Policy for governing the risks of money laundering and terrorist financing

Modena, 18 December 2025 – summary version

Version 5

CONTENTS

1 General aspects

Summary of main topics

This "Policy for governing the risks of money laundering and terrorist financing" (hereinafter also the "Policy"), in line with the Provisions on Organisation, Procedures and Internal controls published by the Bank of Italy on 26 March 2019, describes the duly justified solutions adopted by the Parent Company on the different relevant profiles relating to conduct, organisation, procedures and internal controls. The objective is to ensure full compliance with primary and secondary legislation and effectively counter the (even inadvertent) involvement of the Group Banks and Companies in money laundering and terrorist financing.

The document also defines:

- the preconditions of the process for governing and managing the risk of money laundering and terrorist financing, i.e. the process whereby risk is identified, measured, assessed, assumed, monitored and controlled;
- based on the provisions of the "Group Policy - Internal Control System" (hereinafter "ICS Policy"), the roles and responsibilities of the corporate bodies and organisational units involved in managing the risk of money laundering.

The document also addresses the main areas which the anti-money laundering and counter-terrorism legislation is structured into, including:

- customer due diligence;
- obligations of data and information storage and transmission of the aggregate data to the Bank of Italy's Financial Intelligence Unit (FIU);
- active cooperation required of the Group's banks and companies through the reporting of suspicious transactions;
- personnel training obligations.

The prohibitions and thresholds relating to the use of cash and bearer negotiable instruments are also outlined.

As specifically regards the aspects of countering terrorist financing, the document lays down the obligations regarding the freezing of funds and economic resources, and the associated disclosure and reporting obligations. The same also applies to programmes for countering the development of weapons of mass destruction and countering the activities of States that threaten peace and international security.

2 Content of regulatory sources

2.1 Risk of Money Laundering and Terrorist Financing

2.1.1 Definition of Risk

Consistent with the provisions of the Group Risk Map, the risk of money laundering and terrorist financing (hereinafter also "risk of money laundering") is defined as "*the risk arising from the violation of legal, regulatory and self-regulatory provisions which serve to prevent the use of the financial system for the purposes of money laundering, terrorist financing or financing of programmes for the development of weapons of mass destruction, as well as the risk of involvement in cases of money laundering, terrorist financing or financing of programmes for the development of weapons of mass destruction*".

In the classification of risks adopted by the Bank, the risk of money laundering and terrorist financing refers, in the so-called "first pillar" domain, to operational risk.

2.1.2 Risk governance

2.1.2.1 Organisational Solution of the Parent Company

The Anti-Money Laundering Function

To follow up on the provisions laid down by the Supervisory Authority on anti-money laundering organisation, procedures and controls[1], the Parent Company has established the Anti-Money Laundering Function. The responsibility of carrying out tasks that are legislatively assigned to the Anti-Money Laundering Function is assigned to the Chief AML Officer (CAMLO, see below), assisted by the organisational structures that are generally identified as the "CAMLO Area". The CAMLO Area reports to the Parent Company's managing body (Chief Executive Officer).

With a view to implementing the principle of proportionality referred to by the Bank of Italy - in particular, taking into account the complexity of the activities carried out, total assets, the number of employees and customers, and the risk governance strategy generally adopted - while ensuring efficient risk governance, the entire structure is kept separate from the other Corporate Control Functions.

To correctly carry out its mandate, the Anti-Money Laundering Function:

- complies with the regulatory principle of proportionality and with the specificity of the definition of risk that it is called upon to control, by keeping a separate structure from the rest of the Corporate Control Functions;
- complies with the regulatory requirement of independence, as it is organisationally separate from the Functions involved in risk-taking and line control[2];
- is provided with suitable resources, in terms of quality and quantity, to perform the tasks required with regard to staff numbers, composition and technical-professional knowledge;
- reports directly, or via the Anti-Money Laundering Officer, to the corporate bodies, and has access to all the data, information, archives, corporate assets and all the Group activities performed both at the central offices as well as at the peripheral organisations; it also has access to any and all information that is relevant for its own tasks, and that may be also obtained by means of individual interviews with the staff.

Member of the management body responsible for AML/CFT

In BPER Banca, the role of Member of the management body responsible for AML/CFT is assigned to the Chief Executive Officer (CEO), as a member of the Board of Directors and a subject possessing, as required by the aforementioned provisions:

- at a personal level, the appropriate knowledge, skills and experience in anti-money laundering risk, policies, controls and procedures;
- as part of the corporate position held, in-depth knowledge of the business model of the Bank, the Group and the reference sector;
- adequate availability in terms of time commitment, to ensure the effective performance of the role held as specified below in paragraph 3.3;
- adequate operational support given mainly, in consideration of assessments of consistency with the Group's control system and operational efficiency, by the organisational units of the Parent Company's Anti-Money Laundering Function.

It should also be taken into consideration that the appointment of the Chief Executive Officer as Anti-Money Laundering Officer for the Parent Company is fully in line with the structure and functioning of the Control Function Coordination Committee and the Control and Risk Committee.

The Officer is also always granted full access to all the Bank's activities and to any information relevant to the

[1] See Bank of Italy Provisions on anti-money laundering organisation, procedures and controls of 26 March 2019 and subsequent amendments and additions.

[2] In line with the ICS Policy, the functions deemed to be involved in risk-taking are structures that: contribute to the definition of commercial policies or risk-taking strategies; authorise risk-taking; are remunerated according to corporate results or have objectives that involve risk taking; are coordinated by subjects included in the previous categories.

performance of his/her tasks.

The policies adopted by the Bank to control and manage potential situations of conflict of interest for the Officer and the criteria generally applied to assess, including on an ongoing basis, the persistence of the adequate conditions in terms of time commitment and the limit to the number of offices that can be held simultaneously, are defined in a dedicated governance document valid at a Group level[3], to which reference is made in full.

As set forth by the Supervisory Authority, the Officer must be appointed at the first renewal of the Corporate Bodies, and in any case no later than 30 June 2026.

Chief Anti-Money Laundering Officer

Taking into consideration the requirements established by secondary legislation and with a view to ensuring adequate time commitment, the Parent Company identifies as the Head of the Anti-Money Laundering Function one specific resource, that is entrusted with the responsibility of the Anti-Money Laundering Function of the Parent Company: the Chief AML Officer (CAMLO).

To ensure an efficient management of the money laundering risk, the CAMLO meets adequate independence, competence, professionalism and reputation requirements[4], and in particular:

- holds a role in the Group that lends authoritativeness to the function, requiring it to be placed in an adequate hierarchical-functional position;
- is relieved from direct responsibility for operational areas, to avoid the emergence of conflicts of interest;
- has knowledge of current and prospective company and group operations;
- has adequate knowledge of external and internal regulations;
- reports directly to the Management Body (Chief Executive Officer) and has access to the Board of Directors and to the Board of Statutory Auditors without restriction, either directly or through the Anti-Money Laundering Officer;
- is appointed, with adequate substantiation, by the Board of Directors, having consulted the Board of Statutory Auditors.

Officer responsible for reporting suspicious transactions (Company Delegated Officer)

The company delegation to suspicious transaction reporting pursuant to art. 36, paragraph 6, of Legislative Decree 231/07, is conferred on the Chief Anti-Money Laundering Officer (CAMLO) through an ad-hoc deed of delegation by the Legal Representative.

Officer responsible for ensuring compliance with restrictive measures

In accordance with the provisions of the EBA Guidelines (EBA/GL/2024/14), the senior staff member responsible for ensuring compliance with European Union and national restrictive measures is identified in BPER as the Head of the Anti-Money Laundering Function (CAMLO).

2.1.2.2 Group Organisational Solution

General aspects

Group-wide strategic decisions regarding the governance of money laundering risk are made by the corporate bodies of the Parent Company. The decisions made take account of the specific operations and related risk profiles of each Group company, in order to establish an integrated and consistent risk management policy.

In line with the ICS Policy, the Group-wide money-laundering risk governance model - establishes that the risk of money laundering is taken at a decentralised level, but under the coordination and direction of the Parent Company, which also defines the strategic guidelines for managing the risk of money laundering and anti-

[3] Reference is made to the "*Group Policy on the Suitability of Corporate Officers and Heads of the Main Company Functions*" and to the "*Group Regulation of the Process for Managing Significant Interests of Corporate Officers*" at any time in force.

[4] See: "Group Regulation governing the process for the selection and appointment of the Head of Corporate Control Functions and personnel in charge of data processing and the performance of critical operations".

money laundering controls.

More specifically, the Internal Control System adopted by the Group generally envisages the outsourcing of the Anti-Money Laundering Function to the Parent Company by Group Banks and Companies governed by Italian Law[5], without prejudice to the responsibilities that, as provided for by regulations, remain with them, that have the task of ensuring the correct performance of operations, in particular by carrying out line controls.

Member of the management body responsible for AML/CFT of the Group

To ensure an efficient exchange of information between the Chief Anti-Money Laundering Officer of the Group and the Corporate Bodies of the Parent Company, the Member of the management body responsible for AML/CFT also holds the role of Member of the management body responsible for AML/CFT of the Group.

Anti-Money Laundering Function of the Group

The Anti-Money Laundering Function carries out management and coordination activities, with reference to its mission, for all Group Companies subject to anti-money laundering legislation and in particular:

- Banking Companies of the Group with registered office in Italy (hereinafter also "Italian Banks");
- Non-Banking Companies of the Group with registered office in Italy that are addressees of the anti-money laundering and counter-terrorism obligations[6] (hereinafter also "Non-Banking Companies");
- Both Banking and Non-Banking Companies of the Group that are addressees of the anti-money laundering and counter-terrorism obligations with registered office abroad[7] (hereinafter also "Foreign Companies").

The Anti-Money Laundering Function of the Group is entrusted to the Parent Company's Anti-Money Laundering Function, which assumes the associated coordination tasks at a Group level.

The Chief Anti-Money Laundering Officer of the Group is the Chief AML Officer of the Parent Company, who is assigned the following roles required by law in terms of the obligations for active cooperation required of the recipients:

- Group Delegated Officer for reporting suspicious transactions, as a result of the assignment, by the Group Company, of the power of representation set forth by art. 36, paragraph 6, of Legislative Decree no. 231/2007;
- Suspicious transactions reporting Officer at Group level, whose role is to direct and control, at Group level, all the Group Companies subject to the anti-money laundering regulations.

The Chief Anti-Money Laundering Officer of the Group is also assigned the role of Officer Responsible for ensuring compliance with restrictive measures at Group level.

The objective of concentrating the aforementioned roles in one resource of the Parent Company is to ensure greater cross-cutting knowledge of topics related to this subject, enhance efficiency and strengthen controls. The expertise of the identified resource, in addition to the professionalism and suitability of his/her reporting structure are, under all circumstances, sufficient to ensure and safeguard, the efficient performance of all roles held.

The Chief Anti-Money Laundering Officer of the Group has access, without restrictions, to the Board of the Directors and to the Board of the Statutory Auditors of the Parent Company and of each Company of the Group that has outsourced the AML Function to the Parent Company.

[5]The centralised model is partially waived for Group Companies with registered office abroad and for the Group Company Arca Fondi SGR, in light of specific considerations made in alignment with the content of the ICS Policy, as further specified below.

[6] As at the date of this Policy, the anti-money laundering and counter-terrorism obligations are addressed to the following Non-Banking Companies of the Group:

- BPER Factor S.p.A.;
- Sardaleasing S.p.A.;
- BPER Trust Company S.p.A.;
- Finitalia S.p.A.;
- Arca Fondi SGR.

[7] At the date of this Policy,BPER Bank Luxembourg S.A., with registered office in Luxembourg, is the only foreign Company of the Group.

2.1.2.3 Direction and Coordination of the Parent Company

BPER Banca, in its capacity as the Parent Company, is in charge of defining the guidelines for the governance and management of the risk of money laundering for the entire Banking Group, with a view to pursuing a comprehensive approach to money laundering risk and, in particular, to:

- ensuring adequate implementation of the group-wide money laundering risk governance model, strategies and policies, both at individual Group company level and at a consolidated level;
- ensuring that the money laundering risk governance model is prepared in accordance with the requirements of the Supervisory Authorities, taking into account the specificities of the Group and of its individual companies
- ensuring that the recipient corporate bodies and internal structures of the individual legal entities of the Group have the necessary information to carry out their tasks;
- establishing and approving a Group methodology to evaluate the risks of money laundering that is compliant with the method identified by the Supervisory Authority for the purposes of carrying out the "self-assessment" of the risk of money laundering[8] and conducting periodic assessments of exposure to restrictive measures;
- establishing and approving formalised procedures to coordinate and share relevant information between Group Companies. To this end, the Parent Company establishes, in particular: (i) a shared information base that allows all Group Company to assess customers consistently[9] and (ii) a structured system to exchange information with Group companies, both Italian and foreign, in relation to suspicious transactions, in addition to (iii) ensuring a direct line of communication between the individual Anti-Money Laundering Contacts/Officers of the Group Companies and the Chief Anti-Money Laundering Officer of the Group;
- establishing and approving general standards on customer due diligence, data storage, identification and reporting of suspicious transactions and compliance with European Union and national restrictive measures;
- ensuring the implementation of control systems and procedures operating at the Group level.

These principles are essentially implemented through the adoption of the model for the governance of money laundering formalised in this Policy, which guarantees clarity in the assignment of roles and responsibilities and separation between the functions responsible for the processes of assumption and operational management of risk from those in charge of the management and control of compliance risk, ensuring the independence of roles and responsibilities.

In implementing the guidelines laid down by the Parent Company, the principles of gradualness and proportionality shall also be observed, according to the specific features of the various companies belonging to the Group and falling within the scope of consolidation.

2.1.3 Risk assumption and mitigation

In order to mitigate the risk of money laundering and terrorist financing, the Group adopts the safeguards, controls and procedures identified on the basis of the instructions received from the Supervisory Authority and other competent Authorities, i.e. as a result of the assessment activities carried out by the Anti-Money Laundering Function, in particular through:

- self-assessment of the risk of money laundering and terrorist financing, structured in compliance with specific guidance from the Supervisory Authorities[10] and carried out by taking into account the risk factors associated with the type of customer, geographic area of operation, distribution channels, products and services offered, and the volume and amount of the transactions;
- the periodic assessment of the exposure of the Group Banks to restrictive measures and their vulnerability to possible circumvention of those provisions[11];
- *ex ante* and *ex post* assessments concerning:
    - operations that might have a significant impact on the Group's risk profile, due to their

[8] Bank of Italy provisions on organisation, procedures and internal controls of 26/3/2019, Section Seven.
[9] Information can be shared with foreign Group Companies within the limits allowed by the legislation of the host country.
[10] Pursuant to Bank of Italy provisions on anti-money laundering organisation, procedures and controls of 26 March 2019, Section Seven.
[11] In compliance with the provisions of EBA Guidelines/GL/2024/14 of 14 November 2024.

complexity and extraordinary nature (so-called "OMR");

- the adequacy of products, services, activities, processes or procedures that have not been adopted yet or are already in use, but that are subject to significant changes;
- entry into new markets;
- the appropriateness and/or effectiveness of the organisational measures adopted to prevent or mitigate the risk of money laundering, or the risk that a money laundering event may occur in connection with a regulatory provision not being complied with;
- in the context of extraordinary operations that result in an increase in the Group's business perimeter or customer base through external lines, the risk specifically connected to new customers, both through targeted activities towards high risk subjects and through specific second-level controls on the quality of migrated data.

It is understood that the adoption of the necessary mitigation measures is a regulatory requirement for each recipient of the reference regulations[12].

2.2 Anti-money laundering and counter-terrorism controls

This paragraph outlines the general *standards* regarding the procedures and safeguards defined by the Parent Company for the Group, in order to ensure compliance with the applicable legislation in relation to the main fields of reference, and to ensure that information is consistent and shared on a consolidated level.

2.2.1 Customer due diligence requirements

In order to comply with the reference legislation regarding customer due diligence, the Parent Company requires the following controls to be observed:

- conducting customer due diligence pursuant to articles 17 et seq. of Legislative Decree 231/07:
  - when an ongoing relationship is established;
  - when occasional transactions are performed, as instructed by the customers, that involve transferring or moving means of payment above or equal to the threshold set by the legislator[13], regardless of whether such amounts are transferred by means of one or multiple transactions that appear to be linked to each other in order to carry out a fractioned transaction;
  - when occasional transactions are performed, as instructed by the customers, that consist in the transfer of funds as defined by Art. 3, paragraph. 1, point 9 of Regulation (EU) No. 2015/847[14] of the European Parliament and of the Council, and that exceed the threshold set by the legislator[15];
  - when the Bank acts as intermediary or takes part in a cash money or bearer instruments transfer, performed for any reason between different subjects, for an amount equal to or higher than the threshold set by the legislator[16];
  - when there is a suspicion of money laundering or terrorist financing, regardless of any applicable waiver, exemption or threshold;
  - when there are doubts about the truthfulness or adequacy of the previously obtained customer identification data;
  - under all other assumed circumstances specifically described in the Anti-Money Laundering

[12] Bank of Italy Provisions on anti-money laundering organisation, procedures and controls of 26 March 2019, Section Three, note 6-quater and EBA Guidelines 2022/05, para. 40.
[13] Given the variability over time, the expression "threshold set by the legislator" shall be used in this Policy. As at the effective date of this Policy, the threshold in question is Euro 15,000, as set forth in Legislative Decree no. 231/07.
[14] Under the Regulation "transfer of funds" means any transaction at least partially carried out by electronic means on behalf of a payer through a payment service provider, with a view to making funds available to a payee through a payment service provider, irrespective of whether the payer and the payee are the same person and irrespective of whether the payment service provider of the payer and that of the payee are one and the same, including: a) a credit transfer as defined in point (1) of Article 2 of (EU) Regulation no. 260/2012; b) a direct debit as defined in point (2) of Article 2 of (EU) Regulation no. 260/2012; c) a money remittance as defined in point (13) of Article 4 of Directive 2007/64/EC, whether national or cross border; d) a transfer carried out using a payment card, an electronic money instrument or a mobile phone, or any other digital or IT prepaid or postpaid device with similar characteristics.
[15] As at the effective date of this Policy, the threshold is Euro 1,000, as set forth in Legislative Decree no. 231/07.
[16] As at the effective date of this Policy, the threshold is Euro 15,000, as set forth in Legislative Decree no. 231/07.

Manual or in other internal regulations;

- with reference to customers already acquired, provide for the renewal of customer due diligence or customer profile assessment in the event of an increase in the risk linked to the customer when major variations to the customer's subjective or operational characteristics occur, or in relation to the time or operating parameters defined at any given time;
- identify the customers[17]and verify their identity based on the documents, data or information obtained from reliable and independent sources[18];
- identify the "beneficial owner" of the customers, relationships or individual transactions and verify their identity based on the documents, data or information obtained from reliable and independent sources;
- identify the person, if any, who performs the transactions or makes requests of account opening on behalf of the customers, verify his/her identity based on documents, data or information gained from reliable and independent sources;
- verify the actual existence of the power of representation of the person carrying out the transaction, and acquire the necessary information to identify and verify the identity of the representatives with power of signature;
- verify any political exposure of the subjects identified (the "politically exposed persons") or the presence of their names in lists of terrorist supporters, by consulting specific reference "black lists" or other reliable internal and external sources;
- acquire information on the scope and nature of ongoing relationships and transactions[19], verifying the compatibility of the data and information provided by the customer, also with regard to the overall transactions performed during the relationship with the same;
- carry out, in general and prior to the opening of a new relationship, an overall assessment of reasonableness in consideration of the characteristics of the customer and the nature of the requested relationship. The assessment may also be deferred to automatic assessments resulting from process analyses that, in line with the general principle of a risk-based approach, take into account the type of product, its purpose - if directly inferred from the respective operational or contractual characteristics -, the level of risk, the customer target or distribution channel;
- adopt "enhanced" customer due diligence measures if there is a high risk of money laundering or terrorist financing in order to exclude any potential involvement in illegal activities, as early as from the first contact with the customer.
- adopt "simplified" customer due diligence measures, only if low risk ratings as defined in art. 23 of Legislative Decree no. 231/07 are identified and under circumstances specifically set forth by internal regulations;
- perform continuous monitoring activities during ongoing relationships with the customers, by examining the customer's overall transactions, verifying and updating the data and information acquired also with regard to the origin of funds and resources available to the customer, keeping documents, data and information up to date. As concerns the customers with a higher risk-rating, the information acquired shall be updated at least once a year; for customers with a moderate (medium) risk rating, the information shall be updated at least every two years; for customers with a lower risk-rating, the information shall be re-evaluated and potentially updated every five years;
- have third parties perform due diligence obligations in compliance with the provisions of articles 26 et seq. of Legislative Decree 231/07;
- refrain from establishing ongoing relationships or executing transactions, or terminating already existing ongoing relationships, if it is not possible to comply with customer due diligence obligations,

[17] The identification procedure shall be carried out in the presence of the customer or, if other than a natural person, of the person who performs transactions, without prejudice to cases of "non-face-to-face remote transactions", governed by the following paragraphs.

[18] The possibility of identifying the client on the basis of documents other than ordinary documents may be allowed in the occurrence of exceptional situations, such as, for example, requests received from asylum seekers, refugees or homeless persons, persons who do not have a residence permit but cannot be dispelled, or similar. The documentation acceptable in these circumstances and with reference to specific types of "limited operation" relationships that may be configured for these specific categories of customers must be agreed upon in advance with the Anti-Money Laundering Function.

[19] In particular, information regarding the following shall be acquired and evaluated: the purpose of the relationship; the relationships between the customer and the person who performs the transactions and between the customer and the beneficial owner; the business and economic activity performed and, in general, the business relationships of the customer. The information may be requested to the customer or gathered from the report.

considering also the opportunity to submit a report to the FIU[20], and in all instances in which abstention is expressly required by law[21];

- keep a record of the instances in which the refusal to open a new ongoing relationship or termination of an existing relationship are a consequence of assessments related to anti-money laundering in order to ensure that internal controls are carried out and any potential requests from the Supervisory Authority are followed up. Generally, the regulations and safeguards adopted by the Group's individual legal entities for the purpose of ensuring compliance with the due diligence and abstention obligations must be geared towards avoiding a generalised and preventive bias against access to banking and financial services for entire categories of persons[22];
- in the instances mentioned in the previous paragraph, customers must be informed of their right to contact the bodies in charge of managing controversies;
- refrain from executing transactions suspected of money laundering or terrorism financing. Should it not be possible to abstain, due to legal obligations that provide for document reception, the obligation of immediate reporting of the suspicious transaction shall apply.

2.2.2 Obligations of customer risk profiling

In order to ensure full compliance with applicable legislation on the obligations of customer money laundering risk assessment and risk profiling, the Parent Company establishes the following behavioural and organisational guidelines for the Group:

- identify the money laundering "risk profile" of the customers by adopting a system based on four bands and ensure this is updated on an ongoing basis, also in order to apply differentiated customer due diligence processes based on the risk linked to the customers;
- to this end, adopt processing systems defined by (or shared with) the Parent company, based on the assessment criteria and on the risk factors defined by national law and by the provisions established by the Supervisory Authorities and weighted according to their relative importance;
- in relation to the above, consider as high risk indicators, at least the following:
  - names listed in the national and international [23]anti-terrorism “black-lists”;
  - politically exposed customer (or relative beneficial owner or associated person);
  - customer involved in the reporting of a suspicious transaction;
  - customer subject to criminal investigations or preventive measures;
  - customer and/or beneficial owner resident or with registered office in "high-risk third countries";
  - customer qualified as "fiduciary mandate" or "trust";
  - subjects operating in a sector considered at greater risk of exposure to money laundering;
- consider as a low risk factor, with subsequent exclusion from the obligation of continuous re-assessment of the profile, the classification of the customer under the following Italian or EU entities:
  - banking intermediaries;
  - electronic money institutions (IMEL);
  - stock brokerage firms (SIM);
  - asset management companies (SGR);
  - investment company with variable capital (SICAV);
  - insurance companies;
  - central control authorities;
  - entities responsible for the functioning of the markets[24];
  - Public Administration and European Union Institutions;
- adopt, for the same customer, the highest risk profile among those assigned by all the Group Companies (the “Group risk profile”), requesting the Parent Company - based on clear written substantiation - to provide express authorisation if a lower risk profile is considered more appropriate than that assigned by the other Group companies[25];

[20] Specific assessments as to the conduct to be observed shall be carried out with reference to instances in which the inability to comply with due diligence obligations emerges in relation to "debit" accounts, for which the obligation to abstain from carrying out transactions does not appear to be immediately feasible.
[21] Art. 42, para. 2, of Legislative Decree no. 231/07.
[22] Reference is made to the regulatory principles introduced by the EBA Guidelines on access to financial services of 31 March 2023 (EBA/GL/2023/04), implemented by the Bank of Italy via Note n. 34 of 3 October 2023.
[23] International lists refer to those published at EU level (EU regulations) or by the UN.
[24] Pursuant to Article 3, paragraph 8, of Legislative Decree no. 231/07.
[25] In general, for customers shared with several legal entities of the Group holding active relationships with the Group's Italian Banks, the

- assess the customer risk profile periodically and, in any case, not only at pre-established deadlines on account of a higher risk rating attributed to the customer by the company's Procedures, but also upon the occurrence of events or circumstances that are likely to change the risk profile of the customer [26](e.g. when a person is identified as a PEP or in the case of major changes in the customers' operations or corporate structure).

2.2.3 Enhanced due diligence obligations

In addition to the provisions outlined in the previous sections, the Parent Company establishes the following behavioural and organisational guidelines for the Group:

- adoption of "enhanced measures" for customer due diligence in the event of a high risk of money laundering and terrorist financing. To this end, and with a view to defining the areas in which more in-depth analyses are required, the risk factors laid down by Article 24 of Legislative Decree 231/07 shall be taken into account. [27] These refer to the customer (residency in high-risk geographical areas, business activities characterised by high use of cash, etc.), to products, services or transactions (products that may help anonymity, payments received from third parties without a clear connection with the customers or their business activities etc.) or to geographical factors (high-risk third countries);
- in particular, the adoption of enhanced due diligence methods are always required in the event of:
    - ongoing relationships or occasional transactions with customers and their related beneficial owners, that are identified as politically exposed persons[28];
    - cross-border relationships with a correspondent bank or financial intermediary based in a third country, which involve the execution of payments;
    - customers residing in -or transactions with- high-risk rated third countries;
    - customers who perform transactions characterised by unusually high amounts, or transactions that may generate doubts regarding the purposes for which they are actually pre-ordered;
    - customers who are assigned a "high" money laundering risk profile based on internal calculation procedures, or for which a high risk is perceived;
    - customers whose names are listed in the national and international terrorism "black-lists";
    - relationships established with organisations that may be identified as asset vehicles, such as trust and fiduciary companies, i.e. companies incorporated or capitalised via bearer shares or invested in by trustees;
    - transactions connected with public tenders and financing;
    - relationships established with non-profit organisations;
    - special transactions in cash or bearer negotiable instruments, such as: cross-border movement of cash and bearer negotiable instruments, use of high-denomination banknotes, frequent and unjustified transactions;
- perform in-depth analyses regarding, amongst other things, the following cases potentially exposed to higher risk of involvement in money laundering:
    - recurrence of negative reputation ratings in relation to the customer, the beneficial owner or the person who performs the transactions (in connection with criminal proceedings, tax damage or administrative liability; recurrence of administrative fines due to violations of anti-money laundering provisions; existence of previous suspicious transactions reported to the Financial Intelligence Unit (FIU) or negative news from public information sources), thereby arranging to:

Parent Company, following a criterion of a presumptive nature marked by the principle of proportionality referred to in the supervisory regulations, adopts the general rule according to which, without prejudice to specific situations deserving *ad hoc* deep-dives, the broader set of information generally available and the more structured system of risk factors used for the calculation of the customer profile by the Group Banks, justify maintaining the possibly lower risk band calculated by them with respect to the risk band calculated by other Group companies.

[26] At least in the two highest risk bands.

[27] Further specified and supplemented by the Bank of Italy in the Provisions on customer due diligence published on 30 July 2019.

[28] Without prejudice to cases in which politically exposed persons act in their capacity as public administration bodies. In such cases, due diligence measures proportional to the risk actually detected shall be taken, including in consideration of the provisions of Article 23, para. 2, letter a), point 2 ("simplified due diligence").

(i) further analyse the content of said negative information, contacting the competent corporate departments or gaining further insight into public sources, also in order to consider the opportunity to refrain from continuing existing relationships;
(ii) carry out more frequent, in-depth controls on the transactions put in place by the customer, in order to promptly detect any anomalous/suspicious elements;
(iii) keep up to date the information regarding the origin of funds used for current relationships, as well as the economic and equity/asset situation of the subject concerned (acquiring, by way of example, financial statements, VAT and income tax returns, documents issued by the employer or other intermediaries);

- business activities characterised by high use of cash - such as, by way of example, cash-for-gold, money exchange, gaming and betting, money remittance - by means of:
  (i) verification - including by access to the public registers - of the existence of the required authorisations/licenses;
  (ii) acquisition of the information required to determine the expected movement of cash, in order to identify deviations that may originate suspicious elements;

- business activities linked to sectors highly exposed to corruption risks such as, by way of example, in addition to those involved in the granting of public funding and tenders: health, construction, arms trade, defence, arms industry, mining, waste collection and disposal, production of renewable energies - considered, owing to their characteristics, more exposed to the risk of money laundering or terrorist financing - such as: oil, precious metals, tobacco products, cultural artefacts and other items of archaeological, historical, cultural and religious importance, or of rare scientific value, as well as ivory and protected species - by means of:
  (i) conducting an in-depth analysis of the information on the customer's ownership and control structure, including acquiring and evaluating information on the reputation rating of the customer and of the beneficial owner;
  (ii) observing more careful and frequent analysis and update methods for the information available, in relation to both customer identification and transactions recorded;
  (iii) keeping up to date the information on the origin/destination of funds used for the transactions carried out and regarding the economic and equity situation of the subject concerned (acquiring, by way of example, financial statements, VAT and income tax returns, documents issued by the employer or other intermediaries);

- recurring presence of customers/beneficial owners that hold public roles in areas that may not be included in the definition of "politically exposed persons", but for whom major exposure to the risk of corruption exists, thereby arranging to:
  (i) acquire and keep up to date the information concerning the type of office or role held;
  (ii) constantly monitor the transactions recorded during the relationship, in order to detect, in particular, unjustified cash movement or transactions that are inconsistent with the economic profile of the subject concerned;

- services with a high degree of personalisation (such as asset management) provided to high net worth customers, arranging to:
  (i) conduct specific in-depth analyses regarding the economic/equity situation of the customer and origin/destination of the funds, in addition to
  (ii) analysing the consistency of the service provided with the position of the customer, and
  (iii) continually and regularly updating the acquired data;
  (iv) and by relying, at all stages of the due diligence process, on the support of the operators in charge of the actual management of the accounts at issue and the relationship with the customer;

- transactions (i) involving payment received from third parties without a clear connection with the customer or its activity [29]or (ii) potentially conducive to favouring the anonymity or concealment of the identity of the customer or the beneficial owner[30], by carrying out specific and targeted in-depth analyses aimed at verifying the identity of the subjects

[29]Examples include the payment of invoices by third parties unconnected with the contractual relationship or triangulations of a commercial nature not backed by appropriate supporting documentation, characterised by payments instructed by foreign companies unconnected with the invoice holder, especially if based in high-risk geographical areas. This also includes the collection of collateral from third parties not connected with the customer, especially from abroad and for substantial amounts.

[30] They include, for example, payment involving bearer shares or traceable to services related to the conversion of legal tender currency into virtual currency and vice versa.

involved and ascertaining the consistency of the transaction;

- submit the projects concerning: (i) the adoption of new products or services, (ii) any substantial changes to products or services already offered, (iii) the entry into a new market or (iv) the launch of new activities or commercial practices that may potentially expose the Group to money laundering/terrorist financing risks - to the prior assessment of the Anti-Money Laundering Function, for its verification of potential risks and consequent and appropriate mitigation actions.

2.2.4 Simplified due diligence obligations

In order to ensure compliance with applicable legislation on customer due diligence, the Parent Company establishes the following behavioural guidelines for the Group:

- confine the possibility of adopting simplified due diligence methods to the circumstances where low risk factors occur, such as:
    - opening relationships or performing transactions on behalf of Italian or EU entities considered lower risk listed in the previous section for which, despite the acquisition of ordinary information for due diligence purposes, the adoption of simplified methods is accepted to verify the data provided[31], as is the adoption of a different calibration of the risk factors normally applied in order to take account of the lower risk associated to this type of customer;
    - use of electronic money products, in the event that the conditions laid down under art. 23, paragraph 3, letter a) – f), of Legislative Decree 231/07 are cumulatively observed. In this case, it shall be possible to adopt simplified due diligence methods as regards the extent of the information gathered, as well as the methods and/or timing for their collection, based on specific evaluations that shall be referred to the Anti-Money Laundering Department;
    - other low risk factors connected with: (i) type of product (e.g., products with limited functionalities, subject to specific expense limitations or characterised by ownership transparency); (ii) repeated involvement of a subject among those admitted to listing on regulated markets; (iii) geographical areas where the customer is based/established/registered or the transaction refers to, for which a reduction of the information to gather[32], or of the update frequency may be allowed subject to a specific assessment to be conducted from time to time. Such assessment shall be based on all the elements available, if necessary also by contacting specialised monitoring units;
- the possibility of observing simplified measures shall be ruled out in the event of doubts, uncertainties or inconsistencies relating to the identification data and to the information acquired upon identification of the customer, the person who performs the transactions or the beneficial owner, or whenever money laundering or terrorist financing are suspected;
- during the term of the relationship, verify whether the pre-requisites allowing the observance of simplified due diligence measures persist, and, if such prerequisites are no longer applicable, ordinary due diligence methods shall be observed. In the same manner, ordinary verification methods shall be observed in the event that the monitoring activities on the customer's transactions, or the information acquired during the term of the relationship suggest ruling out that a low level of risk will persist or if a suspicion of money laundering or terrorist financing otherwise arises.

2.2.5 Identification and remote transactions

Customer identification and due diligence obligations must preferably be carried out in the presence of the customer. In cases in which - for subjective reasons connected to the specific case, or linked to the type of product being placed - it becomes necessary to proceed remotely (without the physical presence of the customer or of the person who performs the transactions), the Parent Company requires compliance with the following controls, differentiated in consideration of whether identification is made for the first time (a.k.a. onboarding) or whether operations are being carried out remotely by customers previously identified in person.

As concerns the remote customer onboarding process, the relevant regulations allow for the possibility of using different methods, which will be implemented compatibly with the risk-based approach and subject to validation

[31] More specifically, a statement made formally by the customer, for instance for the purpose of identifying the beneficial owner, may be deemed sufficient.
[32] For example, by acquiring, for the purposes of verification of the information relating to the beneficial owner, a declaration of confirmation of the data signed by the customer under the customer's own responsibility.

by the Anti-Money Laundering Function. However, among the various forms of remote onboarding, particular attention should be given to online onboarding.

New customer identification

A new customer (and, when legally required, the related persons performing the transactions/representatives) can be remotely identified by verifying the ID information reported on the copy of a valid ID document provided by the customer (by fax, mail, e-mail or other IT systems) by means of one of the following methods:

- from public documents, certified private deeds or qualified certificates used for generating digital signatures associated with electronic documents pursuant to Art. 24 of Legislative Decree 82/2005;
- by verifying ownership of a digital identity with at least a significant security level or a certificate used for the generation of a qualified electronic signature, or via electronic identification procedures authorised or recognised by the Agency for Digital Italy pursuant to art. 19, paragraph 1, letter a), of Legislative Decree 231/07;
- by means of a declaration issued by the Italian diplomatic representation or consular authority[33];
- using other verification methods deemed appropriate and proportionate to the risk connected with the type of customer and/or product/service, based on *ad hoc* assessments made, from time to time, by the Anti-Money Laundering Function.
  In this regard, as a result of specific assessments conducted by that structure - aimed at further analysing the risk profile and minimum security requirements to adopt in relation to the possible different remote verification methods - the following shall be generally deemed an appropriate instrument, therefore usable to perform the above-mentioned monitoring activities:
  - bank money transfer ordered by a customer from a current account already held by the same with a banking and financial intermediary based in Italy or in an EU country[34], in addition to other verification methods pursuant to this paragraph;
  - verification of the presence of RID (direct interbank relationship) alignment or, within the scope of SEPA Direct Debit, reception of a SEDA electronic flow in acceptance of a new banking order on the account issued by the beneficiary, if routed to an account held with a banking and financial intermediary based in Italy or in an EU country[35];
  - issuance of a certificate, provided by an Italian or EU banking or financial intermediary, that confirms proper identification in person of the subject in relation to the establishment of an ongoing relationship or to the performance of an occasional transaction. Such certificate shall bear, as a minimum requirement, the identification data of the subject concerned and the reference data of the ID used for the purposes of identity verification;
  - video identity recognition through webcam by an operator responsible for remote identification with concurrent verification of an ID containing a photograph of the holder and a qualified certificate for electronic signature[36];
  - feedback mechanisms based on innovative technological solutions that require forms of biometric recognition assisted by suitable security controls.

Online onboarding

With specific reference to compliance with identification requirements in case of online onboarding and in line with the Supervisory regulations on customer due diligence[37], the Parent Company adopts specific corporate regulations aimed at defining the policies and procedures which the legal entities of the BPER Group shall

[33] As indicated in art. 6, Legislative Decree no. 153/1997.
[34] The presence of an ongoing active relationship at an EU intermediary makes it possible to presume the completion by the latter of due diligence on the subject to be identified. The execution of a bank money transfer on said relationship therefore makes it possible to consider said instrument suitable to verify the subject's identity.
[35] The considerations formulated in the previous note shall apply.
[36] The video identification service can also be outsourced to qualified, duly certified third parties on the basis of specific contracts. Recognition carried out by means of video systems specifically prepared and implemented by qualified and certified persons, together with the simultaneous verification of the identification document, makes it possible to consider that the identity of the subject is verified and, therefore, that the risk associated with identification in the absence of the customer/person performing the transactions is sufficiently mitigated.
[37] Customer due diligence provisions published by the Bank of Italy on 30/07/2019, as amended by the Provisions issued by the Bank of Italy on 13/06/2023, aimed at transposing the content of the European Banking Authority (EBA) Guidelines on the use of remote customer onboarding solutions of 22 November 2022 into Italian law.

abide by. These rules, which are to be kept up to date on an ongoing basis, are drafted in accordance with the guidelines set out in this Policy.

Remote operation and due diligence of customers already identified

as regards customers whose identification data have already been acquired in relation to another current and ongoing relationship, the identification obligations shall be considered observed on the condition that the information held is updated and suited to the customer risk profile and to the characteristics of the new relationship. In this regard, the remote operation systems made available by the Group's legal entities to allow customers to remotely operate their ongoing accounts, insofar as they are supported by adequate IT security safeguards for identification of the customer and authentication of the transactions instructed, are considered appropriate for the fulfilment of the aforementioned identification obligations.

Compatibly with the risk-based approach, the methods deemed appropriate to fulfil the due diligence obligations for customers already identified also include information received:

- through an authorised representative by virtue of a suitable and valid power of attorney issued by the customer;
- by means of an attestation of the customer's signature provided by a public official;
- by means of a statement issued pursuant to Art. 27 of Legislative Decree 231/07, by other financial intermediaries located in EU/EEA countries;
- through other methods previously shared with the Anti-Money Laundering Function that shall verify their appropriateness including in relation to the risk perceived.

2.2.6 Obligations of data and information storage and transmission of aggregate data to the FIU

As concerns data and information storage and transmission of aggregate data, the Parent Company requires that the following safeguards be complied with:

- store the documents, data, information and records concerning the transactions useful to prevent, identify or ascertain possible activities of money laundering or terrorist financing, and to allow performance of the analyses conducted by the FIU or by other competent Authorities;
- specifically, store a copy of the documents acquired upon customer due diligence and of the documents and records related to the transactions, according to the provisions of the applicable national law (Articles 31 and 32, Legislative Decree 231/07) and issued by the Supervisory Authority;
- adopt storage methods suitable to assure their prompt and full accessibility and acquisition, integrity and inalterability, transparency, clearness, completeness, and traceability over time;
- store the documents, data and information acquired[38]for a period of ten years as of the termination of the ongoing relationship or following the occasional transaction performed;
- allow exemptions from the provisions contained in articles 5 and 6 of the Measures of the Bank of Italy of 24 March 2020[39] with exclusive reference to the following Italian or EU subjects:
    - banking intermediaries;
    - electronic money institutions (IMEL);
    - stock brokerage firms (SIM);
    - asset management companies (SGR);
    - investment company with variable capital (SICAV);
    - insurance companies;
    - central control authorities;
    - entities responsible for the functioning of the markets;
- notify the FIU of the aggregate data gathered in compliance with the methods established by the same (S.AR.A. - Aggregate anti-money laundering reporting flows).

In order to guarantee the traceability of customer operations and to facilitate the performance of the control functions by the Bank of Italy and the FIU, pursuant to art. 6 of the Provisions of the Bank of Italy of 24 March

[38] With regard to the foreign Companies of the Group, reference is made to other time requirements, if any, as provided for by local legislation.
[39] Provisions for the storage and provision of documents, data and information for combating money laundering and terrorist financing published by the Bank of Italy on 24 March 2020.

2020 outlined above, the BPER Group generally uses standardised electronic archives compliant with Annex 2 of said Provisions to make the data and information set forth in the aforementioned document available to the relevant authorities.

2.2.7 Personnel training obligations

With regard to personnel training, the Parent Company establishes that the following safeguards be observed:

- comply with the updated guidelines on the methods of perpetration of money laundering and terrorist financing crimes, as provided by the competent Authorities, in particular by the FIU, by Guardia di Finanza (Italian tax police) and by DIA (Anti-mafia Investigation Directorate);
- deliver training courses addressed to all employees and collaborators, so that they may receive appropriate knowledge of relevant regulations and related responsibilities, and so that they will be able to use the instruments and procedures adopted for proper application of the law provisions. More specifically, ongoing specific training shall be provided, as a priority, to personnel in close direct contact with customers or involved in the suspicious transaction reporting process;
- define high-profile, suitable training provided by external organisations for the employees in charge of money laundering risk control at the central Offices, ;
- continually update the educational material in compliance with legislative and regulatory developments;
- monitor actual attendance of employees and collaborators at the training courses provided.

2.2.8 Reporting obligations for suspicious transactions

As concerns the reporting of suspicious transactions, the Parent company establishes that the following protection measures be observed:

- report a suspicious transaction when there is knowledge, suspicion or reasonable grounds to suspect that attempted money laundering or financing of terrorism are being carried out or have been carried out;
- ensure the utmost confidentiality on the identity of the employees who report the suspicious transaction; in this regard, the interested party or third parties must not be informed that a suspicious transaction has been reported or is under way or that an inquiry regarding money laundering or financing of terrorism may be carried out;
- envisage suitable procedures for detecting potentially suspicious transactions by analysing the customers' account activity (periodic monitoring of transactions) and by identifying those transactions that are "unexpected" also based on the anomaly indicators provided by the Bank of Italy and by the FIU or other Local Authorities[40];
- envisage procedures suitable to assure that all documentation concerning transactions which must be reported to the FIU is promptly sent to the Company or Group Delegated Officer for reporting suspicious transactions by the operators and managers of operational centres or organisational units that manage relationships with the customers[41];
- envisage procedures suitable to assure traceability of the reporting process and store evidence of the assessments made by the operators and their Managers in relation to the opportunity to notify or dismiss a potentially suspicious transaction;
- envisage integrated management of corporate information coming from the Group Companies and Banks, as well as from external Companies, in relation to possible events of money laundering or terrorist financing;
- periodically send, according to the methods and criteria defined by the FIU, data and information identified based on objective criteria regarding transactions featuring risks of money laundering or

[40]A specific exception is recognised by the Parent Company with reference to specific lower risk categories, as specified in previous paragraph 2.2.2, which are generally excluded from the activation triggers for unexpected events, given the poor predictability of the rules underlying unexpected events when applied to the aforementioned subjects.

[41] Document transmission must be performed, for the Italian Banks of the Group, through the IT application provided; as regards non-banking companies, document transmission shall be made by means of a specific method that shall be defined in agreement with the Anti-money Laundering Function of the Parent Company (e.g., a Certified Electronic Mail box) to ensure as few intermediate steps as possible, speed, confidentiality and ease of discussion with the reporter.

terrorist financing (the so called “objective communications”);

- store and keep the documentation regarding the data and information collected during the reporting preparatory phase, and ensure access to such archive to internal and external entities appointed to perform inspection functions, for a period of no less than 10 years;
- promptly inform the body appointed with strategic function and the control body about the main problems that have emerged with regard to the procedures for identifying and reporting suspicious transactions;
- appoint the Company Delegated Officer for reporting suspicious transactions so that he/she may examine the reports of suspicious transactions received and may send them to the FIU (without the name of the reporting person) if they are deemed grounded based on the elements available;
- identify the subjects (operators, managers of branches and central offices) who, within the scope of customer relationship management, are bound to report, without delay, the transactions suspected of money laundering and terrorist financing to the Company Delegated Officer for reporting suspicious transactions;
- identify a “Suspicious transactions reporting Officer at Group level” as the addressee of information concerning the transactions reported or filed by the Group foreign companies to their local Authorities and by Companies that have not conferred their delegation to the Group Delegated Officer for reporting suspicious transactions, in order to further analyse both the transactions reported as well as those filed, and evaluate them from a Group standpoint[42].

2.2.9 Requirements for countering terrorism, freezing funds and economic resources and combating the proliferation of weapons of mass destruction

With regard to the freezing of funds, the Parent company requires that the following measures be complied with:

- financial services shall not be provided to natural or legal persons included in the list of persons that commit, attempt to commit, take part in, or facilitate acts of terrorism, or to an entity owned, held or controlled by a designated person or entity or whose beneficial owner is a designated person;
- funds or economic resources, either directly or indirectly, to persons subject to freezing measures or allocating them for their benefit, thus preventing the person, group or entity from obtaining funds, assets or services;
- adopt suitable measures aimed at preventing involvement in programmes for the development of weapons of mass destruction;
- in order to counter terrorism, international money laundering and the proliferation of weapons of mass destruction, introduce specific procedures to verify compliance with regulations applicable to transactions involving assets classified as “dual-use”;
- refrain from taking part, knowingly and intentionally, in activities the object or effect of which is, directly or indirectly, to circumvent the asset freezing measures;
- prevent frozen funds from being transferred, made available or used. In any case, freezing shall be without prejudice to the effects of any seizure or confiscation measures adopted within the scope of criminal or administrative proceedings;
- envisage suitable procedures to detect transactions or names of subjects that are potentially traceable to the freezing obligations in question;
- notify the Financial Intelligence Unit and the Special Currency Police Unit of the Italian tax police (Guardia di Finanza)[43] of any freezing measures adopted in compliance with the provisions of the applicable national legislation[44] and, to this end, envisage procedures suitable to ensure that the Company or Group Delegated Officer for reporting suspicious transactions promptly receives information regarding the identification of potential transactions subject to the obligations herein.

[42] Companies that have not conferred their delegation to the Group Delegated Officer for reporting suspicious transactions shall promptly send, via Certified Electronic Mail (PEC) to the Suspicious transactions reporting Officer at Group level, the documentation pertaining to the transactions reported to the relevant authorities and the reports filed.
[43] or other Authorities provided by national law.
[44] Italian Legislative Decree no. 109 of 22 June 2007

2.2.10 Limits on the use of cash and bearer-negotiable instruments

With reference to limitations on the use of cash and bearer-negotiable instruments the Parent Company requires the following measures to be complied with[45]:

- inform the Ministry of the Economy and Finance, within thirty days, of any infringement of the provisions pursuant to art. 49 of Legislative Decree: 231/07 of which knowledge has been gained[46], more specifically:
    - the prohibition to transfer cash or bearer negotiable instruments in Euro or foreign currency[47], for any reason whatsoever between different persons, when the overall value being transferred is equal to or exceeds the threshold set by law[48];
    - the obligation to indicate the name or company name of the beneficiary and to report the non-transferability clause on bank cheques issued for amounts equal to or exceeding the threshold set by law[49];
    - the obligation to indicate the name or company name of the beneficiary and the non-transferability clause on banker's drafts. In the event of banker's drafts below the threshold set by law[50], the non-transferability clause may be omitted upon written request by the customer and payment of the stamp duty required by law;
    - the obligation to endorse cheques issued to the order of the drawer solely for collection at a Bank or at Poste Italiane S.p.A.;
    - the prohibition to transfer bearer savings bankbooks;
    - the obligation to extinguish bearer passbooks by the date established by Law (31 December 2018);
- observe the required threshold amount[51] for the money remittance service pursuant to art. 1, paragraph 2, letter h-septies.1), no. 6) of Legislative Decree 385/1993 (a.k.a. "money transfer");
- issue bank cheque forms already provided with the non-transferability clause, subject to the possibility for the customer to request, in writing, the issuance of instruments not bearing the said clause, against payment of the relative stamp duty;
- collect cheques issued to the order of the drawer only if endorsed to the bank;
- issue banker's drafts indicating the name or company name of the beneficiary and the non-transferability clause, subject to the above-mentioned exception concerning amounts below the threshold set by law;
- Comply with the obligation to issue savings bank books only in the name of the bearer[52];
- comply with the prohibition to open - in whatever form - either no-name or fictitious name accounts or savings bank books, as well as to issue no-name electronic money products.

2.2.11 Safeguards for the distribution network and traders

The Parent Company requires the following referenced controls to be observed:

- define suitable organisation and IT procedures in order to ensure compliance with the provisions on countering money laundering and terrorist financing;

[45] This obligation shall be complied with only if required by local provisions in force.
[46] In the event of infringements regarding cheques, banker's drafts, bearer passbooks or similar instruments, notification must be given both by the Bank that accepts them for their deposit and by the Bank that extinguishes them, unless there is the certainty that it has already been done by the other obligor.
[47] Transfer shall be prohibited even when carried out with payments below the threshold that appear to be artificially split. However, the transfer may be carried out through banks, electronic money institutions and payment institutions (when these provide payment services other than those under art. 1, paragraph 1, letter b), number 6), of Legislative Decree No. 11 of 27 January 2010) and Poste Italiane S.p.A.
[48] As at the date of entry into force of the Policy, the threshold for the transfer of cash and bearer negotiable instruments is EUR 5,000 (threshold introduced by Law no. 197/2022).
[49] As at the date of entry into force of the Policy, the threshold amount is EUR 1,000 (this threshold was introduced by Law Decree no. 201 of 6 December 2011, converted with amendments into Law no. 214 of 22 December 2011).
[50] As at the date of entry into force of the Policy, the threshold amount is EUR 1,000 (this threshold was introduced by Law Decree no. 201 of 6 December 2011, converted with amendments into Law no. 214 of 22 December 2011).
[51] As at the date of entry into force of the Policy, the threshold amount for money remittance is EUR 1,000.
[52] Pursuant to the provisions of Italian Legislative Decree no. 231/07, art. 49, all bearer savings bank books were extinguished by 31 December 2018.

- within the scope of "collaborative arrangements" entered into with financial agents and other external parties contractually bound with the Group Companies to provide financial products and services off the bank premises, define the rules of conduct aimed at complying with the regulatory framework and therefore at countering money laundering and terrorist financing. The parties above are required to abide by such rules when performing their duties on behalf of the Group, including n particular, with regard to financial agents providing payment services or issuing/distributing electronic money, the obligation to perform customer due diligence also in the event of occasional transactions involving amounts below EUR 15,000;
- require the above-mentioned subjects to promptly inform the reference Group Company about all relevant circumstances and information for the purpose of allowing the latter to evaluate whether to report suspicious transactions;
- provide the subjects concerned with the operational instruments and procedures that may support them in meeting the anti-money laundering requirements when performing transactions;
- provide for the interruption of all relationships with financial agents and other subjects contractually bound with the Group Companies to provide financial products off the bank premises, in case of ascertained breaches of anti-money laundering/counter-terrorism laws;
- define specific training programmes for the subjects in question, so that they may acquire sufficient knowledge of the legal framework and responsibilities connected thereto, and so that they become capable of using the instruments and procedures designed to support them in performing their obligations while monitoring compliance;
- constantly monitor compliance, by the sales and distribution network, with the anti-money laundering/counter-terrorism rules of conduct contractually laid down. In particular, it shall be verified that the appointed financial agents promptly provide the Group Companies[53] with the data and information required under article 31 of Legislative Decree no. 231/07;
- perform, at regular intervals, inspections at the points of operation where the sales staff work;
- monitor collaborators' compliance with the requirements under articles 24 and 25 of Legislative Decree no. 231/2007 – “Enhanced customer due diligence”, in relation to which the Group Company provides its support;
- introduce information systems for sharing data acquired by the sales and distribution staff while performing customer due diligence, with the organisational structures where the customer relationship is originated.

2.2.12 Safeguards for activities with fiduciary companies

The Parent Company requires the following referenced controls to be observed:

- in case of relationships or transactions in the name of or traceable to fiduciary mandates, define organisational procedures to obtain from the fiduciary companies all updated and necessary information to comply with the customer due diligence obligations with specific regard to the process for the identification of the beneficial owner of the fiduciary mandate, while keeping it confidential;
- abstain from finalising any requested transaction, should it be impossible to acquire and verify the information about the identity of the beneficial owner of the fiduciary mandate;
- exclude the possibility of carrying out transactions performed and finalised independently by the beneficial owner of the fiduciary mandate with no explicit mandate by the fiduciary company;
- assess any suspicious transaction reports by taking into account the consistency of the transactions performed with the financial and economic profile of the beneficial owner of the fiduciary company;
- abide by the obligations of beneficial owner of the fiduciary company verification and identification even if the fiduciary company has an ownership interest in the share capital of the customer.

[53] Authorised entities and agents pursuant to article no. 1 para 2, letter nn), of Legislative Decree no. 231/07 submit to their respective intermediary the data acquired in relation to the customer, the the person performing the transaction and the beneficial owner within twenty days of the execution of the transaction.

2.2.13 Safeguards regarding the internal systems for reporting breaches (so-called Whistleblowing)

The Parent Company requires the following safeguards to be in place:

- adopt specific procedures for the internal reporting by employees of potential or actual breaches of the provisions laid down to prevent money laundering and terrorist financing. Such procedures shall be capable of protecting the privacy of both the subjects involved and the reporting party.

2.3 Roles and Responsibilities of the Parent Company

2.3.1 Board of Directors

- the Board of Directors defines, approves and periodically reviews the strategic guidelines and risk management policies regarding money laundering and terrorist financing and monitors compliance with European Union and national restrictive measures for BPER BANCA SpA and its Group[54];
- approves the guidelines for a comprehensive and coordinated internal control system at Group level, designed to promptly detect and manage the risks of money laundering and terrorist financing and to monitor compliance with restrictive measures, while it also ensures its effectiveness over time;
- defines and approves risk objectives and the tolerance threshold;
- with this Policy, approves the governance framework that the Bank and the Group have established for compliance with national and European restrictive measures. In this context, the Board supervises and monitors the Group's internal control system by examining the assessment on the Group's exposure to such measures, periodically drafted by the Parent Company's Anti-Money Laundering Function, for the Parent Company and the Group Banks subject to European regulations;
- approves the appointment of an "Anti-Money Laundering Function", with an independent status and a centralised role at the Parent Company for managing second-level controls on the risk of money laundering and terrorist financing. The Board identifies its tasks and responsibilities, as well as the methods for coordinating and collaborating with other corporate control functions;
- approves the appointment of the Chief Anti-Money Laundering Officer (CAMLO), the Company Delegated Officer responsible for reporting suspicious transactions (and any delegated substitute representatives), the Suspicious transactions reporting Officer at Group level and the Group Delegated Officer for reporting suspicious transactions, and approves their subsequent revocation, if any, after consulting the Board of Statutory Auditors;
- approves the appointment of the Member of the management body responsible for AML/CFT and of the Group assessing and ensuring compliance with the supervisory requirements expressly stated in the Board minutes for appointment;
- ensures that the Anti-Money Laundering Officer is promptly informed of any decision that may affect exposure to money-laundering risk;
- approves the appointment of the Officer responsible for ensuring compliance with restrictive measures for the Bank and at Group level, after consulting with the Board of Statutory Auditors;
- ensures, on an ongoing basis, that the responsibilities and tasks regarding anti-money laundering and countering terrorist financing are allocated within the Group in a clear and appropriate manner, at the same time assuring that the operating and control functions are segregated and that such functions are provided with qualitatively and quantitatively appropriate resources;
- ensures that a suitable, complete and prompt system of information flows to the corporate bodies is in place, always assuring protection of the confidentiality of the subjects that have taken part in the procedure of reporting a suspicious transaction;
- ensures that a document sharing system is put in place giving corporate bodies direct access to the

[54] In compliance with the risk-based approach, the policies shall be commensurate with the magnitude and type of risks which the company's activity is materially exposed to, including by taking into account, in this regard, the outcome of the risk-self assessment exercise performed by the Bank in accordance with the guidance provided by the Supervisory Authority (Bank of Italy provisions on anti-money laundering organisation, procedures and controls of 26 March 2019, Section Seven), as well as the outcome of the restrictive measures exposure assessment (pursuant to EBA Guidelines n. 14 and 15 of 14 November 2024) conducted on the Parent Company and the Group Banks subject to European legislation.

Anti-Money Laundering Function reports, communications with the relevant Authority and Supervisory measures or imposed sanctions;

- defines and approves the formalised procedures for coordination, information sharing and connection between the Parent Company and the Group Companies as regards the management of money laundering risk;
- examines and approves, at least every year, the reports on the activity performed and inspections carried out by the Anti-Money Laundering Function, the adequacy of its human and technical resources and the self-assessment report on money-laundering risks[55];
- examines and approves the restrictive measures exposure assessment of the Group Banks, as well as the effectiveness of the Anti-Money Laundering Function, including the adequacy of the human and technical resources assigned to it, within this scope[56];
- supervises and monitors, through the Anti-Money Laundering Function, the ongoing adequacy and effectiveness of policies, procedures and controls regarding compliance with restrictive measures;
- promotes the adoption of appropriate corrective measures and concurrently assesses their effectiveness as a result of any shortcomings or deficiencies identified during controls, which the Board must be promptly notified of;
- the Board approves the principles for managing relationships with money-laundering/terrorist financing "high-risk" customers and identifies the safeguards to be adopted in order to mitigate the risks associated with transactions with higher risk third countries[57], constantly monitoring their effectiveness.

2.3.2 Board of Statutory Auditors

- audits the Internal Control System set up to monitor the risk of money laundering and terrorist financing;
- monitors compliance with anti-money laundering regulations and makes sure that the System adopted is complete, appropriate and functional;
- evaluates the appropriateness of existing procedures applicable to customer due diligence, information storage and the reporting of suspicious transactions;
- analyses the reasons for the shortcomings, deficiencies and irregularities identified and promotes the adoption of appropriate corrective measures;
- expresses its opinion on the decisions concerning the appointment of the Chief Anti-Money Laundering and the Company Delegated Officer responsible for reporting suspicious transactions and for compliance with restrictive measures, as well as on the definition of the overall architecture for managing and controlling the risk of money laundering and terrorist financing;
- as regards relationships with the Supervisory Authorities, the members of the Board of Statutory Auditors shall promptly inform the Bank of Italy of all facts or actions that come to their knowledge during performance of their functions and that may constitute serious, repeated or systematic violation of applicable legal provisions and of the related enforcement provisions.

2.3.3 Chief Executive Officer[58]

- provides for the implementation of strategic guidelines and risk management policies on money laundering and terrorist financing, as well as those aimed at ensuring compliance with the restrictive measures, as defined by the Board of Directors, and is responsible for taking the necessary measures to ensure the effectiveness of the organisation and monitoring systems on this matter;
- in order to comply with the aforesaid obligation, the Chief Executive Officer examines the

[55] See previous note.
[56] See note n. 102.
[57] More specifically, as part of the Board's strategic decision-making, the Board shall also define instances when decisions pertaining to initiating or continuing relationships with certain customer categories indicative of a significantly high risk of money-laundering/terrorist financing, shall be deferred to a Senior Executive, possibly requiring the latter to seek prior advice from the Anti-Money Laundering Function. The above determinations are reflected in specific internal regulations.
[58] See Bank of Italy provisions of 26 March 2019 on "anti-money laundering organisation, procedures and controls", Section Three, "Management body".

organisational and procedural changes proposed by the CAMLO and formalises and motivates any decision not to accept them;

- with reference to compliance with restrictive measures, adopts an adequate risk management framework and an internal control system, adequate and independent from the activity subject to control;
- oversees the implementation of an internal control system aimed at promptly detecting and managing money laundering risk, in line with the guidelines laid down by the Board of Directors, and ensures its effectiveness over time. In this regard, the Chief Executive Officer also takes into account evidence resulting from risk self-assessment procedures carried out by the Bank, consistently with the instructions received from the Supervisory Authority and the outcome of the restrictive measures exposure assessment[59];
- puts in place the initiatives and actions required to assure that the architecture of the control functions is consistent with the complexity of the activities performed, the size of the internal organisation, the type of products and services offered and the extent of the risk that may be associated with the customer characteristics, guaranteeing the overall reliability of the Internal Control System over time;
- establishes the coaching and training programmes for employees and collaborators on the obligations arising from the regulatory framework on anti-money laundering and terrorist financing;
- sets up the appropriate tools to allow ongoing monitoring of the activities carried out by employees in order to detect any anomalies arising in the conduct, information flows with contact persons and the company departments, and in the relationships with customers;
- ensures that the operating procedures and information systems are appropriate in order to comply with anti-money laundering and counter-terrorism obligations;
- provides for the organisational and procedural changes necessary to ensure that adequate safeguards are in place for protection against the offences of money laundering and terrorist financing;
- establishes the organizational and operational structure necessary to effectively comply with the strategy adopted by the Board of Directors concerning the restrictive measures and, in this context, approves procedures and controls which must be proportionate to the Bank's exposure to such measures and adequate to ensure compliance with them;
- defines the actions and procedures to ensure prompt fulfilment of reporting obligations to the Authorities, as laid down by the legislation on money laundering and terrorist financing;
- as regards reporting suspicious transactions, the Chief Executive Officer defines and oversees the implementation of a procedure to ensure consistency in conduct, full use of relevant information and traceability of the assessment process;
- adopts measures aimed at guaranteeing strict confidentiality on the identity of the persons that have taken part in the reporting procedure as well as the tools (including electronic tools) used for detecting suspicious transactions;
- defines and oversees the implementation of information procedures aimed at ensuring that the employees, at all organisational levels, and the bodies with control functions are aware of the risk factors and company anti-money laundering and terrorist financing safeguards in connection with their tasks and responsibilities;
- defines the management procedures for relationships with customers identified as money laundering/ terrorist financing "high risk", under the principles laid down by the Board of Directors;
- entrusts one or more Senior Executives with the task of initiating or continuing regular relationships or operations with subjects or categories considered as money laundering/ terrorist financing higher risk, under the principles laid down by the Board of Directors and set forth in this Policy;
- in remote operations, the Chief Executive Officer ensures the adoption of IT procedures to ensure automatic detection of potentially suspicious transactions and, more generally, to comply with anti-money laundering regulations;
- ensures that the management bodies of the other companies of the Group carry out the tasks and

[59] See Bank of Italy provisions of 26 March 2019 on "anti-money laundering organisation, procedures and controls", Section Seven.

functions set out in the EBA Guidelines[60] regarding compliance with restrictive measures and that they implement the policies and procedures defined by this Policy in that regard.

2.3.4 Member of the management body responsible for AML/CFT

- ensures that the Board of Directors and the Chief Anti-Money Laundering Officer are provided with the information necessary to fully understand the significance of the money laundering risks which the Bank is exposed to;
- ensures that the issues and actions proposed by the Chief Anti-Money Laundering Officer are assessed by the management body;
- monitors the adequacy and proportionality of anti-money laundering policies, procedures and internal control measures, taking into account the characteristics and risks which the Bank is exposed to. To this end, the Member of the management body responsible for AML/CFT uses the information acquired through the Group information flow system in use or directly acquires the information needed for its assessment from the Bank functions through the Anti-Money Laundering Function;
- assists the Board of Directors in assessing the organisational structure and staffing of the Anti-Money Laundering Function;
- ensures that the Corporate Bodies are periodically informed of the activities carried out by the CAMLO and of discussions with the Authorities[61];
- informs the Corporate Bodies of any breaches and critical issues in anti-money laundering of which the officer has become aware, and proposes organisational and procedural solutions deemed appropriate to address the breaches, having consulted the second level specialist function (Anti-Money Laundering Function);
- verifies that the CAMLO has direct access to all the information needed to carry out his/her tasks, has sufficient human and technical resources and tools available, and is informed of any anti-money laundering shortcomings identified by other internal control functions and the Supervisory Authorities;
- submits to the Parent Company's Corporate Bodies the "Group Anti-Money Laundering Function Report" (including the risk self-assessment and the annual plan), prepared yearly by the Parent Company's Anti-Money Laundering Function.

2.3.5 Member of the management body responsible for AML/CFT of the Group

- ensures that the Parent Company's Corporate Bodies have the information needed to fully understand the significance of the money laundering risks which the Group is exposed to, for them to perform their respective duties;
- ensures that the Chief Anti-Money Laundering Officer of the Group performs his/her duties efficiently.

2.3.6 Chief Corporate & Investment Banking Officer

The Chief Corporate & Investment Banking Officer (CCIBO):

- assesses and authorises the opening of current accounts with correspondent institutions in third Countries for all Group Companies governed by Italian and foreign Law that are subject to anti-money laundering obligations.

2.3.7 Chief AML Officer

The Chief AML Officer - CAMLO - is assigned the following roles referred to in the external regulations:

- Chief Anti-Money Laundering Officer of BPER Banca and the Group's Italian banks and non-banking companies pursuant to the Provisions on organisation, procedures and internal controls

[60] EBA Guidelines (EBA/GL/2024/14), paragraph 4.1.2, point 11.
[61] The information referred to is generally included in the Anti-Money Laundering Report submitted yearly to the Corporate Bodies for approval.

adopted by the Bank of Italy on 26 March 2019;

- Chief Anti-Money Laundering Officer of the Group;
- Officer responsible for reporting suspicious transactions (Company Delegated Officer) for BPER BANCA pursuant to art. 36, paragraph 6, of Legislative Decree 231/07;
- Group Delegated Officer for reporting suspicious transactions under Italian Law, that have delegated the role under art. 36, paragraph 6, of Legislative Decree no. 231/2007 (Group Delegated Officer);
- Suspicious transactions reporting Officer at Group level[62];
- Senior Executive, as set out by the Bank of Italy's Provisions of 30 July 2019 for BPER Banca S.p.A. and other Italian Group Banks applicable to operations with the following type of customers: (i) Italian and foreign politically exposed persons; (ii) individuals residing or entities headquartered in high-risk third countries; (iii) "Russian" or Belarusian" individuals or entities;
- Officer responsible for ensuring compliance with restrictive measures as defined by the EBA Guidelines of 14 November 2014[63];
- Officer responsible for ensuring compliance with restrictive measures at Group level.

2.3.8 Senior Executive delegated to authorise transactions with high-risk Countries

- in compliance with specific enhanced due diligence measures set forth in the internal regulations, receives and assesses transactions from and to high-risk Countries, that are requested to be carried out by the operating units, for the purpose of either authorising or denying their execution;
- periodically reports on the outcome of the aforesaid process.

3. Regulatory framework of reference

- Directive (EU) 2015/849;
- Legislative Decree no. 109 of 22 June 2007;
- Legislative Decree no. 231 of 21 November 2007;
- Legislative Decree no. 231 of 8 June 2001;
- Provisions governing the organisation, procedures and internal controls aimed at preventing the use of intermediaries for the purposes of money laundering and terrorist financing published by the Bank of Italy on 26 March 2019;
- Customer due diligence provisions for combating money laundering and terrorist financing published by the Bank of Italy on 30 July 2019;
- Provisions for the storage and sharing of documents, data and information for combating money laundering and terrorist financing published by the Bank of Italy on 24 March 2020;
- Instructions on objective communications published by the Financial Intelligence Unit (FIU) and the Bank of Italy on 28 March 2019;
- Provisions for submitting aggregate anti-money laundering reports published by the FIU and the Bank of Italy on 25 August 2020;
- Bank of Italy Provisions of 1 August 2023. Amendments to Bank of Italy “Provisions on organisation, procedures and internal controls for anti-money laundering purposes” of 26 March 2019, adopted to incorporate the EBA Guidelines of 14 June 2022 on policies and procedures in relation to compliance management and the role and responsibilities of the AML/CFT Compliance Officer under Article 8 and Chapter VI of Directive (EU) 2015/849;

[62] For all Group Companies governed by Italian or foreign law, that are subject to AML regulations.
[63] For BPER and all the Group Banks governed by Italian law.

- Bank of Italy Provisions of 27 November 2024. Amendments to Bank of Italy “Provisions on organisation, procedures and internal controls for anti-money laundering purposes” of 26 March 2019, aiming at introducing periodic anti-money laundering reporting;
- Bank of Italy Note no. 35 of 3 October 2023. Guidelines amending Guidelines EBA/2021/02 on customer due diligence (EBA/GL/2023/03 – Guidelines on risks associated with customers that are not-for-profit organisations - NPOs).
- EBA Guidelines on remote customer onboarding for the purposes of article 13(1) of Directive (EU) 2015/849 (EBA/GL/2022/15);
- Bank of Italy Note no. 15 of 4 October 2021. EBA Guidelines on customer due diligence (EBA/2021/02);
- Bank of Italy Note no. 34 of 3 October 2023. EBA Guidelines on policies and controls for the effective management of money laundering and terrorist financing (ML/TF) risks when providing access to financial services (EBA/GL/2023/04);
- EBA Guidelines on internal policies, procedures and controls aimed at ensuring the implementation of the European Union and national restrictive measures (EBA/GL/2024/14 e EBA/GL/2024/15), implemented by the Bank of Italy respectively with note no. 48 of 8 April 2025 and no. 52 of 19 May 2025.