Mediolanum Group Policy on Combatting Money Laundering and Terrorist Financing

Board of Directors' meeting of Banca Mediolanum S.p.A. of 8 May 2025

CONTENTS

1. INTRODUCTION

This document describes the principles regarding combating the Risk of money laundering defined for the Mediolanum Group, understood in its corporate group sense and in the sense of the supplementary supervision of credit institutions, insurance undertakings, and investment firms belonging to a financial conglomerate (hereinafter also referred to as the 'Mediolanum Group' or 'Group').

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 have destabilising effects, especially for the banking and financial system.

The changeable nature of the threats of money laundering and terrorist financing, facilitated also by the continued development of technology and resources available to criminals, requires, from the relevant parties, constant adaptation of the prevention and combating oversights. Said persons should also put in place measures to identify, manage and mitigate any risks of non-application or evasion of restrictive measures or international financial sanctions.

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 shall identify and assess the risks of money laundering and terrorist financing to which they are exposed, in order to adopt appropriate mitigation measures. The FATF has also developed rules that allow jurisdictions to identify and assess the risks of potential non-application or evasion of restrictive measures or international financial sanctions and to adopt measures to mitigate these risks. 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 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. Therefore, in order to ensure adequate mitigation of the risks of money laundering and terrorist financing, as well as the risks of non-application or evasion of restrictive measures or international financial sanctions, the relevant entities should have an internal control framework including risk-based policies, procedures and controls and a clear division of responsibilities throughout the organisation.

In this context, the Mediolanum Group is strongly committed to ensuring that the products and services offered are not used for criminal money laundering or terrorist financing, by 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.

1.1 REFERENCE CONTEXT

The Group companies within the scope adopt a Policy consistent with the principles and guidelines contained in this Policy, the structure of which takes into account their own specific characteristics and the risk inherent in the activities carried out, in line with the principle of proportionality and the actual exposure to money laundering risk, taking into account the products and services offered, the type of customers, the distribution channels used for the sale of products and services and the foreseeable developments in these areas, without prejudice to compliance with the specific obligations laid down by the reference local regulations.

This Policy forms part of a broader System of internal Group 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 Group.

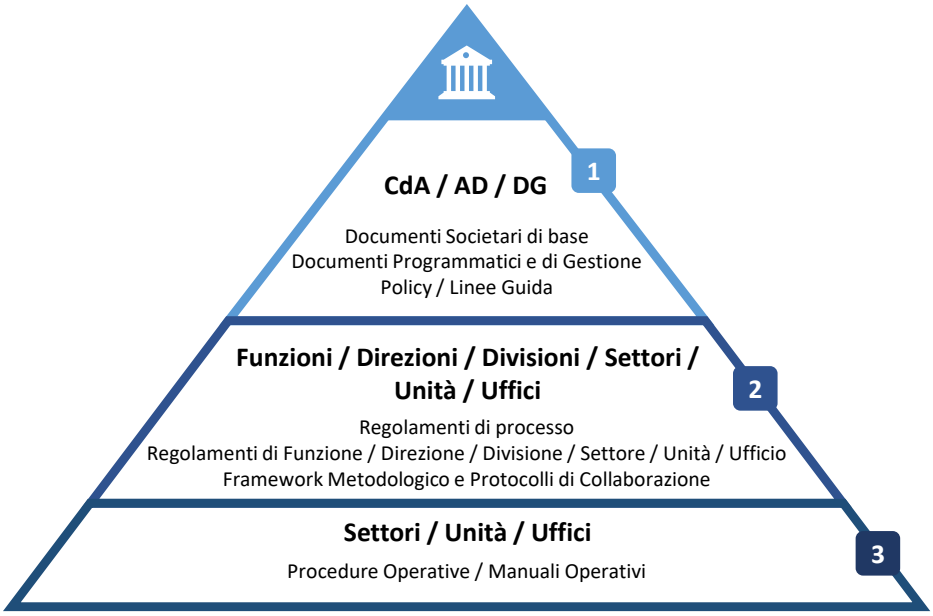
1.2 SCOPE OF THE DOCUMENT

The principles referred to in this Group Policy are implemented in process regulations and/or operating procedures adopted by each Company, in which the tasks, operational and control activities underlying compliance with the regulations in force are better defined. In particular, the obligations of due diligence and reporting of suspicious transactions and second-level controls must be regulated.

These regulations and procedures will describe in more detail the parties involved and their roles and responsibilities within the individual Group companies, for the purposes of monitoring Money Laundering Risk.

This document, with reference to the 'Policy on the procedures for drafting, approving, disseminating and updating the Internal Regulations of the Mediolanum Group', is at the first (top) level of the document pyramid referred to in the following diagram.

Piramide delle fonti di normativa interna



2. GENERAL ASPECTS

The general aspects of this Group Policy in terms of scope of application and responsibility (drafting, approval and updating) are provided below.

2.1 SCOPE OF APPLICATION

This Policy is sent to all Companies belonging to the Mediolanum Group, so that they may adopt it by resolution passed by their Corporate Bodies, without prejudice to any specific provisions laid down by the local regulations and by the respective Supervisory Authorities, except for companies not currently subject to anti-money laundering regulations.[1]

The policy is then sent to the Bodies with Strategic Supervisory Functions of the Group companies within the scope for adoption, in accordance with the principle of proportionality and taking into account local regulations and specific issues.

2.2 RESPONSIBILITY FOR THE DOCUMENT

This document is approved by the Board of Directors of the Parent Company Banca Mediolanum S.p.A.

The Chief Executive Officer defines this Policy, with the support of the Anti-Money Laundering Function, and oversees its enforcement. He also, as AML Representative at Group level, monitors its adequacy and proportionality over time, taking into account the characteristics of the Group and the risks to which it is exposed.

[1] The company Mediolanum Communication S.p.A. is not currently included in the anti-laundering policy

3. DEFINITIONS

For the purposes of this Policy, the following definitions apply:

Due Diligence: activities consisting of:

- 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/Combatting 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 AML 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: the party that establishes an ongoing relationship or carries out transactions with financial intermediaries and other parties falling under the scope of the anti-money laundering obligations.

Compliance Risk: a specific requirement set forth by the law in order not to incur legal or administrative sanctions, significant pecuniary loss or damages to reputation resulting from infringements of mandatory provisions (laws, regulations) or self-regulatory provisions (e.g. code of conduct, self-governance code).

Freezing of funds: the prohibition, by virtue of European Union regulations and domestic legislation, against the movement, transfer, modification, use or management of funds or access to said funds, such as to change the volume, amount, location, ownership, possession, nature, destination or any other change that allows the use of the funds, including portfolio management.

Freezing of economic resources: the prohibition, by virtue of EU regulations and domestic legislation, against the transfer, disposal or use of economic resources in order to obtain funds, goods or services in any manner, including, but not limited to, the sale, leasing, rental or

establishment of real collateral securities.

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 (also known as "first-level controls'): the set of controls aimed at ensuring that transactions are properly carried out. These are performed by the company Organisational 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 company Organisational 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 AML 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 a chain of correspondent accounts therefore has to be used through a PSP. 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.

Trade 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).[2]

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

Family Bankers®: financial advisors authorised to make off-premises offers.

Financing of terrorism: 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, meant to be used, directly or indirectly, in whole or in part, to carry out one or more activities for purposes of terrorism, according to the provisions of criminal laws, regardless of the actual use of the funds and economic resources for the commission of said activities.

FIU (Financial Intelligence Unit): Independent national authorities, autonomous at operational level, whose purpose is the collection and analysis of information received, in order to identify connections between suspicious transactions and underlying criminal activities and prevent and combat money laundering and the financing of terrorism.

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;
- publicly and privately traded securities as well as financial instruments, including, by way of example, but not limited to: stocks and shares; money market instruments; the units of a collective investment undertaking; option contracts, futures, swaps and, more generally, derivatives; interest, dividend or other income and increases in value generated by assets; receivables, offsetting rights, guarantees of any kind, deposits and other financial commitments;
- letters of credit, bills of lading and other securities representing commodities;
- documents showing investments in funds or financial resources;

[2] 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.

- all other export credit instruments;
- life insurance policies.

AML 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 AML 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 compliance risk with respect to the business 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 Company Control Functions, the Financial Reporting Manager, the Director responsible for Controls, the Independent Auditor, the Supervisory Body and the Data Protection Officer.

Internal Audit Function: the Function assigned the task of monitoring the regular course of operations and the evolution of risks, also with on-site inspections, using level three controls and assessing the completeness, adequacy, functionality and reliability of the organisational structure and other components of the Internal control system, and to bring the possible improvements, with particular reference to the Risk Appetite Framework (RAF), to the risk management process and to the measurement tools and their control to the attention of the corporate bodies. 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, terrorism financing and the proliferation of weapons of mass destruction.

Group: understood both in its standing as a corporate group and for the purpose of the supplementary supervision of credit institutions, insurance undertakings and investment firms belonging to a financial conglomerate (hereinafter also referred to as the 'Mediolanum Group' or 'Group').

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: any individual or legal entity, other than an insurance or reinsurance company or an employee thereof and other than an ancillary insurance intermediary, which initiates or performs the distribution of insurance in return for a fee**.**

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.

Restrictive measures: the restrictive measures adopted by the European Union, such as measures regarding the freezing of funds and economic resources, the prohibitions regarding the provision of funds and economic resources, as well as the sectoral economic and financial measures and embargoes on weapons and the measures adopted by the Member States in compliance with their national legal system (to the extent that they apply to financial institutions).

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 AML 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 Financial Intelligence Unit (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 information 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 terrorist financing, as identified by the European Commission in exercising the powers governed by articles 9 and 64 of the AML 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.

Politically Exposed Persons (PEP): a natural person who holds or has held important public offices including:

1.1 Heads of State, Heads of Government, Ministers and Deputy Ministers or Undersecretaries;

1.2 Members of Parliament or of similar legislative bodies;

1.3 members of executive bodies of political parties;

1.4 members of the supreme courts, constitutional courts and other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances;

1.5 members of courts of auditors and the management boards of central banks;

1.6 ambassadors, appointees and senior officers of the armed forces;

1.7 members of the management, direction or supervisory bodies of state-owned enterprises;

1.8 managers, deputy managers or members of the governing body, or equivalent function, 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 natural persons known to have joint beneficial ownership of legal entities or legal institutions or other close business relationships with a politically exposed person;

3.2 natural persons who are the sole beneficial owners of legal entities or legal institutions that are known to have been created de facto for the benefit of a politically exposed person.

Anti-Money Laundering Policy or Policy: the document defined by the body with the management function and approved by the body with a strategic supervisory function.

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.

Money Laundering:

- 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;
- the hiding or concealment of the true nature, origin, location, disposition, movement, or ownership of assets or rights thereon, carried out with the knowledge that these assets derive from criminal activity1 or from participation in such activity;
- 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;
- 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.

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: it 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: with the view of “potential' risks, it refers to the likelihood of the Company to be subject to a direct or indirect damage involving sanctions, criminal consequences, financial losses 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.

Economic resources: assets of any kind, tangible or intangible and movable or immovable, including accessories, appurtenances and yields, which are not funds but can be used to obtain funds, goods or services, that are owned, held or controlled, even partially, directly or indirectly, or through an individual or legal entity, by designated parties, or by individuals or legal entities acting on behalf of or under the direction 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 Italian regulations and the European Union, by the UN Security Council or by the United States, which include (but are not limited to) embargoes and the freezing of assets.

Internal control system: the set of rules, functions, structures, process resources and procedures that aim to ensure, in compliance with sound and prudent management, the achievement of the following objectives:

- 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;
- efficacy and efficiency of the business 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 Subjects: natural persons, legal persons, groups and entities designated as recipients of the Freezing of funds or economic resources on the basis of EU regulations and national legislation.

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

Transaction monitoring system: the IT procedure used for the selection of anomalous operations based on both quantitative, such as the amount or frequency of the transactions and the origin or destination of the flows, and qualitative metrics, such as the type or methods of use of the services and the characteristics of the parties involved.

Beneficial owner: the natural person or persons, other than the Customer, in the interests of whom, ultimately, the ongoing relationship is established, the professional service is rendered or

the transaction is carried out (beneficial owner sub 1), or, in the case of parties other than a natural person, the natural person or persons to whom, in the last instance, direct or indirect ownership of the entity or the relative control is attributable (beneficial owner sub 2).

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 Office, for the management of Enhanced Due Diligence.

4. MONEY LAUNDERING RISK CONTROL MODEL

4.1 ORGANISATIONAL OVERSIGHT

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 and formalised in each company.

In line with eligible corporate governance principles, for each Group company the model acknowledges the central role of the Body with a strategic supervision function 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 Anti-Money Laundering Policy (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. In order to ensure that the Board of Directors has the information necessary to fully understand the relevance of the money laundering risk to which the company is exposed, each Group company appoints – without prejudice to the principle of proportionality and taking into account specific local regulatory provisions – its own anti-laundering Officer.

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 AML Function.

The Group companies appoint their own Head of the AML Function, 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.

In compliance with the proportionality principle and if envisaged in the specific reference regulations, each Group company must also set up a specific AML Function in charge of monitoring money laundering risk, which coordinates and interacts with the other Control Functions, to ensure the internal controls system functions correctly. The Group companies adopt 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. Where the absence or impediment of the AML Manager lasts for more than 3 months, the Body with a Strategic Supervision Function shall meet to replace the Manager.

The Anti-Money Laundering Manager - unless otherwise provided for by specific local regulations - is also appointed as the Manager for reporting suspicious transactions.

The Head of Suspicious Transaction Reports sends, to the national FIU of reference, a specific report, according to the procedures provided for by the legislation in force, when he/she knows, suspects or has reasonable grounds to suspect that the funds, regardless of their size, come from criminal activities or are linked to the financing of terrorism, providing a prompt response, in such cases, to requests for additional information from the FIU and providing the FIU, directly or indirectly, at its request, with all the necessary information.

An effective organisational structure for monitoring money-laundering risk is also based on significant involvement of all company Organisational Structures 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.

The Organisational Structures of each Group company are required to know and comply scrupulously with the laws, regulations and rules issued by the company. In that regard, the Group Companies provide their employees and collaborators with specific operational tools and procedures, including IT, capable of assisting them in complying with money laundering obligations and prepare specific permanent training and professional development programmes for them, so that they have adequate knowledge of the relevant regulations and related responsibilities and are able to deliberately use tools and procedures to assist in fulfilling the obligations.

If the personnel from the Organisational Structures, in carrying out their activities, 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 Group companies in money laundering or terrorist financing, they must provide prompt notification to their manager, who is assigned overall responsibility for the compliance and effective functioning of the first-level controls within its structure; the managers, after conducting the necessary investigations, must promptly involve the AML Function for its own assessments.

If the Operating Structures are assigned the administration and concrete management of relationships with Customers, they are responsible for identifying and performing Customer Due Diligence assigned to them as the first level of control, developing their knowledge regarding the customer and ensuring continuous monitoring over the course of the relationships, based on the underlying risk. These structures are also responsible for carrying out Enhanced Due Diligence in the 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 terrorism financing has been carried out, is being carried out, or is being attempted.

The financial advisors in the Sales Network and agents in financial activities, where present[3], are personally in charge of the identification process and Due Diligence of the Customer 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. In addition, they are responsible for carrying out the Enhanced Due Diligence process in cases envisaged by the regulations and when requested by the Anti-Money Laundering Function or the corporate Organisational Structures.

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

The company 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.

Financial Advisors promptly notify the AML Function, where possible before carrying out the transaction, of 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 carried out, is underway or has been attempted.

[3] Reference should be made, in particular, to the companies Banca Mediolanum S.p.A., Banco Mediolanum SA and Prexta S.p.A.

5. PARTIES INVOLVED

The following section summarises the main parties involved at the Parent Company involved in various capacities in this Group Policy, with a description of their respective roles and responsibilities.

5.1 BOARD OF DIRECTORS

The Board of Directors of the Parent Company defines the Group's money-model for the monitoring of money laundering risk: This is the body with strategic supervision functions tasked with company management functions, to which the Corporate Control Functions, including the Anti-Money Laundering Function, report. The Board of Directors approves updates to this policy as required, as proposed by the Anti-Money Laundering Function.

5.2 RISK COMMITTEE

The Parent Company's Risk Committee supports the Board of Directors in determining the guidelines of the internal control and risk management system, including money-laundering risk. Evaluates this Group Policy before submission to the Board of Directors.

5.3 BOARD OF STATUTORY AUDITORS

The Board of Statutory Auditors of the Parent Company, with specific reference to the monitoring of money-laundering risk, monitors compliance with regulations and the completeness, function and adequacy of anti-money laundering controls, including at Group level, using the internal structures to perform the checks and assessments necessary, and using information flows from the other Corporate Bodies, the AML Function Manager and the other Corporate Control Functions.

5.4 CHIEF EXECUTIVE OFFICER

The Chief Executive Officer of the Parent Company, including as the Group Officer in charge of Anti-Money Laundering, is responsible for ensuring implementation of the strategic guidelines and money-laundering risk governance policies at Group level 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.

5.5 OFFICER IN CHARGE OF ANTI-MONEY LAUNDERING

The Officer in charge of Anti-Money Laundering at the Parent Company is the main point of contact between the Group Head of the Anti-Money Laundering Function and the Board of Directors at the Parent Company and ensures that the latter has the information necessary to fully understand the relevance of the money-laundering risks to which the Group is exposed. The Representative ensures that the Head of the Parent Company's Anti-Money Laundering Function performs his/her duties effectively.

5.6 INTERNAL AUDIT FUNCTION

The Internal Audit Function of the Parent Company is the Central Function of reference for the equivalent functions at the Subsidiaries with the task of continuously verifying the degree of adequacy of the anti-money laundering organisational structure and its compliance with the regulations in force.

5.7 ANTI-MONEY LAUNDERING FUNCTION

The AML Function of the Parent Company is the Central Function of reference for the corresponding functions of the Subsidiaries with regard to money-laundering risk control. As the Company Control Function, it oversees money-laundering risk according to a *risk-based* approach.

It supports the Board of Directors of the Parent Company in defining the Group's money laundering risk management model, and assists the Head of the Group Anti-Money Laundering Function in coordinating activities at Group level on anti-laundering matters.

5.8 ANTI-MONEY LAUNDERING FUNCTION MANAGER

The AML Manager at the Parent Company ('Group Chief AML Officer') 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.

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 AML Function of the Parent Company;
- 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. In order to ensure the enforcement of effective policies and procedures to combat the risk of money laundering at Group level, the Group Chief AML Officer makes use of the resources of the Bank's AML Function.

6. PRINCIPLES RELATING TO COMBATTING MONEY LAUNDERING AND TERRORISM FINANCING

The Group companies 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 Parent Company has defined these 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.

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 AML Function to ensure effective circulation of information at Group level, in order to counteract money laundering risk. The Group Chief AML Officer 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.

In order to achieve appropriate synergies and economies of scale, using highly specialised centres of expertise, the Banking Group and Insurance Group companies may Officer to the Parent Company – based on specific outsourcing agreements, drawn up in compliance with supervisory regulations, and in accordance with the principles stated in the “Corporate outsourcing policy' – the performance of tasks specific to the AML 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 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/or operating procedures that each Group company must adopt.

6.1 CUSTOMER DUE DILIGENCE

The Group companies subject to the obligation to establish anti-money laundering oversights Bank adopts Customer Due Diligence measures proportional to the extent of their 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. 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 company and to declare the scope and nature of the business relationship that it intends to establish, and on the other hand, for the company 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 Group companies adopt appropriate training initiatives for its personnel, as described in paragraph 6.9 below.

Employees of the Organisational Structures in charge of the actual management and administration of customer relationships and the financial advisors in the Sales Network, where present, fulfil Due Diligence obligations by complying with the measures, methods and internal procedures adopted by the Group 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 Organisational Structures, 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;
- the identification, in the cases envisaged by the regulations in force from time to time and by internal regulations, of the Beneficiary, legitimate heirs and any Beneficial Owners, and the acquisition of the relative identification documents;
- verification of the identity of the Customer, the Beneficiary, the Representative, if any, and the Beneficial Owner of the Customer, the Beneficiary and legitimate heirs, based on the documents, data or information obtained from a reliable and independent source or from an obliged party pursuant to AML regulations;
- the collection, signed by the Customer, of the personal data and information useful for the Due Diligence of the subject, also with reference to any Representatives and Beneficial Owners, kept in the company's database, together with the relative documentation, according to the provisions and confidentiality measures dictated by internal regulations;
- the collection and assessment of information on the purpose and nature of the ongoing relationship and any occasional transactions and the relationships between the Customer and Representative, between the Customer and Beneficial Owner, between the Customer and the policyholder (if different from the contracting party) and between the Customer and the designated Beneficiary/ies;
- the collection of the overall assessment of the Investment transaction with regard to the reasonableness of the same, and of the conduct of the Customer and the possible presence of elements of suspicion by the financial advisor who handled the Transaction, where applicable;
- 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 threshold applicable, also making use of any indications from the FIUs;
- when there are doubts regarding the completeness, reliability or truthfulness of the information or documentation previously acquired from the customers.

With specific reference to Transactions in asset management products, Due Diligence must also be carried out:

- in the case of additional payments, disinvestments, liquidations in favour of Beneficiaries and/or heirs;
- contractual changes (e.g. transfer of policy contracts, inclusion of joint account holders of mutual investment funds).

The Group companies fulfil 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.

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

6.1.1 REMOTE ACQUISITION (ONBOARDING) OF CUSTOMERS

In cases of remote operations (carried out without the physical presence of the Customer and Staff), the company which provides for such operations shall pay particular attention to 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.

The AML Function and the Organisational 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 company 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 relevant company'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. Specific documentary evidence of these assessments is kept, with specific prior communication also provided to the Parent Company.

In cases of remote onboarding, the identification data of the Customer and the Representative are acquired and evidence in the form of a copy – received by fax, mail, digitally or in a similar format – of a valid ID document is always obtained, pursuant to the regulations in force. 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 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) resident in the same country where the registered office or a permanent business establishment of the company is located and aged 18 or over. In any case, the establishment of remote relationships by parties presenting FATCA indications (US Persons), falling within the category of Politically Exposed

Persons and marked by 'negative reputational indices' on the basis of the 'lists of names' and of the databases used by the Company.

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

The Group companies also envisage first-level controls on Transactions carried out by Customers acquired through remote onboarding procedures not assigned to a financial advisor of the Sales Network, including through the use of specific transaction monitoring systems.

6.1.2 DUE DILIGENCE CONDUCTED BY OTHER OBLIGED ENTITIES

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.

The Group companies may delegate to another Group company, by virtue of a specific distribution and outsourcing agreement, the fulfilment of the obligations of Due Diligence of the customers, with the exception of the constant control of transactions, without prejudice to the full responsibility of each Company.

In the event of disinvestment/settlement transactions/liquidation of claims ordered by Beneficiaries, legitimate heirs, or on the initiative of Customers, the Group companies may fulfill the obligations of Due Diligence of the customers, without prejudice to the full responsibility of the same for the observance of these obligations, also through EU banking intermediaries (banks, Poste Italiane S.p.A., electronic money institutions - IMEL, payment institutions, securities brokerage companies, savings management companies, SICAV, SICAF, Italian intermediaries registered in the register envisaged by Article 106 of the Consolidated Banking Act, Cassa Depositi e Prestiti S.p.A., insurance companies operating in the life business, microcredit providers, credit institutions, branches of banking intermediaries listed above, with registered office and central management in another Member State or in a third country; banking intermediaries and financial institutions listed above, established without a branch office in the territory of the Italian Republic or the country in which the Group company operates or based in a third country with an effective regime to combat money laundering and terrorist financing);

With specific reference to the identification obligation, it is considered met, even without the physical presence of the person concerned, in cases where:

- the identifying data are acquired from an identity document sent by the same through Certified Electronic Mail (PEC);
- the identifying data result from public deeds, authenticated private documents or qualified certificates used for the generation of a digital signature associated with IT documents;
- the subject is in possession of a digital identity, of maximum security level or of a certificate for the generation of a digital signature, issued as part of an electronic identification scheme included in the list published by the European Commission pursuant to Article 9 of Regulation (EU) no. 910/2014;
- the identifying data are the result of a declaration by the Italian diplomatic legal representation and by the Italian consular authorities or by the country in which the subsidiary carries out its activities.

6.2 CUSTOMER PROFILING

In order to grade the depth and extension of Due Diligence obligations, the Group companies adopt 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, where present, and to the Organisational 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 following table below shows possible risk profiles that can be assigned to customers and the associated frequency for the updating of the information:

Class	Risk profile	Information updating frequency
1	Immaterial	Not exceeding 60 months
2	Low	Not exceeding 60 months
3	Medium	Not exceeding 36 months
4	High	Every 12 months

The scores and rules attributed to the risk profiling system are monitored and periodically updated, also in relation to developments in the regulatory context and leading market practices. The need to share these interventions in advance with the Parent Company remains unaffected, with a view to ensuring a homogeneous approach, within the Group, to customer risk profiling.

As part of a Group, each company 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, additional risk factors are taken into consideration 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 money laundering and 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 company Organisational 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 profile of the customer, a Suspicious Transaction Report is promptly sent to the AML Function so that an in-depth analysis of the case can be performed and submitted to the Suspicious Transaction Reporting Manager for assessments under his/her responsibility, including raising the level of the customer's risk profile if

necessary, keeping records of the assessments conducted.

In assessing the anomalous behaviour of the Customers or the lack of reasonableness of the transactions carried out by the same, it is necessary to take into account all the data and information acquired from the customers.

With regard to risk class 4, equal to a 'high' risk profile, the Group companies consider the following, regardless of the scores assigned by the customer profiling system used, to be high risk:

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 at national level 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 news provided directly by the customer or the reference financial advisor, regarding criminal proceedings, proceedings for fiscal damages, proceedings for the administrative liability of entities, etc.;
    - requests/measures from the Judicial Authority, pursuant to: the Anti-Mafia Code (assessments required by the Criminal Authorities – Anti-Mafia – Preliminary Investigation Phase) or the Anti-Money Laundering regulations (assessments required by the Criminal Authorities pursuant to the Anti-Money Laundering Decree – Anti-Money Laundering – 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;

e) business relationships, professional services and occasional transactions with customers and related beneficial owners who are Politically Exposed Persons, except in cases where such PEPs are acting as Public Administration bodies;

f) Ongoing Relationships, Professional Services and Transactions involving high-risk Third Countries, as well as Customers and Beneficial Owners residing or having their registered office

in high-risk Third Countries and in high-risk geographical areas[45]; the AML Function of the Parent Company may propose, in any case, to the Chief Executive Administrator, the suspension of the opening of relations and the execution of transactions with countries characterised by one or more geographical 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 AML Function of the Parent Company and sent to the AML Managers of the subsidiaries, to ensure correct application also at local level.

g) structures that can be qualified as asset interposition vehicles, such as trusts, fiduciary companies, 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;

j) Customers that benefit from highly personalised consultancy services, offered to customers with assets exceeding Euro 2 million;

k) Customers that benefit from investment banking services.

Apart addition to the case mentioned above, Customers are also considered high-risk if classified as such by the score assigned on the risk profiling system.

Those customers identified in letters a), b), e) and f) above and those indicated by the Suspicious Transaction Reporting Manager, after prudent assessment, as having high money laundering risk, are also considered as being subject to the highest money laundering risk ('watchlist parties').

The Manager may, after due assessment, when analysing specific positions, decrease the scores assigned, keeping a record of the analyses conducted. In any case, it is not permitted to modify

[4] For the purpose of assessing geographical risk, the following risk factors are considered:

1) third countries that authoritative and independent sources believe to lack effective controls for the prevention of money-laundering (such as countries included in the EU/GAFI lists);

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.

6) countries considered at risk of circumvention of the Restrictive Measures.

The geographic risks listed above are considered, 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 point 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.

[5] For the purpose of increasing the risk profile, for high-risk Third Countries not only the Customer's residence, but also their citizenship is relevant.

independently the scores assigned by the remaining Personnel.

This without prejudice to the option of the 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 Group companies 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.

6.3 ENHANCED CUSTOMER DUE DILIGENCE

In the presence of high money laundering risk, the Group companies adopt enhanced Customer Due Diligence measures, according to a risk-based approach, 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.

Based on the model adopted by the Group companies, the enhanced customer due diligence activities are primarily assigned to financial advisors, where present or to the appointed employees, who are required to apply the following measures:

- acquire additional information on the Customer, Beneficiary and Beneficial Owners;
- acquire/update and assess information on the reputation of the Customer, Beneficiary and Beneficial Owners (including any prejudicial elements, also drawing on publicly accessible information through the consultation of open sources, e.g. by using 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 company, 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 Assets and funds used in the business relationship, through a structured process that takes into consideration, primarily, the reliability of the information available, as well as the availability of financial-equity information – produced directly by the Customer or inferred from changes occurring in the relationships (e.g. emolument or dividend crediting, etc.) or to be retrieved through open sources or from public databases (e.g. financial statements, VAT declarations and income statements, notary public deeds, succession declarations, declarations/documents coming from the employer or other intermediaries); in this regard, some aspects, such as the degree of knowledge of the Customer and/or the length of the relationship, the consistency of the profile of the Customer 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;

- conduct more frequent checks on the Continuous Relationship and on Transactions.

The Group companies also require authorisation from a Senior Manager:

- 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 carrying out an investment Transaction in asset management products placed by the same, for a material amount, and in any case exceeding Euro 5,000,000, or Euro 1,000,000, in the case of 'watchlist parties'.

Without prejudice to the general principle according to which the enhanced Due Diligence measures listed above must always be applied when there is a suspicion of money laundering, regardless of any derogation, exemption or applicable threshold, their application is commensurate, in the absence of elements of suspicion, to the Customer's risk, according to a *risk-based approach.*

By virtue of the peculiarity of the business model, the enhanced Due Diligence process adopted for managed savings products (life insurance policies, stakes in UCITS, portfolio and fund management services, etc.)is event-specific, i.e. for each individual Transaction arranged by customers according to a risk-based approach.

Additional information will be acquired regarding the source of the funds used for the transaction, according to a risk-based approach, distinguishing between 'watchlist' parties and other high risk parties.

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, each Group company considers the following transactions to be at the highest risk:

- any investment Transaction (underwriting or additional payment transactions) of Euro 250,000 or more;
- all cases of underwriting of insurance policies where the relationship between the contracting party and the named designated beneficiary is 'other';
- all cases of contractual changes to an insurance policy;
- all cases of changes of the Beneficiary of an insurance policy, if identified by name, where the relationship between the contracting party and the Beneficiary is 'corporate or professional relations' or 'other';
- all cases of activation of payment plans on policies by a party other than the contracting party (third payer) where the relationship between the contracting party and the third payer is 'other'.

Enhanced measures are applied, entailing different levels of controls, proportionate to the amount of the Transaction according to the following clusters:

- Cluster A: Only High-Risk Customers – Transactions for amounts exceeding Euro 50,000 and up to Euro 250,000;
- Cluster B: Transactions for amounts exceeding Euro 250,000 and up to Euro 1,000,000;
- Cluster C: Transactions for amounts exceeding Euro 1,000,000 and up to Euro 5,000,000;
- Cluster D: Transactions for amounts exceeding Euro 5,000,000.

Each cluster corresponds to a different level of controls. With reference to High-Risk Customers, a different level is defined, distinguishing between 'Watchlist' parties and 'other high-risk parties'. In

particular, for the latter category, the amount threshold will be calibrated in relation to the total assets declared by the customer or to the portfolio of investments held with the group, as follows:

- Euro 50,000 in the case of total assets of up to Euro 500,000;
- Euro 100,000 in the case of total assets of between Euro 500,000 and Euro 2,000,000;
- Euro 250,000 in the case of total assets of over Euro 2,000,000.

For high-risk 'Watchlist' customers, the minimum threshold of Euro 50,000 is always applied.

In general, documentation on the source of the funds invested is always required, according to a risk-based approach with particular regard to 'Watchlist' parties, i.e. in the case of:

- Transaction with funding attributable to payments of cash and/or banker's drafts and/or cross-border bank transfers;
- Transactions by new customers who have accounts with Mediolanum for less than 24 months.

Any exceptions are assessed by the Anti-Money Laundering Function, keeping evidence of the analyses carried out.

The Enhanced Due Diligence process adopted for current accounts and assets under custody provides for an assessment of HIGH and MEDIUM risk customers[6] and by the financial advisors of the Sales Network or by the employees to whom it is entrusted, in practice, the management and administration of customer relations through the drafting of a specific report or completion of a specific assessment form. This assessment is carried out at the time of a new survey or as a result of the worsening of the risk level and is updated according to the frequencies envisaged for the updating of the Due Diligence information (see paragraph 6.2).

If these assessments reveal significant critical issue and/or suspicious elements, the Enhanced Due Diligence is brought to the attention of the AML Function to assess the presence of suspicious elements.

With reference to current account operations, the following are considered to have a higher risk of money laundering:

- 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;
- Transactions involving cash or other cash equivalents originating from abroad, in a total amount equal to or exceeding Euro 10,000;
- Transactions involving high-risk third countries;
- 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.

6.4 SIMPLIFIED CUSTOMER DUE DILIGENCE MEASURES

In the presence of immaterial money laundering risk, the Group companies 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;

[6] Total assets in Group products equal to or greater than Euro 250,000

- EU banking intermediaries (banks, Poste Italiane S.p.A., electronic money institutions - IMEL, payment institutions, securities brokerage companies, savings management companies, SICAV, SICAF, Italian intermediaries registered in the register envisaged by Article 106 of the Consolidated Banking Act, Cassa Depositi e Prestiti S.p.A., insurance companies operating in the life business, microcredit providers, credit institutions, branches of banking intermediaries listed above, with registered office and central management in another Member State or in a third country; banking intermediaries and financial institutions listed above, established without a branch office in the territory of the Italian Republic or the country in which the Group company operates or based in a third country with an effective regime to combat money laundering and terrorist financing);
- supplementary pension funds governed by the relevant national decrees, provided that they do not provide for surrender clauses other than those for: permanent disability, cessation of employment that leads to unemployment, or recourse by the employer to mobility procedures, ordinary or extraordinary redundancy temporary redundancy schemes and which cannot serve as a guarantee for a loan outside the cases envisaged 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, a distinction is drawn 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;

Any 'passive' counterparties, i.e. financial intermediaries (domestic and international) with which there are no business relationships but which the company uses, at its own initiative, to finalise transactions on behalf of its customers, holders of relationships (securities dossier transfer transactions, securities purchase/sale transactions, etc.) are excluded from due diligence obligations. Within this scope, 'passive' counterparties assume the role of 'service providers' at the initiative of the Bank and other Group companies 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 no greater than 60 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 Group companies verify 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 simplified Due Diligence do not apply when:

- the conditions for applying the simplified measures are not satisfied, based on the risk indices established by the reference regulations;
- 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 an immaterial risk situation;
- there is in any event a suspicion of money-laundering or financing of terrorism

6.5 OBLIGATIONS TO ABSTAIN

The Group companies do 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, due to their potentially high exposure to the risk of money laundering, but adopt 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 company 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 company will refrain 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 Group companies will refrain 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 of the Parent Company Banca Mediolanum or as proposed by the AML Function;
- credit or financial institutions located 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 Group companies refrain 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.

6.6 CONTROLS TO COMBAT TERRORIST FINANCING

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

- verify whether the Customer, Beneficiary and relevant Beneficial Owners are included in the 'lists' of persons and entities adopted by the UN Security Council, the European Commission, the decrees of the Italian Ministry of Economy and Finance, as well as those of the Office of Foreign Asset Control (OFAC) of the US Treasury Department;
- refrain from carrying out Transactions that involve for any reason persons included in the lists referred to in the previous paragraph, except in cases where not carrying them out is impossible or risks undermining the efforts to prosecute the beneficiaries of terrorist financing;
- apply without delay the freezing obligations envisaged by the UN Security Council, EU Regulations or by adopted at national level or by the Office of Foreign Asset Control (OFAC) of the United States Department of the Treasury on the reports of all parties who have been found to correspond to the lists referred to in the first paragraph;
- do not make cover payments in US dollars;[7]
- inform the Financial Intelligence Unit (FIU) of the measures applied, 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 in compliance with the local regulations of the country in which the Group company operates, 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, Beneficiary and relevant Beneficial Owners or Representatives, personnel must in any event pay specific attention to risk factors which, though not specific to terrorism financing, could indicate, in any case, a risk of terrorist financing.

6.7 REPORTING SUSPICIOUS TRANSACTIONS TO THE FIU

Pursuant to current regulations, the Company companies immediately send to the relevant national FIU, according to the procedures set by the latter, a Suspicious Transaction report when they know, suspect or have reasonable grounds to suspect that money laundering or terrorist financing operations have been carried out or have been attempted, or that, in any case, the funds, regardless of their amount, derive from criminal activities or are connected with terrorist financing.

The financial advisors of the Sales Network, where present, and the employees of the corporate Organisational Structures responsible, in practice, for the administration and management of customer relationships represent the first reporting level, also pursuant to governing regulation. Therefore, it is their duty to continuously monitor the progress of the relationship and the transactions carried out, including through the tools and procedures made available to them, and immediately send a suspicious transaction report to the Anti-Money Laundering Function, in accordance with procedures and operating methods established internally. 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

[7]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.

operations, or when postponement of the transaction may hinder the investigations.

The initiation of the reporting process may also arise from external reports, namely: from requests/orders received from any Supervisory Authority or Public Safety Authority; from requests for further information from the FIU; from the receipt of requests or information from other intermediaries.

Requests for further information from the FIU or from the competent Supervisory Authorities also trigger internal investigations, conducted by the Anti-Money Laundering Function, which may lead to reports of Suspicious Transactions.

In the case of requests from the FIU, the Anti-Money Laundering Function records the request received, launching a specific investigation on the position of the customer(s) concerned.

The Group companies, as part of their organisational autonomy, also make use of transaction monitoring systems. The AML Function assesses the transactions flagged by these Systems and, if there are grounds for suspicion, 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 and information held on record, without including the name of the whistleblower.

The Group companies 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 forbidden for parties obliged to report a suspicious transaction, and to anyone who is aware of it, to communicate to the relevant Customer or third parties that the report was made, that additional information requested by the FIU was sent, or that an investigation in relation to money laundering or terrorism financing is under way or is likely to be undertaken. This prohibition applies:

- to communications sent to the Supervisory Authorities for the sector during the performance of functions envisaged in the reference legislation;
- 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 EU legislation, in cases relating to the same customer or the same transaction, for the sole purpose of preventing money laundering or terrorist financing.

6.8 DATA AND DOCUMENT STORAGE OBLIGATION

In order to fulfil storage obligations for data relating to business relationships and transactions carried out, the Group companies use suitable storage systems 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 Italian Group companies continue 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.

With regard to fulfilling storage obligations, the Group companies 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.

6.8.1 EXEMPTIONS REGARDING DATA STORAGE – ITALIAN GROUP COMPANIES

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 Italian Group companies 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.

6.9 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 Group companies use permanent training programmes and professional updating courses in order to correctly apply the provisions of the AML legislation, 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, where present, to the employees involved in the remote onboarding process, and to the employees of the corporate Organisational 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 AML 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 company.

6.10 INTERNAL SYSTEMS FOR REPORTING INFRINGEMENTS

The Group companies adopt 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.

6.11 SELF-ASSESSMENT EXERCISE FOR MONEY-LAUNDERING RISK

The Group AML Function monitors the assessment of money-laundering risks conducted by the members of the Group, drafting a Group money-laundering risks assessment that takes account of 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;

In this regard, on the basis of the guidelines provided by the Parent Company, the Group companies carry out their own self-assessment exercise, sending the results to the Group Anti-Money Laundering Function, according to the timescales defined by the latter.

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).

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 AML Function.

7. EXERCISE OF THE DIRECTION AND COORDINATION ROLE

Banca Mediolanum, as Parent Company of the Mediolanum Group, defines these strategic guidelines on money-laundering risk management, which will be adopted by the Subsidiaries by means of the necessary resolutions of the respective Corporate Bodies.

The AML Function of the Parent Company is responsible for direction and coordination, for aspects relating to the processes and methodologies to be adopted for the purposes of standardised and synergistic management of money-laundering risk at Group level. The AML Function is involved ex-ante by the Subsidiaries, as required, for the formal issue of binding opinions, as expressly defined in the Direction and Coordination Regulation of the Mediolanum Group, in the event of deviation from these Group principles. The Subsidiaries provide evidence to the Parent Company of any changes to the implementation of the provisions of this document. The Parent Company's AML Function supervises and coordinates the corresponding functions of subsidiaries, where established locally. With reference to the foreign subsidiaries, adequate information flows from and to the Parent Company, periodic or 'event-based', were identified and prepared, in order to direct and share all relevant information for monitoring of the money-laundering risk in scope.

In particular, the AML Function communicates and shares the following with the AML Functions of the subsidiaries:

- contents of the relevant policies of the Function soon to be issued, prior to each of update (event-based);
- the project initiatives in which the subsidiary is involved;
- in addition, by virtue of the outsourcing contracts in place:
    - the annual control plan, with regard to the subsidiary, and any outcomes of interest to the subsidiaries (event-based);
    - the staff training plan (annually).

The AML Functions of the subsidiaries, where present, send the Parent Company's Anti-Money Laundering Function:

- specific information flows at least on a quarterly basis, concerning the main activities carried out, the results of the controls carried out and the main initiatives undertaken to remove the failings identified, prior to approval in the respective Corporate Bodies and the relevant progress report;
- the minutes of the Board meetings for adoption of the Policies under the responsibility of the Function and, more generally, all those dealing with anti-laundering issues (event-based);
- any changes in local regulations and business initiatives that significantly impact money-laundering risk (event-based);
- in a timely manner, the launch of new inspections by local Supervisory Authorities and all interaction with those authorities (event-based);
- the staff training plan (annually);
- significant changes to the organisational structure of the local Function and/or appointments of new Function managers or of any related organisational units.

Similarly, the AML Function of the Bank continuously liaises and aligns with the AML Function of the Parent Company of the Mediolanum Insurance Group, to which it has extended the methodologies described in this Policy and from which it receives a quarterly reporting flow on activities carried out, enabling integrated reporting at Group level. In particular, the Heads of the AML Functions of the Parent Company Banca Mediolanum and the Parent Company of the Mediolanum Vita Insurance Group coordinate to ensure policy and management consistency in relation to money-laundering issues.

The Group Chief AML Officer must, in all cases, be promptly informed, by the AML Officers of the subsidiaries, of the results of control activities carried out by the Supervisory Authorities or any independent Experts at such companies, as well as on any significant event, including reports and inter-relations of any kind with the competent Authorities.

8. REFERENCE REGULATIONS

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.

The main legislative and regulatory references used for the drafting of this document are as follows:

8.1 EXTERNAL REGULATIONS

EU and international regulations, initiatives and agreements:

- Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015, as amended by Directive (EU) 2018/843, on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing;
- 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;
- Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849;
- Regulation (EU) 2024/886 of the European Parliament and of the Council of 13 March 2024 amending Regulations (EU) No 260/2012 and (EU) 2021/1230 and Directives 98/26/EC and (EU) 2015/2366 as regards instant credit transfers in euro;
- Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing; effective from 10 July 2027 and directly applicable in each Member State, with the aim of harmonising anti-laundering rules fully throughout the European Union;
- EBA (European Banking Authority) Guidelines – *GL/2021/02* – of 1 March 2021, under Articles 17 and 18(4) of Directive (EU) 2015/849 on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions (“The ML/TF Risk Factors Guidelines”), repealing and replacing Guidelines *JC/2017/37*, transposed by the Bank of Italy with Note no. 15 of 4 October 2021;
- EBA (European Banking Authority) Guidelines – *GL/2022/05* – of 14 June 2022, on policies and procedures in relation to compliance management and the role and responsibilities of the AML/CFT Compliance Officer under 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 Policies and Procedures in our legal system;
- EBA (European Banking Authority) Guidelines – *GL/2022/15* – of 22 November 2022, on the use of Remote Customer Onboarding Solutions under Article 13 (1)2 of Directive (EU) 2015/849 (AMLD V), adopted by the Bank of Italy with Note no. 32 of 13 June 2023;
- EBA (European Banking Authority) Guidelines – *GL/2023/03* – of 31 March 2023 amending Guidelines EBA/2021/02 on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing

risk associated with individual business relationships and occasional transactions ("The ML/TF Risk Factors Guidelines") under Articles 17 and 18(4) of Directive (EU) 2015/849 ("EBA Guidelines on customers that are not-for-profit organisations");

- EBA (European Banking Authority) Guidelines – *GL/2023/04* – the of 31 March 2023 on policies and controls for the effective management of money laundering and terrorist financing (ML/TF) risks when providing access to financial services (“EBA Guidelines on de-risking");
- EBA (European Banking Authority) Guidelines – *GL/2024/11* – of 4 July 2024, on information requirements for transfers of funds and certain crypto-assets under Regulation (EU) 2023/1113 ("Travel Rule Guidelines");
- EBA (European Banking Authority) Guidelines – *GL/2024/14* – of 14 November 2024, on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures.

Measures adopted over time by the European Union, in relation to international financial sanctions, depending on the circumstances and requirements of security and foreign policy.

Italian regulations:

- AML 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.AR.A.');
  - storage and use of data and information for anti-money laundering purposes;
- Italian Legislative Decree no. 109 of 22 June 2007, and subsequent amendments and additions, on measures for preventing, combatting and suppressing the financing of international terrorism;
- Legislative Decree 15 December 2017, no. 221, enforcement of the mandate to the Government pursuant to Art. 7 of Law no. 170 of 12 August 2016, 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;

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;
- 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;

- FIU communication of 24 March 2022 on Russian and Belarussian deposits pursuant to Regulations (EU) 328/2022 and 398/2022.
- 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.

8.2 INTERNAL REGULATIONS

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

- Code of Ethics;
- Group Code of Conduct;
- Guidelines and the basic principles for intra-Group coordination between Control Bodies and Functions;
- Policy for the Appointment, Removal and Replacement of Corporate Control Function Managers.