



## **Policy on combatting money laundering and terrorist financing**

Board of Directors of 01/08/2024

|          |                                                                                 |           |
|----------|---------------------------------------------------------------------------------|-----------|
| <b>1</b> | <b>FOREWORD.....</b>                                                            | <b>4</b>  |
| 1.1      | REFERENCE CONTEXT .....                                                         | 5         |
| 1.2      | SCOPE OF THE DOCUMENT .....                                                     | 6         |
| <b>2</b> | <b>SCOPE OF APPLICATION .....</b>                                               | <b>7</b>  |
| 2.1      | RECIPIENTS OF THE DOCUMENT.....                                                 | 7         |
| 2.2      | RESPONSIBILITY FOR THE DOCUMENT .....                                           | 8         |
| <b>3</b> | <b>DEFINITIONS.....</b>                                                         | <b>8</b>  |
| 3.1      | DEFINITION OF “MONEY-LAUNDERING” AND “FINANCING OF TERRORISM”.....              | 8         |
| 3.2      | GLOSSARY .....                                                                  | 10        |
| <b>4</b> | <b>ANTI-MONEY LAUNDERING MODEL GOVERNANCE.....</b>                              | <b>19</b> |
| 4.1      | PARENT COMPANY BANCA MEDIOLANUM S.P.A. ....                                     | 22        |
| 4.2      | ITALIAN COMPANIES BELONGING TO THE BANKING GROUP .....                          | 43        |
| 4.3      | FOREIGN COMPANIES BELONGING TO THE BANKING GROUP .....                          | 44        |
| <b>5</b> | <b>GROUP PRINCIPLES FOR COMBATTING MONEY LAUNDERING AND TERRORIST FINANCING</b> |           |
|          | <b>44</b>                                                                       |           |
| 5.1      | CUSTOMER DUE DILIGENCE.....                                                     | 45        |
| 5.2      | CUSTOMER PROFILING .....                                                        | 48        |
| 5.3      | ENHANCED CUSTOMER DUE DILIGENCE .....                                           | 52        |
| 5.4      | SIMPLIFIED CUSTOMER DUE DILIGENCE MEASURES .....                                | 56        |
| 5.5      | OBLIGATIONS TO ABSTAIN .....                                                    | 57        |
| 5.6      | CONTROLS TO COMBAT TERRORIST FINANCING.....                                     | 58        |
| 5.7      | REPORTING SUSPICIOUS TRANSACTIONS TO THE FINANCIAL INTELLIGENCE UNIT (FIU)..... | 59        |
| 5.8      | COMMUNICATION OF INFRINGEMENTS TO THE MINISTRY OF ECONOMY AND FINANCE.....      | 60        |
| 5.9      | OBJECTIVE COMMUNICATIONS .....                                                  | 60        |
| 5.10     | DATA AND DOCUMENT STORAGE OBLIGATION .....                                      | 61        |
| 5.11     | STAFF TRAINING .....                                                            | 62        |
| 5.12     | INTERNAL SYSTEMS FOR REPORTING INFRINGEMENTS.....                               | 62        |
| 5.13     | SELF-ASSESSMENT EXERCISE FOR MONEY LAUNDERING RISK.....                         | 63        |
| 5.14     | SANCTIONING AND REPUTATIONAL RISKS.....                                         | 63        |
| 5.15     | COORDINATION BETWEEN THE ANTI-MONEY LAUNDERING FUNCTION AND THE OTHER CONTROL   |           |
|          | FUNCTIONS .....                                                                 | 64        |

**6 REGULATORY REFERENCES ..... 65**

6.1 FOREIGN REGULATIONS ..... 65

6.2 INTERNAL REGULATIONS..... 68

## 1 FOREWORD

Money laundering and terrorist financing are criminal actions which constitute a serious threat to the lawful economy, also since they can be transnational, and can cause destabilising effects, especially for the banking and financial system.

The changeable nature of money laundering and terrorist financing threats, facilitated also by continuous developments in technology and resources available to criminals, requires constant adaptation of the prevention and combatting controls.

The recommendations of the Financial Action Task Force (FATF) – the main international coordinating body for these matters – envisage that public authorities and the private sector identify and assess the risks of money laundering and terrorist financing to which they are exposed, in order to adopt appropriate mitigation measures.

The Guidelines on risk factors of the European Banking Authority (Guidelines on ML/TF risk factors 2021) define the risk factors that intermediaries must take into account when assessing the risk of money laundering and terrorist financing related to their activities and to individual business relationships or occasional transactions, in order to scale the mitigation measures in a manner commensurate with the risk actually identified.

The prevention and combatting of money laundering are implemented by introducing controls to ensure full awareness of the Customer, the traceability of financial transactions and the identification of suspicious transactions.

Without prejudice to the obligation to calibrate the anti-money laundering organisational structures according to the principle of proportionality and a Risk-Based Approach, the Bank of Italy Provisions on Organisation, procedures and internal controls aimed at preventing the use of intermediaries for the purpose of money laundering and terrorist financing, require the recipients to adopt at least the following minimum organisational controls:

- a) assigning the responsibility for ensuring the adequacy, functionality and reliability of anti-money laundering controls to a company control function;
- b) formalising the assignment of responsibility for the reporting of suspicious transactions;
- c) assigning the task of continuously verifying the degree of adequacy of the anti-money laundering organisational structure and its compliance with the regulations to a company control function (internal auditing function);
- d) appointing a company Representative responsible for AML (hereinafter also the "AML Representative").

Banca Mediolanum S.p.A. (hereinafter also referred to as the “**Bank**” or the “**Parent Company**”) and the Mediolanum Banking Group companies (hereinafter also the “**Group**”) are strongly committed to ensuring that the products and services offered are not used for criminal money laundering or terrorist financing, promoting a culture based on full compliance with current regulations and the effective fulfilment of passive cooperation obligations in order to guarantee greater awareness of customers, storage of documents relating to the

transactions carried out and active collaboration in identifying and reporting suspected money laundering transactions.

The Board of Directors is responsible, in particular, for identifying governance policies for these risks that are adequate with respect to the extent and type of risk profiles to which the Bank's business is actually exposed, taking into account the outcomes of the self-assessment process for money laundering and terrorism financing risks which are the prerequisite for the identification and assessment of the risks of money laundering and terrorist financing.

The CEO prepares the necessary procedures to implement these policies.

The AML Representative ensures that the Board of Directors has the information necessary to fully understand the relevance of the money laundering risks to which the Bank and the Group are exposed and that it is promptly informed of the decisions that may affect the exposure to this risk.

The AML Function continuously checks the suitability of the aforementioned procedures in order to ensure adequate monitoring of the risks, coordinating with other corporate control functions. The Internal Audit Function continuously monitors the level of adequacy of the corporate organisational structure and its compliance with reference regulations, and monitors how well the overall system of internal controls (as defined below) functions.

The AML Representative serves as a liaison between the AML Manager and the Board of Directors.

However, effective risk prevention cannot be delegated to the control functions alone, but must be carried out firstly where the risk is generated, particularly within the operating lines. The Operating Structures are therefore the first owners of the risk management process: as part of daily operations, these structures must identify, measure or assess, monitor, mitigate and report the risks arising from routine business activities in compliance with the risk management process.

In this context, financial advisors in the Sales Network are very important, along with employees of the organisational units responsible for the administration and actual management of customer relations: these parties will be responsible for monitoring operations and reporting any suspicious transactions in accordance with the guidelines prepared by the Bank.

In order to ensure effective prevention of compliance risks, it is essential that the different business structures guarantee the timely involvement of the Anti-Money Laundering Function when new products and services are being offered or there are significant changes to the products and services already offered, so that it can perform its assessments in advance.

## 1.1 REFERENCE CONTEXT

---

The "*Provisions on organisation, procedures and internal controls to prevent the use of intermediaries for the purpose of money laundering and financing of terrorism*" issued by Bank of Italy regulation dated 26 March 2019 and subsequently amended by the regulation of 1 August 2023 (hereinafter also "**Provisions**") provide for the obligation, for the corporate bodies of each recipient, to define and approve a reasoned policy which must indicate the measures that the recipient has adopted in the area of organisational structures, procedures and internal controls, due diligence and data storage.

In order to fully comply with the Provisions – issued by the Supervisory Authority pursuant to art. 7, Legislative Decree no. 231 of 21 November 2007, as amended by Legislative Decree no. 125 of 4 October 2019 and, most recently, Law Decree no. 76 of 16 July 2020 (hereinafter also “**Anti-Money Laundering Decree**”) – the Bank has adopted this policy (hereinafter also the “**Policy**”) which takes into account the uniqueness of the different members of the Group and of the risks inherent in the carried out activities, consistent with the principle of proportionality and with the actual exposure to Money Laundering Risk.

The Policy also takes into account the specific features and complexities of the operations carried out by the Parent Company and other companies of the Group, the products and services provided, the types of customers, the distribution channels used for the sale of products and services and the developments expected in these areas.

In particular, the strategy of the Bank currently aims to offer products and services on an off-premises basis to retail customers residing in Italy, through a network of authorised tied-agent financial advisors.

On a residual basis, there is the possibility of establishing banking relationships through an identification process carried out remotely by Customers, natural persons and residents, or at the Bank's main branch. The transactions of customers not associated with financial advisors are monitored, in all cases, by a special office of the Bank.

This Policy forms part of a broader System of internal Bank controls aimed at ensuring compliance with current regulations, and constitutes the base document for the entire anti-money laundering and anti-terrorism control system of the Banking Group.

In drafting this Policy, the Bank has also taken into account the outcomes of the annual process for the self-assessment of money laundering risk; future updates of the Policy will likewise take into account the outcomes of annual self-assessments conducted on each occasion.

## 1.2 SCOPE OF THE DOCUMENT

---

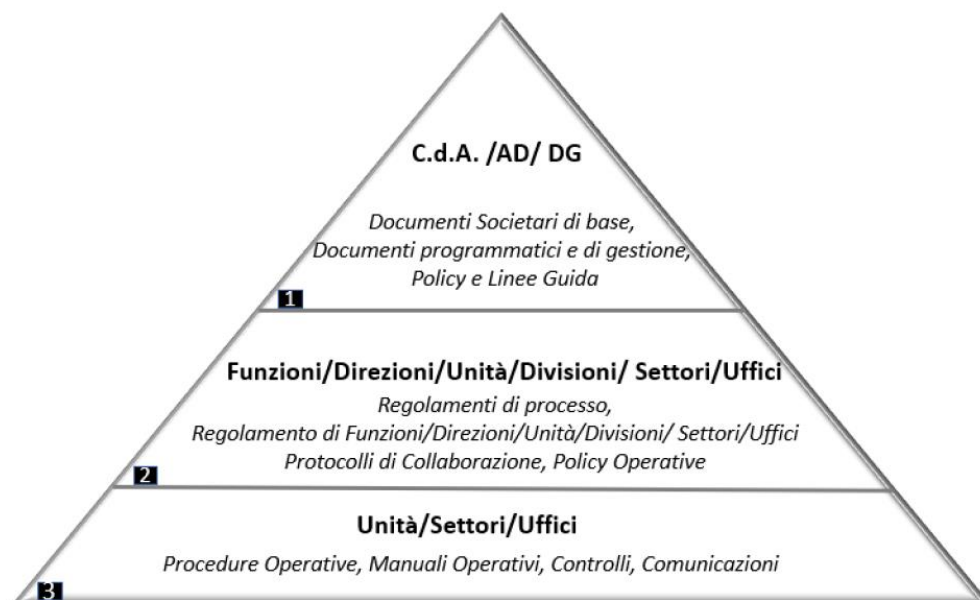
The main goal of this Policy is to define:

- the measures to actually be adopted in terms of organisational structures, procedures and internal controls, due diligence and data storage;
- the governance rules, roles and responsibilities to be adopted by the Group to combat money laundering risk;
- the Group guidelines for combatting money laundering risk, as well as the principles for the management of relationships with customers classified as high risk.

The principles stated in this Policy are reflected in the detailed internal documentation (e.g. process regulations, operating procedures, etc.) where the tasks and the operating and control activities are better described in compliance with the principles and regulations applicable to the monitoring of money laundering risk. Please refer, in particular, to the process regulations – prepared and updated by the Anti-Money Laundering Function – as regards due diligence, reporting of suspicious transactions and second level controls carried out by the Anti-Money Laundering Function which, overall, define in detail the responsibilities, tasks and operating methods applied to money laundering risk management, contained in the “Anti-Money

Laundrying Manual”. This document is at the top level of the pyramid shown in the following diagram representing the logical model of corporate regulations.

Figure 1. Model of corporate regulations



## 2 SCOPE OF APPLICATION

### 2.1 RECIPIENTS OF THE DOCUMENT

This document is approved by the Board of Directors of Banca Mediolanum S.p.A., Parent Company of the Mediolanum Banking Group, and is aimed at all personnel of the Bank, including Family Bankers®.

The policy is then sent to the Bodies with Strategic Supervision Functions of the Banking Group companies for adoption, in accordance with the standard of proportionality and taking into account local regulations and specific issues, on the basis of the following scope of application:

- to all Italian companies subject to the provisions on combatting money laundering and terrorist financing;
- to the banks and financial intermediaries of the Banking Group with offices abroad, in accordance with and compatible with local regulations in force.

This policy is also sent to the investee Mediolanum Vita S.p.A., Parent Company of the Mediolanum Insurance Group (hereinafter also “**Mediolanum Vita**”) to be taken into account when preparing its own policy, with a view to developing a global approach to money-laundering risk within the Mediolanum Conglomerate, in compliance with its specific characteristics and reference regulatory provisions.

Implementation of the guidelines and principles contained in this Policy at Group level is a first step in encouraging appropriate coordination between local anti-money laundering controls and the Bank's Anti-Money Laundering Function to ensure effective circulation of information at Group level, in order to counteract money laundering risk. The Group Chief AML Officer (as defined below) defines standards on combatting

money laundering and terrorist financing applicable at Group level and ensures that the policies and procedures adopted by each Group company comply with the applicable legislative provisions and regulations as well as the aforementioned *standards*.

The Bank, within the scope of its guiding and coordination role, can, if required by the specific operational characteristics, authorise the individual Bank Group companies to partially apply them or implement them on a gradual basis.

## 2.2 RESPONSIBILITY FOR THE DOCUMENT

---

The Policy has been approved by the Board of Directors of the Bank which will also approve any later amendments and/or updates.

The CEO defines the Policy submitted to the Board of Directors for approval, and ensures its implementation. The AML Representative monitors over time that it is adequate and proportionate, taking into account the characteristics of the Bank and the risks to which it is exposed.

The Anti-Money Laundering Function participates in the updating and periodic review of this Policy.

## 3 DEFINITIONS

### 3.1 DEFINITION OF “MONEY-LAUNDERING” AND “FINANCING OF TERRORISM”

---

The definition of “**money laundering**” adopted by the Anti-Money Laundering Decree consists of the following activities:

- a) conversion or transfer of goods carried out in the knowledge that they originate from criminal activity or from participation in such activity, in order to conceal or dissimulate the unlawful origin of the assets or to aid and abet anyone involved in such activity to avoid the legal consequences of their actions;
- b) hiding or concealment of the true nature, origin, location, placement, movement, or ownership of assets or related rights, carried out in the knowledge that these assets derive from criminal activity<sup>1</sup> or from participation in such activity;
- c) purchase, retention or use of assets with the knowledge, at the time of their receipt, that they originated from criminal activity or participation in such activity;
- d) participation in one of the acts referred to in the previous points, conspiracy to commit such an act, any attempt to perpetrate the crime, aiding abetting, incitement of or advice to somebody to commit such an act or facilitate its execution.

Money laundering is considered as such even if the actions that have generated the assets to be laundered were carried out abroad.

Money laundering is normally a three-step process:

**placement:** any proceeds from an offence, even if unintentional, obtained through a series of transactions, is collected and placed with financial and/or non-financial institutions;



- layering:** carried out by completing a series of complex financial transactions, which may appear to be unrelated to each other, aimed at hindering reconstruction of the cash flows;
- integration:** the proceeds of criminal activities re-used in the legal economy, so as to formally appear to be of legal origin.

The three steps are not static and can overlap: the use of financial institutions for criminal purposes may occur in any of the steps described above.

**“Financing of terrorism”** refers to any activity intended for the supply, collection, provision, brokerage, deposit, custody or disbursement of funds and economic resources, by any means and carried out in any manner, to be used, directly or indirectly, wholly or in part, to carry out one or more activities for terrorism purposes, according to the provisions of criminal laws, regardless of the actual use of the funds and economic resources to commit such acts.

The Ministry of Economy and Finance, at the proposal of the Financial Security Committee, issued its own decree ordering the freezing of funds and financial resources held, also through a natural person or legal entity, by a natural person or legal group or body, designated according to criteria and procedures set forth in the resolutions of the United Nations Security Council or one of its Committees.

Pending adoption of the United Nations designations, and in compliance with obligations sanctioned by the United Nations Security Council, the specific restrictive measures of the European Union and initiatives adopted by the judicial authority in criminal proceedings, the Ministry of Economy and Finance, as proposed by its Financial Security Committee, has through its own decree and for a period of six months, renewable in the same form as long as conditions are met, established national freezing measures on funds and financial resources held, also by a third party natural person or legal entity, natural persons, legal entities, groups or bodies who display or attempt to display one or more forms of terrorist conduct, according to criminal laws, or conduct designed to finance programmes for the proliferation of weapons of mass destruction or that threaten peace and national security.

The frozen funds and financial resources cannot be transferred, placed or used.

The **freezing** of “funds” and/or “economic resources” (known as a “financial embargo”) is undertaken against alleged terrorists (“designated parties”, or “natural persons, legal entities, groups and bodies designated as the targets of freezing based on European regulations and domestic legislation”), requiring financial intermediaries to restrict any movement and/or transfer, as well as any act of disposal, sale, leasing, rental, pledging of collateral, or even access in such a way as to change the volume, amount, location, ownership, possession, nature, destination or any other change that allows use of the funds, including portfolio management.

The freezing or “financial embargo” differs from a “trade embargo” related to a ban on trading with sanctioned countries, in order to isolate and place their governments in a difficult internal political and economic position.

## 3.2 GLOSSARY

---

**Due Diligence:** activities that involve:

- verifying the identity of the customer, any representative and any beneficial owner on the basis of documents, data or information obtained from a reliable, independent source;
- acquiring information on the expected scope and nature of the business relationship, and when an occasional transaction is detected in accordance with a risk-based approach;
- exercising constant control during the business relationship.

**Executive (Top Management):** a member of the Board of Directors or the General Manager or other employee Delegated by the management body or by the General Manager to maintain relations with high-risk customers; the executive has a thorough knowledge of the level of money laundering risk to which the recipient is exposed and is sufficiently independent in terms of making decisions that may impact this risk level.

**AML/CTF:** Anti-Money Laundering/Combating Terrorist Financing.

**Risk-based approach:** indicates an approach based on which competent authorities and companies identify, assess and understand the money laundering risks to which the companies are exposed and adopt preventive measures commensurate with those risks.

**Single Electronic Archive (AUI):** an archive, created and managed electronically, on which all information acquired in fulfilling the due diligence obligations is centrally stored, in accordance with the principles of the Anti-Money Laundering Decree and the implementing rules issued by the Bank of Italy.

**Institutional Activity:** activity for which the recipients have obtained registration or authorisation from a Public Authority.

**Shell Bank:** a bank (or the financial intermediary with functions similar to a bank) that does not have a significant structure in the country in which it was established and authorised to exercise its business, and is not part of a financial group subject to effective supervision on a consolidated basis.

**Beneficiary of insurance services:**

- 1) a natural person or entity who, on the basis of the designation made by the contracting party or the insured party, has the right to receive insurance benefits paid by the insurance company;
- 2) any natural person or entity to which payment is made by order of the designated beneficiary.

**Customer(s):** the party establishing a business relationship or carrying out transactions with financial intermediaries or other financial sector operators and with other obliged parties pursuant to the Anti-Money Laundering Decree, normally also identified with other terms such as users, investors, insured parties, contracting parties, buyers, borrowers, etc.

**Compliance Risk:** a specific obligation, required under a given regulation, not to incur legal or administrative sanctions, significant pecuniary loss or damage to reputation resulting from infringements of mandatory provisions (laws and regulations) or self-governance provisions (e.g. code of conduct, self-governance code).

**Freezing of funds:** the prohibition, by virtue of European regulations and domestic legislation, against the movement, transfer, modification, use or management of funds or access to such funds, so as to change the

volume, amount, placement, ownership, possession, nature, destination or any other change that allows use of the funds, including portfolio management.

**Freezing of economic resources:** the prohibition, due to EU laws and national laws, of the transfer, disposal or use of economic resources in order to in any way obtain funds, goods or services, use of economic resources, including for example the sale, lease, rental or pledging of collateral.

**Financial conglomerates:** groups of companies, significantly active in the insurance, banking or investment services sectors, which include at least an insurance company and a company operating in the banking or investment services sectors, and are controlled by a regulated company or carry out activities primarily within the financial sector; for the purpose of this document, please refer to the Financial Conglomerate under the control of Banca Mediolanum S.p.A.

**Correspondent accounts and similar accounts:** accounts held by the banks to settle interbank services and other relationships of any nature, between credit and financial institutions, used to settle transactions on behalf of the customers of the corresponding entities.

**Through accounts:** cross-border correspondent bank accounts between banking and financial intermediaries, used to carry out transactions on their own account or on behalf of customers.

**Line controls (first level controls):** all the controls aimed at ensuring that transactions are properly carried out. These are performed by the Operating Structures themselves (e.g. hierarchical, systematic and sample controls), also through units exclusively responsible for performing control or monitoring tasks and that report to the managers of the Operating Structures, or are carried out as part of back office activities. As far as possible, they are incorporated into the IT procedures.

**Controls on risks and compliance (second level controls):** the set of controls that aim to ensure, inter alia:

- correct implementation of the risk management process;
- compliance with the operating limits assigned to the various functions;
- compliance of corporate operations with all provisions of the law, including self-governance provisions.

The functions responsible for these controls are separate from the operating functions. They help define the risk governance policies and the risk management process.

**Counterparty:** natural persons and legal entities that initiate business relations (other than long-term contractual relationships forming part of the exercise of institutional activities by financial intermediaries or financial sector operators) with the Bank or a Mediolanum Group Company (even if not subject to the obligations set out in the Anti-Money Laundering Decree).

**Cover Payment:** the transfer of funds used when there is no direct relationship between the payment service provider (PSP) of the ordering party and the beneficiary, and therefore a chain of correspondent accounts through a PSP has to be used. Three or more PSPs are involved in a cover payment.

**Identification data of the customer, related beneficial owner and representative:** the name and surname, place and date of birth, registered residence and, if different, the correspondence address and, where assigned, the tax code of the customer, and where assignment is envisaged, also the related beneficial owner and representative. For parties other than a natural person, the name, registered office, enrolment number in the register of companies or in the register of legal entities, where required.

**Identification data of the beneficiary, related beneficial owner and representative:** name, surname, place and date of birth. For parties other than a natural person, the name, registered office, enrolment number in the register of companies or in the register of legal entities, where required. In both cases, at the time of payment of the benefit, also the place of residence and, if different, the correspondence address, the tax code of the Beneficiary and, if such assignment is required, also of the related beneficial owner and representative.

**Cash:** banknotes and coins, in Euro or foreign currencies, that are legal tender.

**De-risking:** the refusal to enter into business relationships or the decision to terminate business relationships with individual Customers or categories of Customers associated with a higher money-laundering risk or the refusal to carry out transactions characterised by a higher money laundering risk.

**Employee:** all Banca Mediolanum employees who belong to the organisational units and/or the local and/or central structures.

**Embargoes:** measures of partial or complete interruption or reduction of economic and financial relations with one or more Third Countries.

**Representative:** the party authorised to act in the name and on behalf of the customer (or the beneficiary of the insurance service) or in any event granted powers of representation that allow it to operate in the name of and on behalf of the customer (or of the beneficiary of the insurance service).<sup>1</sup>

**AML Representative:** the member of the management body responsible for anti-money laundering matters, who is the main point of contact between the Head of the AML Function and the Bodies with strategic supervision and management functions, as identified by the Provisions of the Bank of Italy on the organisation, procedures and internal controls aimed at preventing the use of intermediaries for the purpose of money laundering and terrorist financing, in enforcement of the EBA Guidelines on internal policies and procedures for the management of AML compliance and on the role of the AML Manager.

**Risk factors:** indicate the variables which, individually or combined, can increase or reduce the money laundering risk deriving from individual business relationships or occasional transactions.

**Family Banker®:** the financial advisors of Banca Mediolanum authorised to operate off-premises, in accordance with art. 31, paragraphs 1 and 2, Legislative Decree no. 58 of 24 February 1998 (Consolidated Finance Act).

**Funds:** financial assets and benefits of any nature, also held through third parties who can be natural persons or legal entities, including for example:

- cash, cheques, monetary receivables, bills of exchange, payment orders and other payment instruments;
- deposits with financial entities or other parties, account balances, receivables and bonds of any nature;
- public or private negotiable instruments and financial instruments as defined in art. 1, paragraph 2 of the Consolidated Finance Act, Legislative Decree no. 58 of 24 February 1998;

---

<sup>1</sup> Parties appointed by a public authority to the management of assets of and relationships with the customer or with parties acting on their behalf (for example, official receivers) are considered Representatives.

- interest, dividends or other income and increases in value generated by the assets;
- credit, netting rights, guarantees of any nature, security deposits and other financial commitments;
- letters of credit, bills of lading and other securities representing commodities;
- documents showing investments in funds or financial resources;
- all other export credit instruments;
- life insurance policies pursuant to art. 2, paragraph 1, Legislative Decree no. 209 of 7 September 2005, the Private Insurance Code.

**Anti-Money Laundering Function:** function which is an integral part of the second level internal control system, in charge of preventing and combatting money laundering and terrorist financing, and preventing related transactions.

**Group AML Function:** the organisational structure at Group level, equipped with sufficient decision-making power, used by the Group Chief AML Officer for the purpose of carrying out his or her duties, in accordance with the principle of proportionality and applicable national legislation.

**Company Control Functions:** the Compliance Function, the Risk Management Function, the Anti-Money Laundering Function and the Internal Audit Function.

**Compliance Function:** *the function, an integral part of the second-level Internal Control System, entrusted with the specific task of overseeing, according to a risk-based approach, the management of the risk of non-compliance with respect to the company's activities, by ensuring that procedures are suitable for preventing said risk and, in order to oversee specific regulatory areas, for which forms of specialised oversight are required, making use of suitable and predefined Specialist Units, tasked with overseeing specific phases of the compliance process.*

**Control Functions:** the Corporate Control Functions, the Financial Reporting Manager, the Director responsible for Controls, the Independent Auditor, the Supervisory Body established pursuant to Legislative Decree 231/01 and the Data Protection Officer.

**Internal Audit Function:** the function entrusted with the monitoring, within the scope of third level controls, also with on-site audits, of the regular performance of operations and development of risks, and with assessing the completeness, adequacy, functionality and reliability of the organisational structure and other components of the Internal Control System, bringing to the attention of the corporate bodies possible improvements, with particular reference to the Risk Appetite Framework (RAF), the risk management process and related measurement and control tools. Based on the results of its controls, it puts forward recommendations to the corporate bodies. In addition, taking into account the Group's business model, particular attention is paid to controlling the operations carried out by the sales networks.

**Risk Management Function:** an integral part of the level two Internal Control System, the function entrusted with the responsibility of implementing governance policies and the risk management system, and that cooperates in defining and implementing the RAF while guaranteeing an integrated view of the various risks to the Company Bodies when exercising the control function.

**FATF:** The Financial Action Task Force, a body set up by the OECD, specialising in preventing and combatting money laundering, terrorist financing and the proliferation of weapons of mass destruction.

**Group:** the Mediolanum Banking Group, as governed by art. 60 of the Consolidated Finance Act and all applicable provisions.

**Anomaly indicators:** cases representing anomalous operations or conduct implemented by customers, used to facilitate the assessment, by the obliged parties, of any suspicions of money laundering or terrorist financing.

**Insurance intermediaries:** natural persons or companies with residence or registered office in Italy – enrolled in the single electronic register of insurance intermediaries in compliance with art.109, paragraph 2, letters a), b) and d) of the Code – as well as natural persons or companies with residence or registered office in another Member state of the European Union or in another country in the European Economic Area or a third country, operating in Italy as permanent establishments and included in the list annexed to the register after notification pursuant to articles 116-quater and 116-quinquies of the Code – limited to the distribution, within Italy, of insurance products of the business activities listed in art. 2, paragraph 1, of the Code.

**Means of payment:** cash, bank cheques and postal cheques, banker's drafts and other similar or equivalent cheques, postal orders, credit or payment orders, credit cards and other payment cards, transferable insurance policies, lien policies or other instruments available that allow for the transfer, movement or purchase, including electronically, of funds, securities or financial resources.

**Operations:** the activity requested from the recipient or recognised by the same as part of the opening or performance of a business relationship, or the execution of one or more transactions.

**Remote operations:** operations performed without the customer or personnel assigned by the Bank being physically present. When the customer is not an individual, the customer is considered present when the representative is present.

**Transaction:** the movement, transfer or transmission of means of payment or the trading of assets; a transaction is also the stipulation of an agreement involving assets as part of the exercise of a professional or commercial activity.

**Related transactions:** transactions related to each other, executed to pursue a single goal of a legal nature.

**Split transaction:** a single transaction, from an economic viewpoint, of an amount equal to or higher than the limits established by the Anti-Money Laundering Decree, executed through multiple transactions, individually lower than the above-mentioned limits, carried out at different times and over a certain period of time set as seven days, without prejudice to the existence of the split transaction when the elements to consider it so are present.

**Occasional transaction:** a transaction that is not related to a business relationship in place; an occasional transaction also comprises an intellectual or commercial service, including those that can be carried out instantly, provided to the customer.

**Suspicious Transaction:** operations to report to the FIU when the recipients know, suspect or have reasonable grounds to suspect that money laundering or terrorism financing transactions have been carried out or have been attempted, or that, in any case, the funds derive from criminal activities. The suspicion arises from the characteristics, size and nature of the transactions, their linking or splitting or any other circumstance discovered by reason of the functions exercised, taking into account the economic capacity and the activity carried out by the party to which it refers, based on the elements acquired pursuant to the AML Decree.

**Corporate bodies:** the bodies responsible for strategic supervision (Board of Directors), management (CEO or other management body) and control (Board of Statutory Auditors).

**Non-profit organisations:** a legal person or legal institution or organisation that is mainly engaged in the collection or disbursement of funds for charitable, religious, cultural, educational, social or solidarity purposes.

**Body with control functions:** body responsible for assessing the correctness of administrative activities as well as the suitability of the organisational and accounting structures of the Company; in the different models, the Board of Statutory Auditors, the Supervisory Committee and the Management Control Committee are the bodies with control functions (or Control Bodies).

**Body with management function:** corporate body or its members, responsible for or delegated to management tasks, i.e. the implementation of guidelines issued by the strategic supervisory function. The General Manager is the head of the internal structure and as such participates in the management function.

**Body with strategic supervisory function:** body responsible for all guidance and/or supervision of corporate management (e.g., through the examination and approval of business or financial plans or the strategic transactions carried out by the Company).

**Origin of funds:** indicates the origin of funds specifically used in a business relationship or occasional transaction.

**Origin of assets:** indicates the origin of the customer's total assets, including transferable securities and property.

**EU countries:** countries belonging to the European Economic Area.

**Countries subject to embargo:** Countries for which there is any economic or commercial sanction (with the exception of the administrative sanctions of local authorities) or restrictive measure promulgated, applied, imposed or enforced by the "Office of Foreign Assets Control" (OFAC) of the US Department of the Treasury, the US Department of State, the UN Security Council and/or the European Union and/or any authority of the Italian Republic including the Italian Revenue Agency (Agenzia delle entrate), or by any other authority competent in matters of sanctions.

**Third countries:** countries not belonging to the European Economic Area.

**High-risk third countries:** countries not belonging to the European Union with strategic gaps in their respective national regulatory frameworks to prevent money laundering and terrorism financing, as identified by the European Commission in exercising the powers governed by articles 9 and 64 of the Anti-Money Laundering Directive IV (AMLD IV).

**Personnel:** the employees and those who operate based on relationships that result in their inclusion in the organisation of the obliged party, also in a form other than as an employee, including the financial advisors authorised to operate off-premises, pursuant to art. 31, paragraph 2, of the Consolidated Finance Act, as well as direct producers and intermediaries pursuant to art. 109, paragraph 2, letters c) and e), CAP.

**Politically Exposed Persons (PEPs):** the natural persons indicated in art. 1, paragraph 2, letter dd) of the *Anti-Money Laundering Decree*, or "natural persons who hold or have ceased to hold, for less than one year,

important public offices, as well as their family members and those closely related to these persons, as listed below:

1) *natural persons who hold or have held important public offices are those who hold or held the office of:*

*1.1 President of the Republic, Prime Minister, Minister, Deputy Minister and Under-secretary, President of the Region, Regional Councillor, Mayor of the Provincial capital or metropolitan city, Mayor of a Municipality with a population of not less than 15,000 inhabitants, or similar offices in foreign countries;*

*1.2 Member of Parliament, Senator, Member of the European Parliament, regional councillor or similar offices in foreign countries;*

*1.3 member of political party executive bodies;*

*1.4 judge of the Constitutional Court, judge of the Court of Cassation or the Court of Auditors, State councillor or other members of the Council of Administrative Justice for the Sicily Region or similar offices in foreign countries;*

*1.5 member of the governing bodies of central banks or independent authorities;*

*1.6 ambassador, chargé d'affaires or equivalent offices in foreign countries, senior officer in the armed forces or similar offices in foreign countries;*

*1.7 member of the board of directors, management body or control body of companies controlled directly or indirectly by the Italian State or by a foreign country or investees, to a substantial or total extent, of the Regions, main Provincial municipalities or metropolitan cities or municipalities with a population of not less than 15,000 inhabitants;*

*1.8 director general of local health authorities or hospitals, university hospitals or other national health service entities.*

*1.9 manager, deputy manager or member of the governing body or party carrying out equivalent functions in international organisations;*

2) *family members of politically exposed persons: parents, spouse or civil partner or de facto partner or similar situations of the politically exposed person, the children and their spouses as well as persons in civil or de facto partnerships or similar situations with the children;*

3) *persons with whom the politically exposed persons are presumed to have close ties include:*

*3.1 individuals linked to the politically exposed person due to the joint beneficial ownership of legal entities (including trusts and similar legal arrangements) or who have other close business relationships with the politically exposed person;*

*3.2 natural persons who only formally hold total control of an entity commonly known to have been established, on a de facto basis, in the interests and to the benefit of a politically exposed person.*

**Anti-money laundering Policy or the Policy:** the document defined by the body with management functions and approved by the body with strategic supervisory functions, pursuant to the "Provisions on organisation, procedures and internal controls aimed at preventing the use of intermediaries for the purpose of money-laundering and financing of terrorism", adopted by the Bank of Italy.



**PSP:** Payment Service Provider.

**Account Information Service Providers (AISPs):** a Payment Service Provider that provides services of information on accounts, or online services that provide consolidated information on one or more payment accounts held by the payment services user with another Payment Service Provider or with multiple Payment Service Providers.

**Digital portfolio service providers:** any natural person or legal entity providing services to third parties, on a professional basis, also online, for the safeguarding of private encryption keys on behalf of its customers, in order to hold, store and transfer virtual currencies.

**Providers of services related to the use of virtual currency:** any natural person or legal entity providing services to third parties, on a professional basis, related to the use, exchange or custody of virtual currencies and their conversion from or into legal tender currencies.

**Business and trust-related service providers:** any natural person or legal entity which, on a professional basis, provides one of the following services to third parties:

- establishing companies or other legal entities;
- acting as manager or director of a company, a partner in an association or a similar position with respect to other legal entities or arranging for another person to hold such a position;
- providing a registered office, business, administrative or postal address and other services related to a company, association or any other legal entity;
- acting as trustee in an express trust or similar legal entity or arranging for another person to hold such a position;
- exercising the role of shareholder on behalf of another person or arranging for another person to do so, provided that it is not a company listed on a regulated market and subject to disclosure obligations in accordance with EU regulations or equivalent international regulations.

**business relationship:** a long-term relationship that falls within the exercise of business activities carried out by obliged parties, which is not completed in a single transaction.

**Remote accounts or transactions:** indicates any transaction or account in which the customer is not physically present or is not in the same physical location as the company or person acting on behalf of that company. This includes situations where the customer's identity is verified via video call or similar technology.

**Risk appetite:** With reference to money-laundering risk, both quantitative indicators (e.g. the percentage of customers classified as 'high risk' out of total customers) and qualitative elements (e.g. limitations and restrictions set out in this Policy) may be considered for the purposes of Risk Appetite.

**Money-laundering risk:** the risk arising from a breach of legal, regulatory and self-governance provisions, functional to preventing 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, as well as the risk of involvement in instances of money laundering and financing of terrorism or financing of programmes for the development of weapons of mass destruction.

**Inherent risk:** qualifying as “potential” risk, this refers to the likelihood of the Company suffering direct or indirect damage involving sanctions, penalties, financial or reputational harm, without considering the organisation and the functionality of its monitoring systems and the more general Internal Control System.

**Residual risk:** a summary assessment which takes into account the assessment of the suitability of organisational monitoring, procedural and control systems in place, resulting in the identification of corrective measures to be implemented to mitigate such risk.

**Financial resources:** tangible or intangible assets of any nature and transferable securities or property, including accessories, appurtenances and related income, that are not funds but could be used to obtain funds, goods or services, owned, held or controlled, including partially, directly or indirectly, or through third-party natural persons or legal entities, by designated parties, or by natural persons or legal entities acting on behalf or under the guidance of the latter.

**Sanction lists/lists of sanctioned parties/lists of designated parties:** lists of names of sanctioned parties disseminated by the United Nations Security Council, the European Union and the OFAC.

**Financial Sanctions:** restrictive measures used to counter the activity of States, individuals or organisations that threaten international peace and security and consist IN freezing funds and economic resources owned by persons or organisations of a foreign country and therefore prohibiting their disposal.

**International sanctions:** restrictions of an economic, financial and administrative nature, imposed from time to time, by the Italian and European regulations, by the UN Security Council or by the United States, which include (but are not limited to) embargoes and the freezing of assets.

**Sherpany:** platform adopted by the Corporate Affairs Division to manage the meetings of the Corporate Bodies, which allows secure access to the various documents both online and offline, made available by the various company functions.

**S.I.G.M.A.:** Information System for the Management of Weapon Materials, supporting the institutional operations of Office VI, Department V of the MEF Department of Treasury which, along with a specific team of the Guardia di Finanza and based on the provisions of Italian Law no. 185 of 9 July 1990, as amended by Italian Legislative Decree 105/2012, monitors the activities of credit institutions regarding the financing of transactions governed by Italian Law no. 185/90, for the purpose of combatting terrorism.

**Internal Control System:** the set of rules, functions, structures, resources, processes and procedures that aim to ensure the following, in accordance with the principles of sound and prudent management:

- assessment of the implementation of corporate strategies and policies;
- containment of risk to within the limits set out in the reference framework for determining the risk appetite of the Bank (Risk Appetite Framework - “RAF”);
- protection of the value of assets and protection against losses;
- effectiveness and efficiency of corporate processes;
- reliability and security of corporate information and IT procedures;
- prevention of the risk that the Bank may be involved, even unintentionally, in illegal activities (especially those related to money laundering, usury and terrorist financing);

- compliance of all transactions with the law and supervisory regulations, as well as with internal policies, regulations and procedures.

**Designated Persons:** any person (natural or legal) featuring on an official list of international sanctions.

**Operating Structures:** all remaining organisational units envisaged by the company, which are not Corporate Bodies or Control Functions.

**Beneficial Owner:** natural person(s), other than the customer, in the ultimate interests of whom the business relationship is established, the professional service is provided or the transaction is executed.

**Virtual currency:** the digital representation of value, not issued by a central bank or a public authority, not necessarily related to a currency of legal tender, used as a medium of exchange for the purchase of goods and services and electronically transferred, stored and traded.

**AML WorkFlow:** operational platform, uses by the AML Function, to manage the processes of instruction, assessment and archiving of Evidence and Unexpected Operations and of any Suspicious Transactions, as well as by the AML Operational Control Unit, for the management of Enhanced Due Diligence

#### 4 ANTI-MONEY LAUNDERING MODEL GOVERNANCE

This model to combat money laundering risk is managed at Group level through a specific process aimed at implementing and maintaining rules, procedures and organisational structures that can ensure the prevention and management of the risk in question, by all Group companies.

The model envisages that the primary responsibility in terms of monitoring money laundering risk is assigned to the Corporate Bodies of each company of the Group, according to their respective duties, and in compliance with Parent Company directives. The distribution of tasks and responsibilities money laundering risk monitoring by the corporate bodies and functions must be clearly defined in each company.

In line with eligible corporate governance principles, for each Group company the model acknowledges the central role of the Board of Directors as regards the policies governing the risk in question: the Board is responsible for approval of the anti-money laundering policy as envisaged in the Provisions (in line with the principles of this Policy) and for the adoption of a system suited to the characteristics of the company; to this end, its organisation must be able to address the issue of money laundering risk as carefully as possible and with the necessary level of detail.

The Body with management function is responsible for ensuring implementation of the strategic guidelines and money-laundering risk governance policies approved by the Body with strategic supervisory authority, and is responsible for the adoption of all measures necessary to ensure the effectiveness of the organisation and of the anti-money laundering control system.

The Body with control function, within the scope of its responsibility to oversee compliance with regulations and the completeness, suitability, functionality and reliability of the internal control system, is also constantly in touch with the Anti-Money Laundering Function.

Each Group company is required to appoint - according to the principle of proportionality - its own AML Representative.

An effective organisational structure for monitoring money laundering risk is also based on significant involvement of all Operating Structures and corporate functions, and on the clear definition of their duties and responsibilities. In that context, the role of line controls ("first level controls"), aimed at ensuring the correct performance of transactions, through suitable controls and IT systems, is of fundamental importance.

In compliance with the proportionality principle and if envisaged in the specific reference regulations, each Group company must set up a specific Anti-Money Laundering Function in charge of monitoring money laundering risk.

In order to achieve appropriate synergies and economies of scale, using highly specialised centres of expertise, the Banking Group and Insurance Group companies may delegate to the Parent Company – based on specific outsourcing agreements, drawn up in compliance with supervisory regulations, and in compliance with the principles stated in the "Corporate outsourcing policy" – the performance of tasks specific to the Anti-Money Laundering Function pursuant to current regulations.

Such agreements must also govern the following aspects:

- the objectives of the Function and the content of the outsourced activities;
- the expected service levels;
- the minimum frequency of information flows;
- confidentiality obligations about information acquired in exercise of the function or the activities;
- the possibility of reviewing the service terms in the case of changes in the operations and organisation of the Company.

The Group companies appoint their own Head of the AML Function as well as the Suspicious Transaction Reporting Manager who must ensure compliance with the requirements on anti-money laundering and countering the financing of terrorism, in line with the principles established in this Policy (as defined below).

The subsidiary Mediolanum Vita – parent company of the Mediolanum Insurance Group – sets up its own Anti-Money Laundering Function, and appoints a Manager of this Function and a Suspicious Transaction Reporting Manager. Mediolanum Vita approves its own Policy that defines the actual measures adopted in terms of organisational structures, procedures and internal controls, due diligence and data storage, in line with the principles contained in this Policy and consistent with the regulatory provisions specific to its sector.

From a Group perspective, good workload organisation and circulation of information are crucial, ensuring that any intercompany issues related to the provisions on anti-money laundering and combatting terrorist financing are discussed with the support of appropriate preparatory work, the outcome of which will also be submitted to the Risk Committee of the Parent Company.

As part of the Group guidance and coordination activities, the Corporate Bodies of the Bank (in its capacity as Parent Company) adopt the strategic guidance on money laundering risk management and anti-money laundering controls.

The Parent Company:

- ensures that the corporate bodies and internal structures of each member of the Group, including the control functions, have the information they need to carry out the related tasks;

- defines and approves Group policies and procedures on AML that include: (a) a group methodology for the assessment of money laundering risks in conformity with that indicated in the Provisions; (b) formalised procedures for the coordination and sharing of relevant information between the companies belonging to the Group and a direct reporting line between the Managers/Representatives/Contacts of the AML Functions of the members, including international, of the Group and the Group Chief AML Officer; (c) general standards on customer due diligence, data storage and identification and reporting of suspicious transactions; (d) AML control procedures at Group level;
- guarantees that the Group companies based in Italy promptly implement the corrective measures necessary to overcome the shortcomings in the anti-money laundering controls identified by the Bank of Italy, IVASS, FIU or, in relation to Group companies based abroad, by the competent Authorities.

For the pursuit of the aforementioned purposes, the Parent Company appoints a Group Chief AML Officer, who - among other things - verifies that the policies and procedures of the Group members are in line with the standards defined by the Parent Company as well as compliant with the applicable laws and regulations on anti-money laundering.

In order to pursue a full and concrete implementation of the Group model, the consolidated subsidiaries adopt a Policy consistent with the principles and guidelines described in this Policy, according to a principle of proportionality and based on the specific nature of their activities.

Pursuant to the Provisions in force, in order to increase the standardisation of due diligence on common customers of the Group, and to increase its capacity to prevent and manage money laundering risk, the Parent Company is required to establish – through the creation of a centralised register – a shared database that allows all the Group companies to perform customer due diligence in a standardised manner.

In implementing the above, based on the principle of a risk-based approach, the Bank establishes a shared database for use by all the companies under its direct or indirect control, in which information concerning a customer with a high money laundering risk (e.g. a customer subject to a prior report to the FIU) is shared, maintained and properly updated.

The Anti-Money Laundering Function identifies additional types of information that may be shared where there are placement/distribution relationships (or other significant business relationships) between the Parent Company and the individual subsidiaries (or among the subsidiaries).

The Parent Company adopts suitable technical and organisational measures to guarantee that the data on the shared database is processed in compliance with current national regulations on personal data protection.

The Anti-Money Laundering Functions of the subsidiaries activate appropriate information flows - at least quarterly - to the Group Chief AML Officer regarding the main activities performed, the outcomes of controls and the main initiatives undertaken in order to eliminate any confirmed malfunction.

As regards Banca Mediolanum, the Manager of the Group Anti-Money Laundering Function must in all cases be promptly informed of the results of control activities carried out by companies in the Financial Conglomerate, as well as on any significant event, including reports and inter-relations with the competent Authorities.

## 4.1 PARENT COMPANY BANCA MEDIOLANUM S.P.A.<sup>2</sup>

---

In line with the Provisions, the duties and responsibilities for mitigating the risk of the Bank's involvement in money laundering or terrorist financing will first be referred to the Corporate Bodies.

In particular, the Board of Directors is responsible for determining governance policies for Money laundering risk that are adequate with respect to the extent and type of risk profiles to which the Bank and Group activities are actually exposed. In this perspective, it will carry out its functions with reference not only to the Bank, but also assessing the overall operations of the Group and the risks to which it is exposed. The Chief Executive Officer prepares the procedures necessary to enforce these policies. The AML Representative acts as a liaison between the Head of the AML Function and the Board of Directors and ensures that this body has the information necessary to fully understand the relevance of the money-laundering risks to which the Bank is exposed. continuously check the suitability of the procedures to ensure adequate monitoring of the risk in question, coordinating with the other Corporate Control Functions. The Group Chief AML Officer ensures that the companies belonging to the Group implement the Group's strategies and policies on AML. The Internal Audit Function continuously monitors the level of adequacy of the corporate organisational structure and its compliance with reference regulations, and monitors how well the overall system of internal controls functions.

However, effective risk prevention cannot be delegated to the control functions alone, but must be carried out firstly where the risk is generated, particularly within the Operating Structures and Sales Network, which are the main responsibility of the risk management process.

The model to combat money laundering and terrorist financing therefore envisages involvement of the corporate bodies and Operating Structures of each Group company and the Sales Network, in accordance with the distribution of roles and responsibilities indicated below.

### **Board of Directors**

The Board of Directors is responsible for supervising and checking the enforcement of the internal governance and internal control framework, in order to ensure compliance with the applicable requirements in the context of ML/TF prevention. In particular:

- approves and periodically reviews the strategic guidelines and governance policies for risks related to money laundering and financing of terrorism;
- approves this Policy and is responsible for its periodic review, in order to ensure its effectiveness over time;
- approves the establishment of the Anti-Money Laundering Function, identifying its tasks and responsibilities as well as the methods to be used for coordination and collaboration with the other Corporate Control Functions;
- assesses, at least once a year, the actual functioning and activities of the AML Function, taking account, inter alia, of the conclusions of all the audit activities carried out, also in relation to the

---

<sup>2</sup> The main attributes on compliance with regulations governing anti-money laundering and anti-terrorism are listed below. Please refer to the internal rules on corporate governance for a full analysis of the duties.

adequacy of human resources and techniques assigned to the Head of the AML Function (as defined below);

- approves the guidelines of a systematic and coordinated Internal Control System, essential for the prompt identification and management of money laundering risk and ensures periodic reviews in order to guarantee their effectiveness over time;
- approves the principles for the management of relationships with customers classified as 'high risk';
- continuously ensures that the tasks and responsibilities involved in money laundering risk monitoring are allocated in a clear and appropriate manner, guaranteeing that the Operating Structures and Control Functions are kept separate and provided with adequate qualitative and quantitative resources;
- ensures that an adequate, complete and prompt system of reporting to the Corporate Bodies and among the Control Functions, is prepared, as well as a system for sharing documentation that allows the corporate bodies direct access to the reports of the control functions on AML matters, to the relevant communications with the Authorities and supervisory measures taxes or sanctions imposed;
- ensures that the shortcomings and anomalies identified during the controls at various levels are promptly brought to its attention, and promotes the adoption of appropriate corrective measures of which it assesses the effectiveness;
- ensures the preservation of confidentiality in the suspicious transaction reporting procedure;
- at least on an annual basis, examines the report issued by the Anti-Money Laundering Function Manager on the audit activities carried out, on initiatives undertaken, malfunctions identified and related corrective actions to be applied, as well as on training activities for personnel and members of the sales network, and lastly on communications submitted by the Board of Statutory Auditors and/or by the Supervisory Body; if these communications refer to breaches considered significant, the Anti-Money Laundering Function Manager also provides all related information at the next available meeting;
- receives, including more than once a year, specific updates on the activities considered to be at higher risk of money laundering or terrorist financing;
- at least on an annual basis, examines the report on results of the self-assessment of money laundering risk, carried out by the Anti-Money Laundering Function;
- assesses the risks related to operations carried out with third countries associated with high risks of money laundering, and identifies the measures for mitigating them, monitoring their effectiveness;
- appoints the AML Representative and ensures that the same meets the conditions set forth in the Provisions;
- ensures that the AML Representative is promptly informed of decisions that may affect the Bank's exposure to money laundering risk;
- after consulting the Board of Statutory Auditors, appoints and revokes the Anti-Money Laundering Function Manager and the Suspicious Transaction Reporting Manager;
- defines and approves the criteria for coordinating and managing the Group companies, and for determining the criteria for the execution of instructions issued by the Bank of Italy.

### **Risk Committee**

The Risk Committee provides support to the Board of Directors regarding risks and the internal control system. With specific reference to money laundering risk monitoring:

- assists the Board of Directors by expressing its opinion, at least annually, on the compliance, suitability and actual functioning of the Internal Control System, the corporate organisation and the requirements that must be met by the Corporate Control Functions, and ensures that they are fully compliant with the directives and guidelines issued by the Board of Directors;
- brings any weaknesses detected to the attention of the Board of Directors, recommending appropriate corrective actions and ensuring that the main business risks are identified, measured, managed and monitored adequately. In particular, it expresses an opinion on the qualitative and quantitative adequacy of the Anti-Money Laundering Function, and whether it sufficiently independent;
- assists the Board of Directors in determining corporate “guidelines” and “policies” on risks and the internal control system, also consistent with the predefined risk appetite. In particular, it formulates proposals regarding:
  - the exercise methods for strategic control, management and technical-operational activities with respect to individual companies and the Group;
  - the control structure of the Group, with particular reference to the centralisation choices of specific control functions in accordance with supervisory regulations;
  - the organisational model to support Control Functions, the guidelines on respective activities necessary for the determination of related regulations, and coordination of the various functions;
- makes a prior examination of the action plan and annual report of the Anti-Money Laundering Function, and periodic reports relating to assessment of the internal control and risk management system, including the results of the self-assessment of money laundering and terrorist financing risks carried out by the Anti-Money Laundering Function, and those of particular importance prepared by the Internal Audit Function or by the Board of Statutory Auditors. If necessary, it can ask the Internal Audit Function to carry out checks on specific operating areas, at the same time informing the Board of Directors and the Board of Statutory Auditors;
- has access to all information and data received from the Company Control Functions for the purpose of carrying out their duties.

### **Board of Statutory Auditors**

With specific reference to money laundering risk monitoring, the Board of Statutory Auditors:

- monitors compliance with regulations and the completeness, function and adequacy of anti-money laundering controls, using the internal structures to perform the checks and assessments necessary, and using information flows from the other Corporate Bodies, the Anti-Money Laundering Function Manager and the other Corporate Control Functions. In this context:
  - it carefully assesses the suitability of procedures in place to carry out customer due diligence, record and keep the information and report on suspicious transactions;
  - analyses the reasons underlying any shortcomings, anomalies or irregularities found and encourages the adoption of suitable corrective measures;



- expresses an opinion on the appointment and revocation of the Anti-Money Laundering Function Manager and the Suspicious Transaction Reporting Manager;
- its opinion is sought on the definition of elements of the overall architecture of the management and control system for money laundering risk;
- monitors compliance with provisions of the Decree to the extent of its responsibilities and duties;
- promptly informs the Bank of Italy of all facts emerging while exercising its functions that could qualify as serious, repeated, systematic or multiple violations of applicable laws and related implementing provisions;
- forwards to the Suspicious Transaction Reporting Manager, any reports of transactions independently detected in the performance of its duties.

### **Supervisory Board**

The Supervisory Board provides a prior contribution to the definition of the Organisation, Management and Control Model pursuant to Legislative Decree 231/2001, and continuously monitors compliance with the processes envisaged in the Decree. If a predicate offence is committed, it analyses the causes to identify the most suitable corrective measures. In order to carry out these activities, the Supervisory Board will receive suitable information flows from the various corporate functions and will have unlimited access to all information required to carry out its duties.

The Supervisory Board will also send any reports of suspicious transactions found independently during the exercise of its duties to the Suspicious Transaction Reporting Manager.

### **Chief Executive Officer**

The Chief Executive Officer, also as the AML Representative where appointed:

- ensures the implementation of the strategic guidelines and governing policies on money laundering risk, approved by the Board of Directors, and is responsible for the adoption of all measures necessary to ensure the efficacy of the organisation and the anti-money laundering control system;
- for the purposes of the above, examines the proposals for organisational and procedural interventions presented by the Head of the AML Function and formalises any decision not to accept them, giving reasons;
- ensures periodic communication to the Board of Directors on the activities performed by the Head of the AML Function as well as the transmission to the same Body of sufficiently comprehensive and timely information and data on risks relating to money laundering and terrorist financing;
- informs the Board of Directors of any serious or significant violations of money laundering and terrorist financing and recommends the related corrective actions;
- ensures that the Head of the AML Function (i) has direct access to all the information necessary for the fulfilment of his/her duties, (ii) has human and technical resources and sufficient tools to be able to adequately perform the tasks assigned to him/her and (iii) is informed of incidents and shortcomings identified by internal control systems and supervisory authorities;
- in preparing operating procedures, takes into account the recommendations and guidelines issued by the competent authorities and international bodies;

- defines and ensures the implementation of an internal control system that can readily detect and manage money laundering risk and ensures its continued effectiveness over time, in compliance with the results of the risk self-assessment;
- ensures that the operating procedures and information systems allow the correct fulfilment of customer due diligence and document and information storage obligations;
- as regards the reporting of suspicious transactions, defines and ensures the implementation of a procedure suited to the specific nature of the activities, size and complexity of the Bank, according to the proportionality principle and the risk-based approach; this procedure is capable of guaranteeing reference certainty, standardised conduct, generalised application to the entire structure, full use of relevant information and ability to reconstruct the assessment process;
- with reference to this issue, adopts measures to ensure compliance with confidentiality requirements for the reporting procedure as well as tools, including IT tools, for detecting anomalous transactions;
- defines and ensures the implementation of initiatives and procedures necessary to guarantee prompt fulfilment of reporting obligations to the competent Authorities, as envisaged in anti-money laundering regulations;
- defines this Policy and ensures its implementation;
- defines and ensures the implementation of disclosure procedures to guarantee awareness of risk factors applicable to all the corporate structures involved and the bodies entrusted with control functions;
- defines and ensures the implementation of procedures for managing relationships with customers classified as “high risk”, in compliance with the principles established by the Board of Directors;
- establishes staff training and instruction programmes regarding the obligations envisaged in anti-money laundering regulations; training activities are provided on an ongoing and systematic basis and take into account any developments in the regulations and procedures set up by the Bank;
- defines tools suitable for assessing activities performed by personnel so as to ensure the detection of any anomalies that may emerge, particularly in their conduct, in the quality of communications sent to the authorised contacts and corporate structures as well as in personnel relationships with customers;
- in cases of remote operations (e.g. performed through digital channels), ensures the adoption of specific electronic procedures for guaranteeing compliance with anti-money laundering regulations, in particular the automatic detection of anomalous transactions;
- ensures compliance with the applicable regulations, in cases of outsourcing of the operational tasks of the AML Function, and receives periodic information on the performance of the outsourced activities.

### **AML Representative**

The Bank assigns the role of AML Representative of the same Bank and of the Group to a person identified within the Board of Directors, equipped with the necessary requirements.

Before the appointment, the Board of Directors ascertains the existence of any conflicts of interest on the part of the candidate for the office of AML Representative and the suitability of the measures adopted to prevent and/or manage them. To this end, the Board of Directors considers - at least - the following cases of conflict and the related remedial measures:

- delegations on operating areas subject to verification by the Head of the AML Function;
- direct involvement in transactions that are subject to scrutiny by the AML Function;
- any family relationships or affinity with the Head of the AML Function or with the personnel of the AML Function;
- delegations regarding the management of human and technical resources of the AML Function;
- delegations regarding the preparation and approval of AML policies, procedures and internal control measures.

The Bank adopts specific organisational measures, to be assessed on a case-by-case basis, in order to mitigate any conflicts of interest related to the appointment of the AML Representative; in this regard, the Bank may adopt one or more of the following measures:

- remodelling of the delegations/responsibilities of the AML Representative;
- obligation for the AML Representative to report to the Board on any conflict situations;
- possibility for the Head of the AML Function to report directly to the Board of Directors;
- preparation of periodic reports of the Head of the AML Function directly for the benefit of the Board of Directors.

With regard to the profiles of competence, the AML Representative must have adequate theoretical or practical knowledge in the following areas:

- money laundering risks, AML policies, controls and procedures as well as the business model of the Bank and the sector in which it operates;
- risk management (identification, assessment, monitoring, control and mitigation of the main types of risks of the Bank);
- internal control system.

In consideration of the fact that the position of AML Representative is executive, for directors who do not already carry out executive positions, the Board of Directors verifies that the representative meets the requirements and suitability criteria envisaged for directors with executive positions.

The AML Representative is the main point of contact between the Head of the AML Function and the Board of Directors and ensures that the latter has the information necessary to fully understand the relevance of the money laundering risks to which the Bank and the Group are exposed.

The AML Representative:

- monitors that the policies, procedures and internal control measures on anti-money laundering are adequate and proportionate, taking into account the characteristics of the Bank and the risks to which it is exposed;
- assists the Board of Directors in assessments of the organisational structure and the allocation of resources of the AML Function;
- ensures that the Corporate Bodies are periodically informed of the activities carried out by the Head of the AML Function as well as of any discussions with the Authorities;
- informs the Corporate Bodies of violations and critical issues concerning anti-money laundering of which it has become aware and recommends appropriate actions;

- verifies that the Head of the AML Function has direct access to all the information necessary for the fulfilment of his or her duties, has human and technical resources and sufficient tools and is informed of any shortcomings relating to anti-money laundering identified by the other internal control functions and by the Supervisory Authorities;
- ensures that the problems and proposals for action submitted by the Head of the AML Function are assessed by the corporate bodies.

The AML Representative also verifies the adequacy and completeness of the information and data communicated by the Head of the AML Function to the Corporate Bodies as part of their reports. To this end, the reports of the Head of the AML Function are sent well in advance to the AML Representative.

### **General Manager**

The General Manager is at the top of the internal structure and as such participates in the management function to which he/she reports. In particular, with respect to combatting money laundering and terrorist financing, the General Manager:

- supervises the ordinary management of the Bank, as part of directives set by the CEO, guaranteeing that it functions in compliance with current laws and regulations;
- supports the CEO in defining the responsibilities of the corporate structures and functions involved in the various business processes, so that the relative duties are clearly assigned and any potential conflicts of interest are prevented; he/she will also ensure that significant activities are managed by qualified personnel, with an adequate level of independence of judgement and who have experience and skills that match the duties to be carried out;
- issues specific internal orders, including through the corporate functions responsible, in accordance with the regulatory system defined by the Board of Directors.

### **Internal Audit Function**

In accordance with a risk-based approach, the Internal Audit Function continuously monitors the level of adequacy of the corporate organisational structure and its compliance with reference regulations, and monitors how well the overall system of internal controls functions.

With specific reference to provisions on preventing and combatting the use of the financial system for money laundering or terrorist financing, the Internal Audit Function will, also through audits, verify:

- compliance with the due diligence obligations, both when initiating the relationship and as it develops over time;
- the actual acquisition and orderly storage of the data and documents required by law;
- the functioning of the Single Electronic Archive and alignment between the various sector accounting procedures and the procedure for entering data and managing the Archive;
- the degree of involvement of employees and collaborators and those in charge of the central and peripheral structures in implementing the “active collaboration” obligation.

Moreover, considering the business model of the Bank, particular attention is given to the supervision of operations of the Network of Financial Advisors used by the Bank, carried out by the Internal Audit Function.

Specifically, the Sales Network Audit Unit, within the Internal Audit Function, monitors compliance by the sales network with the rules of conduct, including those relating to combatting money laundering and terrorist financing, referred to in the contractual arrangements and the relevant provisions and guidelines, and contained in the corporate regulations. It carries out this activity using specific remote analysis tools, performing on-site checks and audits, both at the offices of Sales Network collaborators and at the administrative offices of the financial advisors. It conducts the preliminary investigation and submits proposals to the Sales Network Disciplinary Committee on measures to be adopted with regard to Sales Network collaborators who are not compliant with legal and regulatory provisions, as well as with procedures and rules of conduct envisaged internally.

The Sales Network Audit Unit includes the Regulatory Network Monitoring Audit structure, which is assigned the following duties, also in relation to anti-money laundering:

- conducting mass remote audits on the sales network to verify compliance with regulations;
- monitoring the evolution of the internal/external regulatory framework to develop the framework of controls and regulatory indicators;

The Internal Audit Function is also responsible for the whistleblowing process, in which the Bank has identified the Whistleblowing Manager (or WB Manager), specifically appointed by the Board of Directors.

The Function performs follow-ups to ensure that the corrective actions have been adopted for any shortcomings or irregularities found and their suitability for avoiding similar situations in the future.

The Function submits a report, at least annually, to the Corporate Bodies on activities carried out and relative outcomes, without prejudice to compliance with the principle of confidentiality in reporting suspicious transactions.

### **Compliance Function**

The Compliance Function supervises the management of compliance risk, according to a risk-based approach, with regard to company activities, except for the regulatory areas assigned by law to other Control Functions. The Compliance Function, in accordance with the provisions of the Procedure for monitoring and managing reports of suspicious transactions - Market Abuse, assesses and analyses the reports received from the unit that carries out the first-level controls and, if there are reasonable doubts of market manipulation for orders or transactions, promptly informs the General Manager and indicates the names of the customers/employees subject to reporting to CONSOB, in compliance with the provisions on market abuse, attaching detailed sheets of the transactions considered anomalous with all information useful for reconstructing the chronology of the events and the reasons underlying said transactions. Reports sent to the Supervisory Authority are also forwarded to the AML Function.

In the case of requests received from the Supervisory Authorities, the Compliance Function - Exposed Support Unit and Supervisory Instances of Banca Mediolanum sends a copy of the request received by e-mail to the AML Analysis Unit of Banca Mediolanum, which takes steps to register the request received, initiating a specific investigation on the position of the Customer(s) concerned, by entering a specific report in the AML WorkFlow.

### **Risk Management Function**

The AML Function cooperates with the Risk Management Function in defining and implementing policies for the governance of money laundering and terrorist financing risks consistent with the Bank's risk management strategy; in particular, it helps with the definition and periodic updating of the Risk Appetite Framework (RAF) to ensure the correct inclusion and assessment of money-laundering risk.

### **AML Function**

According to a *risk-based* approach, the AML Function is responsible for monitoring money laundering risk and for adjusting the processes in accordance with developments in the related regulatory and procedural environment.

It continuously checks that company procedures are consistent with the objective of preventing and combatting the infringement of external regulations (laws and regulations) and self-governance on the subject of money laundering and terrorist financing.

It pays particular attention to the adequacy of the internal systems and procedures on customer due diligence and storage, as well as of the systems for detecting, assessing and reporting suspicious transactions, the effective detection of other situations subject to disclosure obligations and the appropriate storage of documentation and evidence as required by regulations.

The Anti-Money Laundering Function:

- is a second level control function and is one of the Company Control Functions;
- is independent and its human resources are qualitatively and quantitatively suited to its duties, including economic duties, which can also be initiated independently;
- it must have sufficient personnel with the necessary level of technical-professional skills, also through inclusion in ongoing training programmes;
- always reports directly to the corporate bodies;
- has access to all the Bank activities, including any information relevant to the exercise of its duties;
- collaborates with the other corporate control functions to develop its risk management methodology in line with corporate strategies and operations.

With specific reference to customer due diligence activities, in order to guarantee, at the same time, the effectiveness and efficiency of the processes, the direct involvement of the Anti-Money Laundering Function is required on a risk-based approach, taking into account any objective, environmental or subjective circumstances which significantly increase the money laundering risk.

In implementation of the above, the organisational and operating model defined by the Bank envisages that the AML Operational Monitoring Unit, within the Banking Controls & Knowledge Unit, and the personnel responsible for the management and administration of relationships with customers, to the extent of their respective responsibilities, fulfil their enhanced due diligence obligations in the cases considered high risk, identified in said paragraph 5.3. Within the scope of the process described above, appropriate escalation mechanisms are also defined in cases where the money laundering risk is particularly high.

In addition, the Anti-Money Laundering Function:

- identifies the applicable regulations in terms of monitoring money laundering risk and assesses their impact on internal processes and procedures;
- provides advisory and support activities to the Corporate Bodies, Senior Management and the organisational units of the Bank, regarding issues under its responsibility, especially in the case of new products and services offered or for significant changes to the products and services already on offer, the entry into new markets or the launch of new activities, paying special attention to identifying and assessing risks associated with latest generation products and business practices which include the use of innovative distribution mechanisms and technologies;
- collaborates in the definition of the Internal Control System, procedures and controls aimed at preventing and combatting money laundering risk;
- collaborates in the definition of money laundering risk governance policies and of the various steps in the process for managing this risk;
- continuously verifies the suitability of the money laundering risk management process and the adequacy of the internal control system and procedures, and proposes organisational and procedural modifications needed or advisable to ensure adequate monitoring of this risk;
- ensures the definition and maintenance of controls aimed at guaranteeing compliance with customer due diligence obligations, according to a risk-based approach which requires that such obligations are ranked according to the money laundering risk profile assigned to the customer;
- may carry out the enhanced due diligence process only in cases where – for objective, environmental and subjective circumstances – the money laundering risk is particularly high;
- verifies the reliability of the information system in fulfilling obligations related to customer due diligence, data storage and reporting of suspicious transactions.
- verifies the correct functioning of the information system for the fulfilment of obligations regarding the submission of objective communications;
- analyses and investigates external and internal reports received on alleged suspicious transactions to be submitted to the Suspicious Transaction Reporting Manager, to assess the need for reports to the FIU;
- examines evidence emerging from the automatic detection systems or specific detection systems of the Anti-Money Laundering Function and investigates the results for possible submission to the Suspicious Transaction Reporting Manager to assess the need for reports to the FIU;
- supports the Suspicious Transaction Reporting Manager in submitting reports considered valid to the FIU;
- in association with the Suspicious Transaction Reporting Manager, conducts checks on the functionality of the reporting process and the adequacy of the first level assessments carried out on the operations of Customers and defines procedures for the management of internal reports originating from the first level regarding particularly high risk situations to be treated with due urgency;
- monitors the monthly submission to the FIU by the IT outsourcer of aggregate data registered in the Single Electronic Archive and objective communications;
- submits objective communications to the FIU in accordance with its instructions;
- as regards anti-money laundering issues, collaborates with the Authorities pursuant to Title I, Paragraph II of the Anti-Money Laundering Decree and responds to their requests for information;

- in cooperation with the other corporate functions responsible for training, ensures the setup of a suitable training programme aimed at achieving staff training on an ongoing basis and effectiveness indicators on the training carried out;
- assesses, in addition to basic education, specific training needs, ensuring that adequate theoretical and practical training is provided to people exposed to different levels of ML/TF risks;
- at least once a year prepares a report on the initiatives undertaken, the malfunctions identified and the related corrective actions to be taken, as well as on staff training activities, that it submits directly to the Board of Directors, the Risk Committee and the Board of Statutory Auditors;
- in cooperation with the other corporate functions involved and based on the methods and time frames defined by the Bank of Italy, conducts the self-assessment exercise on money laundering and financing of terrorism risks, the results of which are included in the annual report described above;
- promptly informs the Corporate Bodies of significant breaches or shortcomings identified during the exercise of related tasks;
- periodically informs the corporate bodies, directly, about the progress of the corrective actions taken in the event of shortcomings found in the control activity and about any inadequacy of the human and technical resources assigned to said function and any need to strengthen them;
- prepares specific information flows to the Corporate Bodies, the AML Representative and the Chief Executive Officer;
- for companies in the Financial Conglomerate with which there are service agreements in effect, outsources specific operating duties on the combatting of the Risk of money laundering according to the methods defined in said agreements;
- collects and reviews information flows from the corresponding functions of the foreign subsidiaries of the financial Conglomerate;
- within its area of responsibility, prepares/validates and updates the internal regulations, Policies and regulations on anti-money laundering and anti-terrorism and, if necessary, prepares the related Group guidelines.

In order to allow the Corporate bodies direct access to reports on anti-money laundering, the relevant communications with the Authorities and the supervisory measures imposed or the sanctions issued, the AML Function uses the Sherpany platform as a system for sharing records, which is used by the Corporate Affairs Division for the disclosure of material to the various members of the Corporate Bodies.

The Anti-Money Laundering Function employees must be in a sufficiently independent position to express their personal judgement, express opinions and provide recommendations on an impartial basis; regardless of their hierarchical position within the organisation, they must be free from any effective conflicts of interest arising from professional or personal relationships, or from monetary or any other type of interest that may conflict with their duties; additionally, they must be protected from undue interference that could limit or change their scope of action or the performance of their duties, or that could significantly affect or influence their opinions or the content of their work.

The remuneration and incentive system for Anti-Money Laundering Function personnel must be compliant with supervisory regulations and internal policies.



### **Anti-money Laundering Function Manager**

The AML Function Manager (hereinafter also referred to as the Anti-Money Laundering Manager) is appointed by the Board of Directors, in agreement with the Board of Statutory Auditors.

The Anti-Money Laundering Manager must meet the necessary independence, competence, professionalism and reputation requirements, as well as the integrity and fit and proper requirements identified in this policy, the fulfilment of which – at the time of appointment and consistently thereafter – are assessed by the Board of Directors.

The AML Manager has the time necessary for the effective fulfilment of his/her duties.

In order to guarantee the necessary independence and authority, the Anti-Money Laundering Manager is placed in the appropriate hierarchical-functional position, without any direct responsibilities in operational areas or hierarchically reporting to the managers of those areas.

As regards professionalism and expertise requirements, the Anti-Money Laundering Manager must demonstrate the following characteristics:

- in-depth knowledge of current legal and regulatory provisions on anti-money laundering and anti-terrorism and or previous experience in risk management and/or in control functions;
- in-depth knowledge of the banking-financial sector;
- the capacity to relate with Supervisory Authorities, Investigating Authorities and Corporate Bodies.

With regard to aspects of integrity and fairness, the AML Manager must meet the requirements set forth in Art. 20 of Ministerial Decree 169/2020<sup>3</sup>.

The Board of Directors assesses the characteristics of the candidate and, after consulting the Board of Statutory Auditors, authorises the assignment.

The Anti-Money Laundering Manager:

- participates, where required, in the meetings of the corporate bodies and reports directly to them, coordinating in advance with the AML Representative;
- has access to all necessary corporate documentation to allow performance of the tasks envisaged in the Supervisory regulations;
- verifies the effectiveness of procedures, structures and systems, providing support and advice on management decisions;
- acts as FIU contact for all issues concerning the submission of objective communications and any requests for information.

The Bank has adopted organisational measures and controls aimed at guaranteeing the operational continuity of the AML Function even in cases of absence or impediment, of a temporary nature, of the AML Manager.

---

<sup>3</sup> For more detailed information, refer to the internal regulations “*Policy for the appointment, removal and replacement of Managers of the Corporate Control Functions*”.

The AML Function is divided into Control Units and Staff Units, with well-defined tasks and responsibilities illustrated in detail in the internal regulations prepared (and periodically updated) by the same Function<sup>4</sup>.

Even in the event of the absence or temporary impediment of the AML Manager, the employees of the AML Function are able to guarantee, on an ongoing basis, the monitoring of the reference regulatory framework and compliance with the requirements expressed by the Supervisory Authorities, analysis of the impacts on the business processes deriving from any new obligations relating to the relevant regulatory areas, the performance of second-level controls and the fulfilment of reporting obligations, analysis and investigation of external and endogenous reports received regarding alleged suspicious transactions.

In the event of the absence or temporary impediment of the AML Manager, the AML Representative, for the purpose of exercising his/her functions, liaises with the contact persons of the Control Units and Staff Units of the AML Function, each for matters within their own remit.

Where the absence or impediment of the AML Manager lasts for more than 3 months, the Board of Directors meets to replace the AML Manager or appoint a *pro tempore*<sup>5</sup> AML Manager.

The AML Manager is appointed by the Board of Directors, after consulting the Board of Statutory Auditors, as the Group Chief AML Officer, pursuant to the provisions of the EBA Guidelines on AML Policies and Procedures and the Provisions (also "**Group Chief AML Officer**").

The Group Chief AML Officer:

- works with the AML Managers of the Group's Italian or foreign companies and ensures that said Managers carry out their duties in a coordinated manner and according to policies and procedures consistent with those of the Group;
- supervises the self-assessment of money-laundering risks carried out by the Group companies;
- prepares an assessment of the Group's money laundering risks, taking into account the risks resulting from the individual financial years, the inter-relationships between the individual Group companies and their impact on risk exposure at Group level;
- presents, for the Corporate Bodies of the Parent Company, as part of the annual report, a specific section on exposure to money laundering risks and on the activities of the Group AML Function;
- prepares and submits the Group procedures, methodologies and standards on anti-money laundering to the corporate bodies of the Parent Company, with particular reference to due diligence procedures, and ensures that the policies and procedures of the Group's members are in line with such standards as well as compliant with the applicable legislative provisions and anti-money laundering regulations;
- establishes periodic information flows for all Group companies to share the information necessary for the performance of their duties.

---

<sup>4</sup> As illustrated in more detail in the Organisation of Banca Mediolanum S.p.A. Services and in the Regulations of the AML Function.

<sup>5</sup> See Policy for the Appointment, Removal and Replacement of Heads of Corporate Control Departments.

In order to ensure the enforcement of effective AML/CFT policies and procedures at Group level, the Group Chief AML Officer makes use of the resources of the Group AML Function.

### **Suspicious Transaction Reporting Manager**

Pursuant to Art. 36 of the AML Decree, the Suspicious Transaction Reporting Manager is the legal representative of the recipient or a nominee of the recipient; a mandate may also be granted to the Head of the AML Function, and the Bank of Italy Provisions expressly provide that intermediaries of significant size may assign the mandate for the reporting of suspicious transactions to several parties, defining their specific scope of responsibility and action. The conferral of a mandate is resolved upon by the Body responsible for strategic supervision, after consulting with the Control body. In order to guarantee suitable independence of the whistleblower and possession of the professionalism and integrity requirements, the role of Suspicious Transaction Reporting Manager may be assigned to the Anti-Money Laundering Manager; this decision, in addition to guaranteeing suitable independence of the whistleblower, allows an assessment of the specific anti-money laundering skills of the manager, as well as his/her knowledge of the procedures for effective customer due diligence and profiling adopted by the Bank. In the event of a mismatch, it can acquire useful information from the Anti-Money Laundering Manager for the assessment of suspicious transactions.

In the event of the presence of several Responsible parties, the coordination and sharing of information is fully guaranteed by the architecture of the applications already in use and by the related operating processes. More specifically, the overall management of cases is provided for within the current AML Workflow operational tool in use by the Anti-Money Laundering Function, through the adoption of specific user profiles by the parties involved, guaranteeing the traceability, control and visualisation of the cases. The Board of Directors may appoint replacements for the Suspicious Transaction Reporting Managers - without prejudice to meeting the professionalism and integrity requirements envisaged for the Anti-Money Laundering Manager – who, if the Suspicious Transaction Reporting Manager is absent or otherwise engaged, takes over their powers and duties.

The role and responsibilities of the Manager must be properly formalised and made public within the Operating Structures of the Bank and the Sales Network.

The Suspicious Transaction Reporting Manager:

- has free access to the information flows addressed to the Corporate Bodies and Operating Structures involved monitoring money laundering risk (e.g. requests received from the Judicial Authority or investigating bodies);
- in compliance with the confidentiality obligations envisaged in the Anti-Money Laundering Decree on the identity of parties involved in the transaction reporting procedure, provides - also through the use of suitable databases - information on the names of customers referred to in suspect transaction reports to the managers of structures responsible for the assignment or updating of the customers' risk profiles;
- is aware of and rigorously and effectively applies instructions, systems and indicators issued by the FIU;
- to the extent of their responsibility, manages relations with the FIU and promptly responds to any requests for further information that the FIU may make;

- advises the Operating Structures on the procedures to adopt for reporting any suspicious transactions and the abstention from executing the transactions if necessary;
- based on all available information, promptly reviews the reports of suspicious transactions received from the first level Operating Structures and the communications received from the Board of Statutory Auditors, the Supervisory Body and/or the Internal Audit Function as well as those of which he/she becomes aware when exercising his/her duties;
- submits to the FIU any reports deemed valid, omitting the names of parties involved in the transaction reporting procedure;
- giving adequate justification in writing, files reports not considered valid, keeping a record of the assessments carried out as part of the procedure;
- also uses, in his/her assessments, any elements retrievable from freely accessible information sources;
- communicates the outcome of his/her assessments, by applying organisational methods suited to ensuring compliance with the confidentiality obligations envisaged in the Anti-Money Laundering Decree, to the first level party originating the report;
- helps identify the measures needed to ensure confidentiality and storage of the data, information and documentation relating to the reports, to be submitted for approval of the Board of Directors.

When assessing suspicious transactions, the Manager may obtain useful information from the structure responsible for first-level analysis of the anomalous transactions and use the support of the Anti-Money Laundering Function.

The Manager may at his/her own discretion authorise Anti-Money Laundering Function employees to operate (1) in the suspicious transactions reporting system (Infostat-FIU), in accordance with instructions given by the FIU, (2) within the risk profiling system in order to operationally implement the increase/decrease in the profile of parties analysed, as decided by him/her; (3) within the system for communicating infringements of restrictions on the circulation of cash and bearer instruments (SIAR) and (4) within the GE.SA.FIN. system of prior requests for authorisation to execute transactions/payments on documents representing commodities in the case of countries that are embargoed/sanctioned/under restrictions and/or, within the S.I.G.M.A system, execute transactions/payments relating to weapons materials, as well as to operate, under his/her own responsibility, within the system for the management of aggregate reports (S.Ar.A.).

### **Sales Network**

The financial advisors in the Sales network (Family Bankers ®) are personally in charge, as first level control, of the identification process and due diligence of customers assigned to them, developing knowledge of the customer and ensuring continuous monitoring during the relationship in accordance with the underlying risk. In addition, they are responsible for carrying out the enhanced due diligence process in cases envisaged by regulations and when requested by the Anti-Money Laundering Function or the AML Operational Monitoring Unit.

The financial advisors, within the scope of activities carried out on behalf of the Bank, are required to be informed of and comply with the laws, regulations and provisions issued by the Bank, also in reference to the anti-money laundering rules of conduct, as envisaged in the agency contracts.

The Bank provides its financial advisors with specific operating tools and procedures, manual and IT, to them in complying with anti-money laundering obligations and prepares specific permanent training and professional updating programmes for them, so that they are adequately aware of the reference regulations and related responsibilities and are capable of using tools and procedures to assist in fulfilling the obligations.

All documentation requested and obtained from the customer, both on initial registration and during the constant control of customers, is stored by the Family Banker® for a period of 10 years starting from the day the transaction is executed or the date that the business relationship is closed. The documents are promptly made available, in hard copy or electronic format where possible, at the request of the competent authorities and/or the Corporate Control Functions.

The Bank continuously monitors compliance, by the Sales Network, with anti-money laundering rules of conduct established by regulations and as part of contracts, including through periodic site inspections of the administrative offices of the financial advisors.

As the financial advisors are responsible, in practice, for the administration and management of relationships with the customers assigned to them, they constitute, to all intents and purposes, the first reporting level.

Therefore, financial advisors are responsible for promptly reporting, where possible before executing the transaction, any suspicious transactions, according to the procedures and methods defined internally, when they know, suspect, or have reasonable grounds to suspect that a money laundering or terrorist financing transaction has been executed, is in progress or has been attempted.

### **Operating Structures**

The Operating Structures are the primary owners of the risk management process. During daily operations, these structures are called upon to identify, measure or assess, monitor, mitigate and report risks arising from ordinary business activities in compliance with the risk management process. Moreover, these structures must comply with their assigned operational limits, consistent with the risk objectives and procedures into which the risk management system is divided.

All employees and collaborators of the Operating Structures, within the scope of their assigned duties, are required to be aware of and comply with the laws, regulations and rules issued by the Bank. The corporate documents governing organisational and behavioural aspects of compliance with current regulations, both legal and as defined by the Bank, must be brought to the attention of all personnel by publishing and disseminating them according to the methods envisaged by each Company of the Group.

If, while carrying out their activities, personnel find that the operating processes in place do not comply with reference regulations or the controls adopted are not sufficiently effective to prevent the involvement, even unwittingly, of the Bank or the Group companies in money laundering or terrorist financing, they must promptly inform their line managers.

If the Operating Structures are in charge of the actual administration and management of customer relations, they will also be in charge of identifying and performing due diligence on the customers assigned to them as the first level of control, to get to know the customer, and ensure the continuous monitoring during the relationship in accordance with the underlying risk. The Operating Structures are also responsible for performing the enhanced due diligence in cases envisaged in regulations, and if requested by the Anti-Money

Laundering Function, and are responsible for promptly reporting any suspicious transactions, where possible before executing the transaction, in accordance with internally defined procedures and methods, if they have any suspicion or justified reason to suspect that money laundering or terrorist financing has been carried out, is being carried out, or is being attempted.<sup>6</sup>

Every Structure Manager must, to the best of their ability, arrange personnel management and manage the operating tools provided to them, in order to ensure the constant pursuit of business objectives, and, to the extent of their responsibility, must comply with and ensure compliance with all current laws and regulations, and regulations issued by their company.

Each Manager is responsible for the overall compliance and effective functioning of the first level controls within their structure, adopting suitable controls and information systems.

If while carrying out their duties, the Managers find that the operating processes in place do not comply with regulations or the controls adopted are not sufficiently effective to prevent the involvement, even unwittingly, of the Bank or Group companies in money laundering or terrorist financing, after the necessary investigations they must promptly involve the Anti-Money Laundering Function for its own assessments.

To that end, the Bank provides its employees and collaborators with operating tools and procedures, also in electronic format, that can help them fulfil their relative anti-money laundering obligations, and sets up specific permanent training and professional updating programmes for them to ensure they are aware of the reference regulations and related responsibilities, and can properly use the support instruments and procedures to help them fulfil the requirements.

All documentation requested and obtained from the Family Banker® or directly from customers (both on initial registration and during the constant control of customers) is stored by the Bank for a period of 10 years starting from the day the transaction is executed or the date that the business relationship is closed. The documents are promptly made available, in hard copy or electronic format where possible, at the request of the competent authorities and/or the Corporate Control Functions.

### **Service, Operations & ICT Department**

The Service, Operations and ICT Department is responsible for managing the operating processes of the Bank, provided through the Customer Banking Centre, Product Operations and Sales Support Centre sectors, the Banking Controls & Knowledge Managerial Support Unit and the ICT Division.

It oversees and maintains the IT systems of the Bank and companies to which services are provided. It handles relations with outsourcers and oversees and controls the activities, assessing the services provided and the service levels.

---

<sup>6</sup> This is without prejudice to cases where the transaction has to be carried out as there is a legal obligation to accept the action, or cases where the transaction cannot be postponed taking into account normal operations, or cases where postponement of the transaction could hinder investigations.

It manages direct contacts of existing and prospective customers with the Bank, for IT and devices, through the services available via different channels: telephone (Banking Centre, Automatic Voice Response, text messaging, Mobile Banking) and the Internet (e-mail, chat, internet banking).

The Department also provides a telephone and written support service to the Sales Network (Sales Support Centre) in order to provide quick answers to customers' applications through the financial advisors.

The Department manages the receipt and archiving of incoming documents, customer data, the opening, management and closing of contracts for all products placed by the Bank through the Product Operations Sector, supporting "specialised" organisational units of the Bank and the Product Companies, in compliance with the distribution assignments.

It applies the contractual and economic conditions, receivable and payable, of the various services and products offered by the Bank and the Group, in compliance with procedures and limits established by the Board of Directors and communicated by the Chief Executive Officer and General Manager.

The Service, Operations & ICT Department Manager authorises the start, continuation and maintenance of a business relationship or the execution of an occasional transaction with Politically Exposed Persons, as well as the start, continuation and maintenance of a business relationship involving high risk third countries or the execution of an occasional transaction involving such countries.

If the Service, Operations & ICT Department Manager is absent or otherwise engaged, powers are conferred to the Product Operations Sector Manager to authorise the start, continuation and maintenance of a business relationship or the execution of an occasional transaction with Politically Exposed Persons, as well as the start, continuation and maintenance of a business relationship involving high risk third countries or the execution of a transaction involving such countries.

If the decision to initiate or continue<sup>7</sup> a business relationship is subject to the legal requirement (Politically Exposed Persons, relationships involving High-Risk Third Countries) of authorisation by a senior manager, the AML Function shall give its prior opinion.

If the Senior Manager (or the Head of the Service, Operations & ICT Department or, in the event of his/her absence or impediment, the Head of the Product Operations Sector) decides not to comply with the opinion of the AML Function, the senior manager is required to formalise and justify such a decision and identify the measures that will be adopted to mitigate the risks reported.

The actual exercise of the powers certifies that the main delegated party is absent or otherwise engaged, and releases third parties from any scrutiny or liability in this respect.

Within the Service, Operations & ICT Department, the managerial support organisational unit named "**Banking Controls & Knowledge**" is in charge of defining and documenting the set of first level Anti-Money Laundering controls based on guidance received from the Anti-Money Laundering Function, and constitutes the sole

---

<sup>7</sup> This refers exclusively to the case of Customers who acquire the status of Politically Exposed Persons or who have transferred their residence/registered office to high-risk Third Countries at a later stage after the start of the relationship.

operational contact for the Service, Operations & ICT Department for such matters. In particular, the AML Operating Control Unit, within the Banking Controls & Knowledge Unit:

- oversees the enhanced due diligence process for customers - with high money laundering risk or in a case of increase in the money laundering risk profile due to transfer to high risk, in cases other than those analysed by the Anti-Money Laundering Function, as well as on the periodic expiry of the assigned profiles - and of any transactions with regard to the Insurance Group, for which the Bank carries out distribution activities, it oversees the enhanced due diligence process on transactions deemed high risk, as defined by the Anti-Money Laundering Function of the Mediolanum Vita Insurance Group.
- performs first level controls on transactions ordered by customers, based on parameters and rules agreed with the Anti-Money Laundering Functions of the Bank and Group companies with which specific outsourcing agreements are in place;
- performs first level controls on specific transactions executed by customers (for example: bank transfers for significant amounts, bank transfers in dollars, lack of correspondence between the beneficiary and account holder on incoming bank transfers, transactions executed by trust companies, collections of bills of exchange, transactions involving high-risk third countries and operations on prepaid cards or debit cards, etc.);
- performs continuous monitoring of operations (banking, insurance and financial) of customers not assigned to a financial advisor, based on the parameters agreed with the Anti-Money Laundering Function, coordinating with the Self Customer Marketing Office of the Customer Marketing and Digital Services Division;
- in the event of enhanced due diligence, it guarantees the fastest possible processing times for transactions ordered by customers, involving the Anti-Money Laundering Function in cases in which, due to objective, environmental and subjective circumstances, the money laundering risk is particularly high;
- oversees the preliminary processes for the assessment and subsequent decision on authorisation - by the holders of administrative or management powers or their delegates - of the start, continuation or maintenance of a business relationship or the execution of an occasional transaction with Politically Exposed Persons, as well as the start, continuation or maintenance of a business relationship involving high risk third countries or the execution of a transaction involving such countries.

The Head of the Managerial Support Unit called Banking Controls & Knowledge and the AML Operational Monitoring Unit Manager are granted specific powers to authorise transactions of up to Euro 100,000 and up to Euro 15,000, respectively, involving high-risk third countries.

The Banking Controls & Knowledge Managerial Support Unit also operates the Banking Services Oversight Office, which monitors, inter alia, the transactions of Customers not assigned to a Financial Advisor, in order to detect and/or prevent the fraudulent use of a current account (active fraud), liaising with the Self Customer Marketing Office of the Customer Marketing and Digital Services Division and using the appropriate dashboard made available by the Analytical CRM Office. In addition, it assesses and initiates the removal of the accounts and/or the revocation of the means of payment granted in the event of irregular use of the account, for



suspected fraud as well as for all cases where the AML Function or the Judicial Documents Office highlights an irregularity in the position, keeping evidence of the decisions made.

If assessments and controls carried out by the Service, Operations & ICT Department detect reasonable elements for suspicion, it sends a suspicious transaction report to the Anti-Money Laundering Function, so that this Function may carry out all the appropriate investigations and assessments, coordinating with the Family Banker® or with the employee assigned actual administration and management of the relationship with the customer.

### **Credit Department**

The Credit Department is responsible for guaranteeing adequate implementation of the Bank's credit policy and particularly ensures compliance with the current transparency and usury regulations. It oversees and coordinates operating activities connected with ordinary and special loans, interacting with customers and the Sales Network to finalise the services requested.

On preliminary credit assessment, the Credit Department conducts specific analyses on the various parties involved in order to identify, assess and manage the money laundering risk associated with the transactions, also considering the risk profile assigned to the customers. Once the loan has been granted, the Department focuses specific attention on the allocation of cash flows, especially if the loan has specific restrictions as to its purpose.

If, after the assessments and controls carried out by the Credit Department, there are reasonable elements for suspicion, it sends a Suspicious Transaction Report to the Anti-Money Laundering Function, so that this Function may carry out all the appropriate investigations and assessments, coordinating with the Family Banker® or with the employee actually assigned to administrate and manage the relationship with the customer, providing feedback to the Credit Department.

The Credit Department duly takes into account the analyses conducted by the Anti-Money Laundering Function in its credit rating assessment.

### **Tax Affairs Division**

As part of its assigned duties, the Tax Affairs Division monitors regulations as and when issued, ensuring their correct adoption by the reference structures in the relevant processes for the correct identification of customers.

It monitors the customer classification process for QI, FATCA and CRS purposes, providing guidance on the methods for recovering missing data, as well as specialist advice on specific cases. In this respect, it conducts compliance checks on the processes concerned and on the documentary evidence collected, at its own initiative and/or based on obligations envisaged in the "Compliance Programme" (an obligation introduced on renewal of the QI Agreement - effective from 1 January 2017 - which includes internal procedures, processes and controls to guarantee that the QI correctly fulfils the obligations imposed by the QI Agreement, and complies with applicable FATCA obligations).

It prepares and transmits communications to the Italian Inland Revenue as required by DAC 6 regulations.

### **Corporate Affairs, Legal and Litigation Department**

The Judicial Documents Office of the Corporate Affairs, Legal and Litigation Department oversees the receipt and processing of requests or measures from the Investigating Bodies and the Judicial Authority, recording these in the reference database, and informs the Individual Customer Records Line of the specific code to be assigned to the position of the customer(s) concerned so that such information is taken into due consideration during customer risk profiling.

The Judicial Documents Office also promptly informs the Anti-Money Laundering Function of specific requests and measures, according to the provisions of the current Process Regulations for Reporting Suspicious Transactions.

### **Wealth Management Department**

The Wealth Management Department is in charge of supervising the Bank's advisory services to high-wealth customers, developing the knowledge of 'black' customers<sup>8</sup> not associated with financial advisors and is the internal contact for managing the related business relationships.

It oversees the process of identification and due diligence of private customers not assigned to a Family Banker®, coordinating with the AML Operational Monitoring Unit for the ongoing monitoring of operations during the business relationship, based on the risk.

### **Investment Banking Department**

The Investment Banking Department provides extraordinary finance advisory services to companies whose shareholders are business owners that already have business relationships with the Bank as individuals or prospects, or assistance to business customers in designing and executing transactions such as, for example: debt issues, listings, acquisitions/mergers/sales or joint ventures.

With specific reference to this Policy, the Department oversees the enhanced due diligence of customers/prospects that request advisory services or assistance, reporting any suspicious transactions or anomalous conduct detected to the Anti-Money Laundering Function.

### **Human Resources Department**

At the request of the AML Operational Monitoring Unit, the Human Resources Department oversees the due diligence process on transactions conducted by employees of the Bank who are not assigned to a Family Banker®.

In collaboration with the Anti-Money Laundering Function, the Human Resources Training Sector of the Human Resources Department ensures the planning and provision of specialist training and professional development courses on combatting money laundering and terrorist financing to employees of the Bank and of the Italian companies of the Group.

---

<sup>8</sup> Customers with total assets equal to or greater than Euro 2 million.

### **Sales Network Careers, Planning and Organisation Division**

At the request of the AML Operational Monitoring Unit, the Sales Network Careers, Planning and Organisation Division oversees the due diligence process on transactions conducted by the financial advisors of the Sales Network acting as their office managers.

### **Customer Marketing and Digital Services Division**

In the Customer Marketing and Digital Services Division, the Self Customer Marketing Office manages and administers relationships with customers not assigned to a financial advisor.

As part of the money laundering risk monitoring, the Self Customer Marketing Office, as first level control unit, continuously monitors banking, insurance and financial operations of customers not assigned to a financial advisor, with the support of the AML Operational Monitoring Unit. Therefore, it fulfils the customer due diligence obligations and, where necessary, enhanced due diligence obligations.

If, after conducting the assessments and controls, the Office detects reasonable elements for suspicion, it sends a Suspicious Transaction Report to the Anti-Money Laundering Function, so that this Function may carry out all the appropriate investigations and assessments.

## **4.2 ITALIAN COMPANIES BELONGING TO THE BANKING GROUP**

---

With reference to money laundering risk monitoring, in order to pursue the full and actual implementation of the Group model, the consolidated subsidiaries adopt a policy consistent with the principles and guidelines of this Policy, in accordance with a principle of proportionality and on the basis of the specific nature of its activities.

In compliance with the requirements laid down in the secondary regulations, the Body with strategic supervisory function (after consulting the control body) of each Italian company belonging to the Group appoints its own (i) AML Representative at the first renewal of the Corporate Bodies and, in any case, no later than 30 June 2026 and (ii) the Manager/Representative/Contact of the Anti-Money Laundering Function.

Without prejudice to the need to identify its own AML Representative, each Italian company belonging to the Group carries out its own assessments according to the principle of proportionality (assessments that are illustrated in detail in specific internal documentation) and can proceed with the appointment of the aforementioned Representative both within the scope of the Board of Directors and outside it. This choice must, in any case, be assessed in advance with the Group Chief AML Officer.

The AML Representative serves as a liaison between the respective Manager/Representative/Contact of the AML Function and the Board of Directors and ensures that the same is adequately informed about the money-laundering risks to which each Italian company belonging to the Group is exposed.

Pending the appointment of the AML Representative, this task is carried out by the Chief Executive Officer in office of each Group company.

The Manager/Representative/Contact of the AML Function of each Italian company belonging to the Group works with the Group Chief AML Officer and has direct communication lines with this manager.

The Group Chief AML Officer supervises the activities carried out by the Managers/Representatives/Contacts of the AML Function of the Italian companies belonging to the Group in order to ensure coordination between the activities carried out by them.

#### **4.3 FOREIGN COMPANIES BELONGING TO THE BANKING GROUP**

---

In order to pursue full and real implementation of the Group model, the procedures in place at the foreign subsidiaries and branches must be in line with the Group standards and ensure sharing of the information at consolidated level, without prejudice to compliance with the specific legal requirements of the host country. Consequently, foreign subsidiaries will adopt an anti-money laundering policy in accordance with this policy, based on a principle of proportionality and taking into account the specific nature of the business and local regulations.

In the foreign companies where local regulations envisage such a figure, and in any case in compliance with local regulatory provisions, an AML Representative and AML Manager will be appointed to ensure the correct management of the risk arising from the requirement to comply with all applicable provisions, also as regards the different areas of international operations. The AML Manager ascertains compliance with the Policy approved by the Parent Company and works with the Group Chief AML Manager, taking into account the respective specific requirements and reference regulations, in order to ensure a homogeneous approach to the monitoring of money laundering risk.

### **5 GROUP PRINCIPLES FOR COMBATTING MONEY LAUNDERING AND TERRORIST FINANCING**

The Bank and the companies of the Group adopt procedures and methodologies commensurate to the nature of their business activities and their size, for the analysis and assessment of money laundering and financing of terrorism risks to which they are exposed in conducting their activities, taking into account multiple risk factors.

In that regard, the Bank has defined specific Group guidelines based on the highest standards for combatting money laundering and terrorist financing, with which members of the corporate bodies, employees and collaborators must comply to avoid involvement, even unwittingly, of the Bank and the Group companies in any money laundering or terrorist financing.

The guidelines for fulfilling the obligations in accordance with regulatory provisions are provided below, and are organised, to ensure implementation, into the specific process rules and internal procedures adopted by each company in the Group.

## 5.1 CUSTOMER DUE DILIGENCE

---

The Bank adopts customer due diligence measures proportional to the extent of its exposure to money laundering risk, taking into account specific factors relating to the customer, transaction or business relationship.

The acquisition of information must be for the purpose of assessing, throughout the duration of the Relationship, the consistency of transactions with knowledge of the customer, its activities and its risk profile.

The KYC - Know Your Customer principle, which translates into rules for due diligence, assumes particular relevance also in relation to the principle of "active collaboration" and to the obligation of reporting suspicious transactions (see par. 5.7). The identification of the customer, representative and beneficial owner, if any, with related verification of identity and the collection of information, must take place within the scope of a discussion which is necessary, on the one hand, for the customer to become familiar with the Bank and to declare the scope and nature of the business relationship that it intends to establish, and on the other hand, for the Bank and its personnel to better know the customer, its banking, financial and insurance needs, and to offer the products and services that are most suited to its requirements.

For this purpose, the Bank adopts appropriate training initiatives for its personnel, as described in paragraph 5.11 below.

Employees of the Operating Structures in charge of the actual management and administration of customer relationships and the financial advisors in the Sales Network fulfil due diligence obligations by complying with the measures, methods and internal procedures adopted by the Bank to develop and keep their knowledge of the customer updated, and to report any suspicious transactions.

In order to ensure the correct execution of customer due diligence, the financial advisors and Operating Structures of the Bank, which are responsible for the management and administration of relationships with the customers, arrange:

- identification of customers, any representatives and beneficial owners and the acquisition of related identification documents as well as additional information necessary to determine the risk profile to be associated with the customer, envisaged in the forms of the Bank and companies whose products are placed by the Bank;
- in cases envisaged in current regulations, identification of the beneficiary and any beneficial owner of the beneficiary of an insurance service provided through policies placed by the Bank in its capacity as insurance intermediary;
- verification of the identity of the customer, the beneficiary, the representative, if any, and the beneficial owner of the customer and of the beneficiary, based on the documents, data or information obtained from a reliable and independent source;
- records of customers, representatives, if any, and the beneficial owners, available on the Bank database and the storage of documentation acquired for identification and verification purposes, according to the confidentiality provisions and measures dictated by internal regulations;
- acquisition and assessment of information on the scope and nature of the business relationship and any occasional transactions;

- the collection and assessment of information on the type of relationships between the Customer and Executor, the Customer and Beneficial Owner, the Customer and Policyholder and the individually designated Beneficiaries;
- the acquisition and assessment of information on the origin of the funds employed in investment transactions in Policies, Funds and Asset Management (GPM/GPF) placed by the Bank;
- the constant control of business relationships in order to keep knowledge of the customer and the declared scope of the relationship up to date, and to assess any “unexpected” or anomalous transactions, or transactions that are not consistent with the economic or financial profile of the customer previously known or news of significant events;
- the periodic update of data and information gathered, with a frequency depending on the risk profile previously associated with the customers, asking them to provide, under their own liability, all the up-to-date information needed to allow the due diligence obligations to be fulfilled.

Enhanced due diligence activities are carried out at least at the times and in the circumstances described below:

- when a business relationship is established or when the beneficiary of an insurance policy is designated;
- at the time of execution of an occasional transaction, arranged by the customer, involving the transmission or the handling of payment instruments in an amount equal to or exceeding Euro 15,000, regardless of whether it is executed as a single transaction or through multiple transactions which appear to be connected in order to perform a split transaction or it consists in a transfer of funds, as defined in art. 3, paragraph 1, point 9, of the Regulation (EU) no. 2015/847 of the European Parliament and of the Council, exceeding Euro 1,000;
- when there is a suspicion of money-laundering, regardless of any derogation, exemption or applicable threshold, also based on indicators of anomalies and patterns that are representative of abnormal conduct issued by the FIU, in compliance with the Anti-Money Laundering Decree;
- when there are doubts regarding the completeness, reliability or truthfulness of the information or documentation previously acquired from the customers.

The Bank fulfils the due diligence obligations for new customers as well as for existing customers when appropriate, following a rise in the level of money laundering risk associated with the customer.

For existing customers, the Bank complies with the aforementioned provisions when fulfilling the obligations set out in Council Directive 2011/16/EU of 15 February 2011, on administrative cooperation in the field of taxation and repealing Directive 77/799/EC, as part of the relevant national implementing rules on administrative cooperation in the field of taxation.

The collection of data and information is achieved through a guided process for completion of the “Personal Data Record and Customer Due Diligence Form” and the specific “Addenda to the Personal Data Record and Customer Due Diligence Form” (see par. 5.3).

Due diligence is not required for activities for the purpose of or related to the organisation, functioning or administration of the Bank, taking into account that they do not form part of its institutional activities and that, in performing them, the counterparties of the Bank qualify as providers of goods or services at the initiative of

the Bank, rather than as customers asking to establish a business relationship or to carry out an occasional transaction.

Relationships and transactions carried out at the initiative of the manager providing an individual portfolio management service are also excluded.

Under no circumstances may the due diligence obligations be transferred to shell banks or intermediaries located in high-risk third countries. Furthermore, it is not permitted to establish new Relationships using the identification process through third parties outside the Mediolanum Group, nor to establish new Relationships or to carry out Transactions by Customers with expired identification documents or risk profiles, once the terms granted to them for carrying out the update have passed.

### **Remote acquisition (onboarding) of Customers**

The Bank pays particular attention to remote operations (carried out without the physical presence of the Customer and Bank Staff), in consideration of the absence of direct contact with the customer or the representative, also due to the growing risk of fraud associated with identity theft, including when resorting to the use of public databases.

In this regard, the Bank adopts and maintains specific policies and procedures to fulfil the obligations referred to in Art. 13(1)(a) and (c) of Directive (EU) 2015/849; the AML Function and the Operating Structures involved in the Customer's remote onboarding process carry out specific controls, each to the extent of their competence, to ensure that the remote onboarding solution adopted is in line with expectations and to adequately manage money-laundering risks that could result from the use of this solution.

When considering the possibility of adopting a new solution for the remote onboarding of a Customer, the Bank carries out, in any case, a preliminary assessment of the enforcement of this solution, involving the company structures concerned for the necessary in-depth analyses. In particular, the impact of the use of the Customer's remote onboarding solution on the Bank's risk exposure in relation to its area of activity is assessed, including the impact on money laundering, operational, reputational and legal risks, identifying possible mitigation measures and remedial actions for each risk identified. Suitable documentary evidence of these assessments is kept.

In cases of remote onboarding, the Bank acquires the identification data of the customer and the representative and obtains evidence in the form of a copy – obtained via fax, mail, in digital or similar format – of a valid ID document, pursuant to current regulations. In any case, it is not permitted for Prospects that do not have a digital identity or a certificate for generating a digital signature to open accounts online.

With regard to identification methods, various methods are currently available, at the Customer's discretion, without prejudice to the Customer's right to make use of the possibility of face-to-face identification through a financial advisor of the Bank: (i) through bank transfer, ordered by the Customer, from a banking intermediary based in Italy or in an EU country, (ii) by entering the SPID credentials (in this case the Customer is redirected to the site of the Aggregating Entity, from which he/she may be able to select an Identity Provider and log in to SPID with specific credentials) and, finally, (iii) by issuing a qualified digital signature certificate issued by the Certification Authority (CA) that uses the 'video call' mode with webcam to ascertain the identity of the Customer, a necessary element for obtaining the aforementioned certificate.

With a view to limiting exposure to possible risks of money laundering and/or fraud, the online opening of bank accounts is currently only permitted to natural persons (consumers), aged 18 or over, residing in Italy. In any case, the establishment of remote relationships is not permitted by parties:

- other than natural persons;
- not resident in Italy;
- showing FATCA implications (US Persons);
- falling under the category of Politically Exposed Persons;
- characterised by “negative reputational indicators” based on the “lists of names” and databases used by the Bank.

In these cases, the process for establishing the relationship can only occur through the Bank personnel directly responsible for the customer due diligence process.

Specific first-level controls are also envisaged on Transactions carried out by Customers acquired through onboarding procedures not assigned to a financial advisor of the Sales Network, including through the use of specific software developed internally, in order to detect any possible fraudulent or incorrect use of the accounts.

Where, as a result of the controls carried out, the Operating Structures ascertain, suspect or have reasonable grounds to suspect that a money-laundering or terrorist financing transaction has been carried out, is in progress or has been attempted, they shall promptly report the suspicious transaction to the AML Function, for in-depth analysis and assessment of the case.

In consideration of the aforementioned limitations and the controls adopted by the Bank, the Anti-Money Laundering Function has carried out special checks and has considered that the risk associated with the remote onboarding process is, on the whole, minimal.

## **5.2 CUSTOMER PROFILING**

---

In order to grade the depth and extension of due diligence obligations, the Bank adopts suitable procedures for profiling each customer according to their money laundering risk, which consider the following risk factors:

- relating to the customer, the representative and the beneficial owner;
- relating to products, services, transactions or distribution channels;
- geographic.

This approach is an application of the broader principle of proportionality referred to in current regulatory provisions, the aim of which to maximise the effectiveness of corporate controls and streamline the use of resources.

To that end, the information on the money laundering risk profile is made available to the financial advisors of the Sales Network and to the Operating Structures in charge of the actual management and administration of relationships with customers. In line with the provisions of current regulations, personnel with access to the information on customer risk profiles must maintain the utmost confidentiality, refraining from communicating that information to the customers or to third parties.



The electronic controls available to the Bank<sup>9</sup> allow the determination of a “score”, based on the processing of data and information acquired on initial registration, opening of business relationships, execution of occasional transactions or monitoring of operations undertaken, that represents the level of money laundering risk and the classification of customers into four classes. The table below shows possible risk profiles that can be assigned to customers and the updating frequency of the information:

| <b>Class</b> | <b>Risk profile</b> | <b>Information updating frequency</b> |
|--------------|---------------------|---------------------------------------|
| <b>1</b>     | Immaterial          | Every 48 months                       |
| <b>2</b>     | Low                 | Every 36 months                       |
| <b>3</b>     | Medium              | Every 24 months                       |
| <b>4</b>     | High                | Every 12 months                       |

The Bank monitors and periodically updates the scores and rules attributed to the risk profiling system, also in relation to developments in the reference context and leading market practices.

As part of a Group, the Bank (and likewise the other companies of the Group) in any event assumes, for the same customer, the highest profile among those assigned by all the companies of the Group.

The profiling system ensures that the scores assigned by the electronic system, are consistent with the knowledge of the customer.

In identifying risks relating to the customer, the representative and the beneficial owner, the Bank considers additional risk factors linked to:

- the business activities or profession of the customer and its beneficial owner,
- the reputation of the customer and its beneficial owner,
- the nature and conduct of the customer and its beneficial owner, also in relation to a possible increase in the risk of terrorist financing,

assessing available information and any negative information originating from the media or other information sources considered well-founded and reliable, examining reports on abnormal conduct issued by the Sales Network or employees of the Operating Structures that actually manage and administer the relationships with customers.

Based on all the information acquired, if the financial advisor or employee deem the customer’s conduct to be anomalous or a transaction to be unreasonable, based on the usual operations/assets/income of the customer, a Suspicious Transaction Report is promptly sent to the Anti-Money Laundering Function so that an in-depth analysis of the case can be performed and submitted to the Suspicious Transaction Reporting Manager for

---

<sup>9</sup> The Bank uses GIANOS® GPR software for customer profiling in relation to money laundering risk.

assessments under his/her responsibility, including raising the level of the customer's risk profile if necessary, keeping records of the assessments conducted.<sup>10</sup>

In assessing anomalous conduct by customers assigned to them or the unreasonableness of transactions implemented by such customers, financial advisors take into account all the data acquired from customers and the information in their possession, including that acquired from other intermediaries with the explicit consent of the customer that subscribed to the information service on accounts held with one or more payment service providers, offered by the Bank as an Account Information Service Provider - AISP.

With regard to risk class 4, equal to a "high" risk profile, the Bank considers the following to have the highest money laundering risk, regardless of the scores assigned by the customer profiling system used:

- a) the customers, beneficial owners, designated beneficiaries and representatives for which negative reputational indicators have been identified, based on:
- inclusion of their names in the lists of associated persons or entities for the purpose of applying the freezing obligations envisaged by the UN Security Council, EU Regulations or decrees adopted pursuant to Legislative Decree no. 109 of 22 June 2007 or that of the Office of Foreign Asset Control (OFAC) of the US Treasury Department;
  - negative information originating from the media or other information sources;
  - negative information provided directly by the customer or the reference financial advisor concerning criminal proceedings, tax proceedings and administrative liability of entities proceedings (pursuant to Legislative Decree 231/01), etc.;
  - requests/measures originating from the Judicial Authority, pursuant to the Anti-Mafia Code (assessments required by the Criminal Courts pursuant to Legislative Decree 159/2011 - Anti-Mafia - preliminary investigation phase) or to the anti-money laundering regulations (assessments required by the Criminal Courts pursuant to the Anti-Money Laundering Decree - preliminary investigation phase);
  - attachment orders, full and preventive injunction measures adopted by the Judicial Authority;
- b) the Customers, Beneficial Owners and Executors subject to reporting to the FIU by the Bank or another Group company in the last 5 years, or who continue to pose critical issues;
- c) customers whose funds originate from voluntary disclosure transactions or similar procedures for capital repatriation associated with tax evasion or other crimes, regularisation of which was completed within the previous 5 years;
- d) cross-border through accounts involving the execution of payments with a credit institution or correspondent bank of a third country;

---

<sup>10</sup> For more details and examples of anomalous transactions and conduct that require further analysis by the financial advisors of the Sales Network and the employees that actually manage and administer relations with customers, refer to the Regulations on the process of Reporting Suspicious Transactions.

- e) business relationships, professional services and occasional transactions with customers and related beneficial owners who are Politically Exposed Persons,<sup>11</sup> except in cases where such PEPs are acting as Public Administration bodies;
- f) business relationships, professional services and transactions that involve high-risk third countries, as well as customers and beneficial owners with residence or registered office in high-risk third countries and high-risk geographic areas;<sup>1213</sup>
- g) structures that can be qualified as asset interposition vehicles, such as trusts, fiduciary companies (regardless of related enrolment in the register pursuant to art. 106 of the Consolidated Finance Act), foundations, non-profit organisations, companies with all or part of the share capital held by a fiduciary company, a trust, an entity or similar legal status; companies controlled by fiduciaries;
- h) customers with an anomalous or excessively complex corporate structure, given the nature of the business conducted, foreign parties other than individuals;
- i) customers carrying out a type of business activity characterised by high use of cash or with an involvement in sectors particularly exposed to corruption risks;

---

<sup>11</sup> For the purpose of customer risk profiling, the Bank may also consider customers or beneficial owners that hold public offices in areas not covered by the concept of PEP, but for which significant exposure to the risk of corruption in any event exists. Such a case, though not resulting per se in enhanced due diligence obligations, is assessed along with other subjective and objective factors considered in the overall customer risk profiling.

<sup>12</sup> In order to assess geographic risks, the Bank considers the following risk factors

- 1) third countries that authoritative and independent sources believe lacking in effective controls for the prevention of money-laundering (such as countries included in the EU/GAFI list);
- 2) countries and geographic areas that finance or support terrorist activities or where terrorist organisations operate (such as countries included in the EU/GAFI lists);
- 3) countries subject to sanctions, embargoes or similar measures adopted by competent national and international bodies;
- 4) countries assessed by authoritative and independent sources as non-compliant with international standards on transparency and exchange of information for tax purposes;
- 5) countries and geographic areas assessed as having a high level of corruption or susceptible to other criminal activities, as determined by authoritative and independent sources.

The Bank considers the geographic risks listed above based on the different critical level assigned to each. In implementing this risk-based approach:

- the countries under points 1) and 2) are considered “high-risk third countries”;
- the countries under points 3) which are not already included among those under points 1) and 2) are considered “high-risk geographic areas”;
- the geographic risk factors referred to in points 4) and 5) do not automatically involve the assignment of a high risk profile to the countries concerned, but are assessed for the purpose of a possible increase in the risk level, together with additional relevant factors, using the Basel AML Index, calculated by the Basel Institute on Governance, an independent and non-profit organisation, specialised in combatting corruption and other financial crimes.

The Anti-Money Laundering Function can in any event propose, to the CEO, suspension of the opening of new relationships and the execution of transactions with countries characterised by one or more of the geographic risk factors described above.

The updated list of countries considered higher risk and those with which operations have been suspended is periodically made available to the Board of Directors, as part of the reporting periodically produced by the Anti-Money Laundering Function and sent to the Anti-Money Laundering Managers of the subsidiaries.

<sup>13</sup> For the purpose of increasing the risk profile, for high-risk third countries not only the residence, but also citizenship is relevant.

j) Customers that benefit from investment banking services.

The Bank also adopts strict procedures to adequately consider the risks associated with the offer of services with a high degree of customisation to customers with significant assets, carrying out a specific investigation for the signature of personalised consulting contracts by the AML Operational Control Unit, in order to ascertain whether the Customer should be considered high risk, by verifying, in particular: the presence of negative reputational indices, the use of assets intermediaries (such as trusts and fiduciary companies), Politically Exposed Person (PEP) status, connections with high-risk Third Countries, the presence of pre-existing reports to the FIU against the Customer, the residence of the Customer and/or Beneficial Owners of the relationships in a foreign country, the high degree of customisation of services certified by the Wealth Management Department.

On the occurrence of one or more of the cases listed above, the Customer is classified as high risk and subject to Enhanced Due Diligence. In all other cases, the Customer can only be classified according to the scores assigned by the Customer profiling system (GIANOS® GPR), without prejudice to the updating of the investigation by the AML Operating Control Unit at least every 24 months and in any case when one or more of the individual cases listed above occur.

The Bank also considers customers identified by the Suspicious Transaction Reporting Manager after prudent assessment as having high money laundering risk. The Manager may also decrease the assigned scores, as a result of their assessment after analysing specific positions, retaining evidence of the analyses conducted. In any case, it is not permitted to modify independently the scores assigned by the remaining Personnel.

This without prejudice to the option of the AML Operational Monitoring Unit of AML Function to ask the financial advisors or employees who administrate and manage relationships with the customers to perform the enhanced due diligence process in all cases, including those not listed above, where money laundering risk appears to be particularly high.

In order to ensure correct assessment of the risks related to products, services, transactions or distribution channels, the competent corporate functions of the Bank ensure the involvement of the AML Function from the preliminary analysis and feasibility study phases. The risk must be carefully assessed, in particular, in the case of latest generation products and commercial practices that include the use of innovative distribution mechanisms or technologies for new or pre-existing products.

### **5.3 ENHANCED CUSTOMER DUE DILIGENCE**

---

In the presence of high money laundering risk, the Bank adopts enhanced customer due diligence measures by acquiring additional information on the customer, on the beneficial owner and on any representative, analysing in depth all elements on which the assessments are based as regards the purpose and nature of the relationship, and intensifying the application frequency of procedures aimed at guaranteeing constant control during the business relationship.

As it forms part of the more general due diligence process and in-depth customer due diligence, the application of enhanced due diligence is particularly important, also in connection with the principle of “active cooperation” and the obligation of reporting suspicious transactions (see paragraph 5.7).

Based on the model adopted by the Bank, the enhanced customer due diligence activities are primarily assigned to financial advisors or to the appointed employees, who are required to:

- acquire additional information on the customer and the beneficial owner;
- acquire/update and assess information on the reputation of the customer and/or the beneficial owner (including any prejudicial elements obtained by consulting open sources, for instance through the use of Internet search engines);
- carefully assess the information provided by the customer on the purpose and nature of the relationship, assessing this in relation to the other information already available on opening of the relationship, or in the case of customers who already have a relationship with the Bank, with the activities already identified. In this regard, the following elements are taken into consideration: the number, size and frequency of the transactions performed, the origin/destination of the funds, the nature of activities carried out by the customer and/or the beneficial owner, the reasonable nature of the transactions performed in relation to the customer's overall profile;
- perform in-depth assessments on the Origin of the Customer's Assets and the Source of the Funds used in the business relationship, through a structured process that takes into consideration, first and foremost, the reliability of the information available to the financial advisor and to the Bank, as well as the availability of financial-equity information produced directly by the customer or inferred from movements in the relationship (e.g. emoluments or dividends credited, etc.) or retrievable through open sources or from public databases (e.g. financial statements, VAT and income tax returns, notary deeds, succession declarations, declarations/documents from the employer or other intermediaries). In this regard, certain aspects, such as the degree of knowledge of the customer and/or the seniority of the relationship, the consistency of the customer profile with its financial-equity position, are of a particular importance;
- carry out more frequent assessments and updates of database records and of information collected for know-your-customer purposes.

The Bank also requires authorisation from parties with administrative or management powers or their delegates or, in any event, parties performing an equivalent function:

- before starting, continuing or maintaining a business relationship or executing an occasional transaction with Politically Exposed Persons;
- before starting, continuing or maintaining a business relationship or executing a Transaction involving high-risk Third Countries;
- before starting, continuing or maintaining a business relationship or executing an occasional transaction with trusts, foundations, complex corporate chains, parties with registered offices in foreign countries or fiduciary companies.

Without prejudice to the possibility of involving the AML Function in carrying out Enhanced Due Diligence in cases where, due to objective, environmental or subjective circumstances, money-laundering risk appears to be particularly high, it is in any case mandatory to seek the opinion of the AML Function in advance of the authorisation investigation by the parties with management or administrative powers or by their delegates before starting, continuing or maintaining a business relationship or executing an Occasional Transaction with

Politically Exposed Persons, or before starting, continuing or having business relationships involving High-Risk Third Countries.

If the parties with management or administrative powers or their delegates or, in any case, those who perform an equivalent function decide not to comply with the opinion of the AML Function, they are required to formalise and justify such a decision and to identify the measures that will be adopted to mitigate the risks reported.

The above measures are commensurate with the Customer's risk, also providing for the acquisition of additional information from the Customer and/or the formalisation of the assessments made by the financial advisor of the Sales Network or by the employees who manage and administer, in practice, relations with customers, by filling in specific forms:-

- Customers with a higher risk of money laundering: the formal acquisition of additional data by Customers in the area is envisaged, with particular reference to Politically Exposed Persons, residing in high-risk third countries or geographical areas at high risk, structures qualifying as intermediary asset vehicles and Customers who benefit from services with a high degree of personalisation and the subsequent acquisition, by the Bank, of the form "Addendum to the personal data record and form for customers due diligence" signed by the Customer; solely for Customers classified as PEPs, for all investment transactions in Policies, Funds, portfolio or fund management (GPM/GPF), the "Certification of Origin of Funds Used in the transaction or in the business relationship" form is also provided, signed by the Customer; it is also envisaged that the financial advisor or employee in charge will draw up the appropriate "Customers with HIGH profile anti-money laundering assessment form", sent through the AML WorkFlow, at the due date of the risk profile (validity 12 months) or in occasion of the planned investigation, carried out by the AML Operational Control Unit before starting, continuing or maintaining a Business relationship with the aforementioned Customers; in the case of transactions in investment products (Policies, GPM/GPF, Funds), it is the responsibility of the financial advisor or the appointed employee to fill in the "Transaction Due Diligence" form, acquiring documented information on the Origin of the Funds;
- Customers with high money laundering risk, classified as such by the internal profiling procedure: the entire Enhanced Due Diligence process is managed by the financial advisor or appointed employee, who on expiry of the risk profile (validity of 12 months) or transfer of the customers to "high" risk will be required to draw up the specific AML Assessment Form - Customers with HIGH Risk Profiles" sent through the AML WorkFlow; in the case of transactions with investment products (policies, fund or portfolio management (GPM/GPF)), it is the responsibility of the financial advisor or appointed employee to complete the "Transaction Due Diligence" form, by obtaining documented information on the Origin of the Funds;
- Customers with medium money laundering risk, classified as such by the internal profiling procedure: the entire enhanced due diligence process is managed by the financial advisor or appointed employee, who on expiry of the risk profile (validity of 24 months) will be required to draw up the specific "AML Assessment Form - Customers with MEDIUM Risk Profiles", sent through the AML Workflow, in accordance with a risk-based approach, considering Customers who hold a total equity in Group products (managed or administered) equal to or exceeding Euro 100,000.

Without prejudice to "transactions characterised by unusually high amounts or which raise doubts about the purposes for which they are concretely ordered", which shall always be brought to the attention of the AML Function by the financial advisor or the employee that actually manages and administers relations with Customers or by employees of the Operational Structures as part of the activities performed, irrespective of the risk profile assigned by the customer profiling system, the Bank considers the following transactions to have a high risk of money laundering:

- a) Transactions in cash, frequent and unjustified, characterised by the use of high denomination banknotes in Euro or the presence of banknotes that are damaged or counterfeit;
- b) Transactions involving cash or other cash equivalents originating from abroad, in a total amount equal to or exceeding Euro 10,000;
- c) Transactions involving high-risk third countries;
- d) Transactions relating to oil, weapons, precious metals, tobacco products, cultural artefacts and other moveable assets of archaeological, historical, cultural or religious significance or of rare scientific value, as well as ivory and protected species;
- e) next generation products and commercial practices, including innovative distribution mechanisms and the use of innovative or evolving technologies for new or pre-existing products;
- f) Investments in products placed by the Bank (policies, funds, GPM/GPF), relevant to the income/asset-based profile of the Customer, or in all cases of investment transactions of an amount equal to or greater than Euro 500,000.

In the cases mentioned above, it is the responsibility of the financial advisor or the employee who actually manages and administers relations with Customers, to carry out the Enhanced Due Diligence, collecting documented information on the Origin and/or destination of the funds, and also filling in, in the case of the Transactions referred to in letter f), the 'Transaction Due Diligence' form, to be produced at the request of the AML Function of Banca Mediolanum S.p.A. and/or another Group company.

As indicated in paragraph 4.1 above, in a case of objective, environmental or subjective circumstances that increase money laundering risk, the activities related to customer due diligence are performed directly by the AML Function.4.1

These refer in particular to the cases listed in points a), b), c) and d) of paragraph 5.2 above.

The AML Function must also be involved by the financial advisors and employees of the Operating structures which are entrusted with the actual administration and management of relationships with customers in all cases in which anomalies are identified in the conduct of the customer or the representative, as described above.

In these cases, the enhanced due diligence process envisages the acquisition of information through the financial advisor or employee of the Operating Structure who actually manages and administers the relationships with customers.

The AML Function carries out additional in-depth analyses to verify the consistency of the transactions under scrutiny and between the information collected and that held by the Bank and, if necessary, asks the customer, through the financial advisor or employee concerned, to provide specific documentation.

In cases other than the above, the AML Function uses methods, defined by the Function, to verify the adequacy of the enhanced due diligence process conducted by the AML Operational Monitoring Unit and the financial advisors or employees responsible for the actual management and administration of relationships with customers.

#### **5.4 SIMPLIFIED CUSTOMER DUE DILIGENCE MEASURES**

---

In the presence of low money laundering risk, the Bank may apply simplified customer due diligence measures under the profile of an extension and frequency of obligation fulfilments, in relation to:

- companies listed on a regulated market and subject to disclosure obligations with an obligation to ensure adequate transparency of beneficial ownership;
- public administrations, or institutions or bodies that carry out public functions, in compliance with EU law;
- banking and financial intermediaries listed in art. 3, paragraph 2, of the AML Decree - except for those under letters i), o), s), v) - and banking and financial intermediaries operating in the EU or in a third country with an effective system for combatting money laundering and terrorist financing;
- supplementary pension schemes governed by Italian Legislative Decree no. 252 of 5 December 2005, provided that these do not include redemption clauses other than those in art. 14 of that Decree, and that they cannot be used as collateral for a loan beyond the cases permitted by law;
- pension schemes or equivalent systems that pay pension benefits to employees, for which contributions are paid through deductions from remuneration and do not allow beneficiaries to transfer their rights.

For the correct fulfilment of the above obligations, the Bank distinguishes between “active” and “passive” counterparties.

“Active” counterparties are the customers, i.e. companies that have business relationships with the Group (e.g. placement and/or distribution agreements) or that carry out occasional transactions (e.g. treasury transactions, hot money transactions).

The following, for example, are “active” counterparties:

- institutions/companies holding correspondent and/or settlement accounts;
- companies managing mutual investment funds;
- institutions/companies that are issuers of securities listed through public offers to which the Bank subscribes directly;
- institutions/companies with which professional relationships are in place for the placement of electronic money or financing/investment products;

The Bank excludes from due diligence obligations any “passive” counterparties, i.e. financial intermediaries (domestic and international) with which it has no business relationships but, at its own initiative, it uses to finalise transactions on behalf of its customers, holders of relationships (securities dossier transfer transactions, securities purchase/sale transactions, etc.). Within this scope, “passive” counterparties assume



the role of “service providers” at the initiative of the Bank and not as customers requiring the establishment of a business relationship or execution of an occasional transaction. “Passive” counterparties include, for example, depository banks and companies registered as issuers of securities.

Without prejudice to the need to ensure correct identification of the customer and the beneficial owner before initiating the business relationship or carrying out the transaction, the simplified due diligence measures consist in the option of:

- performing beneficial owner due diligence pursuant to point 2), acquiring a declaration confirming the data, signed by the customer, under its own liability;
- using assumptions for identifying the scope and the nature of the business relationship, where the product offered is intended for a specific use;
- adopting a frequency of 48 months for the purpose of updating the due diligence data collected, without prejudice to the need to arrange due diligence if a new business relationship is opened or there is an increase in the money laundering risk profile due, for example, to the identification of negative reputational indicators concerning the customer and/or the beneficial owner;

The Bank verifies that the assumptions for application of the simplified procedure remain valid, according to the methods and frequency established according to the risk-based approach.

In particular, the measures for a simplified due diligence do not apply when:

- the conditions for application of the simplified measures, based on the risk indicators envisaged in the AML Decree and the Provisions, cease to exist;
- the monitoring activities on overall operations of the customer and the information acquired during the course of the relationship lead to excluding the presence of a low risk situation;
- there is in any event a suspicion of money-laundering or financing of terrorism

## **5.5 OBLIGATIONS TO ABSTAIN**

---

The Bank does not exclude, in a preventive and generalised manner, the possibility of opening or maintaining business relationships with specific categories of customers or potential customers resident or with a regular residence permit in Italy, due to their potentially high exposure to the risk of money laundering, but adopts rigorous processes to assess, on a case-by-case basis, the risk associated with the customer or prospect, keeping evidence of the decisions made.

If the Bank finds it objectively impossible to perform adequate customer due diligence, it must abstain in any case from pursuing the relationship or transactions and, if necessary, must terminate any business relationship already in place and decide whether to submit a suspicious transaction report to the Financial Intelligence Unit (FIU). Before making a Suspicious Transaction Report to the FIU, and in order to exercise any powers of suspension, the Bank will abstain from carrying out transactions that it suspects are associated with money laundering or with terrorist financing.

If it is not possible to abstain as there is a legal obligation to accept the action, or execution of the transaction cannot be postponed due to its nature, or if abstention could hinder the investigations, there is still an obligation to immediately submit a suspicious transaction report.

In any event, the Bank will abstain from initiating any relationships or from carrying out transactions and will end any existing business relationships with:

- Customers who reside or have registered offices in countries and geographic areas assessed as very high risk by the Chief Executive Officer or as proposed by the AML Function
- credit or financial institutions situated in a non-EU country that does not impose obligations equivalent to those in EU directives issued on such matters;
- shell banks, wherever they may be located;
- companies that provide services to shell banks;
- unlicensed banks;
- financial institutions recorded under Section 311 of the USA Patriot Act;
- subjects who, directly or indirectly, are part of fiduciaries, trusts, anonymous companies (or controlled through bearer shares) with registered office in high-risk third countries;
- companies that have issued bearer shares or are investees of nominee shareholders;
- *trusts for which adequate information is unavailable, inaccurate or not updated with respect to the beneficial owners of the trust or its nature or scope or which have subjective or objective circumstances which may indicate the use of a trust in order to conceal anomalous conduct, also in the light of indications provided by the competent authorities;*
- relationships held in the name of trusts where the information available is inadequate, inaccurate or not updated with respect to the beneficial owners;
- payment service providers (agents and/or money transfer companies) who do not carry out financial activities only;
- companies manufacturing weapons or ammunitions;
- legal entities who are direct or indirect investees of one of the above-mentioned parties.

The Bank abstains from offering products/services or carrying out transactions that may facilitate anonymity, or concealment of the identity of the customer or the beneficial owner, as well as from establishing business relationships or remotely carrying out occasional transactions, not assisted by adequate recognition mechanisms and procedures.

## **5.6 CONTROLS TO COMBAT TERRORIST FINANCING**

---

In order to ensure the correct fulfilment of obligations and prohibitions envisaged in current regulations on anti-terrorism, the Bank:

- checks if the customer and beneficial owner are included in the “lists” of parties and entities designated by the UN Security Council, the European Union, Ministry of Economy and Finance decrees, and the Office of Foreign Asset Control (OFAC) of the US Treasury Department;
- refuses to carry out any transactions that involve parties on the lists described in the previous paragraph (presenters, representatives, ordering parties or beneficiaries);

- does not make cover payments in US dollars;<sup>14</sup>
- applies the restrictions envisaged for relationships with all customers where correspondence with the lists described in the first paragraph is confirmed;
- informs the Financial Intelligence Unit (FIU) of the measures applied in accordance with Legislative Decree 109/2007, indicating the parties involved, the amount and nature of the funds or economic resources, within thirty days of the date of entry into force of EU regulations, decisions of international bodies and the European Union, and Ministry of Economy and Finance decrees or, if later, from the date the funds or economic resources were withheld.

In identifying the risks associated with the nature and conduct of the customer and the beneficial owner, personnel must in any event pay specific attention to risk factors which, though not specific to terrorist financing, could indicate a risk of terrorist financing.

## **5.7 REPORTING SUSPICIOUS TRANSACTIONS TO THE FINANCIAL INTELLIGENCE UNIT (FIU)**

---

Pursuant to current regulations, the Bank immediately sends a suspicious transaction report to the FIU when it knows, suspects or has reasonable grounds to suspect that money laundering or terrorism financing transactions have been carried out or attempted or, in any event, that the funds, regardless of their amount, derive from criminal activities.

The financial advisors of the Sales Network and the employees of the Operating Structures actually responsible for the administration and management of relations with customers represent the first reporting level in accordance with current regulations. Therefore, it is their duty to continuously monitor the progress of the relationship and the transactions carried out, including through the tools and procedures available on the BMedNet Portal, and immediately send a suspicious transaction report by entering an SOS sheet into the AML WorkFlow to the AML Function, in accordance with procedures and operating methods established internally, before executing the transaction. The exclusions are cases in which the transaction must be performed as there is a legal obligation to accept the instruction, or in cases where the transaction cannot be postponed when taking into account normal operations, or when postponement of the transaction may hinder the investigations.

In order to facilitate the identification of suspicious transactions, the Bank will refer in particular to the FIU Regulation laying down anomaly indicators issued and periodically updated by the Financial Intelligence Unit (FIU), preparing specific guidelines and plans for training and professional updating for the financial advisors of the Sales Network and employees of the Operating Structures.

The Bank, within the scope of its organisational independence, can also use automatic identification procedures for “anomalous” transactions. The AML Function prepares all procedures relating to the reports received and submits them to the Suspicious Transaction Reporting Manager, who sends them to the FIU if it is considered necessary, based on all elements at his/her disposal and the evidence inferable from the data

---

<sup>14</sup>Cover payments refer to the transfer of funds used when there is no direct relationship between the payment service provider (PSP) of the ordering party and the beneficiary, and a chain of correspondent accounts therefore has to be used through a PSP. Three or more PSPs are involved in a cover payment.

and information held on record, without including the name of the whistleblower. In compliance with IVASS Measure no. 111 of 13 July 2021, the Manager adopts specific expedients to ensure that the insurance companies, with which the Bank, as an intermediary enrolled in section D of the Single Register of Intermediaries, has distribution agreements for life insurance products, are sent the reports of Suspicious Transactions carried out by customers common to the companies concerned, also where the Bank has already forwarded the report directly to the FIU and even if the report does not pertain to the customer's insurance operations.

The Bank and the companies of the Group adopt suitable measures to ensure confidentiality of the identity of individuals submitting a suspicious transaction report; the name of the whistleblower may only be revealed when the Judicial Authority, issuing a justified decree in this regard, deems it indispensable for the purpose of assessing offences to be prosecuted.

It is also prohibited for parties required to report any suspicious transaction, and anybody who has knowledge of it, to inform the customer concerned or any third party that a report has been issued, that additional information requested by FIU has been submitted or information on the existence or probability of investigations into money laundering or financing of terrorism. This prohibition applies:

- to communications sent to the Supervisory Authorities for the sector during the performance of functions envisaged in the AML Decree;
- to communications concerning the sharing of information at the level of banking and financial intermediaries, suitable to ensuring full compliance with the provisions on the prevention of money-laundering and financing of terrorism;
- to communications with other banking and financial intermediaries, external to the Group, operating in a Member State or located in third countries, as long as they apply measures equivalent to those envisaged in the AML Decree, in cases relating to the same customer or the same transaction, for the sole purpose of preventing money laundering or terrorist financing.

## **5.8 COMMUNICATION OF INFRINGEMENTS TO THE MINISTRY OF ECONOMY AND FINANCE**

---

The AML Function and the relevant Operating Structures which, in exercising their functions or activities, learn of infringements of the provisions on limiting the use of cash and bearer securities and the ban on savings accounts that are unnamed or have fictitious names (articles 49 and 50 of the AML Decree), ensure compliance with communication obligations to the Ministry of Economy and Finance within thirty days.

This communication is required from members of the Board of Statutory Auditors when they find breaches of the above-mentioned provisions in the exercise of their control and supervisory functions.

If the transfer has already been subject to a suspicious transaction report in accordance with article 35 of the AML Decree, there is no obligation to inform the Ministry of Economic Affairs and Finance.

## **5.9 OBJECTIVE COMMUNICATIONS**

---

The AML Function Manager is responsible for forwarding objective communications, pursuant to ex article 47 of the AML Decree, to the FIU.

The Manager must ensure the correct functioning of the information system for fulfilling the obligations to issue objective communications and represents the FIU contact for all issues related to the transmission of objective communications and any requests for information.

The AML Function Manager can authorise other natural persons under their responsibility to input and transmit the objective communications.

## 5.10 DATA AND DOCUMENT STORAGE OBLIGATION

---

In order to fulfil storage obligations for data relating to business relationships and transactions carried out, the Bank uses suitable storage systems<sup>15</sup> where the business relationships with customers are registered, together with their related parties and transactions that exceed the materiality thresholds.

For the above purposes, the Bank continues to make voluntary use of the AUI; this decision allows processes and controls already fully consolidated to be maintained, in addition to ensuring the timely availability of information acquired during the due diligence process, both for fulfilling reporting obligations and for any in-depth analysis of individual positions.

The aggregate data recorded is sent to the Financial Intelligence Unit (FIU) every month, which analyses to identify any money laundering or terrorist financing activities.

With regard to fulfilling storage obligations, the Bank will keep:

- the copy or reference of the documents requested for due diligence purposes, for a period of ten years from the end of the business relationship;
- the records and registrations of transactions and business relationships, consisting in the original documents or copies with similar validity as proof in legal proceedings, for ten years from execution of the transaction or termination of the business relationship.

With regard to contracts signed by customers through SPID digital identity and/or with digital signature issued by the company InfoCert as a qualified trust service provider, the Bank uses, by virtue of a specific contract, the electronic archiving service provided by InfoCert itself, pursuant to:

- Legislative Decree 82/2005, the Digital Administration Code (the storage system, as required by Art. 44 of the DAC, guarantees authenticity, integrity, reliability, legibility and availability of electronic documents),
- the AgID (Agency for Digital Italy) Guidelines in force from 1 January 2022<sup>16</sup>,
- CNIPA Resolution no. 11 of 19.02.2004 (technical rules),
- Ministerial Decree of 23 January 2004 (obligations for electronic documents).

with which it has declared full compliance.

### 5.10.1 Exemptions regarding data storage

---

<sup>15</sup> For correct system maintenance, the Bank uses the outsourcer CEDACRI S.p.A. in accordance with a specific outsourcing agreement.

<sup>16</sup> Art. 14-bis and Art. 71 of the Digital Administration Code - Legislative Decree no. 82 of 7 March 2005

Pursuant to art. 8, paragraph 1 of the “*Provisions for the storage and availability of documents, data and information to combat money laundering and terrorist financing*” issued by the Bank of Italy on 24 March 2020 and in force since 1 January 2021, the Bank opted not to apply the provisions set out in articles 5 and 6, regarding business relationships or transactions executed with:

- banking and financial intermediaries pursuant to art. 3, paragraph 2 of the AML Decree, excluding those in letters i), o), s) and v), with registered office in Italy or another Member State;
- banking and financial intermediaries with registered office in a third country with low money laundering risk and in accordance with the criteria indicated in Annex 1 to the provisions on customer due diligence;
- The parties referred to in art. 3, paragraph 8 of the AML Decree;
- The provincial treasury of the State or the Bank of Italy.

### **5.11 STAFF TRAINING**

---

Professional qualification and updating activity for personnel assumes continuity and a systematic nature within the programmes that take into account the development of regulations and procedures.

To this end, the Bank uses permanent training programmes and professional updating courses in order to correctly apply the provisions of the AML Decree, recognise transactions related to money laundering or terrorist financing and adopt the correct conduct and procedures. These programmes ensure, inter alia, the awareness and updating of the knowledge of staff regarding how the customer's remote *onboarding* solution works, the associated risks and the customer's remote onboarding policies and procedures aimed at mitigating these risks.

Particular attention is paid to the financial advisors of the Sales Network, to the employees involved in the remote onboarding process, and to the employees of the Operating Structures that administer and manage, in practice, the transactions of the Customers as well as those involved in the process of reporting suspicious transactions. Specific training programmes are implemented for the staff who work in the Anti-Money Laundering Function.

The qualification and professional updating of staff is carried out on a continuous, systematic basis within the scope of the internal programmes that take account of developments in the rules and procedures.

If an external supplier is used, the AML Manager ensures that the persons tasked with the provision of training have the anti-money laundering knowledge required to guarantee the quality of instruction and that the content thereof is adequate for the specific needs of the Bank.

### **5.12 INTERNAL SYSTEMS FOR REPORTING INFRINGEMENTS**

---

The Bank adopts specific whistleblowing procedures for internal reporting by employees and collaborators, regarding potential or actual infringements of the provisions governing money-laundering and financing of terrorism.

These procedures guarantee:

- protected confidentiality of the identity of the whistleblower and the alleged perpetrator of the infringements, without prejudice to the rules governing investigations and proceedings initiated by the judicial authority in relation to the subject matter of the reports;
- protection of the whistleblower against retaliatory, discriminatory or in any event unfair conduct following the report;
- development of a specific reporting channel, anonymous and independent, proportionate to the nature and size of the obliged party.

These procedures are brought to the attention of all personnel by the Internal Audit Function.

### **5.13 SELF-ASSESSMENT EXERCISE FOR MONEY LAUNDERING RISK**

---

Pursuant to art. 15 of the Anti-Money Laundering Decree, the Bank conducts an annual self-assessment of money laundering risk, coordinating the exercise carried out by each Group company, and conducts a Group self-assessment exercise.

The self-assessment is performed by assessing the exposure to the risk of involvement in situations of money laundering for each business line considered significant, based on its nature, organisation, operational specifics and complexity, considering the risk factors linked to operations, products and services, types of customers, distribution channels and geographic area, as well as the sector-specific risk factors set out in Title II of the current European Banking Authority Guidelines on customer due diligence and risk factors (EBA/GL/2021/02). As an insurance intermediary enrolled in Section D of the Single Register of Intermediaries and pursuant to IVASS Measure no. 111 of 13 July 2021, the Bank considers insurance intermediation as a separate line of business, in addition to banking and financial activities.

The self-assessment is conducted based on a methodology that includes the following macro-activities:

- identification of inherent risk;
- Vulnerability analysis;
- determination of residual risk;
- remedial actions identified for any existing critical issues and for the adoption of suitable measures to prevent and mitigate money laundering risk.

The exercise is promptly updated when new significant risks arise or there are significant changes to existing risks, in operations or in the organisational or corporate structure.

The results of the self-assessment exercise and the adjustment measures defined in light of its results and the related degree of progress are illustrated in specific chapters of the Annual Report produced by the Anti-Money Laundering Function.

### **5.14 SANCTIONING AND REPUTATIONAL RISKS**

---

The obligations described in this Policy, aimed at the correct fulfilment of requirements related to combatting money laundering and terrorist financing, must be strictly complied with, based on the respective areas of responsibility, by all personnel and in particular by those who manage and administer relationships with

customers, given the correlation imposed by the Anti-Money Laundering Decree between the extent of money laundering risks and the preventive measures adopted by recipients of the provisions; and this not only during the start of a new relationship or the execution of an occasional transaction, but also for the entire duration of the relationship with the customer.

Note that, pursuant to the provisions of the Anti-Money Laundering Decree:

- where the Bank is held liable, exclusively or concurrently, for serious, repeated, systematic or multiple violations of the provisions regarding customer due diligence, retention and reporting obligations, or in terms of organisation, procedures and internal controls, as well as the related implementing provisions adopted by Supervisory Authorities, an administrative sanction of Euro 30,000 to Euro 5,000,000 or 10% of the total annual turnover is applied, when this percentage is greater than Euro 5,000,000 and the turnover is available and determinable;
- without prejudice to the provisions of the previous point, an administrative sanction from Euro 10,000 to Euro 5,000,000 is applied to parties who perform administration, management and control functions for the Bank who, by not fulfilling all or part of the tasks directly or indirectly related to the function or to the assignment, have enabled, facilitated or in any case made possible the violations referred to in the previous point, or have had a significant impact on the Bank's exposure to the risk of money laundering or terrorism financing. If the benefit achieved by the perpetrator of the violation is greater than Euro 5,000,000, the administrative sanction is increased to twice the amount of the benefit achieved, provided that this amount is determined or determinable.

Lastly, note that, in the event of incorrect application of the obligations envisaged in anti-money laundering regulations, additional risks are related to sanctions applicable to the Bank in terms of the administrative liability of legal entities, pursuant to Legislative Decree 231/2001.

## **5.15 COORDINATION BETWEEN THE ANTI-MONEY LAUNDERING FUNCTION AND THE OTHER CONTROL FUNCTIONS**

---

The interaction between the Anti-Money Laundering Function and the other Control Functions falls within the more general coordination among all the control functions and bodies, as defined by the Board of Directors in order to ensure correct functioning of the internal control system.

Therefore, reference should be made to the specific document "Guidelines and basic principles for coordination between Control Bodies and Functions", approved by the Board of Directors of the Bank.

This document refers to the basic principles of the Internal Control System and was drawn up as part of the broader process of implementing supervisory provisions on Internal Control Systems, and in order to promote and guarantee proper functioning of the Internal Control System as a whole, through profitable interaction between corporate bodies, their internal committees, independent auditors and the control functions.

The document is defined and organised in accordance with regulatory requirements established by the Bank of Italy and incorporates the current documentation of the Banking Group, rationalising its illustration.



## 6 REGULATORY REFERENCES

The set of provisions on combatting money laundering and terrorist financing aim to dictate measures to protect the integrity of the economic and financial system and the fairness of conduct of the operators expected to comply.

These measures are proportional to the risk in relation to the type of Customer, business relationship, professional service, product or transaction and their application, taking into account the specific nature of the activities, the size and complexity of the obliged parties expected to comply with obligations under their responsibility.

### 6.1 FOREIGN REGULATIONS

---

Below are the main reference regulations adopted at EU and national levels:

#### ***Preventing and combatting money laundering and financing of terrorism***

##### European regulations

Within the EU, the main laws on preventing and combatting money laundering and financing of terrorism are currently found in Directive (EU) 2018/843 of the European Parliament and of the Council dated 30 May 2018 (AMLD VI) *which amends Directive (EU) 2015/849 on preventing the use of the financial system for the purpose of money laundering or terrorist financing and amending Directives 2009/138/EC and 2013/36/EU (AMLD V) and Directive 2015/849/EC of the European Parliament and of the Council dated 20 May 2015 on preventing the use of the financial system for the purpose of money laundering or terrorist financing, amending Regulation (EU) no. 648/2012 of the European Parliament and of the Council and repealing Directive 2005/60/EC of the European Parliament and of the Council, and Commission Directive 2006/70/EC (AMLD IV).*

Also note Commission Delegated Regulation (EU) 2016/1675, as amended and supplemented from time to time, which supplements Directive (EU) 2015/849/EC of the European Parliament and of the Council as regards the list of high-risk third countries.

Lastly, note the EBA Guidelines - *GL/2021/02* - of 1 March 2021, pursuant to art. 17 and art. 18, paragraph 4 of Directive (EU) 2015/849 on customer due diligence measures and on factors which credit and financial institutions should consider when assessing money laundering risk associated with individual business relationships and occasional transactions ("Guidelines on Money Laundering Risk Factors"), which repeal and replace the guidance *JC/2017/37* transposed by the Bank of Italy with Note no. 15 of 4 October 2021.

On 14 June 2022, the EBA also published the "*Guidelines on policies and procedures relating to compliance management and the role and responsibilities of the anti-money laundering officer pursuant to Article 8 and Chapter VI of Directive (EU) 2015/849*" ("EBA Guidelines on AML Policies and Procedures"). By means of a provision of 1 August 2023 - published in the Official Gazette of the Italian Republic on 16 August 2023 - the Bank of Italy amended the Provisions in order to fully enforce the EBA Guidelines on AML Policies and Procedures in our legal system.

On 11 November 2022, the EBA also published the “*Guidelines on the use of remote customer onboarding solutions for the purposes referred to in Art. 13(1) of Directive (EU) 2015/849*” (“Guidelines on the use of remote customer onboarding solutions”), adopted by the Bank of Italy with Note no. 32 of 13 June 2023.

On 31 March 2023, the EBA also published:

- the “*Guidelines on policies and controls for the effective management of money laundering and terrorist financing (ML/TF) risks in providing access to financial services*” (“EBA Guidelines on de-risking”);
- the “*Guidelines laying down amendments of the EBA/2021/02 guidelines, pursuant to Art. 17 and Art. 18(4) of Directive (EU) 2015/849 on customer due diligence measures and on factors which credit and financial institutions should consider when assessing money laundering and terrorist financing risks associated with individual business relationships and occasional transactions (“Guidelines on ML/TF Risk Factors”)*” (“EBA Guidelines on customers that are non-profit organisations”).

### National regulations

At national level, the main current reference regulations are:

- Anti-Money Laundering Decree and implementing provisions issued by the Supervisory Authorities on:
  - organisation, procedures and internal controls;
  - customer due diligence;
  - objective communications;
  - aggregate anti-money laundering reports (or “S.A.R.A.”);
  - storage and use of data and information for anti-money laundering purposes;
- Legislative Decree no. 109 of 22 June 2007, as amended, on measures for preventing, combatting and suppressing the financing of international terrorism.

The decrees issued by the Ministry of Economy and Finance (MEF) and the models and patterns of anomalous conduct issued by FIU, complete the national reference framework.

Also note the following measures/notes of the Bank of Italy:

- Provisions applicable to organisation, procedures and internal controls to prevent the use of intermediaries for the purpose of money laundering and financing of terrorism - *1 August 2023*.
- Bank of Italy Provisions on customer due diligence - *30 July 2019*.
- Provisions for the storage and availability of documents, data and information to combat money laundering and terrorist financing – *24 March 2020*;
- Instructions on objective communications - *28 March 2019*;
- FIU provisions for the sending of aggregate anti-money laundering reports - *25 August 2020*;
- FIU measure containing the anomaly indicators - *12 May 2023*;
- Note no. 15 of 4 October 2021, with which the Bank of Italy fully implemented the Guidelines of the European Banking Authority on customer due diligence and risk factors (EBA/GL/2021/02), consequently updating the Bank of Italy Provisions on customer due diligence issued on 30 July 2019;

- Note no. 32 of 13 June 2023, with which the Bank of Italy implements the EBA Guidelines on Remote Onboarding Solutions;
- Note no. 34 of 3 October 2023, with which the Bank of Italy implements the EBA Guidelines on de-risking;
- Note no. 35 of 3 October 2023, with which the Bank of Italy implements the EBA Guidelines on customers that are non-profit organisations;
- Indications for obliged entities on the application of anti-money laundering obligations in the provision of private banking services and activities.

Lastly, note IVASS Measure no. 111 of 13 July 2021 on anti-money laundering obligations for insurance companies and insurance intermediaries operating in the life business.

### ***Financial sanctions***

- The main statutory references in force at international level are reported below: United Nations Charter (1945) relating to restrictive measures aimed at promoting the maintenance or restoration of international peace and security;
- Treaty on the European Union of 1992, title V relating to the provisions on the common foreign and security policy and subsequent amendments;
- Treaty on the Functioning of the European Union of 1957, title IV relating to the provisions on foreign policy and common security, with particular reference to the application of restrictive measures and subsequent amendments;
- Regulation (EU) 2021/821 of the European Parliament and Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items;
- European Union regulations implementing both UN resolutions and autonomous decisions taken under the Common Foreign and Security Policy (CFSP) containing restrictive measures against regimes involved in serious violations of human rights and countries involved in the development of programmes of unauthorised nuclear enrichment;
- FATF recommendations aimed at providing operational guidelines for the application of financial sanctions;
- Code of Federal Regulations, Title 31 - Money and Finance: Treasury, Subtitle B - Regulations Relating to Money and Finance, Chapter V - Office of Foreign Assets Control, Department of the Treasury, Part. 501 - Reporting, Procedures and Penalties Regulations;
- Appendix A to CFR Part 501 - Economic Sanctions Enforcement Guidelines;
- "A Framework for OFAC Compliance Commitments".

At national level, reference is made to the following main measures:

- Legislative Decree 109/2007 "Measures to prevent, combat and suppress the financing of terrorism and the activities of countries that threaten international peace and security, in enforcement of Directive 2005/60/EC", which incorporates the rules to combat the financing of terrorism and

establishes the Financial Security Committee (CSF) to monitor and enforce measures to freeze funds and economic resources and subsequent amendments;

- Legislative Decree no. 231 (hereinafter, the “Decree”), as amended by Legislative Decree no. 90 (hereinafter, the “Transposition Decree”) and Legislative Decree 125/2019, containing amendments and additions to Legislative Decree 90/2017, as amended;
- The Provision issued by the Bank of Italy on 27 May 2009, with operating instructions for exercising enhanced controls against the financing of programmes for the proliferation of weapons of mass destruction;
- Legislative Decree 15 December 2017, no. 221, enforcement of the mandate to the Government pursuant to Art. 7 of Law no. 170, for the adjustment of national legislation to the provisions of European legislation for the purpose of reorganising and simplifying the procedures for authorising the export of dual-use products and technologies and the application of sanctions relating to commercial embargoes, as well as for any type of export operation of proliferating materials;
- FIU communication of 24 March 2022 on Russian and Belarussian deposits pursuant to Regulations (EU) 328/2022 and 398/2022.

## 6.2 INTERNAL REGULATIONS

---

This Policy is part of the broader context of internal regulations which, in particular, include:

- the Code of Ethics;
- Group Risk Culture Policy
- the Organisational Model pursuant to Legislative Decree 231/2001 which specifies the preventive control mechanisms and subsequent controls adopted to identify the conduct required in relation to money laundering risk, and to implement timely actions if any anomalies are found;
- the Guidelines and basic principles for Group coordination between Control Bodies and Functions
- the internal Whistleblowing Policy;
- the Policy for the appointment, removal and replacement of Managers of the Corporate Control Functions;
- the Regulation on the process for managing Politically Exposed Persons;
- the Anti-Money Laundering Function Regulations that illustrate the main guidelines, organisational architecture, processes and instruments adopted by the Anti-Money Laundering Function to carry out its duties;
- the Regulations on the due diligence process describing the due diligence process stages, including enhanced due diligence and simplified due diligence, the logic underlying assignment of the risk profile and due diligence on an ongoing basis;
- the Regulations on the process for reporting suspicious transactions that describe the internal process stages required before reporting suspicious transactions;
- the Regulations on the storage of documents, data and information, Anti-Money Laundering Reports (S.Ar.A.) and second level AML controls, that describe the process stages relating to tracking the

second level anti-money laundering controls, including those relating to storage and recording, identifying any actions to mitigate the risks detected;

- the Regulations on the process for opening of a new bank account online;
- the Counterparties Management Operating Procedure;
- the Operating Procedure for Master Data Management for Parties other than Individuals;
- the Operating Procedure for Monitoring transactions on Selfy Current Accounts not assigned to Financial Advisors;
- the internal operating manuals of the Anti-Money Laundering Function and the Operating Structures, which describe in detail the operating processes and elements that form the basis of the money laundering risk control models.

This regulatory, operating and procedural corpus aims not only to comply with mandatory legal provisions, but also to avoid the Bank's involvement, even unwittingly, in money laundering and terrorism events.