Policy on Anti-Money Laundering and Combating Terrorist Financing of the Mediolanum Group

Meeting of the Board of Directors of Banca Mediolanum S.p.A. of 23 April 2026

CONTENTS

1. INTRODUCTION

This document describes the guidelines on combating anti-money laundering risk defined by the Mediolanum Group, in terms of both the corporate group and for the purposes of the supplementary supervision of credit institutions, insurance undertakings and investment firms forming part of a financial conglomerate (hereinafter also the "Mediolanum Group" or the "Group").

Money laundering and terrorist financing are criminal phenomena which, partly because of their potential transnational dimension, pose a serious threat to the legal economy and can have destabilising effects, particularly for the banking and financial system.

The evolving nature of the threats of money laundering and terrorist financing, also facilitated by the continuous evolution of technology and the means available to criminals, requires the obligated entities to adapt prevention and combating measures on an ongoing basis. They should also put in place measures to identify, manage and mitigate any risk of non-implementation or evasion of restrictive measures or international financial sanctions.

The recommendations of the Financial Action Task Force (FATF) – the main international coordinating body in this area – require public authorities and the private sector to identify and assess the risks of money laundering to which they are exposed, in order to take appropriate mitigation measures. The FATF has also developed rules that allow jurisdictions to identify and assess the risks of potential non-implementation or evasion of restrictive measures or international financial sanctions and to take measures to mitigate such risks.

The European Banking Authority's 2021 Guidelines on ML/TF risk factors define the risk factors that intermediaries must take into account when assessing the risk of money laundering and terrorist financing related to their activities and their ongoing business relationships or occasional transactions, so as to adopt mitigation safeguards that are proportionate to the actual risks.

In addition, the reference European regulatory framework was recently strengthened with the adoption of Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 (the AMLR – Anti-Money Laundering Regulation), part of the "anti-money laundering package" of the European Union. The Regulation establishes a set of rules directly applicable from 10 July 2027 in all Member States, with the aim of harmonising requirements for the prevention of money laundering and terrorist financing and strengthening the effectiveness of enforcement measures.

Money laundering prevention and combating is implemented by introducing safeguards designed to ensure full information on the customer, the traceability of financial transactions and the identification of suspicious transactions. Therefore, in order to ensure adequate mitigation of money laundering and terrorist financing risks, as well as the risks of non-implementation or evasion of restrictive measures or international financial sanctions, obligated entities should have established an internal control framework comprising risk-based policies, procedures and controls and a clear allocation of responsibilities across the organisation.

The Mediolanum Group is strongly committed to preventing the products and services offered from being used for criminal purposes of money laundering and terrorist financing, promoting a culture within the Group based on full compliance with current provisions and the effective fulfilment of passive collaboration obligations, aimed at ensuring in-depth knowledge of customers and the preservation of documents relating to transactions carried out, and active collaboration aimed at identifying and reporting suspicious money laundering transactions.

- The Mediolanum Group also adopts, according to a risk-based approach, specific measures to prevent and effectively mitigate the risk of non-implementation or avoidance of targeted financial sanctions, implementing organisational, procedural and technological safeguards capable of ensuring the timely identification of the designated persons, the continuous monitoring of transactions and the adequate updating of control systems, in accordance with the applicable European and national legislation.

1.1 BACKGROUND

The Companies of the Group in scope adopt a Policy that is consistent with the principles and guidelines contained in this Policy, the structure of which takes account of their specific nature and the risk inherent in their activities, in accordance with the principle of proportionality and with 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 foreseeable developments in such areas, without prejudice to compliance with the specific requirements prescribed by the relevant local legislation.

This Policy is part of the Group's broader system of internal controls aimed at ensuring compliance with current legislation and serves as the foundational document for the Group's entire system of anti-money laundering and anti-terrorism safeguards.

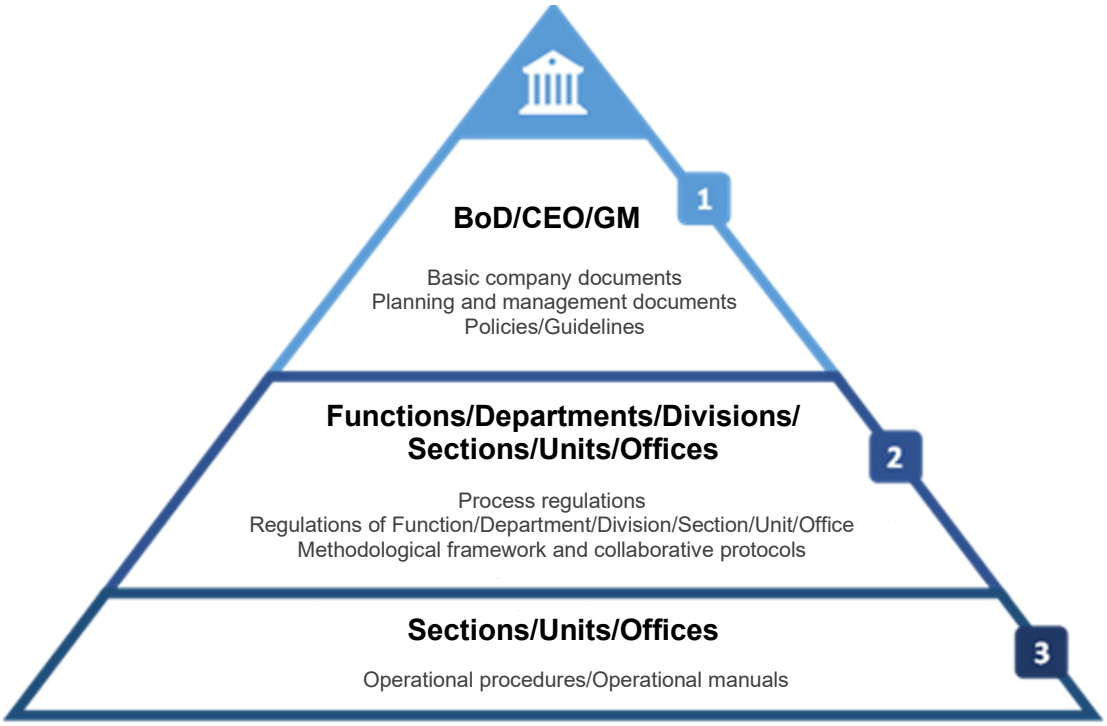
1.2 SCOPE OF THE DOCUMENT

The principles set forth in this Group Policy are implemented in process regulations, methodological frameworks and/or operational procedures, which set out in greater detail the tasks and the operational and control activities underpinning compliance with the requirements of the legislation. In particular, the obligations of due diligence, suspicious transaction reporting and second-level controls must be regulated.

These documents will describe in more detail the processes, operational activities, tools and stakeholders, and their roles and responsibilities within the individual Group Companies to safeguard against money laundering risk and the risk of non-compliance with restrictive measures.

The document entitled "Policy on Procedures for Drafting, Approving, Disseminating and Updating the Internal Regulations of the Mediolanum Group" is positioned at the first (top) level of the documentary pyramid in the diagram below.

Pyramid of internal regulatory sources



2. GENERAL ASPECTS

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

2.1 SCOPE OF APPLICATION

This Policy is sent to all the Companies making up the Mediolanum Group, so that they can adopt it by resolution of their own corporate bodies, without prejudice to any specific provisions of local regulations and the respective Supervisory Authorities, with the exception of companies not currently covered by anti-money laundering regulations.[1]

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 implementation. In his capacity as the Group-level Anti-Money Laundering Officer, he or she monitors over time that the Policy remains adequate and proportionate, taking into account the characteristics of the Group and the risks to which it is exposed.

[1] Mediolanum Comunicazione S.p.A. is not currently included in the anti-money laundering policy.

3. DEFINITIONS

The following definitions apply for the purposes of this Policy:

- **Account Information Service Provider (AISP)**: a payment service provider that offers account information services, i.e. online services that provide consolidated information on one or more payment accounts held by the payment service user with another payment service provider or several payment service providers.
- **Administrative body in its management function**: the administrative body responsible for the daily management of the obligated entity.
- **Administrative body in its supervisory function**: the administrative body that acts in its role of supervising and monitoring management decisions.
- **Administrative body**: the body, or bodies of a obligated entity, appointed in accordance with national law, with the power to establish the strategic guidelines, objectives and general management of the obligated entity, which oversees and monitors management decisions and includes persons who effectively direct the business of the obligated entity; if no such body is in place, the person effectively directing the business of the obligated entity.
- **AML questionnaire (AQ):** the questionnaire divided into three sections to collect information from the customer during due diligence on investment transactions in managed savings products, with reference to the nature and purpose of the transaction, the origin of the funds used and the reports of the parties involved in the transaction.
- **AML WorkFlow**: a management platform used by the Anti-Money Laundering Function to manage the preparation, assessment and filing of evidence and unexpected events and any suspicious transactions and used by the AML Operational Oversight Office to manage enhanced due diligence processes.
- **AML/CTF (Anti Money Laundering/Counter-Terrorist Financing)**: actions taken to combat money laundering and terrorist financing.
- **Anomaly indicators**: cases of anomalous customer transactions or behaviour, aimed at facilitating the assessment by obligated entities of any suspicious money laundering or terrorist financing profiles.
- **Anti-Money Laundering Function**: the function, an integral part of the second-level internal control system, responsible for preventing and combating money laundering and terrorist financing transactions.
- **Anti-Money Laundering Officer**: the member of the administrative body responsible for anti-money laundering, who is the main point of contact between the Head of the Anti-Money Laundering Function and the bodies with strategic oversight and management functions, as identified by the Bank of Italy Provisions on the organisation, procedures and internal controls aimed at preventing the use of intermediaries for the purposes of money laundering and terrorist financing, in implementation of the EBA Guidelines on internal policies and procedures for the management of anti-money laundering compliance and the role of the anti-money laundering officer.
- **Anti-Money Laundering Policy or Policy**: the document defined by the body with management functions and approved by the body with strategic supervisory functions pursuant to the provisions on the organisation, procedures and internal controls designed to prevent the use of intermediaries for the purposes of money laundering and terrorist financing adopted by the Bank of Italy.

- **Assets**: assets of any kind, whether movable or immovable, tangible or intangible, and the legal documents or instruments in any form, including electronic or digital, that attest to the right of ownership or other rights over the assets.

- **Authorised signatory**: the party delegated to operate in the name and on behalf of the customer (or the beneficiary of the insurance benefit) or who is in any case granted powers of representation that enable him or her to operate in the name and on behalf of the customer (or beneficiary of the insurance benefit)[2].

- **Basic information**:
  a) in relation to a legal entity: (i) the legal form and name of the legal entity; (ii) the deed of incorporation, and the articles of association if contained in a separate deed; (iii) the address of the registered or official office and, if different, the principal place of business, and the country of creation; (iv) the list of legal representatives; (v) where applicable, a list of shareholders or members, including information on the number of shares held by each shareholder and the categories of those shares and the nature of the associated voting rights; (vi) where available, the registration number, the unique European identifier, the tax identification code and the identifier of the legal person; and (vii) in the case of foundations, the assets held by the foundation in order to pursue its aims;
  b) in relation to a legal institution: (i) the name or unique identifier of the legal institution; (ii) the deed of incorporation of the trust or equivalent deed; (iii) the purpose(s), if any, of the legal institution; (iv) the assets held in or managed by the legal institution; (v) the place of residence of the trustees of the express trust or persons holding equivalent positions in the similar legal institution and, if different, the place from which the express trust or similar legal institution is administered;

- **Beneficial owner**: any natural person who ultimately owns or controls a legal entity, an express trust or a similar legal institution.

- **Beneficiary of the insurance benefit:**
  1) a natural person or entity other than a natural person that, on the basis of the designation made by the policyholder or the insured, is entitled to receive the insurance benefit paid out by the insurance company;
  2) any natural person or entity other than a natural person for whom payment is made on the instruction of the designated beneficiary.

- **Biometric data**: personal data relating to the physical, physiological or behavioural characteristics of a natural person that allow or confirm their unique identification, such as facial images or dactyloscopic data, obtained and processed by technical means.

- **Business relationship**: a business, professional or commercial relationship related to the professional activities carried out by an obligated entity that is established between an obligated entity and a customer, also in the absence of a written contract, for which a certain repetitiveness or duration is presumed, either when it is established or subsequently.

- **Cash**: i) currency; ii) bearer marketable instruments; iii) assets used as highly liquid reserves; and iv) prepaid cards;

- **Commercial embargoes:** measures for the interruption or reduction, in whole or in part, of economic and financial relations with one or more sanctioned countries.

[2] Parties mandated by a public authority to administer the customer's assets and relations or to represent it (such as receivers in bankruptcy) are considered authorised signatories.

- **Competent Authority:**
  a) a Financial Intelligence Unit (FIU);
  b) a Supervisory Authority;
  c) a public authority that has the task of investigating or prosecuting money laundering, associated predicate offences or terrorist financing, or the task of tracing, seizing or freezing and confiscating the proceeds of crime;
  d) a public authority with responsibilities for combating money laundering or terrorist financing.
- **Compliance Function:** the function that, as an integral part of the second-level internal control system, is entrusted with the specific task of overseeing, according to a risk-based approach, management of compliance risk with regard to corporate activity, ensuring that procedures are adequate to prevent this risk and making use, for the oversight of certain regulatory areas for which specialised safeguards are provided, of appropriate, pre-defined Specialist Units, responsible for overseeing specific phases of the compliance process.
- **Control Functions:** the Corporate Control Functions, the Financial Reporting Officer, the Director in Charge of Controls, the External Auditor, the Supervisory Body and the Data Protection Officer.
- **Control of the legal entity**: the possibility to exercise, directly or indirectly, significant influence and to impose relevant decisions within the legal entity.
- **Control through an equity investment in the company**: direct or indirect ownership of 50% plus one of the shares or voting rights or other equity investment in the company.
- **Corporate bodies**: all bodies with strategic supervision functions (Board of Directors), management functions (CEO or other body to which management functions are assigned) and control functions (Board of Statutory Auditors).
- **Corporate Control Functions:** the Compliance Function, Risk Management Function, Anti-Money Laundering Function and Internal Audit Function.
- **Corporate organisational structures**: all the remaining organisational units provided for by the company regulations other than the corporate bodies and the Control Functions.
- **Correspondence relationship**: (a) the provision of banking services by a credit institution as the correspondent of another credit institution as respondent, including the provision of a current or other liability account and related services such as liquidity management, international transfers of funds as defined in Article 4(25) of Directive (EU) 2015/2366, clearing of cheques, switching accounts and foreign exchange services; and (b) relations between credit institutions and between credit institutions and financial institutions, including where similar services are offered by a correspondent institution to a respondent entity, and including relationships established for the purpose of securities transactions or transfers of funds as defined in Article 4(25) of Directive (EU) 2015/2366, crypto-asset transactions or transfers of cryptoassets.
- **Correspondent accounts and similar relationships**: accounts kept by banks for the settlement of interbank services and for other relationships, however named, between banking and financial intermediaries used for the settlement of transactions on behalf of the customers of the corresponding entities.
- **Counterparty**: natural and legal persons that establish a business relationship (other than contractual long-term relationships that are part of the institutional activity of financial intermediaries and other parties performing financial activities) with the Bank or Conglomerate Company (also if not subject to the obligations established in the Anti-Money Laundering Decree).

- **Cover payment:** the transfer of funds used when there is no direct relationship between the payment service provider (PSP) of the payer and the payee, and it is therefore necessary to use a chain of correspondent relationships between PSPs. Three or more PSPs are involved in a cover payment.

- **Credit institution**: an undertaking whose business is to collect deposits or other repayable funds from the public and grant loans on its own account. A branch of a credit institution, on the other hand, means a place of business that constitutes an unincorporated part of an institution and that directly carries out, in whole or in part, operations relating to the business of that institution, irrespective of whether its head office is located in a Member State or in a third country.

- **Criminal activity**: any type of criminal involvement in the commission of any offence punishable, in accordance with national law, by a prison sentence or detention order of a maximum duration of more than one year or, for Member States whose legal system provides a minimum threshold for offences, any offence punishable by a prison sentence or detention order of a minimum duration of more than six months.

- **Crowdfunding intermediaries**: an undertaking, other than a crowdfunding service provider, whose activity consists of matching or facilitating matching, through an internet-based IT system open to the public or to a limited number of financiers, between:
  a) project owners, i.e. any natural or legal person pursuing the objective of obtaining funding for projects, consisting of a pre-defined operation or series of operations with a particular objective, including the raising of funds for a specific cause or event, irrespective of whether such projects are proposed to the public or to a limited number of funders;
  b) financiers, meaning any natural or legal person that contributes to the financing of projects, by means of loans, with or without interest, or donations, even when such donations entitle the donor to a non-material benefit.

- **cryptoassets:** a digital representation of a value or a right that can be transferred and stored electronically, using distributed ledger technology or a similar technology, except where it falls within the categories of financial instruments; deposits, funds and the others referred to in Article 2(4) of Regulation (EU) 2023/1114.

- **Cultural goods**: the goods listed in Annex I to Regulation (EC) No 116/2009.

- **Customer/Customers**: a party that establishes business relationships or carries out transactions with financial intermediaries and other parties performing financial activities as well as with other recipients of the obligations set out in the Anti-Money Laundering Decree, normally also identified by other terms, such as users, investors, insured persons, policyholders, buyers, entrusted persons, etc.

- **De-risking:** the refusal to enter into a continuing relationship or the decision to terminate a continuing relationship with individual customers or categories of customers associated with a higher risk of money laundering or the refusal to carry out transactions entailing a higher risk of money laundering.

- **Designated persons:** natural or legal persons, groups and entities designated as recipients of measures for the freezing of funds or economic resources on the basis of Community regulations and national legislation.

- **Digital portfolio service providers**: any natural or legal person that provides third parties, in a professional capacity, including online, with services to safeguard private cryptographic keys on behalf of their customers, in order to hold, store and transfer virtual currencies.

- **Due diligence**: activities consisting of:
  - verifying the identity of the customer, any authorised signatory and any beneficial owner on the basis of documents, data or information obtained from a reliable and independent source;
  - acquiring information on the intended purpose and nature of the ongoing business relationship and, when relevant according to a risk-based approach, of the occasional transaction;
  - constant monitoring during the ongoing business relationship.
- **Economic resources**: assets of any kind, whether tangible or intangible, and property, movable or immovable, including accessories and appurtenances, which are not funds but which can be used to obtain funds, goods or services, owned, held or controlled, including partially, directly or indirectly, or through an intermediary natural or legal person, by designated persons or by natural or legal persons acting on behalf or under the direction of the latter.
- **Electronic money**: monetary value stored electronically, including in magnetic storage, represented by a claim on the issuer that is issued upon receipt of funds to effect payment transactions pursuant to Article 4(5) of Directive 2007/64/EC and is accepted by natural or legal persons other than the issuer of electronic money.
- **Embargoed countries**: Countries subject to any economic or commercial sanction (other than administrative sanctions applied by local authorities) or restrictive measures promulgated, applied, imposed or enforced by the "Office of Foreign Assets Control" (OFAC) of the Department of the Treasury of the United States of America, the Department of State of the United States of America, the United Nations Security Council, the European Union and/or any Authority of the Italian Republic including the Revenue Agency, or any other competent authority with regard to sanctions.
- **Employee**: all employees of the Mediolanum Group, whether belonging to organisational units and/or regional structures and/or central structures.
- **Establishment**: the effective operation by an obligated entity of an economic activity in a Member State or third country other than the country in which its head office is located, for an indefinite period of time and with a stable infrastructure, including a branch or subsidiary and, in the case of credit and financial institutions, an infrastructure that qualifies as an establishment in accordance with prudential regulations.)
- **EU countries**: Countries in the European Economic Area.
- **Express trust**: a trust intentionally established by the settlor, *inter vivos* or *mortis causa,* usually in the form of a written document, to place assets under the control of a trustee for the benefit of the beneficiary or for a specific purpose.
- **Family Bankers®**: the financial advisors of Banca Mediolanum authorised to sell via indirect channels, pursuant to Article 31(1) and (2), of Legislative Decree No. 58 of 24 February 1998 (Consolidated Law on Finance).
- **FATF:** the Financial Action Task Force, based at the OECD and specialised in the field of preventing and combating money laundering, terrorist financing and the proliferation of weapons of mass destruction.
- **Financial conglomerates**: groups of undertakings, active to a significant extent in the insurance and banking sectors or in investment services, that include at least one insurance company and one company operating in the banking sector or in investment services and are headed by a regulated entity, or which mainly conduct business in the financial sector; for the purposes of this document, reference is made to the financial conglomerate headed by Banca Mediolanum S.p.A. (hereinafter also the Conglomerate).

- **Financial Institution**: an undertaking other than a credit institution or an investment firm, carrying out one or more activities listed in Annex I to Directive 2013/36/EU of the European Parliament and of the Council, such as, for example: the management of payment instruments, trading in financial instruments, participation in undertakings, portfolio and mutual fund management, custody and administration of securities.)
- **FIU (Financial Intelligence Unit):** independent and operationally autonomous national authorities, engaged in collecting and analysing information to identify the connection between suspicious transactions and underlying criminal activity so as to prevent and combat money laundering and terrorist financing.
- **Freezing of funds and economic resources**: prohibition on movements, transfers, alterations or use of funds attributable to designated persons. Access to assets and any intervention to change the amount, location, ownership or nature of the assets is precluded, effectively preventing any transaction permitting their use, including portfolio management.
- **Funds or other assets**: any asset, including, but not limited to, financial assets, economic resources, including oil and other natural resources, assets of any kind, whether tangible or intangible, movable or immovable, regardless of how they were acquired, and documents or legal instruments in any form, including electronic or digital, that result in a right or interest concerning such funds or other assets, including bank credits, travellers cheques, bank cheques, payment orders, shares, securities, bonds, drafts, letters of credit, and any interest, dividend or other income or value arising from or generated by such funds or other assets, as well as any other asset that could be used to obtain funds, goods or services.
- **Gambling services**: service involving a stake in games of chance, including those involving elements of skill, such as lotteries, casino games, poker and betting, provided in physical premises or, regardless of the method, remotely, by electronic means or other communication technology, and at the request of the individual recipient of services.
- **Group Anti-Money Laundering Function:** the organisational and operational structure of coordination at Group level, with sufficient decision-making power, used by the Group Chief AML Officer to carry out his or her tasks, in accordance with the principle of proportionality and applicable national legislation.
- **Group**: a group of undertakings which includes a parent undertaking, its subsidiaries, as well as undertakings linked by a relationship within the meaning of Article 22 of Directive 2013/34/EU on the obligation to prepare consolidated financial statements.
- **High-risk third countries**: countries not in the European Economic Area whose legislation indicates strategic shortcomings in their national systems for the prevention of money laundering and terrorist financing, as identified by the European Commission in the exercise of the powers referred to in Articles 9 and 64 of the Fourth Anti-Money Laundering Directive.
- **High-value goods**: the goods listed in Annex IV of Regulation (EU) 2024/1624.
- **Identification data of the beneficiary, the beneficial owner and the authorised signatory:** their name and surname, place and date of birth. In the case of persons other than natural persons: their name, registered office, registration number in a company register or in a register of legal entities where provided for. In both cases, at the time of payment of the benefit, the registered residence and, if different, the domicile, the tax code of the beneficiary and, where provision is made for their assignment, also of the relevant beneficial owner and authorised signatory.

- **Identification data of the customer, the relevant beneficial owner and the authorised signatory**: the first and last name, the place and date of birth, the registered address and, where different, the domicile and, where assigned, the tax code of the customer and, where assigned, of the relevant beneficial owner and the authorised signatory. In the case of persons other than natural persons: their name, registered office, registration number in a company register or in a register of legal entities where provided for.
- **Indirect control of a legal entity**: control of intermediate legal entities in the ownership structure or in various chains of the ownership structure, in which direct control is identified at each level of the structure.
- **Inherent risk:** according to a "potential" risk approach, the likelihood of the Company suffering direct or indirect damage of a sanctioning, criminal, financial or reputational nature, without considering the organisation and operation of its organisational safeguards and its more general system of internal controls.
- **Insurance intermediaries:** natural persons or companies having their residence or registered office in Italy – entered in the single electronic register of insurance intermediaries referred to in Article 109, paragraph 2, letters a), b) and d) of the Code of Private Insurers – as well as natural persons or companies having their residence or registered office in another Member State of the European Union, in a country that is a member of the European Economic Area or in a third country, operating in Italy under the establishment regime – registered in the list attached to the register pursuant to the notification referred to in Articles 116-quater and 116-quinquies of the Code – engaged solely in the distribution in Italy of insurance products belonging to the classes of activity listed in Article 2, paragraph 1 of the Code.
- **Internal Audit Function:** the function which is entrusted with monitoring, with a view to third-level controls, including onsite controls, the regular performance of operations and the evolution of risks and with assessing the completeness, adequacy, functionality and reliability of the organisational structure and other components of the internal control system, bringing possible improvements to the attention of corporate bodies, with particular reference to the Risk Appetite Framework (RAF), the risk management process and the tools for measuring and controlling such risks. Based on the results of its controls, it makes recommendations to the corporate bodies. In addition, in view of the Group's business model, particular attention is paid to monitoring the operations carried out by the Sales Networks.
- **Internal control system**: the set of rules, functions, structures, resources, processes and procedures which, in accordance with sound and prudent management, is designed for:
  - monitoring the implementation of corporate strategies and policies;
  - containing risk within the limits indicated in the reference framework for determining the Group's risk appetite (Risk Appetite Framework or RAF);
  - safeguarding the value of assets and protect against losses;
  - ensuring the effectiveness and efficiency of corporate processes;
  - guaranteeing the reliability and security of corporate information and IT procedures;
  - preventing the risk that the Group may be involved, voluntarily or unintentionally, in illegal activities (with particular regard to those related to money-laundering, usury and terrorist financing);
  - ensuring the compliance of transactions with laws and supervisory regulations, as well as internal policies, regulations and procedures.

- **International sanctions:** economic, financial and administrative sanctions imposed from time to time by the Italian or European Union legal system, the United Nations Security Council (UN), the United States, which include (but are not limited to) embargoes and the freezing of assets.
- **Legal entity identifier**: alphanumeric reference code complying with the ISO 17442 standard assigned to a legal entity.
- **Line controls ("first-level controls")**: the set of controls designed to ensure that transactions are executed properly. These controls are performed by the same corporate organisational structures (e.g. hierarchical and systematic controls and spot checks), including through units dedicated exclusively to control or oversight tasks that report to the heads of the corporate organisational structures, or are carried out in the back office context; where possible, they are incorporated into IT procedures.
- **Mixed financial holding company**: an undertaking, other than a financial holding company or a mixed financial holding company, that is not a subsidiary of another undertaking, whose subsidiaries include at least one credit institution or financial institution.
- **Mixed non-financial holding company**: an undertaking, other than a financial holding company or a mixed financial holding company, that is not a subsidiary of another undertaking, whose subsidiaries include at least one obligated entity.
- **Money laundering risk**: the risk arising from the violation of provisions of law, regulations and self-regulations functional to the prevention of the use of the financial system for the purposes of money-laundering, financing of terrorism or financing of programmes for the development of weapons of mass destruction, as well as the risk of involvement in episodes of money laundering, financing of terrorism or financing of programmes for the development of weapons of mass destruction.
- **Money laundering:**
  - the conversion or transfer of property, knowing that such property is derived from any offence or offences or from an act of participation in such offence or offences, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an offence or offences to evade the legal consequences of his actions;
  - the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property, knowing that such property is derived from an offence or offences or from an act of participation in such an offence or offences;
  - the acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from an offence or offences or from an act of participation in such offence or offences;
  - participation in, association or conspiracy to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the offences established above.

  Money laundering is considered as such even if the activities that generated the goods to be laundered took place outside national borders. The knowledge, intent or purpose that must constitute an element of such conduct may be inferred from objective factual circumstances.
- **Non-profit organisations:** a legal person or legal institution or organisation mainly responsible for the collection or disbursement of funds for charitable, religious, cultural, educational, social or solidarity purposes.

- **Occasional transaction**: a transaction not attributable to an existing business relationship; intellectual or commercial services, including those carried out instantaneously for the customer, also constitute occasional transactions.
- **Operations**: the activity requested of or identified by the recipient as part of the establishment or performance of an ongoing relationship or of one or more transactions.
- **Origin of assets**: the origin of the customer's total assets, including both movable and immovable assets.
- **Origin of funds**: the origin of the funds specifically used in an ongoing business relationship or an occasional transaction.
- **Parent Company**:
  a) for groups whose head offices are situated in the European Union, an obligated entity that is a parent undertaking controlling one or more subsidiary undertakings and is not itself a subsidiary of another undertaking in the European Union, provided that at least one subsidiary is an obligated entity;
  b) for groups whose head office is located outside the European Union, where at least two subsidiaries are obligated entities established outside the European Union, an undertaking within that group established in the European Union that:
    i. is an obligated entity;
    ii. is an undertaking that is not a subsidiary of another undertaking that is an obligated entity established in the European Union;
    iii. is sufficiently relevant within the group and has a sufficient understanding of the group's operations;
    iv. is responsible for the implementation of obligations and requirements at group level.
- **Partnership for the sharing of information**: a mechanism allowing for the sharing and processing of information between the obligated entities and, where appropriate, the competent authorities referred to in point 44) a), b) and c) of Regulation (EU) 2024/1624, for the purposes of preventing and combating money laundering, associated predicate offences and terrorist financing, at national or cross-border level, and regardless of the form of this partnership.
- **Payment instruments**: cash, bank and postal cheques, bank drafts and other similar or comparable cheques, postal orders, credit or payment orders, credit cards and other payment cards, transferable insurance policies, pledge policies and any other available instrument that allows the transfer, handling or acquisition, including by electronic means, of funds, securities or financial assets.
- **Person with whom the persons are known to have close ties**: a natural person who is known to have joint beneficial ownership of legal entities or legal arrangements or any other close business relationship with a politically exposed person, or a natural person who is the sole beneficial owner of legal entities or legal arrangements known to have been established for the benefit of a politically exposed person.
- **Politically exposed persons (PEPs)**: the natural persons referred to in Article 1(2)d) of the Anti-Money Laundering Decree, i.e. "natural persons who occupy, or have ceased to occupy within the last year, prominent public functions, as well as their family members and known close associates, as listed below:

1) natural persons who occupy or have occupied prominent public functions are persons who hold or have held the position of:

1.1 President of the Republic, Prime Minister, Minister, Deputy Minister and Under-Secretary, President of the Region, regional councillor, mayor of a provincial capital or metropolitan city, mayor of a municipality with a population of no less than 15,000 and similar offices in foreign states;

1.2 deputy, senator, MEP, regional councillor and similar offices in foreign states;

1.3 member of the central governing bodies of political parties;

1.4 judge of the Constitutional Court, magistrate of the Court of Cassation or of the Court of Auditors, councillor of state and other members of the Board of Administrative Justice for the Sicilian Region and similar offices in foreign states;

1.5 member of the governing bodies of central banks and independent authorities;

1.6 ambassador, chargé d'affaires or equivalent positions in foreign states, high-ranking officer in the armed forces or similar offices in foreign states;

1.7 member of the administrative, management or control bodies of companies controlled, including indirectly, by the Italian State or by a foreign state or owned, predominantly or wholly, by the Regions, by municipal authorities of provincial capitals and metropolitan cities and by municipalities with a total population of no less than 15,000;

1.8 general manager of local health units (ASL) and hospital, university hospital and other health service institutions;

1.9 director, deputy director and member of the management body or entity performing equivalent functions in international organisations;

2) family members of politically exposed persons are: parents, spouses, civil partners or cohabitees or similar of the politically exposed person, his children and the spouses, civil partners, cohabitees or similar of his children;

3) known close associates of Politically Exposed Persons are:

3.1 natural persons who are connected with the Politically Exposed Person by reason of their joint beneficial ownership of legal entities (including trusts and similar legal institutions) or who have close business relationships with the Politically Exposed Person;

3.2 natural persons who only formally hold total control of an entity known to be constituted, in fact, in the interest and for the benefit of a Politically Exposed Person."

- **Precious stones and metals**: the stones and metals listed in Annex V to Regulation (EU) 2024/1624.
- **Privacy coins**: cryptoassets that have intrinsic characteristics designed to anonymise information on transfers of cryptoassets, systematically or optionally;
- **Providers of services relating to companies and trusts**: any natural or legal person that provides, in a professional capacity, one of the following services to third parties:
  - establishing companies or other legal persons;
  - acting as a director or officer of a company, partner in an association or a similar function with respect to other legal persons or causing another person to perform such a function;
  - providing a registered office, business, administrative or postal address and other services related to a company, association or any other legal entity;
  - occupying the role of trustee in an express trust or similar legal institution or causing another person to act in such a capacity;
  - exercising the role of shareholder on behalf of another person or causing another person to act in such a capacity, provided that it is not a company listed on a regulated market and subject to disclosure requirements in accordance with Community law or equivalent international rules.
- **PSP:** Payment Service Provider.

- **Related transactions**: two or more transactions of identical or similar origin, destination and purposes or other relevant characteristics over a specified period.
- **Remote relationships or transactions:** any transaction or relationship where the customer is not physically present, i.e. not in the same physical place as the company or a person acting on its behalf. This includes situations where the customer's identity is verified via video link or similar technology.
- **Remote transactions**: transactions performed without the physical presence of the customer and the Group's designated staff. When the customer is a party other than a natural person, it is regarded as present whenever the authorised signatory is present.
- **Residual risk:** a summary opinion that takes account of the assessment of the suitability of the organisational, procedural and control safeguards in place, with the ensuing identification of the corrective measures to be taken to mitigate it.
- **Restrictive measures:** restrictive measures adopted by the European Union, such as measures relating to the freezing of funds and economic resources, prohibitions on the provision of funds and economic resources, as well as sectoral economic and financial measures and arms embargoes and measures adopted by Member States in accordance with their national legal system (to the extent that they apply to financial institutions).
- **Risk and compliance controls ("second-level controls")**: the set of controls designed to ensure, *inter alia*:
  - the correct implementation of the risk management process;
  - the observance of the operational limits assigned to the various functions;
  - the compliance of company operations with regulations, including self-imposed regulations.

  The functions responsible for these controls are separate from the operational functions. They help to define risk governance policies and the risk management process.
- **Risk appetite**: the level of risk (overall and by type) that the Company intends to assume in pursuit of its strategic objectives. With reference to money laundering risk, both quantitative indicators (e.g. the percentage of customers classified as high risk out of the total number of customers) and qualitative elements (e.g. the limitations and restrictions set out in this Policy) may be considered for the purposes of the Risk Appetite.
- **Risk factors**: variables that, individually or in combination, may increase or reduce the money laundering risk deriving from individual ongoing relationships or occasional transactions.
- **Risk Management Function**: the function that, as an integral part of the second-level internal control system, is responsible for implementing governance policies and the risk management system and that collaborates in defining and implementing the RAF, ensuring, in the exercise of the control function, an integrated picture of the various risks to the corporate bodies.
- **Risk-based approach**: refers to an approach whereby the competent authorities and companies identify, evaluate and understand the money-laundering risks to which the companies are exposed and take measures to address these risks.
- **S.I.G.M.A.:** Sistema Informatico Gestione Materiali Armamenti (Information System for the Management of Armament Materials), in support of the institutional activities of Office VI of Directorate V of the Treasury Department of the MEF which, on the basis of the provisions of Law No. 185 of 9 July 1990, as amended by Legislative Decree No. 105/2012, has the task of supervising, together with a specific nucleus of Italian law enforcement agency Guardia di Finanza, the activities of credit institutions with regard to the financing of the transactions regulated by Law No. 185/90, for the purposes of combating terrorism.

- **Sanctions list/lists of sanctioned persons/lists of designated persons**: the list sof the names of sanctioned persons distributed by the United Nations Security Council, the European Union, OFAC and OFSI.
- **Senior Executive (Senior Management)**: a director or the general manager or other employee delegated by the body with management functions or the general manager to monitor relations with high-risk customers; the Senior Executive has appropriate knowledge of the level of money laundering risk to which the recipient is exposed and has sufficient autonomy to take decisions that affect this level of risk.
- **Service provider for crypto-activities**: a legal person or other undertaking whose employment or activity consists in the provision of one or more crypto-activity services to customers on a professional basis and which is authorised to provide services for crypto-activities.
- **Services for cryptoassets**: any services and activities listed below in relation to any cryptoassets: provision of custody and administration of cryptoassets on behalf of customers; management of a cryptoassets trading platform; exchange of cryptoassets with funds; exchange of cryptoassets with other cryptoassets; execution of cryptoassets orders on behalf of customers; placement of cryptoassets; receipt and transmission of cryptoassets orders on behalf of customers; provision of portfolio management on cryptoassets; provision of cryptoassets transfer services on behalf of customers.
- **Shell bank**: a bank (or financial intermediary that performs functions similar to those of a bank) without a significant structure in the country in which it was established that is authorised to conduct its business and does not belong to a financial group subject to effective supervision on a consolidated basis.
- **Shell company**: for credit institutions and financial institutions other than crypto service providers: a credit institution, financial institution or institution carrying out activities equivalent to those carried out by credit institutions and financial institutions, established in a jurisdiction where it has no physical presence, which allows it to exercise real direction and management and which is not connected to any regulated financial group.
- **Sherpany**: the platform adopted by the Corporate Affairs Division to manage meetings of the corporate bodies, which grants secure access to the various documents, both online and offline, made available by the various corporate functions.
- **Staff**: employees and individuals who in any case operate on the basis of relationships that determine their inclusion in the Bank's organisation, also in forms other than an employment relationship, including financial advisors authorised to sell through indirect channels pursuant to Article 31(2) of the Consolidated Law on Finance, and direct producers and brokers pursuant to Article 109(2)c) and e) of the Code of Private Insurers.
- **Supervisor**: the body to which responsibilities are assigned to ensure compliance by the obligated entities with AML/CTF requirements, including those of AMLA in the performance of the tasks entrusted to it.
- **Supervisory Authority**: a public body or public authority that monitors the self-regulatory bodies in the exercise of supervisory functions, or the AMLA when acting as a supervisor.
- **Suspicious transaction**: transactions to be reported to the Financial Intelligence Unit when the recipients know, suspect or have reasonable grounds to suspect that money laundering or terrorist financing transactions have been carried out or attempted, or that the funds originate from criminal activities. Suspicion is based on the characteristics, size and nature of the transactions, their connection or splitting or any other circumstances known, due to the duties performed, taking into account the economic capacity of, and activity carried out by, the party concerned, on the basis of the information obtained pursuant to the anti-money laundering decree.

- **Targeted financial sanctions**: the freezing of assets and the prohibition on making funds or other assets available, directly or indirectly, to persons and entities designated in accordance with Board decisions.
- **Terrorist financing:** any activity directed, by any means, to the supply, collection, provision, intermediation, deposit, custody or disbursement of funds and economic resources, however carried out, intended to be, directly or indirectly, in whole or in part, used for the performance of one or more acts for the purposes of terrorism, as provided for by criminal laws, regardless of the actual use of such funds and economic resources for the commission of the aforementioned acts. The knowledge, intent or purpose that must constitute an element of such conduct may be inferred from objective factual circumstances.
- **Third countries**: any jurisdiction, independent State or autonomous territory that is not part of the Union and which has its own legislation or regime for the application of AML/CFT rules;
- **Transaction monitoring system*:*** the IT procedure used to select anomalous transactions based on quantitative parameters, such as the amount or frequency of transactions and the origin or allocation of flows, and qualitative parameters, such as the type or conditions of use of the services and the characteristics of the entities involved.
- **Transaction**: activities consisting of the handling, transfer or transmission of payment instruments or the undertaking of contractual arrangements with financial content; entering into a contractual arrangement with financial content within the framework of professional or commercial activity also constitutes a transaction.
- **Transition accounts**: cross-border correspondent banking relationships between banking and financial intermediaries, used to carry out transactions in their own name and on behalf of customers.
- **UN financial sanctions**: mandatory restrictive measures decided by the United Nations Security Council (UNSC), pursuant to Article 41 of Chapter VII of the UN Charter.
- **Virtual currency**: the digital representation of value, not issued by a central bank or public authority, not necessarily linked to a legal tender currency, used as a means of exchange for the purchase of goods and services and transferred, stored and traded electronically.
- **Virtual IBAN**: an identifier that ensures that payments are redirected to a payment account identified by an IBAN other than the identifier.

4. STAKEHOLDERS

Below are the main actors of the Parent Company, involved in various capacities within the scope of this Group Policy, with a description of their respective roles and responsibilities.

4.1 BOARD OF DIRECTORS

The Parent Company's Board of Directors defines the model for monitoring money laundering risk at Group level.

It is the body with strategic oversight functions to which a corporate management guidance role is assigned and to which the Corporate Control Functions, including the Anti-Money Laundering Function, report.

The Board of Directors approves updates to this Policy from time to time, at the proposal of the Anti-Money Laundering Function.

4.2 RISK COMMITTEE

The Parent Company's Risk Committee provides support to the Board of Directors in determining the guidelines for the internal control and risk management system, including for money laundering risk.

It assesses this Group Policy before it is submitted to the Board of Directors.

4.3 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 the regulations and the completeness, functionality and adequacy of anti-money laundering controls, including at Group level, using internal structures to carry out the necessary checks and inspections and using information flows from other corporate bodies, the Head of the Anti-Money Laundering Function and the other Corporate Control Functions.

4.4 CHIEF EXECUTIVE OFFICER

The Chief Executive Officer of the Parent Company, also in his/her capacity as Group Anti-Money Laundering Officer, implements the strategic guidelines and governance policies for money laundering risk at Group level approved by the body with strategic oversight functions and is responsible for adopting all necessary measures to ensure the effectiveness of the anti-money laundering organisation and control system.

4.5 ANTI-MONEY LAUNDERING OFFICER

The Anti-Money Laundering Officer of the Parent Company acts as the main point of contact between the Head of the Group Anti-Money Laundering Function and the Board of Directors of the Parent Company and ensures that the latter has the information necessary to fully understand the significance of the money laundering risks to which the Group is exposed. The AML Officer ensures that the Head of the Anti-Money Laundering Function of the Parent Company performs his or her duties effectively.

4.6 INTERNAL AUDIT FUNCTION

The Parent Company's Internal Audit Function is the central function of reference for the corresponding functions of the Subsidiaries, with the task of continuously verifying the adequacy of the anti-money laundering organisational structure and its compliance with current legislation.

4.7 ANTI-MONEY LAUNDERING FUNCTION

The Anti-Money Laundering Function of the Parent Company is the central function of reference for the corresponding functions of the Subsidiaries to monitor the risk of money laundering and non-compliance with restrictive measures. In its capacity as Corporate Control Function, it oversees the risk of money laundering and non-compliance with restrictive measures, based on a risk-based approach.

It supports the Parent Company's Board of Directors in defining the model for monitoring the risk of money laundering and non-compliance with restrictive measures of the Group, and assists the Head of the Group Anti-Money Laundering Function in coordinating activities at Group level for these areas.

4.8 HEAD OF THE ANTI-MONEY LAUNDERING FUNCTION

The Group Chief AML Officer is appointed by the Board of Directors, following consultation with the Board of Statutory Auditors, as the Group Anti-Money Laundering Officer, pursuant to the EBA Guidelines on AML policies and procedures.

the Group Anti-Money Laundering Officer:

- collaborates with the AML Officers of the Italian or foreign Group Companies and ensures that these Officers carry out their duties in a coordinated manner and according to policies and procedures consistent with those of the Group;
- supervises the money-laundering risk self-assessment conducted by the Group's corporate bodies;
- prepares an assessment of the Group's money-laundering risks, taking into account the risks resulting from the individual exercises, the interrelations between the individual Group Companies and their impact on risk exposure at Group level;
- submits to 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 Parent Company's Anti-Money Laundering Function;
- develops and submits Group anti-money laundering procedures, methods and standards to the management bodies of the Parent Company, with particular reference to due diligence procedures, and ensures that the policies and procedures of Group members are in line with such standards and comply with the applicable anti-money laundering laws and regulations;
- establishes periodic information flows from all Group Companies to share the information required for the performance of its duties. In order to ensure the implementation of effective anti-money laundering risk policies and procedures at Group level, the Group Anti-Money Laundering Officer makes use of the resources of the Bank's Anti-Money Laundering Function.

4.9 HEAD OF COMPLIANCE WITH RESTRICTIVE MEASURES

The Board of Directors of the Parent Company, Banca Mediolanum S.p.A., has also assigned to the Head of the Anti-Money Laundering Function the role of Head of Compliance with Restrictive Measures at Group level, without prejudice to the ultimate responsibility for compliance with restrictive measures of each Group entity and the need for each Group entity to identify, internally, a contact person required to ensure full compliance with the regulatory provisions on restrictive measures, pursuant to the EBA Guidelines on policies, procedures and internal controls aimed at ensuring the implementation of EU and national restrictive measures.

The contact persons of each Group entity activate specific information flows to the Head of Compliance with Restrictive Measures at Group level regarding the activities carried out and promptly inform them of any critical issues or breaches identified.

The Head of Compliance with Restrictive Measures at Group level is entrusted with the task of developing, implementing and maintaining up-to-date policies, procedures and controls appropriate to ensure compliance with the restrictive measures on the part of the Bank and the Group Subsidiaries, in a manner proportionate to their exposure to the aforementioned restrictive measures.

Specifically, the Head of Compliance with Restrictive Measures, also with the support of the Anti-Money Laundering Function:

- adopts the necessary measures to ensure compliance with the provisions of the EBA Guidelines on (i) the assessment of exposure to restrictive measures and (ii) the effectiveness over time of relevant policies, procedures and controls;
- periodically provides specific information – as detailed in the EBA Guidelines – to the body with strategic oversight and management functions of the Company;
- reports all violations of restrictive measures to the competent national Supervisory Authorities and cooperates effectively and constructively with them.
- periodically provides, in the context of the quarterly report on the activities carried out by the Anti-Money Laundering Function, adequate information to the corporate bodies on the exposure of the Bank and the Group's subsidiaries to restrictive measures.

The Head of Compliance with Restrictive Measures may assign and delegate the duties assigned to him or her to other members of staff acting under his or her direction and supervision, provided that the Head of Compliance with Restrictive Measures remains ultimately liable for the proper performance of these duties.

5. CONTROL MODEL FOR THE RISK OF MONEY-LAUNDERING AND NON-COMPLIANCE WITH RESTRICTIVE MEASURES

5.1 ORGANISATIONAL SAFEGUARDS

The model for countering the risk of money laundering and evasion of restrictive measures is managed, at Group level, through a specific process aimed at implementing and maintaining rules, procedures and organisational structures that are designed to ensure the prevention and management of the risk in question, by all Group Companies.

The model provides that primary responsibility for monitoring the risk of money laundering and non-compliance with restrictive measures falls within the remit of the corporate bodies of each Group Company, each according to its respective responsibilities and in accordance with the guidelines of the Parent Company. The allocation of duties and responsibilities in this area by the corporate bodies and functions must be clearly defined and formalised in each Company.

Consistent with the accepted principles of corporate governance, the model recognises, for each Group Company, the centrality of the body with strategic oversight functions with regard to the risk governance policies in question: it is responsible for approving the Anti-Money Laundering Policy (in line with the principles of this Policy) and for adopting a system appropriate to the characteristics of the undertaking; in this regard, it is organised in such a way that it can address the issue of the risk of money laundering and non-compliance with restrictive measures with due care and 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 risk of money laundering and non-compliance with restrictive measures to which the Company is exposed, each Group Company appoints its own Anti-Money Laundering Officer, without prejudice to the principle of proportionality and taking into account specific local regulatory provisions.

The body with management functions is responsible for the implementation of the strategic guidelines and policies governing money laundering risk approved by the body with strategic oversight functions and is responsible for adopting all necessary measures to ensure the effectiveness of the organisation and control system for anti-money laundering and compliance with restrictive measures.

The control body, within the framework of its responsibility for supervising compliance with regulations and the completeness, adequacy, functionality and reliability of the internal control system with regard to anti-money laundering, also liaises constantly with the Anti-Money Laundering Function.

The Group Companies appoint a Head of the Anti-Money Laundering Function, who is responsible for ensuring compliance with anti-money laundering and counter-terrorist financing requirements, and restrictive measures, in line with the principles established in this Policy; if the Anti-Money Laundering Function is included in the Compliance Function, responsibility for monitoring the risk of non-compliance with restrictive measures may also be assigned to the Compliance Officer.

In accordance with the principle of proportionality and where provided for in the specific applicable regulations, each Group company also establishes a specific Anti-Money Laundering Function, responsible for overseeing the risk of money laundering and non-compliance with restrictive measures, which coordinates and interacts with the other Control Functions, in order to ensure the proper operation of the internal control system. Each Group Company adopts organisational measures and safeguards designed to ensure the business continuity of the Anti-Money Laundering Function, also in case of the absence or impediment, of a temporary nature, of the AML Officer. If the absence or impediment of the AML Officer continues for more than three months, the body with strategic oversight functions meets in order to replace the Officer.

The AML Officer – unless otherwise provided for by specific local regulations – is also appointed as the Suspicious Transaction Reporting Officer.

The Suspicious Transaction Reporting Officer forwards a relevant report to the relevant national FIU, according to the procedures provided for by the legislation in force, whenever he knows, suspects or has reasonable grounds to suspect that the funds, regardless of their amount, originate from criminal activities or are related to the financing of terrorism, responding promptly, in such cases, to requests for further 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 the risk of money-laundering and non-compliance with restrictive measures is also based on the broad involvement of all the corporate organisational structures and on a clear definition of the duties and responsibilities of these functions. In this context, line controls ("first-level controls"), designed to ensure the proper performance of transactions by using appropriate safeguards and information systems, play a crucial role.

The Organisational Structures of each Group company are required to be familiar with and strictly abide by the applicable laws, regulations and by the rules issued by the company. In this regard, Group companies provide their employees and contractors with operational tools and procedures, including computerised ones, to assist them in complying with the relevant requirements for the purposes of combating money-laundering and non-compliance with restrictive measures and prepare specific long-term training and CDP programmes so that they have adequate knowledge of the relevant legislation and related responsibilities and are able to use tools and procedures to help them fulfil their obligations.

When the staff of the Organisational Structures, in the performance of their activities, discover that operational processes do not comply with the relevant rules or the safeguards adopted are not effective in preventing the Company or the Group from being involved, including unwittingly, in money laundering or terrorist financing transactions, they must promptly notify their manager, who has overall responsibility for the compliance with and effective operation of first-level controls within his structure; when carrying out the necessary investigations, the managers immediately involve the Anti-Money Laundering Function in the relevant assessments.

Where the Operational Structures are assigned the administration and management of customer relations in practice, they are responsible for the process of identifying and carrying out due diligence on their customers as the first level of control, developing customer knowledge and ensuring ongoing monitoring throughout the relationship, in accordance with the underlying risk. They are also responsible for carrying out the enhanced due diligence process in the cases provided for by law and where required by the Anti-Money Laundering Function, and for promptly reporting, where possible before the transaction is carried out, any suspicious transactions, according to the procedures and modalities defined internally, when they know, suspect or have reasonable grounds to suspect that an anti-money laundering or terrorist financing transaction has been carried out, is in progress or has been attempted.

The financial advisors of the Sales Network and the agents engaged in financial activities, if any[3], personally manage the process of identification and Due Diligence on the Customers assigned to them as the first level of control, developing customer knowledge and carrying out ongoing monitoring during the relationship, according to the underlying risk. They are also responsible for carrying out enhanced due diligence in the cases provided for by law and where required by the Anti-Money Laundering Function and the corporate organisational structures.

As part of their activities, financial advisors are required to know and comply with the laws, regulations and rules issued by the relevant Company, also with reference to the rules of conduct for anti-money laundering purposes, as stipulated in the agency agreements.

The company constantly monitors compliance by the Sales Network with the anti-money laundering rules of conduct established by law and contractually, including through periodic checks at the administrative offices of the financial advisors.

[3] In particular, reference is made to Banca Mediolanum S.p.A., Banco Mediolanum SA and Prexta S.p.A.

Given that the financial advisors are responsible, in practice, for administering and managing relations with the Customers assigned to them, they constitute, for all intents and purposes, the first reporting level.

The financial advisors promptly report any suspicious transactions to the Anti-Money Laundering Function, where possible before the transaction is carried out, according to the procedures and modalities defined internally, when they know, suspect or have reasonable grounds to suspect that an anti-money laundering or terrorist financing transaction has been carried out, is in progress or has been attempted.

6. PRINCIPLES ON COMBATING THE RISK OF MONEY LAUNDERING AND NON-COMPLIANCE WITH RESTRICTIVE MEASURES

The Group Companies adopt procedures and methods commensurate with the nature of its business and size for the analysis and assessment of the money laundering risk to which it is exposed in the exercise of its business, taking into account multiple risk factors.

In this regard, the Parent Company has defined these specific Group guidelines, based on the highest standards for combating money laundering and terrorist financing, to be followed by all members of corporate bodies, employees and contractors in order to prevent the Bank itself and Group companies from being involved, including unwittingly, in money laundering and terrorist financing.

The incorporation of the guidelines and principles set out in this Policy at the Group level is a preliminary step towards encouraging adequate coordination between local anti-money laundering safeguards and the Anti-Money Laundering Function of the Parent Company and ensuring the effective circulation of information at the level of the Group, in order to combat the risk of money laundering. The Chief AML Officer defines standards for combating 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 and regulatory provisions and the above standards.

In order to achieve appropriate synergies and economies of scale, exploiting highly specialised competence centres, the companies of the Banking Group and those of the Insurance Group may delegate to the Parent Company – on the basis of specific outsourcing agreements, drawn up in compliance with supervisory regulations and in accordance with the principles set out in the "Company Outsourcing Policy" – the performance of the duties of the Anti-Money Laundering Function pursuant to current legislation.

The said agreements must regulate at least the following issues:

- the objectives of the function and the content of outsourced activities;
- the expected service levels;
- the minimum frequency of information flows;
- the confidentiality obligations with respect to any information acquired in the exercise of the function or activities;
- the possibility of reviewing the conditions of the service if changes occur in the Company's operations and organisation.

Below are some guidelines on the fulfilment of obligations in accordance with regulatory provisions, which are set out, for the purposes of their full implementation, in the specific Process Regulations and/or operational procedures that each Group Company must adopt.

6.1 INTEGRITY OF EMPLOYEES AND FINANCIAL ADVISORS AND CONFLICT OF INTEREST MANAGEMENT

Mediolanum Group staff involved in activities relevant to the prevention of money laundering and terrorist financing must meet appropriate requirements of integrity, good repute and professionalism, and act in accordance with the principles of propriety, independence of judgement and responsibility.

In this context, the Group adopts reasonable procedures to prevent and manage conflicts of interest that may affect the performance of the tasks assigned to financial advisors and employees who actually manage and administer customer relations pursuant to this Policy.

6.2 CUSTOMER DUE DILIGENCE

Group Companies subject to the obligation to establish control safeguards in the area of anti-money laundering adopt customer due diligence measures proportional to the extent of the money laundering risk to which they are exposed, taking into account specific factors regarding the customer, the transaction and the business relationship.

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

If the business relationship involves more than one product or service, the Group Companies ensure that customer due diligence measures involve all products and services.

The KYC (know your customer) principle, which is incorporated into due diligence rules, is also of particular importance in connection with the principle of active collaboration and the obligation to report suspicious transactions. The identification of the customer, any authorised signatory and the beneficial owner, along with the relevant identity verification and information gathering, must therefore take place through dialogue. This is necessary, both for the customer to become acquainted with the company and to declare the purpose and nature of the ongoing relationship they intend to establish, and for the company and its staff to learn more about the customer's banking, financial and insurance needs, enabling them to offer the products and services best suited to the customer's requirements.

To this end, the Group Companies adopt appropriate training initiatives for their staff, as described in paragraph 6.11 below.

The employees of the corporate organisational structures responsible for the management and administration of customer relations in practice and the financial advisors of the Sales Network, where present, fulfil their due diligence obligations by complying with the measures, methods and internal procedures adopted by the Group, so as to develop and maintain information on customers and report any suspicious transactions.

If the Group Companies are unable to comply with the obligation to apply customer due diligence measures, they refrain from carrying out an operation or starting a business relationship, terminate the business relationship and consider whether to report a suspicious transaction to the competent FIU in relation to the customer.

In order to ensure the proper performance of customer due diligence, the financial advisors – where present – and employees of the corporate organisational structures entrusted with the management and administration of customer relations in practice, are responsible for:

- the identification of customers, any authorised signatories, beneficial owners and the acquisition of the relevant identification documents as well as any additional information necessary to determine the risk profile to be associated with the customer;
- the identification, in the cases provided for by the legislation in force from time to time, of the beneficiary, the legitimate heirs and any relevant beneficial owners and the acquisition of the relevant identification documents;
- verification of the identity of the customer, the beneficiary, any authorised signatories and any beneficial owner of the customer, the beneficiary and their lawful heirs, on the basis of documents, data or information obtained from a reliable and independent source or from another obligated entity pursuant to anti-money laundering legislation;
- the acquisition, at the customer's signature, of personal data and information useful for customer due diligence purposes, including with reference to any authorised signatories and beneficial owners, kept in the register of companies together with the corresponding documents, in accordance with the confidentiality provisions and measures laid down by internal regulations;
- the acquisition and assessment of information on the purpose and nature of the ongoing relationship and any occasional transactions and relations between the customer and the

authorised signatory, between the customer and the beneficial owner, between the customer and the insured party (if different from the policyholder) and between the customer and the designated beneficiary or beneficiaries;
- the acquisition of the overall assessment of the investment transaction with regard to its reasonableness, the customer's behaviour and whether there are suspicious factors, on the part of the financial advisor responsible for the transaction, where applicable;
- the constant monitoring of ongoing relationships, in order to update information about the customer and the declared purpose of the relationship, and to assess any "unexpected" transactions that are anomalous or inconsistent with the economic and financial profile of the previously known customer or significant events;
- the periodic updating of the data and information collected, at intervals depending on the risk profile previously associated with customers, asking them to provide, under their own responsibility, all necessary and up-to-date information to enable the fulfilment of due diligence obligations.

Due diligence activities must be carried out at least at the times and under the circumstances indicated below:

- when an ongoing relationship is established or the beneficiary of an insurance policy is designated;
- when an occasional transaction is carried out on the instruction of the customer, which involves the transmission or movement of payment instruments of an amount equal to or greater than €10,000, regardless of whether it is carried out in a single transaction or in several transactions that appear linked to carry out a split transaction or which consists of a transfer of funds, as defined in Article 3(1)(9) of Regulation (EU) No 2023/1113, whose value is at least €1,000;
- when an occasional transaction is executed in cash with a value of at least €3,000, regardless of whether the transaction is executed with a single transaction or through related transactions;
- when there is suspicion of money laundering, regardless of any applicable exception, exemption or threshold, making use of any indications from FIUs;
- when doubts arise as to the completeness, reliability or truthfulness of the information or documentation previously obtained from customers.

With specific reference to transactions in asset management products, due diligence activities must also be carried out according to a risk-based approach:

- in the case of additional payment transactions, divestments or settlements in favour of beneficiaries and/or heirs;
- contractual changes (e.g. assignment of policy provisions, inclusion of joint holders of investment fund units).

The Group Companies comply with the provisions on due diligence in respect of new customers and customers already acquired, when appropriate due to the increase in the level of money laundering risk associated with the customer.

Due diligence is not required for activities intended for the purpose of or related to the organisation, functioning and administration of the Company, given that they are not part of the institutional activities of the same and that, in carrying out their activities, the Company's counterparties qualify as suppliers of goods and services at the initiative of the same, rather than as customers requesting the establishment of a business relationship or the execution of an occasional transaction.

Relationships and transactions undertaken on the initiative of the manager in the provision of portfolio management services are also excluded.

6.2.1 REMOTE CUSTOMER ONBOARDING

In the case of remote operations (carried out without the physical presence of the customer and the appointed staff), the company that arranges such operations pays particular attention in the light of the absence of any direct contact with the customer or the authorised signatory, also considering the increasing risk of fraud related to identity theft, and also using public databases.

The Anti-Money Laundering Function and the corporate organisational structures involved in the remote customer onboarding process carry out appropriate controls, each within its remit, to ensure that the remote onboarding solution adopted is in line with expectations and to adequately manage the money laundering risks that may arise from this solution.

When considering the possibility of adopting a new solution for the remote customer onboarding, the Company, in any case, carries out a preliminary assessment of the implementation of this solution, involving the corporate structures concerned for the necessary investigations. In particular, attention is paid to the impact of using the Customer remote onboarding solution on the risk exposure of the Company concerned in relation to its area of activity, including the impact on money laundering, operational, reputational and legal risks, identifying possible mitigation measures and corrective actions for each risk. Appropriate documentary evidence is kept of such assessments and specific prior notice is given to the Parent Company.

In case of remote onboarding, the identification data of the customer and the authorised signatory are acquired and compared with a copy – obtained by fax, post, certified email, in electronic format or by similar methods – of a valid identification document, pursuant to current legislation. In any case, the online establishment of relationships with regard to prospects that do not have a digital identity or a certificate for the generation of their digital signature is not permitted.

With a view to limiting exposure to possible risks of money laundering and/or fraud, the online opening of banking relationships is currently only permitted for natural persons (consumers) resident in the same country where the registered office or a permanent establishment of the Company is present. However, the establishment of remote relationships by persons with FATCA (US Persons) indications, falling within the category of politically exposed persons and characterised by “negative reputational indicators” on the basis of the “lists of names” and databases used by the Company, is not permitted.

In such cases, a relationship may only be established through the staff, who directly handle the due diligence process.

The Group Companies also provide specific first-level controls on the transactions carried out by customers acquired through remote onboarding procedures not assigned to a financial advisor of the Sales Network, also through the use of appropriate transaction monitoring systems.

The Anti-Money Laundering Function is duly involved in any case in all projects to develop the remote customer onboarding channel.

6.2.2 DUE DILIGENCE PERFORMED BY OTHER OBLIGATED ENTITIES

Under no circumstances may due diligence obligations be entrusted to shell banks or intermediaries established in high-risk third countries. It is also not permitted to establish new relationships using the identification process conducted by third parties outside the Mediolanum Group, or to establish new relationships or carry out transactions with customers whose identification documents or risk profile have expired, after the deadlines given to these customers to update them.

The Company may entrust to another Group Company, under a specific distribution and outsourcing agreement, the fulfilment of customer due diligence obligations, except for the ongoing monitoring of operations and without prejudice to the full responsibility of each Company.

In the event of transactions for the divestment/settlement of relationships/settlement of claims arranged by beneficiaries, legitimate heirs, or at the initiative of customers, the Group Companies

may fulfil their customer due diligence obligations, without prejudice to their full responsibility for compliance with these obligations, also through EU banking and financial intermediaries (banks, Poste Italiane S.p.A., electronic money institutions, payment institutions, securities brokerage companies, asset management companies, SICAVs, SICAFs, Italian intermediaries listed in the register provided for in Article 106 of the Consolidated Banking Act, Cassa Depositi e Prestiti S.p.A., insurance companies operating in the life business, micro-credit providers, mutual guarantee funds, branches of banking and financial intermediaries listed above, with registered office and central administration in another Member State or in a third State, as well as banking and financial intermediaries listed above and established without a branch in Italy or the country in which the Group company operates or with registered office in a third country with an effective anti-money laundering and counter-terrorist financing system in place).

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

- the person's identification data are obtained from an identity document sent by the person concerned by Certified Electronic Mail (PEC);
- the person's identification data result from public documents, authenticated private entries or qualified certificates used for the generation of a digital signature associated with computer documents;
- the person has a digital identity with a maximum level of security or a certificate for the generation of digital signatures, issued under an electronic identification scheme included in the list published by the European Commission pursuant to Article 9 of Regulation (EU) No 910/2014;
- the identification data come from a declaration by the diplomatic representation and the consular authority of Italy or the country in which the subsidiary conducts its business.

6.3 SAFEGUARDS RELATING TO RESTRICTIVE MEASURES

The Group provides comprehensive, systematic and continuous monitoring of restrictive measures, in compliance with the applicable European and national regulatory framework and according to a risk-based approach. This safeguard is integrated into the system of internal controls and the relevant corporate processes, in order to prevent, identify and mitigate the risk of non-implementation or circumvention of sanctions, as well as to ensure timely adaptation to any updates of sanction regimes.

In particular, the Group Companies adopt organisational, procedural and technological safeguards capable of ensuring an effective process of identifying the designated persons, continuous monitoring of relationships and transactions and timely management of any matches with the lists of sanctioned persons. In this context, the roles and responsibilities of the structures involved are formalised, ensuring adequate information flows, mechanisms for escalation and traceability of decisions taken.

Controls are provided for to prevent the establishment or continuation of relationships and the execution of transactions with persons subject to restrictive measures that include, inter alia: (i) the identification and verification of customers with simultaneous screening of the applicable sanctions lists; (ii) automatic and continuous control of counterparties and transactions through screening systems; (iii) the management and analysis of alerts generated by the systems, with any operational block and escalation; and (iv) the timely updating of lists and control parameters in the IT systems.

These safeguards are constantly updated in order to mitigate the risk of non-implementation or avoidance of restrictive measures, in accordance with the applicable European and national legislation.

6.4 CUSTOMER PROFILING

In order to apply varying levels and scope of due diligence obligations, the Group Companies adopt appropriate procedures to profile each customer according to money laundering risk, which take into account risk factors:

- relating to the customer, the authorised signatory and the beneficial owner;
- relating to products, services, transactions or distribution channels;
- that are geographical.

This approach constitutes an application of the broader principle of proportionality referred to in the current legislative provisions, the aim of which is to maximise the effectiveness of corporate safeguards and rationalise the use of resources.

In this regard, information on the money laundering risk profile is made available to the financial advisors of the Sales Network, where present, and to the corporate organisational structures responsible for the management and administration, in practice, of relations with customers. In accordance with applicable legislation, the staff who have access to information on the customer's risk profile must maintain the utmost confidentiality, refraining from disclosing this information to customers themselves or to third parties.

The following table shows the possible risk profiles attributable to customers and the frequency with which the information is updated.

Class	Risk profile	Frequency of updates to information
1	High	Within 12 months
2	Medium	Within 30 months
3	Low	Within 48 months
4	Immaterial	Within 60 months

The scores and rules attributed to the risk profiling system are monitored and updated periodically, also referring to the evolution of the regulatory environment and leading practices in the market. It remains necessary to share these measures with the Parent Company in advance, with a view to ensuring a homogeneous approach to customer risk profiling within the Group.

As part of a Group, each Company uses for a single customer the highest profile among those assigned by all the Companies of the same Group.

The profiling system ensures that the scores assigned by the computerised system are consistent with the information acquired on the customer.

In identifying the risks relating to the customer, the authorised signatory and the beneficial owner, the Company takes into account additional risk factors related to:

- the activity or profession carried out by 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,

valuing the information available, assessing negative news from the media or other sources considered well-founded and reliable, examining reports of anomalous conduct originating from the Sales Network or from employees of the corporate organisational structures who manage and administer customer relations in practice.

On the basis of all the information obtained, if the financial advisor or employee considers the

customer's conduct to be anomalous or the transaction to be unreasonable in the light of the customer profile, they promptly send a suspicious transaction report to the Anti-Money Laundering Function so that it can carry out the necessary investigations and submit the case to the Suspicious Transaction Reporting Officer for the relevant assessments, including a possible increase in the customer's risk profile, keeping evidence of the assessments made.

All data and information acquired from customers must be taken into account when assessing anomalous customer behaviour or any lack of reasonableness of the transactions carried out by them.

With regard to risk class 4, corresponding to the "High" risk profile, the Group Companies consider the following, regardless of the scores assigned by the customer profiling system in use, to be at high risk:

a) customers, beneficial owners, beneficiaries designated by name and authorised signatories whose reputational indicators are negative, on the basis of:
    - the recurrence of names on the lists of persons or associated entities for the purposes of applying the freezing obligations pursuant to Legislative Decree No. 109 of 22 June 2007 and directly applicable EU regulations;
    - the recurrence of names on the United Nations (UN) financial sanctions lists or entities controlled by them, for which, during the period between the publication of the UN lists and formal transposition into the European Union, the Group Companies must ensure the preservation of records relating to: funds or other assets managed on behalf of the customer at the time of the publication of the sanctions, transactions attempted by the customer and transactions carried out on behalf of the customer;
    - the recurrence of names on the lists issued by OFAC (Office of Foreign Assets Control) and OFSI (Office of Financial Sanctions Implementation);
    - negative news from the media or other information sources;
    - negative information provided directly by the customer or by the relevant financial advisor or distributor, concerning criminal proceedings, proceedings for loss of revenues to the state and proceedings for administrative liability of entities, etc.;
    - requests/orders from judicial authorities pursuant to the Anti-Mafia Code (investigations required by the criminal authorities – Anti-Mafia – preliminary investigation stage) or anti-money laundering legislation (investigations required by the criminal authorities pursuant to the Anti-Money Laundering Decree – Anti-Money Laundering – preliminary investigation stage);
    - sequestration orders, or real protective and prevention measures adopted by the judicial authorities;

b) customers, beneficial owners and executors that have been reported to the FIU by the Bank or another Group Company in the last five years, or that continue to present critical elements;

c) customers whose funds originate from voluntary disclosure operations or similar procedures for the repatriation of capital linked to tax evasion or other offences, the settlement of which took place in the previous five years;

d) cross-border correspondent relationships (or payable-through accounts or transit accounts) involving the execution of payments with a corresponding credit or financial institution in a third country;

e) ongoing business relationships, professional services and occasional transactions with customers and the relevant beneficial owners who are politically exposed persons, unless these politically exposed persons are acting as public administration bodies;

f) Business relationships, professional services and transactions involving high-risk third countries, as well as customers and beneficial owners resident or with registered offices in high-

risk third countries and high-risk geographical areas[4]-[5]; the Anti-Money Laundering Function of the Parent Company may, in any case, propose to the Chief Executive Officer the suspension of the opening of relationships and the carrying out of transactions with countries characterised by one or more of the geographical risk factors described above. The updated list of countries considered to be at higher risk and those with which operations have been suspended is periodically made available to the Board of Directors, as part of the report produced periodically by the Anti-Money Laundering Function of the Parent Company and sent to the Anti-Money Laundering Officers of the Subsidiaries, so that it is also correctly applied at the local level.

g) structures classed as asset protection vehicles, including trusts, fiduciary companies, foundations, NGOs, companies whose share capital is held, wholly or in part, by a fiduciary company, trust or similar legal entity or scheme and investees of fiduciary companies;

h) customers with an anomalous or excessively complex company structure, given the nature of the activity carried out, and foreign entities other than natural persons;

i) customers with types of economic activity characterised by high cash use or related to sectors particularly exposed to corruption risks;

j) customers that benefit from highly personalised advisory services offered to customers with assets of more than €2 million, customers that have entered into GPM/GPF asset management contracts, with a value in excess of €5 million;

k) customers benefiting from investment banking services;

l) customers benefiting from residence permits issued on an "investor" basis, within the scope of so-called investor residence programmes.

The Group Companies also consider the following to be at HIGH money laundering risk:

m) the customers, beneficial owners and authorised signatories identified at the disposal of the STR Officer following a prudent assessment of the same;

n) parties other than natural persons that present a high-risk beneficial owner pursuant to points a), b), c), e) and f);

---

[4] In order to assess geographical risks, the following risk factors are considered:

1) third countries that authoritative and independent sources believe lack effective money laundering prevention measures (such as countries on the EU/FATF lists);

2) countries and geographical areas that finance or support terrorist activities or where terrorist organisations operate (such as countries on the EU/FATF 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 falling short of compliance with international standards on transparency and the exchange of information for tax purposes;

5) countries and geographical areas assessed as being highly corrupt or permeable to other criminal activities by authoritative and independent sources.

6) countries considered at risk of circumvention of restrictive measures.

The geographical risks listed above are taken into account according to the different level of criticality attributed to them. Pursuant to this risk-based approach:

- the countries included in points 1) and 2) are considered "high-risk third countries";
- the countries included in point 3), which are not already included in points 1) and 2), are considered "high-risk geographical areas";
- the geographical risk factors referred to in points 4) and 5) do not automatically entail the assignment of a high-risk profile to the countries concerned, but are assessed for the purposes of a possible increase in the risk profile together with the other relevant factors, using the "Basel Index AML" calculated by the "Basel Institute on Governance", a non-profit centre of expertise specialised in combating corruption and other financial crimes.

[5] For the purpose of increasing the risk profile, both the Customer's residence and the latter's nationality are considered in the case of high-risk third countries.

o) customers, beneficial owners and authorised signatories that are the subject of a request for clarification from the FIU.

In the cases described above, the parties referred to in letters a), b), e), f) and m) are considered to have a higher money laundering risk ("subjects of interest").

Enhanced due diligence measures are applied to customers classified as HIGH risk.

However, the Anti-Money Laundering Function may nevertheless ask the financial advisors or the employees to that manage and administer customer relationships in practice carry out the enhanced due diligence process in all cases, including those not listed above, in which the risk of money laundering appears particularly high.

The AML Officer may also decrease the scores assigned following his or her own assessment of specific positions, while keeping evidence of the analyses performed. In any event, no other staff member may autonomously change the scores assigned.

In order to ensure the correct assessment of risks relating to products, services, transactions or distribution channels, the competent corporate functions of the Group Companies ensure the involvement of the Anti-Money Laundering Function right from the preliminary analysis and feasibility study phases. The risk must be carefully assessed, particularly in the case of new generation products and business practices that include distribution mechanisms or innovative technologies for new or existing products.

6.5 ENHANCED CUSTOMER DUE DILIGENCE

Where there is a high risk of money laundering, the Group Companies adopt enhanced customer due diligence measures, using a risk-based approach, obtaining additional information on the customer, the beneficial owner and any authorised signatory, exploring the elements underpinning the assessments of the purpose and nature of the relationship, and intensifying the frequency of application of procedures to ensure constant monitoring throughout the ongoing relationship.

According to the model adopted by the Group Companies, enhanced customer due diligence activities are primarily the responsibility of financial advisors, where present, or designated employees, who are required to apply the following measures:

- obtaining more information about the customer, the beneficiary and any beneficial owners;
- acquiring/updating and evaluating information on the reputation of the customer, the beneficiary and any beneficial owners (including any prejudicial information, including by drawing on publicly accessible information through consultation of open sources, through, for example, the use of online search engines);
- carefully assessing the information provided by the customer on the purpose and nature of the relationship, linking it to the other information known at the time of opening or, in the case of customers that already have relationships with the Company, to the transactions effectively recorded; in this regard, factors such as the number, size and frequency of transactions carried out, the origin/destination of funds, the nature of the activity carried out by the customer and/or the beneficial owner, and the overall reasonableness of transactions performed in relation to the customer profile, are taken into consideration;
- carefully assessing the relationships between the customer and any other parties involved in the relationship, such as: the beneficial owner, the authorised signatory, the joint holders of relationships, the guarantors (surety providers or other parties providing guarantees in the context of a credit line) and the beneficiaries;
- carrying out in-depth checks on the origin of funds employed in the business relationship, through a complex process that takes into account, first of all, the reliability of the information available, considering any availability of economic and financial information produced directly by the customer or identifiable from changes in the relationship (e.g. emolument credits, dividend credits, etc.) or available through open sources or public

databases (e.g. financial statements, VAT and income statements, notarial documents, succession declarations and declarations/documents from the employer or from other intermediaries); in this regard, aspects such as the degree of knowledge of the customer and/or the length of the relationship, and the degree of consistency between the customer's profile and his or her economic and financial situation, are particularly significant;
- more frequently verifying and updating personal data and information collected for customer due diligence purposes;
- carrying out more frequent checks on the ongoing relationship and transactions.

The Group Companies also require the authorisation of a Senior Executive:

- before starting, continuing or maintaining a business relationship or carrying out an occasional transaction with politically exposed persons;
- before commencing, continuing or entering into a business relationship or executing a transaction involving third Countries at high risk;
- before carrying out an investment transaction in asset management products placed by the same, of a significant amount, and in any case exceeding €5,000,000, or €1,000,000 in the case of "subjects of interest".

The enhanced due diligence measures also provide for an assessment of HIGH and MEDIUM[6] risk customers by the financial advisors of the Sales Network or by employees who are, in practice, responsible for the administration and management of customer relations, by drawing up a specific report or by compiling a specific assessment sheet for customers that have banking relationships. This assessment is carried out at the time of a new survey or as a result of the worsening of the level of risk and is updated according to the frequencies provided for updating due diligence information.

If such assessments reveal material critical and/or suspicious factors, the enhanced due diligence is brought to the attention of the Anti-Money Laundering Function to assess the presence of suspicious factors.

Without prejudice to "transactions for unusually large amounts or in relation to which there are doubts as to the purpose for which they are actually intended", which must always be brought to the attention of the Anti-Money Laundering Function by the financial advisor or by the employee who manages and administers customer relations in practice or by the employees of the corporate organisational structures in the context of the activities carried out, the Bank considers the following transactions to be at higher risk, regardless of the risk profile assigned by the customer profiling system:

a) Frequent and unjustified cash transactions, characterised by the use of large-denomination euro banknotes or the presence of damaged or counterfeit banknotes;

b) Transactions involving payment in cash or securities originating abroad for a total amount of the equivalent of €10,000 or more;

c) Cheque payment transactions of an amount exceeding €250,000;

d) Transactions involving high-risk third countries;

e) Transactions relating to oil, arms, precious metals, tobacco products, cultural artefacts and other movable property of archaeological, historical, cultural or religious importance or of rare scientific value, as well as ivory and protected species;

f) Transfer of sums originating from cryptoassets or virtual assets.

Without prejudice to the general principle that the enhanced due diligence measures listed above must always be applied when there is suspicion of money laundering, regardless of any applicable exception, exemption or threshold, the application of these to **transactions on asset management products** (life insurance policies, mutual fund units, GPM/GPF) is by event – or by individual

[6] Total assets in Group products of €250,000 or more

transactions ordered by customers – and commensurate, in the absence of suspicious factors, with the customer's risk and/or the amount of the transaction, according to a risk-based approach.

With the exception of customers within the category of politically exposed persons or resident in high-risk third countries, for which no limits of amount are established, provision is made for enhanced due diligence of the investment transaction, in order to obtain more information on the origin of the funds used for the transaction, according to a risk-based approach, applying the following thresholds:

- in the case of "subjects of interest": €50,000, regardless of the total amount of assets declared by the customer in the customer data and due diligence form;
- in the case of other customers classified as high risk, thresholds for the amount apply that are calibrated in relation to the total assets declared by the customer on the customer data and due diligence form as follows:
  - €50,000 in the case of total assets up to €500,000;
  - €100,000 in the case of total assets between €500,000 and €2,000,000;
  - €250,000 in the case of total assets exceeding €2,000,000.

Regardless of the risk profile, enhanced due diligence measures are applied to the transaction in all cases of:

- Investment transactions in insurance policies with a financial component amounting to €250,000 or more, and investments in mutual funds and GPM/GPF amounting to €500,000 or more;
- Investment transactions on behalf of third parties;
- Transactions for the subscription of an insurance policy where the relationship between the policyholder and the designated beneficiary is of the type "other";
- change of policyholder of an insurance policy;
- change of beneficiary of an insurance policy, if designated by name, between the policyholder and the beneficiary classed as a "business or professional relationship" or "other";
- co-subscription or change of holders of units in UCIs, where the relationship between the main subscriber and co-subscribers is of the type: "business or professional relationships" or "other";
- activation of payment plans on policies by a party other than the policyholder (the so-called third-party payer) with a relationship between the policyholder and the third-party payer classed as "other".

6.6 SIMPLIFIED CUSTOMER DUE DILIGENCE

In the event of an immaterial risk of money laundering, the Group Companies may apply simplified customer due diligence measures in terms of the extent and frequency of requirements, in respect of:

- companies admitted to trading on a regulated market and subject to disclosure obligations that impose an obligation to ensure adequate transparency of beneficial ownership;
- public administrations, or institutions or bodies carrying out public functions, in accordance with European Union law;
- EU banking and financial intermediaries (banks, Poste Italiane S.p.A., electronic money institutions, payment institutions, securities brokerage companies, asset management companies, SICAVs, SICAFs, Italian intermediaries listed in the register provided for in Article 106 of the Consolidated Banking Act, Cassa Depositi e Prestiti S.p.A., insurance

companies operating in the life business, micro-credit providers, mutual guarantee funds, branches of banking and financial intermediaries listed above, with registered office and central administration in another Member State or in a third State, as well as banking and financial intermediaries listed above and established without a branch in Italy or the country in which the Group Company operates or with registered office in a third country with an effective anti-money laundering and counter-terrorist financing system in place);

- supplementary pension schemes governed by the relevant national decrees, provided they do not contain surrender clauses other than those for: permanent disability, termination of employment resulting in unemployment, or recourse by the employer to redundancy procedures, ordinary or extraordinary earnings guarantee fund and provided they cannot serve as collateral for a loan outside the cases provided for by law;
- pension schemes or similar schemes which pay employees benefits, where contributions are paid by deducting remuneration and which do not allow beneficiaries to transfer their rights.

In order to correctly fulfil the above obligations, “active counterparties” are differentiated from “passive counterparties”.

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

Examples of active counterparties include:

- institutions/companies with correspondent and/or settlement accounts;
- mutual fund management companies;
- institutions/companies issuing securities on the market through public offers in which the Bank participates directly;
- institutions/companies with which business relationships exist for the placement of electronic money or financing/investment products.

Due Diligence obligations do not apply in case of “passive” counterparties, i.e. financial intermediaries (domestic and non-domestic) with which there is no ongoing business relationship, but which are used, on one’s own initiative, to carry out transactions on behalf of Customers, holders of relationships (e.g. securities dossier transfers, securities trading, etc.). In this sense, passive counterparties are “service providers” at the initiative of the Bank and other Group Companies and not customers that require the establishment of a business relationship or the execution of an occasional transaction. By way of example, Passive Counterparties include custodian banks and companies registered as issuers of securities.

Without prejudice to the need to ensure the correct identification of the Customer and Beneficial Owner before the establishment of an ongoing business relationship or the execution of a transaction, simplified due diligence measures consist of the possibility of:

- verifying the Beneficial owner sub 2), obtaining a declaration signed by the Customer confirming his data, under the latter’s own responsibility;
- using assumptions in identifying the purpose and nature of the business relationship, where the product offered is intended for a specific use;
- adopting a frequency of less than 60 months for the purposes of updating the data collected for due diligence, without prejudice to the need to do so in the event of the establishment of a new ongoing business relationship or an increase in the money laundering risk profile, due, for example, to the detection of negative reputational indicators on the Customer and/or the beneficial owner.

The Group Companies verify that said requirements for the simplified procedure continue to apply, with the methods and frequency established according to the risk-based approach.

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

- the conditions for the application of simplified measures are no longer met, on the basis of the risk indicators provided for in the relevant legislation;
- the monitoring of all of the customers' transactions and the information obtained during the course of the relationship result in the exclusion of an immaterial risk situation;
- there is, in any case, a suspicion of money laundering or terrorist financing.

6.7 ABSTENTION OBLIGATIONS

The Group Companies do not rule out in advance and in a generalised way the possibility of establishing or maintaining business relationships with specific categories of customers or potential customers who are residents, or who have a regular residence permit, by reason of their potentially high exposure to the risk of money laundering, but adopt rigorous processes to assess the risk associated with such customers or potential customers on a case-by-case basis, while keeping evidence of the decisions taken.

When the Company is objectively unable to carry out customer due diligence, it refrains from establishing, executing or continuing the relationship or the transaction (so-called abstention obligation), thus terminating the existing business relationship, where appropriate, and assessing whether to make a suspicious transaction report to the FIU. Before reporting the suspicious transaction to the FIU and in order to possibly exercise its right to suspend the same, the Company refrains from carrying out transactions for which it suspects there is a connection with money laundering or terrorist financing.

Where abstention is impossible because there is a legal obligation to receive the deed, or the execution of the transaction by its nature cannot be postponed, or abstention may hinder investigations, there still applies the obligation to immediately report the suspicious transaction.

The Group Companies in any case refrain from establishing relationships or executing transactions and terminate existing business relationship with:

- Customers resident or with their registered office in countries and geographical areas assessed as particularly high risk, as identified from time to time by the Chief Executive Officer of the Parent Company, Banca Mediolanum, on the proposal of the Anti-Money Laundering Function;
- credit or financial institutions located in a non-EU state which does not impose obligations equivalent to those laid down in the relevant Community Directives;
- shell banks, wherever these are located;
- companies that provide services to shell banks;
- unlicensed banks;
- financial institutions registered in section 311 of the USA Patriot Act;
- parties of which the following are part, directly or indirectly: fiduciary companies, trusts, limited companies (or companies controlled through bearer shares) located in high-risk Third Countries;
- companies that have issued bearer shares or in which nominee shareholders hold shares;
- trusts for which adequate, accurate and up-to-date information is not available regarding the beneficial ownership of the trust and the nature and purpose of the trust, or that present subjective or objective circumstances that might indicate a use of the institution of the trust to disguise anomalous conduct, also in the light of the recommendations of the competent authorities;
- fiduciary relationships for which adequate, accurate and up-to-date information on beneficial ownership is not available;

- payment service providers (money transfer agents and/or companies) not exclusively engaged in financial activities;
- companies engaged in the manufacture of arms and ammunition;
- legal entities directly or indirectly owned by any of the above entities.

The Group Companies refrain from offering products/services or from carrying out transactions that could favour anonymity or concealment of the identity of the customer or beneficial owner, and from establishing ongoing business relationships or carrying out occasional transactions remotely that are not supported by adequate identification mechanisms and procedures.

Finally, the provision of cryptoasset services and the management of crowdfunding platforms is not envisaged.

6.8 COUNTER-TERRORIST FINANCING CONTROLS

In order to ensure the proper fulfilment of the obligations and prohibitions established by current anti-terrorism legislation, the Group Companies:

- verify whether the customer, the beneficiary and the relative beneficial owners are on the "lists" of persons and entities adopted by the UN Security Council, the European Commission, the decrees of the Ministry of Economy and Finance, as well as the list of the Office of Foreign Asset Control (OFAC) of the Department of the Treasury of the United States;
- refrain from carrying out transactions involving persons on the lists referred to in the above paragraph for any reason, except where not carrying them out is impossible or risks frustrating efforts to pursue the beneficiaries of a terrorist financing operation;
- apply without delay the obligations laid down in EU Regulations and national decrees;
- keep records of transactions attempted or carried out on behalf of persons included on the sanctioned UN lists;
- do not make cover payments7 in US currency;
- notify the FIU of the measures applied, indicating the parties involved, the amount and nature of the funds or economic resources, within 30 days from the date of entry into force of the EU regulations, the decisions of the international bodies and of the European Union and in compliance with the local rules of the country in which the Group Company operates, or, if later, from the date of its holding of the funds and economic resources.

In identifying the risks associated with the nature and behaviour of the customer, the beneficiary and the relevant beneficial owners or authorised signatories, the staff pay particular attention, in any case, to the risk factors that, although not specific to terrorist financing, may indicate a risk of terrorist financing.

6.9 REPORTING OF SUSPICIOUS TRANSACTIONS TO THE FIU

Pursuant to the applicable regulations, the Group Companies, before carrying out the transaction, send a suspicious transaction report to the FIU without delay when they know, suspect or have reasonable grounds to suspect that money laundering or terrorist financing transactions have been carried out or attempted, or that the funds, regardless of their size, originate from criminal activities.

The financial advisors of the Sales Network, if present, and the employees of the corporate organisational structures responsible for the administration and management of customer relations

[7] Cover payment refers to the transfer of funds used if there is no direct relationship between the payment service provider (PSP) of the payer and the payee, and it is therefore necessary to use a chain of correspondent relationships between PSPs. Three or more PSPs are involved in a cover payment.

in practice are, also pursuant to the applicable regulations, the first reporting level. It is therefore their duty to continuously monitor the progress of relationships and operations, also using the tools and procedures provided to them, and to forward a suspicious transaction report without delay to the Anti-Money Laundering Function, according to the procedures and operational methods established internally: this does not apply whenever the transaction must be carried out because there is a legal obligation to receive the deed, or the transaction cannot be postponed in the light of normal operations, or where postponing the transaction may hinder investigations.

The start of the reporting process may also result from external reports, i.e.: from requests/orders received from any supervisory or public safety authority; from requests for further information from the FIU; or from the receipt of requests or information from other intermediaries.

Requests for more information from the FIU or the competent Supervisory Authorities also activate internal investigations conducted by the Anti-Money Laundering Function, which may result in suspicious transaction reports.

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

Within the scope of their organisational autonomy, the Group Companies also make use of transaction monitoring systems. The Anti-Money Laundering Function assesses the transactions highlighted by such systems and, in case of suspicious elements, submits them to the Suspicious Transaction Reporting Officer; if the latter believes such reports to be justified in the light of all the information at his disposal and the evidence available from the data and information stored, the Officer sends them to the FIU, omitting the reporting person's name.

The Group Companies adopt appropriate measures to ensure the confidentiality of the identity of persons reporting a suspicious transaction; the name of the reporting person may only be disclosed when the Judicial Authority, providing in this regard with a reasoned decree, considers it essential for the purposes of ascertaining the offences for which proceedings are being carried out.

Anyone required to report a suspicious transaction and anyone who is aware of it must not notify the customer concerned or third parties of the report, or of the provision of further information requested by the FIU, or of the existence or likelihood of investigations into money laundering or terrorist financing. This prohibition does not apply to:

- communications made to sectoral Supervisory Authorities in the performance of the roles provided for by the reference regulations;
- communications concerning the sharing of information at the level of banking and financial intermediaries, so as to ensure proper compliance with regulations on the prevention of money laundering and terrorist financing;
- communications with other banking and financial intermediaries outside the Group in a Member State or in third countries, provided these apply measures equivalent to those provided for in EU legislation, in connection with cases relating to the same customer or the same transaction, exclusively for the purpose of preventing money laundering or terrorist financing.

The Group Companies adopt strict procedures to respond to requests for information from their FIUs as soon as possible and, in any case, within five working days from receipt of the request or any other more or less short deadline imposed by the FIUs.

6.10 OBLIGATION TO RETAIN DATA AND DOCUMENTS

In order to fulfil the obligations to store data relating to business relationships and transactions carried out, the Group Companies use special storage systems, where the business relationships of customers, links and transactions above the materiality threshold are recorded.

For the purposes of the above, the Italian Group Companies continue to use the CCA on a voluntary basis; this choice allows the Company to maintain processes and safeguards that have already been extensively consolidated, and ensures the timely availability of information acquired during due diligence, both for the fulfilment of signalling obligations and for possible investigations of individual positions.

With regard to the fulfilment of conservation obligations, the Group Companies retain:

- a copy, or the details, of the documents required for due diligence purposes, for a period of ten years from the end of the ongoing relationship;
- the records and entries of ongoing transactions and relationships, consisting of original documents or copies having a similar evidentiary effect in judicial proceedings, for a period of ten years from performance of the transaction or termination of the ongoing relationship.

6.10.1 DATA RETENTION EXEMPTIONS – ITALIAN GROUP COMPANIES

Pursuant to Article 8, paragraph 1, of the "*Provisions for the retention and making available of documents, data and information to combat money laundering and terrorist financing*" issued by the Bank of Italy on 24 March 2020 and in force since 1 January 2021, the Bank and the Group's Italian companies may not apply Articles 5 and 6 in relation to ongoing relationships or transactions with:

- banking and financial intermediaries covered by Article 3, paragraph 2, of the anti-money laundering decree, excluding those referred to in letters i), o), s) and v), based in Italy or in another Member State;
- banking and financial intermediaries based in a third country characterised by a low money laundering risk and in accordance with the criteria indicated in Annex 1 to the provisions on customer due diligence;
- persons referred to in Article 3, paragraph 8, of the anti-money laundering decree;
- the provincial treasury of the state or the Bank of Italy.

6.11 STAFF TRAINING

Staff qualifications and continuing professional development are continuous and systematic as part of organic programmes that take account of changes in legislation and procedures.

In this regard, the Group Companies adopt ongoing training and professional development programmes for staff, aimed at correctly applying the provisions of the anti-money laundering rules, recognising transactions relating to money laundering and terrorist financing, as well as the evasion of restrictive measures, and adopting the conduct and procedures to be adopted. These programmes ensure, inter alia, that staff are made aware of and have up-to-date knowledge of the operation of the customer remote onboarding solution, the associated risks and the customer remote onboarding policies and procedures aimed at mitigating such risks.

Particular attention is paid to the Sales Network advisors, where present, employees involved in the remote onboarding process and employees of the corporate organisational structures that administer and manage customer transactions in practice, as well as employees involved in the suspicious transactions reporting process. Specific training programmes are implemented for staff belonging to the Anti-Money Laundering Function.

The training and development programmes for staff carried out during the reference period and planned for the following year are detailed in the reports produced by the Anti-Money Laundering Function.

If training is provided by an external supplier, the AML Officer ensures that the parties entrusted therewith have the anti-money laundering knowledge required to ensure the quality of training and that the latter's content is adapted to the Company's specific characteristics.

6.12 INTERNAL SYSTEMS FOR REPORTING BREACHES

The Group Companies adopt specific procedures for the reporting by their employees and contract staff of potential or actual breaches of the provisions laid down to prevent money laundering and terrorist financing (whistleblowing).

These procedures ensure:

- the confidentiality of the identity of the whistleblower and the alleged perpetrator of the violations, without prejudice to the rules governing investigations and proceedings initiated by the judicial authority in relation to reported facts;
- the protection of the whistleblower against any retaliatory, discriminatory or unfair conduct resulting from whistleblowing;
- the development of a specific anonymous and independent whistleblowing channel, proportionate to the entity's nature and size.

All staff of the Internal Audit Function are made aware of these procedures.

6.13 SELF-ASSESSMENT EXERCISE

6.13.1 SELF-ASSESSMENT EXERCISE ON EXPOSURE TO MONEY-LAUNDERING RISK

The Group Anti-Money Laundering Function oversees the assessment of money laundering risks carried out by the members of the Group, preparing an assessment of the Group money laundering risks, taking into account the risks resulting from the individual exercises, the interrelations between the individual Group Companies and their impact on risk exposure at Group level.

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

The self-assessment is carried out by evaluating the exposure to money laundering risk of each business line considered relevant, due to its nature, organisation, specificity and operational complexity, taking into account risk factors related to operations, products and services, the type of customers, the distribution channels and the geographical area, as well as sectoral risk factors provided for by Title II of the European Banking Authority Guidelines on risk factors for customer due diligence (EBA/GL/2021/02) in force.

The self-assessment is conducted according to a method that includes the following macro-activities:

- identification of inherent risk;
- vulnerability analysis;
- assessment of residual risk;
- remedial actions identified in relation to any existing critical issues and for the adoption of appropriate measures to prevent and mitigate money laundering risk.

The exercise is promptly updated in case of new significant risks or changes to existing risks, operations or the organisational or corporate structure.

The results of the self-assessment and the adjustment initiatives defined in the light of the results and their state of progress are described in specific chapters of the annual report produced by the Anti-Money Laundering Function.

6.13.2 SELF-ASSESSMENT OF EXPOSURE TO RESTRICTIVE MEASURES

In accordance with the EBA Guidelines (EBA/GL/2024/14) on policies, procedures and internal controls to ensure the implementation of EU and national restrictive measures, in force since 30 December 2025, the Parent Company conducts an annual assessment of its exposure to restrictive measures and its vulnerability to circumvention, taking into account risk factors relating to customers, products and services, distribution channels and geography.

The methodology used to assess the Group's exposure to restrictive measures was developed with reference to the principles used to conduct the self-assessment of money-laundering and terrorist financing risks, which involve the following stages:

- identification of the inherent risk of exposure to restrictive measures;
- vulnerability analysis, through an assessment of corporate safeguards to prevent the risk of breaches of restrictive measures;
- determination of the residual risk of breaches of the restrictive measures to which the Group is exposed, based on the level of inherent risk and the robustness of the mitigation safeguards;
- identification of appropriate corrective measures (remedial actions) to deal with any critical issues identified.

The exercise is promptly updated in case of new significant risks or changes to existing risks, operations or the organisational or corporate structure.

The results of the self-assessment and the adjustment initiatives defined in the light of the results and their state of progress are described in specific chapters of the annual report produced by the Anti-Money Laundering Function.

In this regard, the Group Companies, where applicable due to the nature of the business and the types of products/services offered, carry out their own self-assessment of exposure to restrictive measures, on the basis of the guidelines provided by the Parent Company, sending the results to the Group Anti-Money Laundering Function, according to the timescales defined by the latter.

7. EXERCISING THE MANAGEMENT AND COORDINATION ROLE

Banca Mediolanum, as the Parent Company of the Mediolanum Group, defines these strategic guidelines on the management of money laundering risk and non-compliance with the restrictive measures, which are adopted by the Subsidiaries through the necessary resolutions of the respective corporate bodies.

The Parent Company's Anti-Money Laundering Function is responsible for guiding and coordinating aspects relating to the processes and methods to be adopted for the uniform and synergic management of money laundering risk and the risk of non-compliance with restrictive measures at Group level. The Anti-Money Laundering Function is involved ex ante by the Subsidiaries when binding opinions need to be formally issued, as expressly defined by the Guidance and Coordination Regulations of the Mediolanum Group, in the event of deviations from these Group principles. The Subsidiaries provide evidence to the Parent Company of any changes in the incorporation of the contents of this document. The Anti-Money Laundering Function of the Parent Company carries out supervision and coordination activities in relation to the corresponding

functions of the Subsidiaries, where established locally. With reference to foreign Subsidiaries, adequate periodic or "event-based" information flows from and to the Parent Company have been identified and prepared in order to address and share any information that is relevant to monitoring the risk of money laundering and of non-compliance with restrictive measures.

In particular, the Anti-Money Laundering Function of the Parent Company communicates and shares with the Anti-Money Laundering Functions of the Subsidiaries:

- the contents of the Policies pertaining to the function to be issued shortly, prior to each update thereof (on an event basis);
- the project initiatives in which the Subsidiary is involved;
- and, pursuant to the outsourcing contracts in place:
    - the annual control plan, insofar as it is of interest to the Subsidiary, and any findings of interest to the Subsidiaries (by event);
    - the resources training plan (annually).

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

- specific information flows at least once a quarter, concerning the main activities carried out, the results of the controls performed and the main actions taken to remove any irregularities, before approval by their corporate bodies, and their relevant progress;
- the minutes of Board meetings transposing the Policies within the function's remit and, more generally, all those dealing with issues relating to anti-money laundering (on an event basis);
- any changes in local legislation and business initiatives that significantly impact the risk of money laundering and non-compliance with restrictive measures (by event);
- without delay, any new inspections commenced by the local supervisory authorities and any interaction with them (on an event basis);
- the resource training plan (annually);
- any significant changes in the organisational structure of the local function and/or the appointment of new heads of the function or any relevant organisational units.

Likewise, the Bank's Anti-Money Laundering Function liaises and is continuously aligned with the Anti-Money Laundering Function of the Parent Company of the Mediolanum Insurance Group, to which it has extended the methods described in this Policy and from which it receives a quarterly reporting flow of the activities carried out, allowing for integrated reporting at Group level. In particular, the Heads of the Anti-Money Laundering Functions of the Parent Company Banca Mediolanum and of the Parent Company of the Mediolanum Vita Insurance Group are coordinated in order to ensure consistent guidance and management in relation to anti-money laundering issues.

The Group Chief AML Officer must in any case be promptly informed, by the AML Officers of the Subsidiaries, of the results of the controls carried out by the Supervisory Authorities or by any independent experts within the Companies, as well as of any significant event, including relationships and interrelations of any nature with the competent authorities.

8. REFERENCE REGULATIONS

The overall anti-money laundering and counter-terrorist financing provisions are intended to lay down measures aimed at protecting the integrity of the economic and financial system and the correct conduct of operators required to comply with them.

These measures are proportionate to the risk based on the type of customer, the ongoing relationship, the professional service, the product or the transaction, and their application takes into account the specific nature of the activity, as well as the size and complexity of the obligated entities fulfilling their respective obligations.

The main legislative and regulatory references used to draw up this document are as follows:

8.1 EXTERNAL REGULATIONS

International and EU legislation, 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 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council by identifying high-risk third countries with strategic deficiencies;
- Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain cryptoassets 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; takes effect on 10 July 2027 and will be directly applicable in each of the Member States, with the aim of comprehensively harmonising anti-money laundering rules throughout the European Union;
- EBA (European Banking Authority) Guidelines - *GL/2021/02* - of 1 March 2021, pursuant to Article 17 and Article 18(4) of Directive (EU) 2015/849 on customer due diligence measures and the factors that credit institutions and financial institutions should take into account when assessing the risks of money laundering and terrorist financing associated with individual business relationships and occasional transactions (Guidelines on ML/TF risk factors), which revoke and replace the *JC/2017/37* guidelines, 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 relating to the management of compliance and the role and responsibilities of the anti-money laundering officer pursuant to Article 8 and Chapter VI of Directive (EU) 2015/849 ("EBA Guidelines on AML Policies and Procedures"). By order of 1 August 2023 – published in the Official Journal of the Italian Republic on 16 August 2023 – the Bank of Italy amended the Provisions in order to fully implement 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 client onboarding solutions for the purposes indicated in Article 13(1) of Directive (EU) 2015/849, transposed 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, containing amendments to the EBA/2021/02 Guidelines pursuant to Articles 17 and 18(4) of Directive

(EU) 2015/849 on customer due diligence measures and on factors that credit institutions and financial institutions should take into account when assessing the risks of money laundering and terrorist financing associated with individual business relationships and occasional transactions ("ML/TF Risk Factor Guidelines") ("EBA Guidelines on Customers that are Non-profit Organisations");

- EBA (European Banking Authority) Guidelines - *GL/2023/04* – 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 De-risking Guidelines");
- EBA (European Banking Authority) Guidelines - *GL/2024/11*– of 4 July 2024, on information requirements relating to transfers of funds and certain crypto-activities pursuant to Regulation (EU) 2023/1113 ("Travel Rule Guidelines");
- EBA (European Banking Authority) Guidelines - *GL/2024/14* – of 14 November 2024 on policies, procedures and internal controls to ensure the implementation of Union and national restrictive measures;
- Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items.

Measures taken over time by the European Union regarding international financial sanctions, depending on the circumstances and needs of security and foreign policy.

National legislation:

- Legislative Decree No. 109 of 26 June 2007 on "Measures to prevent, combat and suppress terrorist financing and the activity of countries threatening international peace and security", implementing Directive 2005/60/EC, as amended by Legislative Decree No. 90/2017 implementing Directive 2015/849/EC and Legislative Decree No. 125/2019 implementing Directive 2018/843 of the European Parliament;
- Legislative Decree No. 231 of 21 November 2007 implementing Directive 2005/60/EC on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing and Directive 2006/70/EC laying down implementing measures, as amended by Legislative Decree No. 90/2017 implementing Directive 2015/849/EC and Legislative Decree No. 125/2019 implementing Directive 2018/843 of the European Parliament
- Legislative Decree No. 221 of 15 December 2017, implementation of the delegation to government referred to in Article 7 of Law No. 170 of 12 August 2016, for the adaptation of national legislation to the provisions of European legislation for the purposes of reordering and simplifying procedures for the authorisation to export dual-use products and technologies and the application of sanctions in the field of trade embargoes, as well as for each type of operation to export proliferating materials;
- Law No. 220 of 9 December 2021 on measures to combat the financing of enterprises producing anti-personnel mines, cluster munitions and sub-munitions.
- Law No. 185 of 9 July 1990 on the new rules on control of the export, import and transit of armament materials.

The national reference framework also includes the decrees of the Ministry of Economy and Finance (MEF) and the schemas of anomalous behaviour issued by the FIU.

The following orders/notes from the Bank of Italy are also reported:

- Provisions on the organisation, procedures and internal controls designed to prevent the use of intermediaries for money laundering and terrorist financing - *1 August 2023*.
- Bank of Italy customer due diligence provisions - *30 July 2019*.

- Provisions for the storage and making available 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 sending aggregate anti-money laundering reports - *25 August 2020*;
- FIU Order on anomaly indicators - 12 May 2023;
- Bank of Italy Order of 27 May 2009 laying down operational guidelines for the exercise of enhanced controls against the financing of programmes for the proliferation of weapons of mass destruction;
- FIU Communication of 24 March 2022 on Russian and Belarusian deposits in accordance with Regulation (EU) 328/2022 and Regulation (EU) 398/2022.
- Instructions for the detection and reporting of suspicious transactions - Financial Information Unit for Italy - of 18 December 2025;
- Note No. 15 of 4 October 2021, with which the Bank of Italy fully implements the Guidelines of the European Banking Authority on risk factors for customer due diligence (EBA/GL/2021/02), updating accordingly the Bank of Italy customer due diligence Provisions 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;
- Instructions for obligated entities on the application of anti-money laundering obligations in the provision of private banking services and activities.

Lastly, IVASS Order 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 includes, in particular, the:

- Code of Ethics;
- Group Code of Conduct;
- Guidelines and basic principles for Group coordination between control bodies and functions;
- Policy for the Appointment, Removal and Replacement of Heads of the Corporate Control Functions.