reporting channel implemented by each Company in Euricom Group. Where not present, it is possible to use the reporting channel implemented by the Parent Company which can be accessed via the following link <https://euricom.it/IT/WHISTLEBLOWING/>.

Investigations will be carried out guaranteeing the maximum confidentiality of whistleblowers, without prejudice to legal obligations. Euricom Group guarantees that no retaliatory action will be carried out against whistleblowers.

In addition, Euricom Group undertakes to transmit data and information concerning suspicious transactions regardless of the relevance and amount of the suspicious transactions by sending an electronic communication without delay to the UIF on the internet, via the portal INFOSTAT-UIF of the Bank of Italy.

Finally, all Companies in the Group undertake to communicate promptly to the Group information relating to reports of suspicious transactions made to the UIF to interrupt or prevent the formation of contractual relationship with the contractor and the beneficial owner of any kind.

### **DISCIPLINARY SYSTEM**

All Recipients are contractually obliged to comply with the principles of this Policy. This compliance is an integral part of contractual agreements.

Failure to comply by Employees will involve the application of disciplinary and sanctioning measures, up to termination of the contractual relationship, depending on the gravity of the act committed

Infringements by Third Parties may lead to termination of the contractual relationship, as well as possible compensation for damages.

Failure to comply by directors and Supervisory Bodies will entail suspension or removal from office.

#### **APPROVAL OF THIS DOCUMENT AND SUBSEQUENT UPDATES**

This *Policy* was approved by Euricom S.p.A Board of Directors, which provides for the obligation to adopt the same by all Companies in the Group so that they can implement the content through a resolution of the Administrative Bodies, adapting it if necessary to company needs and the regulations of the country of reference.

Any updates to this document connected to national or international regulatory changes to matters relating to anti-money laundering and/or to new money laundering risk indicators related to products, services, *business* lines, geographical areas, etc., will have to be submitted again for approval to the Board of Directors.