MONTEPASCHI GROUP
POLICY ON THE 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

2.1 AML-CFT REGULATORY FRAMEWORK

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 Financing Terrorism (CFT) 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 (hereinafter, also the Decree).

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, as amended by the Bank of Italy Provision of 1 August 2023;
- **Provision of 28 March 2019** setting out instructions on **objective communications;**
- **Provision of 30 July 2019** laying down implementing provisions on **customer due diligence,** as amended by the Bank of Italy Provision of 13 June 2023;

- **Provision of 24 March 2020** laying down implementing provisions for **storage and availability** of documents, data and information regarding anti-money laundering and counter-terrorism financing;
- **Provision of 25 August 2020** laying down provisions for submitting **aggregated AML reports.**
- **Provision of 12 May 2023** on **anomaly indicators** for intermediaries to facilitate the identification of suspicious transactions, effective from 1 January 2024.

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 CFT 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 organisational and behavioural 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 behaviours 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.

2.2. THE REGULATORY FRAMEWORK CONCERNING EMBARGOES

All the restrictive measures established to counter the financing of terrorism and all the illicit or suspicious activities that threaten international peace and security can be either commercial, such as import/export restrictions from/to a Country, or financial, such as the partial or total blocking of funds transfer but also operational limitations and freezing of funds.

Restrictive measures include international financial sanctions, also referred to as embargoes, implemented by the Italian State, foreign agencies (OFAC) and supranational organizations (UN, EU) through a series of obligations that the bank is required to comply with.
Certain restrictive measures (sanctions) are imposed to all the UN Member States by the Council to implement the Resolutions adopted by the UN Security Council under Chapter VII of the UN Charter. Furthermore, sanctions may be adopted, or autonomously decided, by the European Union through Council regulations, which are immediately enforceable in each Member State to ensure their timely and simultaneous application.
On an international level, there are regulations that establish specific prohibitions or restrictions on investing in certain industrial sectors or importing/exporting from/to "high or significant risk Countries". In particular, it regards **UN Security Council (UNSC) resolutions under Article 41 of Chapter VII of the UN Charter,** through which restrictive measures are imposed with regard to persons and/or Countries, and the **Council Regulation 428/2009/EC of May 5, 2009** and subsequent amendments, with regard to the Community framework, by which an EU regime is established in order to control exports, transfer, brokering and transit of dual-use items.
Finally, at national level, embargoes are regulated as follows:

- Primary Legislation:
  - Legislative Decree No. 221/2017, which amended and simplified authorization procedures to export dual-use items and technologies and sanctions on trade embargoes as well as all types of export operations of proliferating materials.

- Secondary Legislation:
  - Bank of Italy Provision of 27 May 2009 containing operational guidelines for exercising stronger controls over the financing of weapons of mass destruction proliferation programs.

Finally, all the regulations issued by the US Authorities are relevant to the Bank's activity in view of the reputational aspects and the reference to these regulations in contractual undertakings involving the potential application of sanctions with extraterritorial effect (so-called US 'secondary sanctions'). Such regulatory provisions are contained in the US Patriot Act and in the measures relating to economic and trade sanctions issued by the US Government through the Treasury Department's Office of Foreign Assets Control (OFAC).

3 – GROUP MODELS AND METHODOLOGIES

3.1 – GENERAL ASPECTS

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

- adopt appropriate organisational 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.

With regard to international sanctions (so called Embargoes), legislation requires certain measures to be taken, such as:

- imports/exports blockade from or to a country and related regulations. The ban may be either general, involving all types of goods unless specifically authorised, or restricted to certain types of goods, e.g. armaments (refer to customs code);
- total or partial restrictions on financial transfers from/to a Country;
- prior authorization requirement in order to carry out transfers;
- Obligation to notify transfers (outgoing or incoming);
- Prohibition to fund, provide financial assistance or make subsidised loans available to the Government (directly or in some cases indirectly via affiliated companies or participation in international financial institutions);
- prohibition to finance customers operating with sanctioned countries;
- implementation of restrictive measures against Russian and Belarusian subjects.

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).

3.2 - CUSTOMER DUE DILIGENCE

3.2.1 – GENERAL ASPECTS

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.

Due diligence obligations:

- are fulfilled:
  - towards new customers before the establishment of an ongoing relationship or the execution of an occasional transaction;
  - towards existing customers, whenever due diligence is appropriate in light of a change in the level of money laundering or terrorist financing risk associated with the customer or where there are suspicions or doubts as to the accuracy or adequacy of information previously obtained from the customer;
- and consist of the following activities:
  - 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 continuous monitoring throughout the entire duration of the customer relationship.

To this end, the Bank - through its employees and/or through agents/financial advisors authorised to make off-premises offers and who come into direct contact with the Customer- obtains the information required by the regulations and collects any other relevant documentation as specified in this Policy and in the Bank's procedural documents.

3.2.2 - Customer remote onboarding

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. In this case, identification is based on the acquisition of the qualified electronic signature certificate, which is 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.

However, the customer due diligence measures adopted by the Bank do not automatically prevent or deny access to financial services for high-risk customers or entire categories of high-risk customers who would be entitled to such access under the applicable regulations.

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 standard or enhanced customer due diligence measures to customers according to a risk-based approach.

3.2.3 – Pre-Implementation Assessment and ongoing monitoring of processes for opening remote relationships.

The processes of remote customer identification and onboarding are formalized and detailed in the internal regulations. The model for overseeing these processes includes:

I. the preliminary assessment of the remote onboarding solution (so-called Pre-Implementation Assessment) aimed at:
(i) assessing the adequacy of the solution in terms of the completeness and accuracy of the data and documents to be collected, as well as the reliability and independence of the information sources used;

(ii) assess the impact of the use of the solution on business risks including operational, reputational and legal risks through the involvement of the relevant technical and specialist functions;

(iii) identify mitigation measures and corrective actions for each identified risk;

(iv) define ex ante tests to assess ICT and fraud risks and end-to-and tests on the operation of the solution.

II. ongoing monitoring of the onboarding solution adopted through periodic and event-driven controls to ensure its proper functioning over time (so-called Ongoing Monitoring).

III. the review of preliminary assessment in the remote onboarding solution (so-called Pre-Implementation Assessment) when structural changes in the solution adopted or certain events occur such as:

(i) changes in the exposure to risks in the areas of anti-money laundering and countering the financing of terrorism, as well as embargoes;

ii) shortcomings detected for our solution to work;

iii) an increase in attempted fraud;

(iv) changes in legislation.

3.2.4 – Standard due diligence obligations

Generally, the Bank uses a risk-based approach to identify the types of customers to whom ordinary due diligence measures may be applied. This includes cases where "low risk indicators" are present, as indicated in Annex 1 of the Bank of Italy's Provision on customer due diligence of 30 July 2019 (hereinafter "The Provision").

The "low risk indicators" relevant for the application of standard measures relate to the type of customer, executor or beneficial owner, the geographical area of residence or where the headquarters are located, and specific products, services and distribution channels. In all cases, the identification and verification of the customer, executor and beneficial owner are carried out and all data and documents necessary for their full identification (e.g., name, legal nature, registered office and, where available, tax code) are obtained and retained, thus reducing the depth, scope and frequency of the other steps of the standard due diligence process.

3.2.5 – Enhanced due diligence obligations

The Bank applies **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 the Decree. These enhanced measures include, inter alia, the involvement of roles of responsibility commensurate with the level of risk identified in relation to the customer.

The involvement of the Anti-Money Laundering Function is required in the following cases:

- natural and legal persons included in the lists of persons or entities subject to fund-freezing measures under European regulations or decrees pursuant to Legislative Decree 109/07, as well as those closely associated with them;
- a cross-border correspondent banking relationship established 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 ultimate beneficial owner is a politically exposed person[1];
- situations involving risk elements that require the application of specific confidentiality measures;
- situation with a higher risk of money laundering or terrorist financing due to objective, environmental or subjective contingencies;
- customers classified as a "Trust", Money Transfer services and Virtual Currency Exchanges;
- MP Fiduciaria customers;

Moreover, before entering into, continuing or maintaining an ongoing relationship with Politically Exposed Persons or Correspondent Entities of third countries, it is necessary to obtain the appropriate authorisation from the General Manager or his delegate, after obtaining the opinion of the Anti-Money Laundering Function. In the case of delegates pursuant to Article 25 of

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

Legislative Decree 231/07 belonging to the Anti-Money Laundering Function, this authorisation is included in the enhanced due diligence process.

In all other cases, the application of enhanced measures is commensurate with the level of risk attributed to the customer. If the risk is considered medium/high, or if certain risk factors are present regardless of the score assigned, the involvement of the Head of the business unit responsible for the commercial management of the customer is required.

Examples of such cases are:

- customers residing or based in high-risk third countries or in the case of ongoing relationships, professional services and operations involving high risk countries;
- legal entity customers with an Executor identified as a PEP or indirect PEP, regardless of the risk profile;
- services offered through networks of financial agents, financial advisers, contractors and agents;
- 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 engaged in a type of economic activity that is particularly exposed to the risk of money laundering or in "controversial" sectors of activity[3] or cash-intensive commercial activities, such as cash-for-gold, money exchange, gambling/betting, including on-line, arms industry, mining, waste collection and disposal, renewable energy production, companies operating in the crypto-asset sector, construction, procurement of pharmaceutical instruments;
- 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).

The involvement of the Head of the business unit responsible for the commercial management of the customer is also required in the event of any IT errors that might prevent the real-time calculation of the customer's money laundering risk.

Enhanced verification measures include acquiring additional information on the customer and the beneficial owner, investigating the purpose and nature of the relationship and increasing the frequency of procedures aimed at ensuring continuous monitoring during the ongoing relationship. In cases where it has not been possible to identify the beneficial owner in accordance with the objective and substantial criteria set out in Article 20 of the Decree, the reasons must be documented.

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

[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.

(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 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 of Legislative Decree 231/07 (resident and non-resident PEPs);
- individuals residing in Italy who hold **public office, that do not fall** within the definition of PEPs, but are nevertheless exposed to a significant risk of corruption and money laundering;
- 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).

3.3 - CUSTOMER PROFILING

The Bank adopts suitable procedures aimed at defining the money laundering and terrorist financing risk profile (RPs) 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 over time (so-called profiling).

On the basis of customer profiling, which is also conducted periodically, the Bank applies standard or enhanced measures, which include the involvement of roles of responsibility

commensurate with the customer's identified risk level. The prior opinion of the Anti-Money Laundering Function is required in accordance with the responsibilities set out in document 1030D01289, the "*Group Anti-Money Laundering and Counter-Terrorism Financing Directive*".

Furthermore, the Bank has put in place an IT procedure to assess the customer's risk profile and to consistently define a re-evaluation time frame appropriate to the risk level calculated; the re-evaluation frequency depends on the process identified in the last assessment carried out or, in the absence of a KYC questionnaire, on the customer's risk profile, as specified below:

<table>
<tr><th>Risk class (RP)</th><th>Score</th><th>Due diligence process</th><th>Evaluation</th><th>Re-evaluation frequency</th></tr>
<tr><td>Immaterial</td><td><=5</td><td rowspan="2">Standard</td><td rowspan="2">Automatic Acceptance</td><td>8 years (*)</td></tr>
<tr><td>Low</td><td>>=6 e <=12</td><td>6 years</td></tr>
<tr><td>Medium</td><td>up to medium*(**)
>=13 e <=24</td><td rowspan="2">Enhanced</td><td rowspan="2">Business Unit Manager</td><td>2 years</td></tr>
<tr><td>High</td><td>>=25</td><td>1 year</td></tr>
<tr><td colspan="5"></td></tr>
<tr><td colspan="2">In the case of specific risk elements</td><td>Enhanced</td><td>Validation Function AML</td><td>1 year</td></tr>
</table>

*Expected also for positions authorised by the AML-CFT Function independently of the defined risk score

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

Moreover, 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.

Finally, within the scope of the advanced tools mentioned above, "trigger events" have been identified that can prompt an earlier re-evaluation. These include changes to the personal data of the beneficial owner and legal representative, or changes to the RP generated by the presence of certain high-risk factors as set out in the Provision.

The responsibility for a customer's due diligence process rests with the customer's relationship management unit, which typically handles the establishment of new ongoing relationships,

executes any occasional transactions, periodically re-evaluates existing customers, and ensures ongoing monitoring of the customer relationship.

3.4 - 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 products 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.

3.5 – REPORTING OF SUSPICIOUS TRANSACTIONS

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.

3.6 – DATA RETENTION

The Bank retains all documents and records all data obtained through the customer due diligence process, ensuring the traceability of customer transactions to facilitate the Bank of Italy's and the FIU's control functions, including inspections.

To this end, the Group's financial intermediaries based in Italy set up a Single Electronic Archive (*Archivio Unico Informatico* or *AUI*) that enables them to provide information to the Bank of Italy and the FIU according to the technical standards specified in Annex 2 of the Provisions on data retention. This archive electronically stores all identification data and other information related to ongoing business relationships and customer transactions as required by applicable Law.

In this regard, in response to the recent updates 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 for exemption from registration obligations as expressly provided. In particular, data and information regarding transactions arranged by banking and financial intermediaries, which fall under the cases specified in Article 8 of the Provisions on Data Retention and Article 3 of the Provisions on Aggregate Data are not recorded in the Single Electronic Archive.

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

As for transactions and ongoing 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 KEY PROCESSES

4.1 – MONEY-LAUNDERING AND TERRORIST FINANCING RISK MANAGEMENT

The "Money-Laundering and Terrorism Financing Risk Management" process is the process by which the following activities are carried out within the Group in order to mitigate the risk of non-compliance with anti-money laundering and counter-terrorism financing requirements:

- Identifying the risk of non-compliance with AML requirements, through continuous monitoring of changes in legislation and the assessment of impacts on business processes and procedures, as well as AML-CFT risk identification and assessment on a risk-based approach;
- Management and mitigation of money laundering and terrorism financing risk by implementing and monitoring non-compliance risk mitigation actions set out in the

Annual Plan (AML Plan) or identified by the Governance of the Bank as applied by all relevant business functions in the implementation of procedures (internal regulations, IT applications, operational processes, controls);

- Compliance checks (ex-ante and ex-post) in the regulatory areas assigned by ownership by defining and monitoring risk indicators and their evolution over time. The aim is to find possible non-compliance situations as well as to carry out the ex-ante and ex-post control activities;
- Provide advisory and support on AML/CFT issues either to business structures or to the Top Management Bodies in business issues and processes where the risk of money laundering and terrorist financing is relevant, by carrying out the fulfilments foreseen by the supervisory regulations and performing a preliminary conformity assessment in this area when offering new products/services;
- AML/CFT risk monitoring and control by analysing the information flows received from Level I and other control functions related to operational anti-money laundering requirements and by implementing risk monitoring controls and constantly verifying their adequacy;
- Conducting AML self-assessment by carrying out preliminary activities necessary to complete the so called "System" and "Operational" Questionnaires as well as to determine the residual risk;
- Reporting to Top Corporate Bodies and Supervisory Authorities, more specifically preparing to report annually to the Corporate Bodies and the Supervisory Board as well as preparing to report periodically on the activities performed and any specific requests from the Supervisory Authorities;
- Providing specific AML/CFT training courses by organizing an adequate training plan together with the other corporate functions responsible for training. The aim is to achieve a continuous training of employees and collaborators.

The Group's specific rules and responsibilities regarding this process are detailed in the internal document, "Group Anti-Money Laundering and Counter-Terrorism Directive".

4.2 – MANAGEMENT OF RELATIONS WITH SUPERVISORY AUTHORITIES TO COMBAT MONEY LAUNDERING AND TERRORISM FINANCING

The AML/CFT Regulatory Relationship Management process is the process by which activities are carried out within the Group to manage, analyse, direct and monitor all communications with regulators on matters related to anti-money laundering and counter terrorism financing. The objective is to oversee these activities, including the archiving of documents in a single repository.

The following activities are carried out as part of this process:

- Management of relations with Supervisory Authorities (Anti-Money Laundering), managing, analysing and addressing communications and requests from Supervisory Authorities regarding conformity in the field;
- Handling of administrative procedures related to anti-money laundering through the examination of counterclaims relating to administrative proceedings notified to the Bank by the competent authorities (GdF and FIU) as well as representing the Bank before the MEF, by being responsible for the proceedings census in the related application and for allocation to the Provision for Risks and Charges and possible sanctions payments, in coordination with the Budget Function.

The Group's specific rules and responsibilities regarding this process are detailed in document 1030D01289, the "Group Anti-Money Laundering and Counter-Terrorism Directive".

4.3 – MANAGEMENT OF OPERATIONAL REQUIREMENTS TO COMBAT MONEY LAUNDERING AND TERRORISM FINANCING

The AML/CFT Operational Requirements Management process is the process by which the following activities are carried out within the Group in order to comply with regulatory requirements:

- Limiting the use of cash and bearer securities, by carrying out regulation requirements concerning limitations to the use of cash and bearer bonds/securities;
- Managing adequate customer due diligence obligations, by executing the activities of customer due diligence (or enhanced due diligence) in the cases established by the Italian Law (Legislative Decree 231/07 and subsequent amendments) depending on the customers risk profile;
- Managing suspicious transactions reporting obligations, by carrying out the activities of reporting of suspicious transactions by executing the delegations of authority of the Board of Directors (ex art. 36 Legislative Decree 231/07) and monitoring requests received from the FIU;
- Managing obligations regarding counter terrorism financing, by verifying the transposition of Sanction List updates as well as reporting the FIU and MEF on capital freezing measures (ex-Legislative Decree 109/07);
- Managing data retention obligations, by verifying the reliability of the Information System by updating the Archivio Unico Informatico (AUI), making any revisions, periodically sending aggregated data to the FIU and transmitting to the FIU the notifications required by regulations;
- Monitoring the proper implementation of international financial sanctions (financial embargoes);
- Limitations on deposits with Russian/Belarusian subjects, by monitoring the timely application of internal rules that transpose EU regulations on limitations on deposits with Russian/Belarusian nationals/entities or residents;
- Peripheral monitoring of anti-money laundering and counter-terrorism obligations, by supervising the situation related to customer due diligence (KYC), following the arrangement of pending practices, supporting the Network on other issues regarding the subject and assessing the opportunity to maintain relationships.

The Group's specific rules and responsibilities regarding this process are detailed in the internal document, "Group Anti-Money Laundering and Counter-Terrorism Directive".

5 - MPS GROUP ORGANIZATIONAL FRAMEWORKS AND CONTROL BODIES

To effectively manage the risk 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 Head of the Level 1 AML-CFT

Function, who reports directly to the Chief Executive Officer and also performs this function centrally 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 centralised unit for the management of the internal violations reporting system, with the responsibility of supervising the activities of receiving, analysing and evaluating alerts forwarded by employees via the Whistleblowing procedure.

6 – REVISION AND UPDATE OF THE POLICY

The Anti-Money Laundering Function reviews the policy at least annually, updates it if and where necessary and prepares the text for approval by the Board of Directors on the proposal of the Chief Executive Officer.

Any amendments to the Policy approved by the Board of Directors of the Parent Company are subsequently communicated to all branches and subsidiaries (Italian and foreign) for implementation.