Policy for the prevention of money-laundering and terrorist financing

Contents

1. Introduction and general aspects

The Parent Company of the Anima Holding Group (hereinafter the "Group") is Anima Holding S.p.A. (hereinafter the "Parent Company"), a company listed on the Mercato Telematico Azionario organized and operated by Borsa Italiana S.p.A. and which is responsible for the strategic guidance and coordination of the Group.

The Group is present in Italy and abroad through companies controlled directly or indirectly by the Parent Company.

Due to the business conducted by the Group, the individual subsidiaries must adopt adequate safeguards to prevent the risk of money laundering and terrorist financing, in compliance with the applicable Italian and European legislation.

Following the publication by the Bank of Italy of new "Provisions on organizational arrangements, procedures and internal controls to prevent the use of intermediaries for the purposes of money laundering and terrorist financing" (hereinafter the "Provisions") the Parent Company became subject to certain specific anti-money-laundering and anti-terrorist-financing obligations.

The Bank of Italy has affirmed the principle that the Provisions apply to all Italian groups (i.e. those with an Italian parent company), including those whose parent company performs a mere holding company function. The Parent Company must therefore adopt the strategic guidelines concerning money laundering risk management and anti-money-laundering controls.[1] Specifically, under the new regulations, the Parent Company is required to:

- ensure that the corporate bodies of the other Group companies implement Group strategies and policies in their own company;
- develop a global approach to money laundering risk by defining and approving:
  a) a Group approach to assessing money laundering risks in compliance with the regulations;
  b) formalized procedures for coordinating and sharing relevant information among the Group companies;
  c) general standards on customer due diligence, data retention and the identification and reporting of suspicious transactions;
- establish a common information base that enables all Group companies to evaluate customers in a uniform manner;
- develop appropriate organizational solutions to ensure compliance with the applicable provisions in the Group's various areas of operation and, at the same time, ensure that risk management takes account of all the assessment and measurement resources available to the individual Group members;
- ensure, as a group engaged in cross-border transactions, that the procedures at the branches and Group companies based outside of Italy meet Group standards and allow the sharing of information within the Group, including the notification of suspicious transactions, without

[1] See the document "*Resoconto alla Consultazione contenente le principali valutazioni e scelte compiute per l'emanazione delle Disposizioni in materia di organizzazione, procedure e controlli interni volti a prevenire l'utilizzo degli intermediari a fini di riciclaggio e di finanziamento del terrorismo*", where in response to the question of whether the provision that gives the Parent Company responsibility for strategic decisions on the management of money laundering risk also applies to parent companies that perform a mere holding company function and are not required to be entered in registers or watch lists, the Bank of Italy replied that the provisions apply to all Italian groups (i.e. those with an Italian parent company), including those whose parent company performs a mere holding company function.

prejudice to compliance with the limits imposed or the specific obligations provided for by the host country's legal system.

In order to fully comply with the new obligations introduced by the Provisions, the Parent Company has adopted this Policy, which delineates the organizational model, rules and solutions adopted at the Group level to combat money laundering and terrorist financing risks. The principles indicated in this Policy must be set out and detailed in internal rules issued by the individual companies.

2. Definitions

2.1. Money laundering

Money laundering is the process by which the proceeds of criminal activity are reintroduced into the legal economy in a manner designed to obscure or conceal their illicit origin.
Money laundering is one of the most serious criminal activities in the financial market, as it profoundly alters market mechanisms and normal competitive conditions and impacts the efficiency and stability of the financial system.

Italian anti-money-laundering regulations adopt an "all crimes" approach, i.e. all willful offenses predicate money laundering.

Money laundering is typically a three-stage process:

1. **placement/smurfing**: in this phase the proceeds of unlawful activity enter the financial system, often through a series of small transactions;
2. **layering**: the execution of a series of complex financial transactions, which may not be apparently connected to each other, in order to hinder the tracking of financial flows;
3. **integration**: the reuse of the proceeds of criminal activities in the legal economy, giving them the formal appearance of being of legal origin.

The three stages are not static and may overlap: financial institutions can be exploited for criminal purposes in any of these stages.

For the purposes of Italian legislation on preventing and combating the use of the economic and financial system for the purpose of money laundering and terrorist financing, money laundering means:

a. the conversion or transfer of assets, knowing that they originated with a criminal activity or participation in such activity, in order to obscure or conceal the illicit origin of the assets or to help anyone involved in that activity to escape the legal consequences of their actions;
b. obscuring or concealing the real nature, origin, location, use, movement or ownership of the assets or rights over them, in the knowledge that such assets originated with a criminal activity or participation in such activity;
c. the purchase, possession or use of assets while being aware at the time of their receipt that such assets originated with a criminal activity or participation in such activity;
d. participating in the conduct referred to in the preceding letters, conspiring to commit such conduct, attempting to perpetrate it, helping, instigating or advising someone to commit it or facilitating its execution.

Money laundering is considered as such even if the activities that produced the assets to be laundered took place outside Italy.

Self-laundering is the crime provided for in Article 648-ter-1 of the Criminal Code, which punishes those who, after committing a predicate offense, replace, transfer or conceal the proceeds of the crime itself (money, assets or other benefits) in order to invest or integrate them into economic, financial, entrepreneurial or speculative activities.

2.2. Terrorist financing

Terrorist financing involves the use of funds of legitimate or illegal origin for terrorist purposes.

Terrorist financing means any activity directed, by any means, at the supply, collection, fundraising, intermediation, deposit, custody or disbursement, in any manner, of funds and economic resources that are directly or indirectly, in whole or in part, usable to engage in one or more actions for the purpose of terrorism in accordance with criminal law, regardless of the actual use of the funds and economic resources to commit those actions.

3. Regulatory framework

3.1. Money laundering

3.1.1. International regulations

The international anti-money-laundering regulatory framework is composed of a range of sources represented by international standards, European regulations and international conventions.

The recommendations of the Financial Action Task Force (FATF) represent the key standards in the area of preventing and combating money laundering and terrorist financing, which countries are required to implement within their respective legal, administrative and financial systems.
In 1990, the FATF issued forty Recommendations on preventing and combating of money laundering, with the addition in 2001 of nine Special Recommendations specifically dedicated to the financial fight against international terrorism. The recommendations were completely revised in February 2012 with the issue of the new International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, divided into forty Recommendations.
The innovative elements also included the expansion of the scope of the predicate crimes of money laundering to include tax violations and the refinement of the preventive obligations of customer due diligence activities, which was intended to clarify their adaptation to the characteristics of the risk and increasing their stringency in cases of greater exposure.
The anti-terrorist-financing standards introduced in 2001 were also incorporated into the Recommendations with appropriate Special Recommendations. Specific measures were also adopted to address the financing of the proliferation of weapons of mass destruction, in accordance with the United Nations Security Council Resolution.

3.1.2. European Union regulations

The EU regulations on preventing and combating money laundering and terrorist financing have reflected the evolution of international principles over time, with the aim of creating a harmonized regulatory

environment among the Member States.
The fourth anti-money-laundering directive (Directive (EU) 2015/849) on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, which took effect ten years after the third Directive, strengthens the system of prevention of the Member States in line with the guidelines set out in the 2012 Recommendations of the FATF.
Finally, the fifth anti-money laundering directive (Directive (EU) 2018/843) sought to increase the general transparency of the economic and financial system, updating the regulations to take account of emerging trends and services based on modern technologies, which are becoming increasingly widespread as alternative financial systems. Accordingly, the goal is to adopt new measures to ensuring greater transparency for financial transactions, companies and other legal entities, as well as trusts and legal institutions with similar structures or functions.

Of particular importance for the purposes of this Policy are the joint guidelines of the European Supervisory Authorities issued pursuant to Article 17 and Article 18, paragraph 4, of Directive (EU) 2015/849 on simplified and enhanced customer due diligence measures and on the factors that credit and financial institutions should take into account when assessing the money-laundering and terrorist-financing risks associated with individual business relationships and occasional transactions.

3.1.3. Italian regulations

The anti-money-laundering legislative framework is represented by Legislative Decree 231 of 21 November 2007, as amended by Legislative Decree 90 of 25 May 2017 and, most recently, Legislative Decree 125 of 4 October 2019 transposing fourth and fifth directives and the related implementing provisions issued by the Minister for the Economy and Finance, Italy's Financial Intelligence Unit for Italy and sector supervisory authorities within the scope of their areas of responsibility.

3.2. Terrorist financing

3.2.1. International regulations

United Nations
The strategic lines of the fight against the financing of international terrorism were drawn by the UN in 1999 with the New York Convention, which laid the international foundations for the suppression of terrorist financing and the extension to the latter of the existing system of safeguards for preventing and combating money laundering.
With a 1999 Resolution, the UN Security Council introduced a procedure for freezing the funds and economic resources held by persons connected with the Al-Qaeda terrorist network as a specific measure for the fight against terrorism, on the basis of a blacklist maintained by a special committee (Sanctions Committee). From 2001 to 2012 new resolutions concerning Al-Qaeda and the Taliban were adopted and updated.

In 2014, in order to face the new threat of ISIL, the UN Security Council extended the sanctions imposed against Al-Qaeda to the affiliates of ISIL and the al-Nusra Front, requiring member states to adopt specific measures to counter the new phenomenon of "foreign terrorist fighters", including the criminalization of related material and financial support activities.
Measures were also introduced to block financial flows associated with kidnappings for the purpose of ransom, with trade in stolen oil and with trade in stolen archaeological treasures and to systematize and strengthen the existing system of penalties.

Between 2016 and 2017, the Security Council adopted measures specifically aimed at reinforcing international cooperation in the fight against terrorism, giving a central role to information exchange and collaboration between countries and between the authorities involved in various capacities.

GAFI recommendations
During a plenary meeting held shortly after the New York attacks of 11 September 2001 (29 and 30 October 2001), the FATF issued eight Special Recommendations (nine since 2004) devoted specifically to the financing of terrorism. They defined standards to provide a stronger regulatory foundation for certain sectors deemed most exposed to the risk of terrorist financing (money transfer services, cross-border wire transfers, cash couriers and operations of non-profit organizations).
In February 2012 the Special Recommendations were incorporated in the 40 new Recommendations, whose scope encompasses preventing and combating money laundering, terrorist financing and the financing of the proliferation of weapons of mass destruction.

3.2.2. European Union regulations

In implementation of the UN Security Council resolutions that introduced measures to freeze funds, the European Union has adopted specific common positions and regulations.
Blacklists are updated with adoption of specific amendments to the regulations, on the basis of which the European Commission has prepared its own consolidated list (Financial Security Database) of all individuals and organizations currently subject to international financial sanctions in Europe .
In response to the terrorist actions of recent years, the European Union adopted Directive (EU) 2017/541 on combating terrorism.
In addition, in order to improve prevention measures to effectively combat the financing of terrorism, in particular with regard to the new ways in which terrorist groups finance and carry out their operations, the fifth anti-money-laundering directive was adopted (Directive (EU) 2018/843 of 30 May 2018).

3.2.3. Italian regulations

National regulations on terrorist financing were organized with Legislative Decree 109 of 22 June 2007, containing “measures to prevent, counter and repress the financing of terrorism and the activity of countries that threaten international peace and security”, issued in implementation of Directive 2005/60/EC.

Legislative Decree 109/2007 requires those subject to anti-money-laundering regulations to meet a variety of obligations, reflecting the dual nature of enforcement action focused on freezing funds (notification requirements) and the reporting of suspicious transactions (reporting requirements).
The reporting requirements pursuant to Article 8, paragraph 1, of Legislative Decree 109/2007 were then incorporated into Legislative Decree 231/2007 as amended, following the extension of the regulations to prevent and combat money laundering to include terrorist financing in all areas of application (customer due diligence, reporting of suspicious transactions, document retention, internal controls, risk assessment and management).
An essential role in identifying suspicious transactions for reporting is played by anomaly indicators, in particular those specific to the financing of terrorism contained in the 2010 Bank of Italy measure, which focus particular attention on identifying terrorists (lists), the location of counterparties (areas at risk) and non-profit organizations, and other subsequent communications issued by Italy’s Financial Intelligence Unit (FIU).

4. Organizational model

4.1. Roles and responsibilities

The Group's organizational model vests the corporate bodies of the individual companies with primary responsibility for monitoring the risks of money laundering and terrorist financing, each in accordance with their respective areas of competence and in compliance with the legislation applicable to their countries, consistent with instructions received from the Parent Company.

The subsidiaries establish specific anti-money-laundering departments and appoint the related managers and a head of suspicious transaction reporting ("STR Manager").

The names of the STR Managers of each Group company are notified to the Board of Directors of Anima Holding.

The Anti-Money-Laundering Department of Anima SGR is the hub for activities related to legislation on the fight against money laundering and terrorist financing and for the suspicious transaction reporting of the Italian subsidiaries.

Strategic Supervision Body of the Parent Company
The Strategic Supervision Body approves and periodically reviews the Policy setting out the strategic guidelines for managing money laundering risk and the related control system.
At least annually, it examines the report of the Compliance & AML Office of Anima SGR concerning strategic guidance activities in the area of combating money laundering and terrorist financing at the Group level.

Control Body
The Control Body monitors compliance with legislation and the completeness of the strategic guidelines for managing money laundering risk and the related control system.

Anima SGR Compliance & AML Office
The Compliance & AML Office of Anima SGR performs a proactive and advisory role with regard to the competent corporate bodies in the following areas:

- developing a global approach to money laundering risk with regard to the Group methodology for assessing money laundering risks and the general standards of customer due diligence, data retention and the identification and reporting of suspicious transactions;
- developing appropriate organizational solutions to ensure compliance with the applicable provisions in the Group's various areas of operation and, at the same time, ensure that risk management takes account of all the assessment and measurement resources available to the individual Group members;
- periodically reviewing the Policy.

Furthermore, the Compliance & AML Office:

- ensures that the corporate bodies of the other Group companies implement Group strategies and policies in their own company;
- establishes a common information base that enables all Group companies to evaluate customers in a uniform manner and ensures the sharing of relevant information among Group companies;

- conducts a Group self-assessment exercise and coordinates self-assessment exercises conducted by the anti-money-laundering departments of the individual companies;
- analyzes the results of the activity performed by the individual anti-money laundering departments of the Group companies, including the results of the self-assessment exercise;
- at least annually, reports to the corporate bodies and top management on the results of the activity carried out.

Internal Audit Department
The Parent Company's Internal Audit Department verifies the correct execution of the process defined in the Policy.

5. Managing money laundering and terrorist financing risks

5.1. Group methodology for assessing money laundering risk

The assessment of money laundering risk is performed annually or when new business lines are opened. The assessment is conducted by the anti-money laundering department of the individual Group companies and, for the Group, by the Compliance & AML Office of Anima SGR. The assessment comprises the following macro-activities:

1. **identification of inherent risk**: risks are assessed with a specific analysis of all company areas, identifying the scope of operations. For areas identified as exposed to money laundering risks, the operations, products and services offered, customers, delivery channels and the geographical area and countries of operation will be assessed. To perform the analysis, at least the following aspects must be considered: operations, products and services, customers, delivery channels and geographical area and countries of operation. Based on the findings of the analysis, each company area is assigned an inherent money laundering risk score on a scale from 1 to 4;

2. **vulnerability analysis**: an analysis is conducted of the adequacy of the organizational structure and of the prevention and monitoring measures with respect to the risks previously identified in order to determine the level of vulnerability of the individual company areas: following this assessment, which takes account of the results of the checks performed by the control functions, a score is assigned on a scale from 1 to 4;

3. **determination of the residual risk**: the level of residual risk is assessed based on the level of inherent risk and the robustness of the mitigation measures. The assessment uses a matrix that combines the assessments of inherent risk and vulnerability assigned previously, thereby specifying the relative residual risk on scale from 1 to 4. The overall residual risk level of the individual company is the result of the residual risk values of the individual business lines/business areas identified and weighted using the weight assigned to the individual area for each business line/business area;

4. **remedial measures**: following the determination of the residual risk level for individual company areas and the company as a whole, the management body identifies and proposes, together with the anti-money-laundering department of each Group company, any remedial measures or adjustments to be adopted in order to prevent and mitigate residual risks.

To carry out the self-assessment exercise, each Group company must evaluate at least the following aspects:

- structuring by business lines;
- inclusion of the list of risk factors deemed relevant for the company in order to identify the potential risk (inherent risk). Risk factors are grouped into uniform groups on the basis of valuation drivers (customers, transactions, distribution channels);
- the creation of a check list for the assessment of the risk mitigation controls necessary. These controls are based on applicable regulatory provisions and market best practices.

5.2. Principles and rules for customer due diligence

Customer due diligence consists of the following activities, which are governed by the provisions of Article 18 of Legislative Decree 231/07:

a) identification of the customer and verification of identity;
b) identification of the beneficial owner and verification of identity;
c) the acquisition and evaluation of information on the purpose and nature of the business relationship;
d) constant monitoring of the relationship with the customer over its entire duration, obtaining a holistic view of the transactions of the customer.

Adopting a risk-based approach, the stringency and scope of due diligence obligations are adjusted depending on the degree of money laundering and terrorist financing risk associated with the individual customer. Specific simplified and enhanced due diligence measures are envisaged for different types of customers or products. These measures are adjusted in accordance with the specific features of the delivery process for the products and services of the subsidiaries, collective asset management portfolios and individual asset management portfolios, which may be conducted directly or indirectly through authorized third-party intermediaries.

5.2.1. Distribution and customer due diligence through authorized third-party intermediaries

The distributor plays the role of mere intermediary in the relationship between subsidiaries and investors, who therefore becomes the customer holding the relationship with the subsidiary.
A distribution agreement must be entered into with the distributor intermediary. Under the terms of the agreement, the distributor shall manage and maintain direct contact with customers on an ongoing basis and perform due diligence obligations, in particular:

a) identification of the customer and verification of the customer's identity;
b) identification of the beneficial owner and verification of the beneficial owner's identity;
c) acquisition and evaluation of information on the purpose and nature of the business relationship.

Subsidiaries must constantly monitor the relationship with the customer.

5.2.2. Direct distribution

Subsidiaries are required to perform all phases of retail and institutional customer due diligence.
The subsidiaries pay particular attention to remote operations, in consideration of the absence of direct contact with the customer or the executor, taking account of the risk of fraud connected with identity theft.

5.3. General criteria for assessing customer risk

The Group has a complex computerized anti-money-laundering system to profile and classify customers and all parties involved in the related relationships (beneficial owners, executors, delegates, etc.) in accordance with the associated money laundering risk.

The computerized profiling system is updated on an ongoing basis not only with data and information from management systems, but also with additional information collected from list matching activities (anti-money-laundering, anti-terrorism, PEP and internal investigation lists) and the results of other control activities of the Anti-Money Laundering Department. The profiling software determines a score representative of the level of risk and classifies customers into five classes (low, medium-low, medium, medium-high, high).

The operating units conduct enhanced customer due diligence activities for all positions classified as high risk, which are identified and extracted on a monthly basis by the computerized anti-money laundering system using control algorithms for subjective and/or operational anomalies (trigger events).

The anti-money-laundering departments of the individual companies assess the adequacy of the enhanced due diligence process and, if necessary, submit proposals for changes to the customer profiling system to the Strategic Supervision Body.

5.3.1. High risk factors

The profiling system classifies at least the following types in the high risk bracket:

1. business relationships or transactions with customers and their beneficial owners who are classified as politically exposed persons;
2. persons for whom the competent authorities have notified the subsidiaries of measures deemed relevant in the anti-money-laundering/anti-terrorism area;
3. persons identified in the list matching process;
4. customers who carry out unusually large transactions;
5. relationships and transactions involving high-risk third countries;
6. persons who, on the basis of an assessment of additional risk factors considered relevant, are classified as high risk.

Additional risk factors are identified by each subsidiary in at least the following categories:

- high risk factors relating to the customer, executor and beneficial owner:
  - business relationships established in unusual circumstances;
  - arrangements that qualify as asset-holding vehicles;
  - companies with unusual or excessively complex ownership structure;
  - types of business particularly exposed to money laundering and corruption risks
- geographical high risk factors
- high risk factors related to products, services, transactions or delivery channels:
  - securities transfers between third parties without supporting documentation and wire transfers with payors or beneficiaries other than the holders of the relationships with the asset management company;
  - large-value wire transfers from and to a foreign country that are not associated with an authorized intermediary.

5.3.2. Enhanced customer due diligence

Enhanced due diligence measures consist in the acquisition of more information on customers and beneficial owner where the customer is classified as high risk.
The enhanced due diligence measures for subsidiaries must at least consist of:

- acquiring more information relating to:
  - the identity of the customer and the beneficial owner or the ownership and control structure of the customer and the nature of the business of the customer and the beneficial owner;
  - the business relationship;
  - the destination of funds;
- acquiring better quality information, in particular confirming the identities of the payor and beneficiary account holders and verifying the sources of income and wealth;
- updating information more frequently, with more frequent reviews of the business relationship and transactions.

5.3.3. Low risk factors and simplified customer due diligence

In situations with a low risk of money laundering and terrorist financing, it is possible to apply simplified customer due diligence measures in terms of the extent and frequency of assessments.

Subsidiaries consider at least the following aspects:

- low risk factors relating to the customer, executor and beneficial owner;
  - companies listed on a regulated market
  - public administrations or institutions or bodies that perform public functions, in accordance with European Union law;
  - banks and financial intermediaries in jurisdictions with an effective anti-money-laundering and terrorist financing regime;
- Low risk factors related to products, services, operations or delivery channels;
  - regulated supplementary pension products or social security programs or similar systems that pay pension benefits to employees, where contributions are paid by deductions from wages and which do not allow beneficiaries to transfer their rights.

6. Data retention

The subsidiaries adopt data-retention methods that ensure the retention of information for a period of ten years from the termination of the business relationship or the date of the transaction.
Data relating to the transmission of information to the authorities must be retained for at least ten years.
Subsidiaries must establish data-storage systems.

7. Training

All employees and associates of the subsidiaries must undergo training on money laundering and terrorist financing risks at specified intervals.
In addition to the generic training program, employees in direct contact with customers and the personnel of units potentially involved in processes “sensitive” to the risk of money laundering and terrorist financing must undergo specific training to acquire the skills appropriate to their duties.

The training and education program is developed by the management body, in agreement with the anti-money-laundering department of each subsidiary.

Internal anti-money-laundering rules must be disseminated and brought to the attention of all employees and external associates of Anima SGR.

8. Identification and reporting of suspicious transactions

Subsidiaries report transactions to the competent authorities when they know, suspect or have reasonable grounds for suspecting that money laundering or terrorist financing is in progress or has been carried out or attempted.
The Group adopts the common reporting practice of reporting suspicious transactions even where there is a well-founded belief that certain funds, although not necessarily of unlawful origin, are nevertheless intended for use in the commission of crimes (corruption, creation of slush funds, tax evasion, etc.).

The individual subsidiaries give their own suspicious transaction reporting managers ("STR Managers") responsibility for assessing reports received and their transmission to the authorities.
STR Managers are responsible for:

- evaluating in the light of all the available information any suspicious transactions reported by the competent organizational units and any other such transactions of which they have otherwise become aware during the performance of their duties;
- transmitting well-founded reports to the competent authorities, omitting the names of the parties involved in the transaction reporting procedure;
- retaining documentation of all assessments.

The transmission and retention of data must be carried out in a manner that ensures the confidentiality of the identity of the person submitting the report.

The Parent Company shall establish a common information base to ensure access to information on the reports transmitted and those deemed unfounded, accompanied by the motivation for the decision of the STR Managers of the subsidiaries.