Group
Anti-Money Laundering (AML) Policy – Overview

Contents

1 Scope

The Anti-Money Laundering Group Policy applies to CDP S.p.A. (the "Parent Company") and to CDP Group companies that are recipients of the obligations referred to in Decree 231 of 2007, the so-called "Anti-money laundering decree".

The Companies ensure in any case that their operations comply with the provisions of these Group regulations, according to the principle of proportionality and taking into account the independent decision-making powers of their Corporate Bodies and in particular of Supervised Entities, as well as specific sector regulations that may apply to the latter.

2 General principles

2.1 Money laundering risk

Money laundering risk is the risk arising from the violation of laws, regulations and governance regulations functional to the prevention of the use of the financial system for the purposes of money laundering, terrorist financing or financing of programmes for the development of weapons of mass destruction (hereinafter "anti-money laundering legislation"), as well as the risk of involvement in money laundering and terrorist financing cases or the financing of programmes for the development of weapons of mass destruction.

In the Policy, any reference to the purpose of anti-money laundering or the risk of money laundering must always be understood as including the purpose of combating terrorist financing or the risk of terrorist financing.

The Recipient Companies also apply the safeguards referred to in the Policy in order to combat the financing of programmes for the development of weapons of mass destruction.

2.2 Risk-based approach

The Group Policy establishes the rules that the CDP Group intends to applies for the various relevant profiles regarding organisational structures, procedures and internal controls, due diligence and data retention, applying the risk-based approach and, in particular, the results of the annual self-assessment of money laundering risk exposure.

The Recipient Companies adopt the Policy taking into account the nature, size and complexity of the activity carried out as well as the type and range of services provided. To this end, the Recipient Companies:

- carry out an overall assessment, updated at least annually, of their exposure to money laundering risk (self-assessment of money laundering risk exposure), according to the methodology;
- adopt the measures they consider most appropriate to prevent the risk of money laundering, consistent with their exposure to this risk;
- ensure the Policy is correctly implemented in their own internal regulations;

- ensure, each within their area of responsibility and in coordination with Human Resources, the provision of continuous training courses for personnel most involved in anti-money laundering processes, to be planned also considering the concrete risks detected as a result of the regulatory developments or the control and self-assessment activities carried out on a continual basis;
- ensure, for the purposes of effective management of the risk of money laundering and terrorist financing, that when establishing and/or during the business relationships and/or when executing the transaction, the risk profiles of individual customers actually identified and related risk mitigation measures are considered, also for the purpose of assessing the obligation to refrain, and paying particular attention to any decisions to exclude single customer or entire categories of customers with a high risk of money laundering (so-called "de-risking"*").*

3 Self-assessment of exposure to money laundering risk

Without prejudice to the obligation to ensure compliance with the laws and regulations on anti-money laundering, including the Policy, and by applying the risk-based approach, Recipient Companies may modulate their organisational structure, operating and control procedures, as well as information systems according to the level of risk to which they are concretely exposed, taking into account the nature, size and complexity of the activity carried out and the type and range of services provided.

To this end, the Recipient Companies carry out an overall assessment, periodically updated, of their risk exposure (the self-assessment of money laundering risk exposure), in accordance with the provisions of the Policy.

4 Roles and responsibilities of the Corporate Bodies

4.1 Board of Directors

The Board of Directors of the Parent Company approves and periodically reviews the strategic guidelines and policies for governing the risks associated with money laundering; in compliance with the risk-based approach, it ensures that policies are appropriate to the extent and type of risks to which the Group's activities are concretely exposed, as represented in the risk self-assessment document.

4.2 Chief Executive Officer

The Chief Executive Officer of each recipient Company is responsible for implementing the strategic money laundering risk guidelines and policies defined by the Parent Company, and contained in the documents implementing the Policy approved by the respective Boards of Directors, and is responsible for adopting all necessary measures to ensure the effectiveness of the anti-money laundering control system and organisation. For such purposes, the Chief Executive Officer examines the proposals for organizational and procedural interventions presented by the AML function and formalizes, giving reasons, any decision not to accept them.

4.3 Senior manager Responsible for AML/CFT

Without prejudice to the collective responsibility of the corporate body, the board of directors appoints a member of the management body as senior manager responsible for anti-money laundering. The assignment of the role is shown in the appointment minutes of the board of directors. The assignment is executive in nature.

4.4 Group senior manager Responsible for AML/CFT

The Parent Company appoints a member of the board of directors as senior manager responsible for anti-money laundering at group level. The assignment is executive in nature.

4.5 Board of Auditors

The Board of Auditors of the recipient Company supervises compliance with legislation and the completeness, functionality and adequacy of anti-money laundering control systems.

In carrying out its duties, it uses internal structures to carry out necessary controls and audits, as well as information flows from the other Corporate Bodies, the AML/CFT compliance officer and other internal control functions.

5 Structure of anti-money laundering safeguards

5.1 First level structures

First line of defence (so called “line structures”) are the structures responsible for managing relations with customers and/or counterparties benefiting from disbursements, which ultimately bear responsibility for decisions regarding the establishment or continuation of business relationships with the customer or counterparty.

The Recipient Companies can set up specialized competence centres to perform customer due diligence and other I level activities and controls. Line structures and competence centres, together, represent the first line of defence for AML purposes.

5.2 Anti-Money Laundering (AML) function

The Recipient Companies set up a function specifically dedicated to the prevention and management of money laundering risks (hereinafter, the "AML function") which, together with the Head, represents the second line of anti-money laundering defence, according to a decentralised model, except as provided for by the Policy on the outsourcing of the AML function.

The activities of the AML function are planned annually through the preparation of an "**Activity Plan**", which defines the areas of action and interventions, including from a Group perspective, that are considered priorities for the management of money laundering risk.

In order to produce a risk-based activity plan that is aligned with the requirements to cover the risk the recipient Company is actually subject to, the AML function drafts the Plan, taking into account the results of the Self-assessment of money laundering risks, the Compliance Risk Assessment and planned control activities.

The AML function submits directly the **Annual AML Report**, defined in accordance with applicable supervisory provisions, to the Corporate Bodies and to the Supervisory Body.

5.2.1 AML/CFT compliance officer

The appointment and removal from office of the AML/CFT compliance officer are overseen at management level by resolution of the Board of Directors, after consulting with the Board of Auditors. The documents providing for appointment and removal from office must clearly and comprehensively indicate the circumstances and reasons for the decision.

The AML/CFT compliance officer must meet requirements of reputation, honesty and integrity and sufficient time to perform functions effectively, independently and autonomously.

The AML/CFT compliance officer reports directly to the Corporate Bodies and has direct access to the Board of Directors and the Board of Auditors to report on the Annual AML report, the progress of the corrective actions adopted in response to deficiencies found in the control activity and the results of the assessment on human and technical resources assigned to the AML function and the need to strengthen them

The Parent Company ensures that the AML function operates on an ongoing basis even in the event of termination of its functions or unavailability for a period of time of the AML/CFT compliance officer.

In line with the principle of proportionality, the Parent Company designates as AML/CFT compliance officer at Group level the AML compliance officer of the Parent Company.

5.2.2 AML approach at Group level

The Parent Company ensures the development of a coordinated and coherent approach to money laundering risk at Group level, in particular through:

- a group methodology for assessing the l money laundering risks exposure in accordance with the method indicated in regulations of the Supervisory Authority;
- general standards on customer due diligence, data and information retention, reporting of suspicious transactions;
- formalised procedures for coordinating and sharing relevant information among the AML functions of the CDP Group for all areas of activity related to anti-money laundering obligations, also for the purposes of identifying suspicious transactions;
- procedures regarding anti-money laundering controls at Group level, such as, for example, procedures that define specific methodologies for carrying out controls

5.3 Money Laundering Reporting Officer

The Money Laundering Reporting Officer (“MLRO") is the legal representative of the recipient Company or the AML/CFT compliance officer in the capacity of representative of the recipient Company, as he/she meets necessary requirements of independence, authority and professionalism.

The Recipient Companies ensure that the MLRO carries out his/her activities with independent judgment and in compliance with confidentiality obligations to protect the identity of reporting parties, also regarding members of Corporate Bodies and other corporate functions.

To carry out his/her duties, the MLRO may request any information deemed necessary both from the structure that carried out the first level analysis on anomalous transactions, and from any other company structure that has had contact with the counterparties being assessed.

The Recipient Companies ensure that the MLRO, in carrying out his/her duties, is supported by appropriate IT procedures (transaction monitoring).

5.4 Internal Audit function

The Internal Audit function continuously verifies, as part of the Audit Plan approved by the board of directors, the degree of adequacy of the corporate organisational structure and its compliance with applicable regulations and supervises the functioning of the overall internal control system.

5.5 IT systems

The Recipient Companies ensure that the procedures and internal controls implementing the Policy are supported by suitable IT applications, designed to allow, in the presence of adequate levels of effectiveness and efficiency, the simplification of processes, the sharing of information, the automation of controls and the traceability of assessments carried out.

5.6 Training

For all organisational units the Recipient Companies adopt the necessary initiatives to ensure training, information and updates on an ongoing basis regarding anti-money laundering legislation, the Group Policy, the procedures in place for customer due diligence, data and information retention, and reporting of suspicious transactions.

6 Assessment of risk profiles attributable to customers

The Policy establishes the general criteria which the Recipient Companies observe, in order to assess the risk profiles associated with customers and, consequently, to configure the methods for carrying out due diligence.

Customer risk profiles are assigned before an business relationship is established or a transaction is executed. Subsequently, and throughout the duration of the relationship, the customer's risk profile is constantly monitored, in order to detect any changes in the information on which the previous assessment was based.

The evaluation systems and decision-making processes adopted ensure consistent behaviour within the entire company structure and the traceability of controls and assessments carried out, as well as demonstrating to the authorities that the specific measures taken are adequate for the risks that have actually been identified.

6.1 General criteria for the assessment of the Risk Profile

To assess the money laundering and terrorist financing risk profile attributable to every customer, each recipient Company considers at least the following assessment aspects, where relevant in relation to the specific activity carried out, which refer to the characteristics of the customer, their conduct and specific aspects of the transaction or business relationship.

The Recipient Companies obtain information to identify the customer’s risk profile from all relevant information sources and documents.

6.1.1 Customer risk factors

With reference to the customer, beneficial owner and, where relevant, the executor, the Recipient Companies take into account at least the following aspects:

- the **legal nature;**
- the **main activity carried out**;
- the **conduct** at the time of completion of the transaction or establishment of the business relationship;
- **the geographic area of reference**, meaning at least: (i) the country of residence, domicile or registered office; (ii) the country from where the funds originate (e.g. in loan repayment transactions); (iii) the location of the activity carried out; (iv) the countries with which the customer or beneficial owner and, where relevant, the executor have material connections.

In any case, the Recipient Companies will verify whether the customer or the beneficial owner or controlling partners (pursuant to Article 2359 of the Italian Civil Code), as identified on the basis of reliable and independent sources, are included in the lists of persons and entities associated with terrorist financing activities, the financing of programmes for the proliferation of weapons of mass destruction and countries that threaten international peace and security, adopted by the UN, the European Union or other institutions and bodies involved in combating international terrorism, such as the Office of Foreign Asset Control (OFAC) of the US Department of the Treasury.

The Recipient Companies also use, as tools, risk indicators and communications on the prevention of terrorist financing published by the FIU.

6.1.2 Risk factors concerning the business relationship or transaction

With reference to the transaction or business relationship, Recipient Companies shall take into account at least the following aspects:

- the **type** of transaction carried out or business relationship established;
- the **methods** of carrying out the transaction or establishing the business relationship;
- the **amount** of the transaction;
- the **frequency** and **volume** of transactions and duration of the business relationship;
- the **reasonableness** of the transaction or of the business relationship in relation to the activity carried out by the customer and the extent of available economic resources;
- **the geographic destination area** of the product and the subject matter of the transaction or business relationship.

The Recipient Companies shall pay attention to new or innovative products or services, in particular in the event that, for the offering of these products or services, new technologies or new payment methods are used.

The Recipient Companies shall also consider whether the product, service or transaction are normally associated with the use of cash and whether they allow significant-amount transactions.

The Recipient Companies shall assess the reasonableness of the business relationship or transaction in relation to the activity carried out and the overall economic profile of the customer and the beneficial owner identified with the criterion of ownership or control, taking into account all available information (e.g., income and asset capacity) and the nature and purpose of the business relationship.

6.2 High risk factors

When assessing money laundering and terrorist financing risk associated with customers, the Recipient Companies shall take into consideration at least the high risk factors indicated below, where relevant in relation to the specific activity carried out.

In particular, high risk factors may be relevant for the application of enhanced measures during customer due diligence as defined below.

The high risk factors related to the customer, executor and beneficial owner are:

- high-risk geographic areas;
- relations with financial intermediaries outside the European Union (EU);
- politically exposed persons (PEPs);
- ongoing relationships established in unusual circumstances;
- negative news:
- legal persons or arrangements that are personal asset-holding vehicles;
- the ownership structure of the company appears unusual or excessively complex given the nature of the company's business;
- prevalent high risk economic activity.

High risk factors related to products, services, transactions or distribution channels:

- transactions with unusually high amounts or where there are doubts as to the purpose;
- transactions with high risk purposes, as they relate to oil, weapons, precious metals, tobacco products, cultural artefacts and other movable property of archaeological, historical, cultural and religious importance or of rare scientific value, as well as ivory and protected species;
- new generation products, which include the use of distribution mechanisms or innovative technologies for new or existing products.

Geographical high risk factors:

- third countries which authoritative and independent sources consider to be lacking in effective safeguards to prevent money laundering;
- countries and geographic areas assessed as having a high level of corruption or permeability to other criminal activities by authoritative and independent sources;
- countries subject to sanctions, embargoes or similar measures adopted by the United Nations, the European Union[1], the USA (Office of Foreign Assets Control);
- countries and geographic areas that finance or support terrorist activities or in which terrorist organisations operate;
- countries assessed by authoritative and independent sources as lacking compliance with international standards on transparency and the exchange of information for tax purposes.

6.3 Customer profiling

The Recipient Companies shall define the risk profile attributable to each customer based on overall assessment aspects and the risk factors described in the Group Policy, as well as on additional assessment aspects and risk factors that may be relevant on the basis of the specific characteristics of the activity carried out, without prejudice to the need to share information with other Group AML functions, in order to maintain a uniform and coordinated approach to customer assessment as well as the comparability of assessment outcomes for shared customers.

The Recipient Companies, in compliance with the aforementioned risk-based approach, define the depth and extent of the due diligence measures adopted in the various areas of due diligence, to each risk class.

The production of the risk profile shall be based, as far as possible, on IT algorithms and procedures.

7 Customer due diligence

In the Policy, any reference to the customer or customers encompasses the beneficiaries of disbursements, including subsidies, not attributable to a business relationship with the Recipient Company and executed on behalf of third parties (e.g. State).

Customer due diligence consists of the following activities:

[1] This includes restrictive measures adopted by national authorities pursuant to Article 4 of Legislative Decree 109/2007 implementing United Nations Security Council Resolutions to combat the financing of terrorism and the financing of proliferation programs for weapons of mass destruction and against the activity of countries that threaten international peace and security.

- identification of the customer and any executor;
- identification of the beneficial owner;
- verification of the identity of the customer, any executor and beneficial owner based on documents, data or information obtained from a reliable and independent source;
- acquisition and evaluation of information on the purpose and intended nature of the business relationship and, where there are high risk factors, of the occasional transaction;
- conducting ongoing monitoring of the business relationship.

In the Internal Procedure on anti-money laundering, the Recipient Companies define the responsibilities, duties and operating methods for performing **activities** and first **level controls** aimed at ensuring the correct fulfilment of customer due diligence obligations.

7.1 Scope

The obligation to perform customer due diligence activities arises at the times and in the cases indicated below:

a) when an business relationship is established;
b) when executing a transaction ordered by the customer not attributable to an business relationship and for an amount equal to or greater than 15,000 euros, regardless of whether it is carried out as a single transaction or with several fractioned transactions;
c) where there is suspicion of money laundering or terrorist financing, regardless of any applicable deferral, exemption or threshold: to this end, the first level structures shall use the anomaly indicators issued and periodically updated by the FIU in order to facilitate the identification of suspicious transactions;
d) when doubts arise as to the completeness, reliability or truthfulness of information or documentation previously obtained from customers.

In the cases indicated under a) and b), customer due diligence can be considered fulfilled if customer due diligence have already been performed in relation to other existing business relationships and the information on the customer, the executor and the beneficial owner are complete, reliable and updated. Activities to identify and verify the identity of the customer, executor and beneficial owner are carried out by the first-level structures before the business relationship is established or the occasional transaction is executed.

7.2 Ongoing monitoring

The Recipient Companies shall carry out ongoing monitoring on existing business relationships, in order to keep the customer's risk profile up to date at all times, and to promptly identify information potentially relevant for the purpose of specific obligations.

The ongoing monitoring carried out by the first level structures consist first of all in updating the data and information previously obtained, with the start of a new due diligence procedure, according to the timing determined on the basis of the risk profile assigned to the customer.

7.3 Obligation to notify asset freezing measures

The Recipient Companies shall adopt organisational and procedural safeguards aimed at ensuring compliance with the obligation to promptly notify the FIU of asset freezing measures applied to **designated persons** (i.e. natural and legal persons, groups and entities specifically identified by the United Nations and the European Union as recipients of restrictive measures to "freeze" funds and economic resources held by them), as well as information on funds and economic resources held by designated persons, in accordance with provisions of Article 7 of Legislative Decree 22 June 2007, n. 109 of, with the European Union Regulations (e.g. Regulation (EU) No 269/2014) and with the communications published by the FIU.

The AML functions of each Recipient Company shall in any case notify the FIU, pursuant to the aforementioned legislation, of data relating to transactions or business relationships, as well as any other available information attributable to persons that are designated or being designated.

7.4 Abstention Obligation

When the Recipient Companies are not able to comply with customer due diligence obligations, they must not establish the business relationship or execute the transaction. If due diligence cannot be carried out for an existing business relationship, the Recipient Companies will not maintain the relationship.

In view of the high risk of money laundering and terrorist financing, first level structures shall refrain from establishing a business relationship or executing transactions or, where possible, shall immediately terminate the already existing business relationship at least in cases where the following entities are directly or indirectly involved:

- financial institutions that have their registered office in a jurisdiction in which they are not physically present and that are not affiliated to a regulated financial group;
- trust companies, trusts, anonymous companies or companies controlled through bearer shares, established in countries outside the European Union with strategic deficiencies in their national systems for the prevention of money laundering and terrorist financing, as identified by the European Commission in accordance with Article 9(2) of Directive (EU) 2015/849. These measures shall also apply to other legal entities, otherwise referred to, with their registered office in those Countries, whose beneficial owner cannot be identified or their identity verified;
- natural or legal persons subject to sanctions requiring the freezing of funds and economic resources, officially issued by the UN, the European Union and/or OFAC, subject to specific exemptions, licenses or authorisations[2];
- companies producing anti-personnel mines, cluster munitions and sub-munitions subject to the prohibition of financing referred to in Law 220/2021.

[2] See the Group Policy "Sanctions and Embargoes".

Even in the absence of a specific obligation, abstention must be assessed in all cases where, during due diligence procedures, the first level structures identify elements of inconsistency or criticalities that may constitute significant anomalies for anti-money laundering purposes.

8 Enhanced due diligence obligations

8.1 General principles

The Recipient Companies shall apply enhanced customer due diligence measures when there is a high risk of money laundering.

The Recipient Companies, in the internal regulations implementing the Policy, carry out their own independent assessments according to the specific characteristics of their customers and products, defining cases which must always be considered as high risk, and in any case in compliance with specific regulatory provisions on the subject and with the general standards defined and approved by the Parent Company in the Policy.

8.2 Enhanced due diligence measures

Enhanced due diligence measures may include the following:

a) obtaining further information relating to the customer, beneficial owner and executor, the nature and purpose of the business relationship;
b) a better quality of the information to be obtained;
c) a greater frequency of updates to information obtained, in order to promptly identify any specific risk indicator;
d) requesting authorisation from a Senior Manager, after having obtained the opinion of the AML function, to open or continue the business relationship or to carry out the transaction.

The Senior Manager is a corporate figure responsible for following relationships with own high-risk customers.

The decision-making processes adopted ensure the traceability of the controls carried out and the assessments conducted, also to demonstrate to the authorities that the specific measures taken are adequate for the risks actually identified.

9 Retention of documents, data and information

9.1 General principles

The Recipient Companies shall retain documents, data and information useful for preventing, identifying or ascertaining any money laundering or terrorist financing activities and to allow for analysis to be carried out by the competent authorities.

The Recipient Companies shall ensure that documents obtained during due diligence on the customer, executor and beneficial owner are retained in accordance with law and with legislation in force.

The Recipient Companies shall also ensure that IT systems allow for the storage of all relevant data and information.

10 Reporting of Suspicious Transactions

The Recipient Companies should file a suspicious transaction report to the FIU when they know, suspect or have reasonable grounds to suspect that money laundering or terrorist financing operations are underway or have been carried out or attempted or that the funds, regardless of their extent, come from or are (even potentially) involved in criminal activity.

The FIU issues and periodically updates:

- Specific risk indicators to facilitate the detection of suspicious transactions, including specific indicators for “public administrations”;
- instructions for detecting and reporting suspicious transactions to ensure the timeliness, completeness and confidentiality of reporting.

For the reporting obligation to arise, it is not necessary to be certain that money laundering or terrorist financing operations are ongoing or have been carried out or attempted, but the existence of a suspicion suffice, i.e. the existence of reasonable grounds for suspicion, including the detection of some of the anomaly indicators issued by the FIU, is sufficient.