

MONTEPASCHI GROUP

POLICY ON PREVENTION AND COUNTERING OF MONEY LAUNDERING AND TERRORISM FINANCING

1 - OVERVIEW

1.1 – KEY REGULATIONS AND GUIDANCE

This document sets forth the Montepaschi Group's global anti-money laundering and counter-terrorism financing Policy and is applied to all subsidiaries and foreign branches.

Standards are to be considered complementary and applicable since they are not in conflict with the provisions issued by the local Authorities.

1.2 – RECIPIENTS AND METHODS OF IMPLEMENTATION

The Policy is intended for the Parent Company and all Group Companies.

The Group Companies implement the Policy by resolution of their own Managing Boards, aligning responsibilities, processes and internal rules with respect to their own structure and size.

2 – GENERAL PRINCIPLES

The laundering of proceeds from illegal and criminal activities is one of the most serious forms of crime in the financial markets and is an area of specific interest for organized criminal activities.

Money laundering has a significant negative impact on the entire economy: reinvesting illegal proceeds in legal activities and collusion between individuals or financial institutions and criminal organizations deeply affect market mechanisms, undermine the efficiency and fairness of financial activities and have a weakening effect on the economy. Financing terrorist activities may involve using legally derived proceeds and/or criminally derived proceeds.

The changing nature of money laundering and terrorist financing, also facilitated by the continuous evolution of technology, requires a constant adaptation of the prevention and contrast measures.

The Anti-Money Laundering (AML) and Counter Terrorism Financing (CTF) regulatory framework is based on a comprehensive set of national, EU and international regulatory sources.

At an international level, a key contribution to regulatory harmonization has come from the Financial Action Task Force (FATF), the foremost international body active in the fight against money laundering, terrorist financing and the proliferation of weapons of mass destruction.

In fulfilling its responsibilities, the FATF established a set of international standards, the "40 recommendations", to which a further 9 special recommendations were added in 2001 to combat international terrorism financing. The subject was fully revised in February 2012 with the adoption of International Standards on Combating Money Laundering and the Financing of

Terrorism & Proliferation, then summarized in the new "40 Recommendations".

As part of the fight against the proliferation of weapons of mass destruction, the United Nations prepared a set of measures to combat financing of proliferation programs, including the prohibition to assist or finance any persons involved in such activities.

In implementing the Resolutions adopted in the framework of the United Nations, the European Union issued a set of provisions in order to implement restrictive measures such as the freezing of funds and economic resources of persons or entities involved in developing proliferation-sensitive activities.

The FATF has developed guidelines to implement the financial sanctions adopted by the United Nations.

Specific measures addressing the proliferation of weapons of mass destruction have recently been included in the Recommendations, in accordance with the resolutions of the United Nations Security Council.

EU guidelines on preventing the use of the financial system for money laundering and terrorist financing are contained in **EU Directive 2015/849** of the European Parliament and of the Council of 20 May 2015 (Fourth Anti-Money Laundering Directive), implemented by EU Directive 2018/843 (Fifth Anti-Money Laundering Directive).

At a national level, prevention and fight against money laundering and terrorism financing is regulated by the following primary laws:

- **Italian Legislative Decree no. 109 of 22 June 2007** and subsequent amendments and supplements which sets forth "Provisions to prevent, counter and repress the financing of terrorism and the activity of Countries that threaten peace and international security", implementing Directive 2015/849 as modified by EU Directive 2018/843;
- **Italian Legislative Decree no. 231 of 21 November 2007**, and subsequent amendments and supplements implementing Directive 2015/849/EU, which modifies Directive 2009/138/EC and 2013/36/EU, modified by Directive 2018/843/EU on preventing use of the financial system for the purpose of money laundering and terrorist financing.

The Montepaschi Group (hereinafter "The Bank") has transposed these decrees in its internal regulatory documents.

At a general level, the Bank has adopted this "Policy on combating money laundering and terrorist financing" (hereinafter Policy) as an expression of its commitment to combat the aforementioned criminal phenomena on an international basis, paying particular attention to contrast, in the awareness that the pursuit of profitability and efficiency must be combined with the continuous and effective monitoring of the integrity of corporate structures.

The Policy applied within the Bank describes the policy adopted by the Group in accordance with the rules and principles dictated by national and EU regulatory provisions, in compliance with the relevant international standards and is applied to each Group entity jointly with the Directive of Anti-Money Laundering and Counter-Terrorism Group, the Code of Ethics and internal procedures that implement the local primary and secondary legislation in force specifying processes, roles and responsibilities.

The current Policy was approved by the Parent Company's Board of Directors.

Considering that at an international level the sources of EU and national regulations referred to

are the same, the AML and CTF guidelines are applied at Group level by both the domestic and foreign entities in coherence with applicable laws, and are published on Banca MPS's website along with the document "AML declaration" available at the link:

<https://www.gruppomps.it/static/upload/aml/aml-declaration.pdf>,

and "Wolfsberg Questionnaire" available at the link:

https://www.gruppomps.it/static/upload/16-16-01-18_aml_ctf-questionnaire.pdf

The Bank is committed to complying with this regulatory framework as well as any implementing provisions issued by the Bank of Italy on customer due diligence, data and information retention, organization, procedures, controls and enhanced controls against the financing of programs aimed at the proliferation of weapons of mass destruction.

The Bank is thoroughly committed to ensuring that operational organization and the control system are complete, adequate, functional and reliable for strategic supervision, to protecting the Group from tolerance or admixture of forms of illegality that can damage its reputation and affect its stability.

For these reasons, the Montepaschi Group has adopted organizational and behavioral rules and monitoring and control systems aimed at ensuring compliance with current legislation by the administrative and control bodies, staff, collaborators and consultants of Group companies. These controls are also consistent with the rules and procedures established by the personal data protection code.

The Bank also relies on indicators of anomalies and patterns of irregular behaviors in the economic and financial environment, which are issued over time by the Financial Intelligence Unit (FIU) regarding potential money laundering and terrorist financing activities.

3 – GROUP MODELS AND METHODOLOGIES

Obligations deriving from the national regulatory framework for the prevention of money laundering and terrorism financing require the Bank to:

- adopt appropriate organizational structures, procedures and internal control measures; perform "customer due diligence" with a risk-based approach;
- retain data and information;
- report suspicious transactions;
- apply restrictions on the use of cash and bearer securities, applicable to all subjects, and report infringements of art. 49 and 50 of Legislative Decree 231/07 to the Ministry of Economy and Finance (MEF);

with regard to counter-terrorist financing activities, Italian legislation requires the obligated parties to do the following:

- freezing of funds and economic resources of certain persons included in EU lists;
- informing the Financial Intelligence Unit (FIU) of the measures applied for the freezing of funds, or the Special Currency Police Unit of the *Guardia di Finanza* (Financial Police) in case of economic resources;
- informing the FIU of suspicious transactions, business relationships and any other information available regarding parties included in the blacklists published by the FIU itself;

- reporting suspicious transactions which, on the basis of available information, are either directly or indirectly related to terrorist financing activities;

The main requirements set forth by the described regulatory framework are therefore:

- obligation to adopt consistent and coherent procedures for analysis and evaluation of the risks related to money laundering and terrorism financing and establish supervision, controls and procedures needed to mitigate and manage those risks.
- customer due diligence, through which the Bank acquires and verifies information regarding the identity of a customer and any beneficial owner, as well as the purpose and intended nature of the relationship or of the transaction, whilst ensuring the constant monitoring of all transactions undertaken by the customer;
- a risk-based approach, whereby customer due diligence obligations are divided into different degrees of due diligence commensurate with the customer's risk profile;
- obligation to retain documents, data and information in order to allow their timely acquisition, transparency, completeness, inalterability and integrity, and an overall and prompt accessibility.
- reporting of suspicious transactions;
- refraining from entering into any new customer relationship, conducting occasional transactions or maintaining an existing customer relationship where due diligence has not been conducted or it is suspected that there may be a link to money laundering or terrorist financing;
- limitations on the use of cash or bearer securities;
- monitoring all transactions with natural and legal persons and/or with Countries included in European Union Council Lists, OFAC Lists or in the Provisions issued by the National Authorities containing specific restrictive measures for combating terrorism;
- monitoring transactions entered into with countries considered non-cooperative in matters of tax, financial supervision and anti-money laundering, generally referred to as "tax havens" or "offshore financial centres";
- adopting appropriate staff training programs to ensure the implementation and proper application of laws and regulations;
- providing FIU with "objective communications" in accordance with specific instructions regarding methods and frequency of communications;
- obligation to disclose any breaches or infringements that may come to the attention of the Control Bodies in carrying out their tasks;
- obligation to adopt procedures to manage internal reporting of violations submitted by employees (Whistleblowing).

3.1 - CUSTOMER DUE DILIGENCE

The Bank undertakes all customer due diligence measures when:

- establishing business relations;
- performing occasional transactions, arranged by customers, such as wire transfers or other transactions equal to or above the applicable designated threshold, regardless of whether the transaction is carried out in a single operation or in several related operations or that it consists of a transfer of funds, exceeding the legal limits;
- there is a suspicion of money laundering or terrorist financing, regardless of any

derogation, exemption or designated threshold that may apply;

- there are doubts about the veracity or adequacy of previously obtained customer identification data.

The due diligence obligations

- are fulfilled:
 - towards new customers before the establishment of an ongoing relationship or the execution of an occasional transaction,
 - towards those already acquired, whenever the due diligence is appropriate in consideration of the changed level of money laundering or terrorist financing risk associated with the customer.
- Customer due diligence obligations are as follows:
 - identifying the Customer, the beneficial owner and the executor and verifying their identity on the basis of documents, data or information obtained from a reliable and independent source;
 - obtaining and assessing information on the purpose and intended nature of the business relationship;
 - performing ongoing monitoring of the customer's behaviour throughout the business relationship

The Bank identifies low-risk customers applying a risk-based approach, to whom a simplified due diligence procedure may be applied taking into account the risk indicators specifically outlined by the relevant regulations with respect to well-defined customer types (e.g. companies listed on a regulated market for which adequate transparency of ultimate beneficial ownership is ensured, public administrations, credit or financial institutions resident in Member States or third countries with equivalent money laundering and terrorist financing prevention systems) or products, services and transactions categories (e.g. life insurance contracts with premium within the threshold permitted by regulations).

The Bank always applies enhanced customer due diligence measures where:

- customers residing or based in high risk third countries or in the case of ongoing relationships, professional services and operations involving high risk countries;
- a correspondent banking relationship is set up with a bank or an institution located in a third country,
- relationships or transactions in which the customer or the ultimate beneficial owner is a politically exposed person¹,
- the customer is a legal person that has issued bearer shares and is controlled by a trustee.

acquiring additional information about the customer and the beneficial owner, investigating the purpose and nature of the relationship and ensuring frequent application of the procedures aimed at guaranteeing constant control during the ongoing relationship and keeping track of the reasons for which it was impossible to identify the beneficial owner, in accordance with the objective and substantial criteria indicated in art. 20 of Legislative Decree 231/07.

In order to comply with the obligations of enhanced due diligence, counter terrorism financing and financing of the proliferation of weapons of mass destruction, the Bank has adopted

¹ Politically Exposed Persons (PEP); individuals, resident and non-resident, that are entrusted with a prominent public office or have ceased to hold office for less than a year, their family members and those having close ties with them as listed by art. 1, paragraph 2, letter dd) Legislative Decree 231/07.

control procedures capable of verifying the consistency between customer identification data obtained through the due diligence process and that contained in the lists produced by the EU and other international institutions and bodies, such as:

- individuals, resident and non-resident, that are entrusted with a prominent public office or have ceased to hold office for less than a year (PEP), their family members and those having close ties with them according to the definition of art. 1 c. 2 letter dd;
- (PEPs Politically Exposed Persons, resident, and not resident);
- natural and legal persons operating, even partially, in States which do not impose equivalent measures and regulations, according to the guidelines of the Bank of Italy or other national or supranational institutions engaged in the prevention of crime;
- natural and legal persons subject to embargo measures or freezing of funds/economic resources and financial assets (UN, EU, OFAC).

3.2 - CUSTOMER PROFILING

The Bank adopts suitable procedures aimed at defining the money laundering and terrorist financing risk profile attributable to each customer, based on the information acquired and analyses carried out, with reference both to the assessment elements indicated in the Provision itself and to further elements that may be adopted.

After profiling each customer is included in a predefined risk class.

The Bank has put in place an IT procedure to assess the customer's risk profile and to consistently define a revaluation time frame appropriate to the risk assessed; the frequency of revaluation depends on the stage of the last assessment carried out or, in the absence of a KYC questionnaire, on the customer's risk profile, as specified below:

Risk profile	Re-evaluation timetable
Low/irrelevant	until 4 years after the last customer due diligence
medium	until 2 years after the last customer due diligence
high	until 1 year after the last customer due diligence

3.3 - OBLIGATIONS FOR ABSTAINING

The Bank refrains from establishing, executing or continuing the relationship, operations and professional services (so-called abstention obligation) in the event of an objective impossibility to carry out customer due diligence, assessing whether to report a suspicious transaction to the FIU.

In those cases, in which abstention is not possible, as there is a legal obligation to execute the operation which cannot be postponed or if to decline it could hinder the investigation, the Bank is nonetheless obliged to report the suspicious transaction immediately.

Moreover, if after further evaluation or downstream of the reporting process, elements of high risk emerge which could affect the legal and/or reputational profile of the Bank or the Group,

the Bank reserves the right to limit or terminate the business relationship with the customer.

The Bank shall not enter into or continue a correspondent relationship with a shell bank and with entities which allow access to correspondent relationships to a shell Bank. It shall not enter in a business relationship with entities whose ownership structure (corporate, fiscal and financial) is characterized by a high degree of opacity which prevents the clear identification of the beneficial owner or the nature and purpose of the structure.

In addition, the Bank refrains from entering into or continuing a business relationship with persons particularly exposed to the risk of money-laundering/terrorist financing, such as:

- Trust companies, with the exception of those included, or required to be included, in the Register of Financial Intermediaries pursuant to article 106 of the Italian Banking Act – separate section of the Trust Companies – that have their registered office in a country specified by the FATF as having a higher risk of money laundering or apply measures that are not compliant with the requirements imposed by Italian Legislative Decree no. 231/07 or by European Directives;
- Trusts for which appropriate, accurate and updated information on the beneficial ownership of the trust and its nature and purpose is not available;
- Gaming companies, including on-line gambling, casinos and Bingo operators for which authorisation and/or licenses required under Italian legislation have not been issued and/or verified;
- affiliated entities and agents of payment service providers (referred to in the definition of art.1 c. 2 letter nn) and electronic money institutions that do not comply with the provisions of Chapter V of Legislative Decree 90/17 in Articles 43 et seq.
- Private limited companies or companies controlled through bearer shares, headquartered in high-risk Countries.

The Bank uses all the information acquired during the due diligence process regarding its customers and their transactions to determine whether a transaction or business relationship is, directly or indirectly, linked to persons or entities involved in money laundering, terrorist financing or in the development of weapons of mass destruction.

3.4 - SUSPICIOUS TRANSACTIONS REPORT

Whenever the Parent Company or any Group company suspects or has reasonable grounds for suspecting that a money laundering or terrorist financing operation has been or is being conducted or attempted:

- it submits a suspicious transaction report to the Financial Intelligence Unit (FIU), if the transaction is based in Italy;
- if the transaction is based in another Country, it complies with the provisions of local legislation and, where the latter provides for the application of measures that are equivalent to those laid down by EU Law, it promptly informs the Parent Company's Group Head of Anti-Money Laundering, taking all the necessary precautions to protect the identity of the persons reporting the suspicious transaction.

The Bank has put in place procedures and processes to monitor, identify and report suspicious activities in accordance with the timing and methods required by applicable Law. Employees promptly report any knowledge or suspicion of money laundering, terrorist financing or other criminal activities to their Manager and/or Delegated Person within the reporting process. Until the report is submitted, employees refrain from executing the transaction, unless that is impossible as there is a legal obligation to accept the deed or the execution of the operation

cannot be postponed due to the normal conduct of business or where it might obstruct investigations. In these cases, the report is submitted immediately after the transaction has been executed.

Grounds for suspicion include the characteristics, scale and nature of the transaction and any other circumstance whatsoever which comes to the employees' knowledge as a result of their duties, also taking into account the financial scope and nature of the business carried out by the subject of the suspicious transaction, as understood from the information acquired by the Bank as a result of its activities.

To limit the Bank's risk of involvement – even if unintentional – in the illegal activities mentioned above, an enhanced due diligence process is activated in fund transfer arrangements where the players involved in this type of transaction (originator, beneficiary, the banks involved in the fund transfer) may lead to the suspicion of money laundering, terrorist financing or violations of applicable international restrictions on certain goods, persons or entities.

Downstream of the reporting process, the Bank and/or the MPS Group may limit and/or interrupt the business relationship with customers, in particular where said relationship may constitute a significant legal or reputational risk for the MPS Group.

These limitations may, for example, concern the access to certain types of products or the interruption of the services offered by the Bank or the Group.

3.5 – DATA RETENTION

The Bank retains all documents and records all data obtained through the customer due diligence process, so that they may be used for any investigations into possible money laundering or terrorist financing transactions, or to comply with requests for information from the Regulators or from other competent Authorities.

To that end, the Group's financial intermediaries based in Italy have set up a Single Electronic Archive (AUI – Archivio Unico Informatico), which electronically stores all identification data and other information regarding ongoing business relationships and customer transactions as required by applicable Law.

Regarding customer due diligence measures, the Bank keeps copies or records of all documents required for a period of ten years after the business relationship has ended.

As for transactions and business relationships, all supporting evidence and records, e.g. original documents or copies admissible in court proceedings, are kept for a period of ten years after the execution of the transaction or after the business relationship has ended.

4 – LIST OF PROCEDURES

4.1 – MONEY-LAUnderING AND TERRORIST FINANCING RISK MANAGEMENT

The "money-laundering and terrorism financing risk management" procedure is performed within the Group to mitigate the risk of non-compliance with anti-money laundering and counter-terrorism financing requirements. The procedure involves the following activities:

- Identifying the risk of non-compliance with AML/CTF requirements;
- Gap analysis and assessing the status of compliance;

- Management and mitigation of AML/CTF risks;
- Compliance controls (ex-ante and ex-post);
- Advisory and support on AML/CTF issues;
- On-going AML/CTF risks monitoring and control;
- Reporting to top management, governing bodies, supervisory bodies and regulators;
- Providing specific AML/CTF training courses.

Group rules and responsibilities regarding the procedure are reported in internal regulation "Group Directive on Anti-Money Laundering and Counter-Terrorism Financing".

4.2 – MANAGING RELATIONS WITH SUPERVISORY AUTHORITIES ON AML AND CTF ISSUES

The "managing relations with Supervisory Authorities" procedure is performed within the Group to manage, analyze, steer and monitor all communications with Regulators for matters regarding Anti-Money Laundering and Counter Terrorism Financing, one of the objectives being to archive documents in a single repository.

Within this procedure the following activities are performed:

- managing relations with Supervisory Authorities on AML and CTF issues;
- managing AML administrative proceedings initiated by the relevant Authority (MEF – Ministry of Economy and Finance).

Group rules and responsibilities regarding the procedure are reported in internal regulation "Group Directive on Anti-Money Laundering and Counter-Terrorism Financing".

4.3 – MANAGING OPERATIONAL REQUIREMENTS FOR COUNTERING OF MONEY LAUNDERING AND TERRORISM FINANCING

The procedure for "managing operational requirements for countering of money laundering and terrorism financing" is performed within the Group with the goal of meeting all regulatory requirements through the following activities:

- Implementation of requirements concerning limits to the use of cash and bearer securities;
- Implementation of obligations concerning customer due diligence;
- Implementation of requirements on AML/CTF suspicious activity reporting;
- On-going supervision of procedures implemented against terrorism financing;
- Management of obligations related to data/information collection and retention.

Group rules and responsibilities related to this procedure are reported in internal regulation "Group Directive on Anti-Money Laundering and Terrorism Financing".

5 - MPS GROUP ORGANIZATIONAL FRAMEWORKS AND CONTROL BODIES

In accordance with current regulations, the Parent Company has established its organizational structure and corporate governance so as to protect the interests of the Group while, at the same time, ensuring sound and prudent management and to avoid the risk - even if unintentional - of any direct involvement in acts of money laundering and/or terrorist

financing.

To that end, in accordance with the Internal Control System adopted by the Group, the Board of Directors and Statutory Auditors are involved in mitigating the above risks through clearly defined tasks and responsibilities.

In addition, the Parent Company has established a centralized unit for the management of the internal violations reporting system, with the responsibility of supervising the activities of receiving, analyzing and evaluating alerts forwarded by employees via the Whistleblowing procedure.

6 – REVIEWING AND UPDATING THE POLICY

The AML/CTF Department reviews the policy at least annually, updates it if and where necessary and submits the new text to the Chief Executive Officer for the approval of the Board of Directors.

Any changes to the Policy are subsequently disclosed to all branches and subsidiaries (Italian and foreign) in order to apply all necessary implementations.