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), as amended by EU Directive 2018/843 (Fifth Anti-Money Laundering Directive) and in the Guidelines issued from time to time by the European Banking Authority (EBA) .

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.

Finally, there is also secondary legislation at national level that was issued by the Bank of Italy and the Financial Information Unit ("FIU") and it is contained in the following regulatory sources:

- **Provision of 24 August 2010** setting out the **anomaly indicators** for financial intermediaries to facilitate the identification of suspicious transactions;
- **Provision of 26 March 2019** laying down the implementing provisions on **organisation, procedures and internal controls** aimed at preventing the use of financial intermediaries and other entities for the purposes of money laundering and terrorist financing;
- **Provision of 28 March 2019** setting out instructions on **objective communications;**
- **Provision of 30 July 2019** laying down implementing provisions on **customer due diligence;**
- **Provision of 24 March 2020** laying down implementing provisions for **storage and availability** of documents, data and information regarding anti-money laundering and counter-terrorist financing;

- **Provision of 25 August 2020** laying down provisions for submitting **aggregated AML reports.**

The Montepaschi Group (hereinafter "The Bank") implements the above regulations in its internal regulatory documents.

At a general level, the Bank has adopted this "Policy on combating money laundering and terrorist financing" (hereinafter the "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 Group Directive on Anti-Money Laundering and Counter-Terrorism Financing, 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/wol/wolfsberg-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 (Office of Foreign Assets Control), OFSI Lists

(Office of Financial Sanctions Implementation HMT), UN Lists (Consolidated United Nations Security Council Sanctions List) 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.

In cases where the Bank uses remote identification methods as permitted by Legislative Decree no. 231/07, Article 19(1)(a)(2) and (5), it adopts special procedures for carrying out its due diligence obligations, also in view of the risk of fraud associated with identity theft.

Customer onboarding with remote identification is based on the acquisition of the qualified electronic signature certificate, generated after an identification process carried out through:

- the use of the Public Digital Identity System (SPID) or Electronic Identity Card by means of secure and regulated electronic identification techniques and procedures that are authorised or recognised by the *Agency for Digital Italy*;
- the video-identification procedure, regulated by the Bank of Italy in implementation of the Anti-Money Laundering Decree in Annex 3 of the "Provisions on Customer Due Diligence".

In all cases, the remote identification process involves collecting the customer's and any executor's identification data in electronic format, as well as performing verifications and checks on the authenticity of the data, in addition to those provided for in-person identification, according to a risk-based approach, including through telephone contact on a certified number (welcome call) or a money transfer carried out by the customer *via* a banking and financial intermediary based in Italy.

With a view to limiting exposure to potential money laundering and/or fraud risks, no remote relationships may be established by persons:

- other than natural persons;
- who are not residents in Italy

The Bank applies ordinary, simplified or enhanced customer due diligence measures to customers following a risk-based approach.

3.1.1 – Simplified due diligence obligations

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 "low risk indicators" specifically outlined by Annex 1 of the Provision on customer due diligence of 30 July 2019 (hereinafter "The Provision").

The relevant "low risk indicators" in order to apply a simplified due diligence procedure are based on the type of customer, executer or beneficial owner, the geographical area of residence or in which the head office is established, specific product, service or distribution channel.

More specifically, the following are subject to simplified due diligence measures:

- Public Administrations, Institutions or Bodies performing public functions, in accordance with the law of the European Union;
- Companies listed on a regulated market and subject to disclosure requirements, including ensuring adequate transparency of ultimate beneficial ownership;
- the Community credit and financial institutions listed in article 3 (2) of the Anti-money laundering Decree – except for those at the letters i), o), s), v) – and the credit and financial institutions residing in Member States or third countries with effective money laundering and terrorist financing systems;

- customers, executors or beneficial owners residing or established in geographical areas with a low money laundering risk.

The Bank does not apply simplified due diligence measures:

- when doubts, uncertainties or inconsistencies arise regarding the identifying data and information gathered during identification of the customer, executor or beneficial owner;
- if the conditions for simplified customer due diligence cease to apply based on the risk indicators provided for by the anti-money laundering decree and relevant secondary regulation;
- if monitoring of overall operations carried out by the customer and the information gathered throughout the relationship exclude a low risk type;
- whereas, however, the suspect of money laundering or terrorist financing arises.

The AML Function has exclusive responsibility over the evaluation and authorization of simplified due diligence measures. The application of simplified due diligence entails the same obligations to identify and verify the identity of the customer, the executor and the beneficial owner, acquiring all the data necessary for their complete identification (name, legal nature, registered office, and, where applicable, tax code) and performing all the steps of the ordinary due diligence process, albeit reducing their level of depth, scope and frequency, as provided for in the Provision on Due Diligence.

3.1.2 – Enhanced due diligence obligations

The Bank is required to apply **enhanced customer due diligence measures** in the presence of customers or situations with a **higher risk of money laundering or terrorist financing** and in all cases referred to in Article 24 of Italian Legislative Decree 231/07 as well as in specific cases identified by the Bank.

The Bank always applies enhanced customer due diligence measures in case of a higher risk of money laundering or terrorist financing as the following:

- customers residing or based in high risk third countries or in the case of ongoing relationships, professional services and operations involving high risk countries;
- natural and legal persons included in the lists of persons or entities subject to measures aimed at freezing funds provided by European regulations or decrees pursuant to Legislative Decree 109/07, and those having close ties with them;
- a cross-border correspondent banking relationship set up with a bank or an institution located in a third country, based on geographic high risk factors (as reported in Annex 2 of Bank of Italy's provisions on Customer Due Diligence)
- relationships or transactions in which the customer or the ultimate beneficial owner is a politically exposed person[1],
- customers classified as a "Trust",
- customers subject to investigation in the last 48 months, or those having close ties with them;
- customers reported to the Financial Intelligence Unit (FIU) in the last 24 months;

[1] Politically Exposed Persons (PEPs): as listed by art. 1, paragraph 2, letter dd) Legislative Decree 231/07.

Before entering into, continuing or maintaining an ongoing relationship with Politically Exposed Persons or Correspondent Entities of third countries, the Bank obtains specific authorisation from the General Manager or his delegate as provided for in Article 25 of Legislative Decree 231/07.

The Bank also applies enhanced customer due diligence measures in cases where the following additional risk factors are present:

- legal persons qualifying as financial vehicles (Trusts, Trust companies, Foundations);
- companies that have issued bearer shares or that have a company issuing bearer shares within their control chain structure;
- relationships or transactions in which the customer and the ultimate beneficial owner hold a public office other than those listed for politically exposed persons[2];
- companies owned by Trusts, Trust companies, Foundations, joint-stock companies through multiple levels of participation or cross holdings;
- customers carrying out economic activities particularly exposed to risk in "controversial" sectors of activity[3] or cash-intensive commercial activities, such as cash-for-gold, money exchange, gaming/betting including on-line gambling, Bingo operators, arms trade, arms industry and war trade, mining industry, , or companies operating in crypto-assets;
- customers participating in public contracts or receiving public financing (health care, construction, waste collection and disposal, production of renewable energy, mining, supply of pharmaceutical instruments);
- customers that during on-boarding or reactivation of an ongoing relationship after a period of inactivity turn out to have no anti-money laundering profile assigned through the specific tools used by the Bank in order to support anti-money laundering processes,

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 full compliance with current legislation and with the provisions of the Group Directive on Anti-Money Laundering and Counter-Terrorist Financing and in line with the Group's Code of Ethics, the Bank does not support transactions with customers operating in controversial sectors that (i) are not compliant with current national legislation and (ii) are not, where applicable, authorised in advance by the competent Italian national authorities, in particular:

- the production, transit and/or marketing of armament materials;
- the production and sale of light marijuana, adult entertainment venues;
- cash-intensive commercial activities other than those listed above, such as non-regulated charities and NGOs, the production of precious metals and stones, money remittances.

Furthermore, the Bank pays particular attention to compliance with restrictive measures put in place by the Italian State, foreign bodies (OFAC) and/or supranational bodies (UN, EU). These measures may be of a commercial nature (e.g. blocking of imports/exports) or of a financial

[2] Public office other than those held by Politically Exposed Persons (PEPs) as referred to in note 1), applying to all those holding office in, but not limited to, public bodies, consortia, associations of a public nature as listed at section A 8) of Annex 2 of the Provision.

[3]. an economic sector is "controversial" if the goods / services manufactured / offered and / or the ways in which they are produced / offered are in contrast with the widely shared values of ethics and sustainability, even when services or activities are lawful and therefore not in contrast with legal obligations.

nature, such as partial/total blocking of money transfers from or to a specific country or limitations on operations and/or freezing of funds held with financial intermediaries.

In order to comply with the obligations set out in Italian Legislative Decree 109/07 - aimed at preventing and combating the financing of terrorism and the activities of Countries threatening international peace and security, through the application of restrictive measures to "freeze" funds and economic resources held by natural and legal persons, groups and entities specifically identified by the United Nations and the European Union ("designated subjects") - and the enhanced verification obligations set out in Italian Legislative Decree 231/07, the Bank has adopted automatic control procedures. These procedures are 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 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 (Sanction Lists UN, EU, HMT, OFAC).

3.2 - CUSTOMER PROFILING

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

After profiling, each customer is included in a risk class predefined by the Bank according to the risk profiling table shown below:

Risk class	Ranking
Insignificant	<=5
Low	>=6 and <=12
Medium	>=13 and <=24
High	>=25 and <= 40
high*	>40

*In case of specific high risk factors or rp >40

and it is evaluated via 3 separate procedures based on further enquiries commensurate to the actual risk assessed: a 'green' process carried out by the Business Unit specialist, a 'yellow' process assigned to the Manager of the Business Unit in charge of the relationship with the customer and a 'red' process managed centrally by the Anti-Money Laundering Function, in accordance with the roles and responsibilities set forth in the "Group Directive on Anti-Money Laundering and Counter-Terrorism Financing".

For customers classified as requiring a simplified due diligence procedure, upon authorization of the Anti-Money Laundering Function, a specific 'white' process is to be carried out by the Business Unit Manager of the Branch in charge of the relationship with the customer, with a lower degree of the extent and frequency of requirements and a 8 year revaluation deadline, unless the conditions for applying simplified due diligence measures should cease.

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:

KYC Procedure	Evaluation*	Risk Profile	Revaluation Time Table
white	Business Unit Manager	all**	8 years
green	Business Unit Specialist	insignificant (<=5)	8 years
green	Business Unit Specialist	low (>=6 and <=12)	6 years
yellow	Business Unit Manager	up to medium*** (>=13 e <=24)	2 years
yellow	Business Unit Manager	high (>=25 and <= 40)	1 year
red	AML-CFT Department	all****	1 year

*based on the business model

**the white process is only activated for customers subject to simplified due diligence measures, authorized by the AML-CFT Department and does not take account of the risk profile

***In case of certain risk factors regardless of the rp risk score

****In case of high risk factors or rp >40

Finally, the Parent Company has implemented technologically advanced tools to support anti-money laundering processes, alongside the traditional applications already in use:

- Robotic Process Automation (RPA) applied to data collection activities in the areas of customer due diligence and reporting of suspicious transactions;

- Artificial Intelligence Engine, based on statistical components and predictive indicators (Predict Index AML) built with Data Analytics techniques, applied to the regular customer review process.

The Business Unit responsible for the relationship with the customer, usually in charge of establishing and overseeing a new ongoing relationship or executing one-off transactions, is also responsible for performing customer due diligence procedures, , periodically revaluating existing customers and conducting ongoing monitoring of the relationship.

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 enhanced due diligence 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. These limitations may concern i.e. customer access to certain types of product or result in the interruption of services offered by the Bank or Group Companies in connection with the account/relationship.

The Bank does not enter into a correspondent relationship with a shell bank and refrains from entering into relationships 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.

To this end, the Bank takes all measures to ensure that it does not deliberately and knowingly collaborate with financial institutions that in turn operate with shell banks.

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 and betting companies, including on-line gambling, casinos and Bingo operators for which authorisation and/or licenses required under Italian and international 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 231/07 in Articles 43 et seq.;
- Private limited companies or companies controlled through bearer shares, headquartered in high-risk Countries;
- Customers operating in the production and sale of light marijuana or adult entertainment venues, if it is unable to verify the authorisations required by law.

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, and in no way it supports transactions involving weapons that are controversial and/or banned by international treaties, e.g. nuclear, biological and chemical weapons, cluster bombs, weapons containing depleted uranium, anti-personnel landmines.

With regard to the production, transit and/or marketing of armament materials other than those mentioned above, the Group may support transactions that have been duly authorised by the competent authorities and are compliant with applicable and current legislation.

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, or proceeds from criminal activities, regardless of their size, in accordance with the updated organizational model and operating modes provided in reference internal regulation. Until the reporting process is complete, the Bank and/or the Group 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.

3.5 – DATA RETENTION

The Bank retains all documents and records all data obtained through the customer due diligence process, so that the traceability of customer transactions may be ensured, in order to facilitate the Bank of Italy and the FIU in performing their control functions, even for inspection purposes.

To that end, in order to allow the Bank of Italy and the FIU to access information in accordance with Annex 2 of the Provisions on data retention (AUI – Archivio Unico Informatico), the Group's financial intermediaries based in Italy set up a Single Electronic Archive (AUI) which electronically stores all identification data and other information regarding ongoing business relationships and customer transactions as required by applicable Law.

In this regard, in response to the changes introduced by the "Provisions on data retention and access to documents, data and information" and the "Provisions on aggregate data transmission", the Bank has decided to adopt certain principles of exemption from registration obligations set forth; in particular, data and information regarding transactions initiated by banking and financial intermediaries included among those listed in Article 8 of the Provision on retention and Article 3 of the Provision on aggregate data are not registered in the Single Electronic Archive (AUI).

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

To effectively manage the risks of money laundering and terrorist financing, the Bank has identified the organisational functions, resources and procedures that are consistent with and proportionate to the type and size of activity carried out, the organisational complexity as well as the operational characteristics.

The Parent Company's Anti-Money Laundering Function is in charge of monitoring such risks, the responsibility for which at Group level is assigned to the Chief Risk Officer, who reports directly to the Board of Directors and also has the central responsibility for the function for the Group's Italian Subsidiaries.

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 Bank 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 Anti-Money Laundering Function 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.