Group policy for governing the risks of money laundering and the financing of terrorism

Modena, 10 June 2021 – summary version

CONTENTS

1 MAIN TOPICS COVERED

2 PURPOSE OF THE DOCUMENT

3 REGULATORY REFERENCE FRAMEWORK

4 BEHAVIOURAL GUIDELINES FOR THE BPER GROUP

5 ROLES AND RESPONSIBILITIES

1 Main topics covered

The document addresses the main areas on which anti-money laundering and counter-terrorism legislation is based, including:

- customer due diligence;
- obligations of data and information storage and of transmission of the aggregate data to the FIU (financial intelligence unit);
- active cooperation required from 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 securities are also outlined.

As specifically regards the aspects of combatting the financing of terrorism, the obligations regarding the freezing of funds and the associated reporting obligations are reported.

The main updates to the previously in force "Group Policy for governing the risk of non-compliance with the anti-money laundering and counter-terrorism legislation" (2019 edition), simultaneously repealed, concern:

- the update of certain regulatory provisions made to Legislative Decree 231/07 in 2019/2020, and in particular: by Legislative Decree no. 125 of 4 October 2019 , by Decree Law no. 124 of 26 October 2019, regarding tax matters and Decree Law no. 76 of 16 July 2020 regarding digital simplification and innovation;
- the acknowledgement of certain provisions for the storage and provision of documents, data and information for combatting money laundering and financing of terrorism published by the Bank of Italy on 24 March 2020;

2 Purpose of the document

The Policy lays down the guidelines applicable to the conduct, organisation, procedures and internal controls that the Group adopts to assure full compliance with primary and secondary legislation, in order to effectively react to the involvement, even unintentional, of the Banks and Companies belonging to the BPER banking Group in money laundering and terrorism financing.

3 Regulatory reference framework

- EU Directive 2015/849;
- Legislative Decree no. 109 of 22 June 2007;
- Legislative Decree no. 231 of 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 terrorism financing published by the Bank of Italy of 26 March 2019;
- Customer due diligence provisions for combating money laundering and terrorism financing published by the Bank of Italy on 30 July 2019;
- Provisions for the storage and provision of documents, data and information for combating money laundering and financing of terrorism published by the Bank of Italy on 24 March 2020.

4 BEHAVIOURAL GUIDELINES FOR THE BPER GROUP

Definition of risk

Consistent with the provisions of the Group Risk Map, the risk of money laundering and terrorism 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, terrorism 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, terrorism financing or financing of programmes for the development of weapons of mass destruction”.

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

Risk governance

The Group is equipped with a risk governance model, according to which the risk of money laundering is assumed at the decentralised level, but under the coordination and direction of the Parent Company, which defines the strategic guidelines for managing the risk of money laundering and anti-money laundering controls, while risk management activities are carried out centrally by the Parent Company.

The organisational solution provides for the identification, by the Parent Company, of an organisational unit responsible for the anti-money laundering department[1], on the staff of the Chief Executive Officer and who operates at the Group companies, making use of a "Anti-money Laundering Department Reference Officer".

The Anti-Money Laundering Department carries out, in particular, 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[2] (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[3] (hereinafter also "Foreign Companies").

The Anti-Money Laundering Department also performs a second level control function regarding anti-money laundering and counter-terrorism for the Parent Company and the Group Companies with registered office in Italy.

In order to correctly perform its office, the Anti-Money Laundering Department shall:

- act independently, since it is separate from the other control functions and is detached, in terms of organisation, from the functions involved in risk assumption;
- be 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;
- report directly to the bodies with strategic supervisory functions and have 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 shall also have 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.

The Head of the Parent Company's Anti-Money Laundering Department (CAMLO) is assigned the following roles indicated in the regulations:

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

[2] As at the date of this Policy, the Non-Banking Companies of the Group that are addressees of the anti-money laundering and counter-terrorism obligations are:

- Emilia Romagna Factor S.p.A. (BPER Factor);
- Sardaleasing S.p.A. (SARDAFACTORING);
- Optima S.p.A. SIM;
- BPER Trust Company S.p.A.
- Finitalia S.p1

[3] At the date of this Policy, the foreign Companies of the Group are BPER Bank Luxembourg S.A., with registered office in Luxembourg.

- Head of the anti-money laundering department pursuant to the Provisions on organisation, procedures and internal controls adopted by the Bank of Italy on 26 March 2019;
- Responsible Officer for BPER BANCA pursuant to art. 36, paragraph 6, of Legislative Decree 231/07;
- Responsible Officer for Group Companies under Italian Law, that have delegated the role envisaged in art. 36, paragraph 6, of Legislative Decree no. 231/2007 (Group Responsible Officer);
- Group Responsible Officer for foreign companies without assignment of the delegation of the role as provided for by art. 36, paragraph 6, of Legislative Decree no. 231/07.

BPER Banca, in its capacity as Parent Company, is responsible for defining the guidelines on governance and management of the risk of money laundering for the entire Banking Group and, in particular:

- ensuring adequate implementation of the model for the governance of the risk of money laundering and Group strategies and policies, both at the individual Group company level and at the consolidated level;
- ensuring that the model for the governance of the risk of money laundering is prepared in accordance with the requirements of the Supervisory Authorities, taking into account the specific features of the Group and of the individual Group companies belonging to it;
- establishing and approving a Group methodology for evaluating the risks of money laundering compliant with that identified by the Supervisory Authority for the purposes of carrying out the "self-assessment" of the risk of money laundering[4];
- establishing and approving formalised procedures for the coordination and sharing of relevant information between Group Companies. To this end, the Parent Company establishes, in particular, a shared information base that enables all Group Companies to evaluate customers in a homogeneous fashion[5];
- establishing and approving the general standards on customer due diligence, data storage and identification and reporting of suspicious transactions.

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.

Risk assumption and mitigation

In order to mitigate the risk of money laundering and terrorism financing, the Group adopts the protection measures and implements the controls and procedures identified based on the instructions received by the Supervisory and other competent Authorities, i.e. as a result of the assessment activities carried out by the Anti-Money Laundering Department, in particular through:

- self-assessment of the risk of money laundering and terrorism financing, organised in compliance with specific guidelines of the Supervisory Authorities[6] and carried out by taking into account the risk factors associated with the type of customer, geographic area of the transactions, distribution channels and the products and services offered;
- “ex ante” evaluations concerning the appropriateness of activities or processes and procedures not yet adopted, in order to represent the risk of money laundering that would be assumed if such activities/processes/procedures were performed or introduced without adopting further mitigation measures, and in order to identify proposals aimed at mitigating the same risk;

[4] Bank of Italy provisions on organisation, procedures and internal controls of 26/3/2019, Section Seven.
[5] The sharing of information with the foreign Companies of the Group applies to the limits permitted by the legislation in the host country.
[6] Pursuant to Bank of Italy provisions on anti-money laundering organisation, procedures and controls of 26 March 2019, Part Seven.

- "ex post" evaluations concerning verification of the appropriateness and/or effectiveness of the organisational measures adopted to prevent or mitigate the risk of money laundering, i.e. the risk that the event connected with failure to observe a regulatory provision occurs.

Anti-money laundering and counter-terrorism controls

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

4.1 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,[7] regardless of whether such amounts are transferred by means of an individual transaction or several 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 transferring funds as defined by Art. 3, paragraph. 1, point 9 of (EU) Regulation No. 2015/847[8] of the European Parliament and Council, and that exceed the threshold set by the legislator[9];
    - when the Bank acts as intermediary or takes part in a cash money or bearer security transfer, performed for any reason between different subjects, having an amount equal to or higher than the threshold set by the legislator[10];
    - when there is a suspicion of money laundering or terrorism financing, regardless of any applicable derogation, exemption or threshold;
    - when there are doubts about the truthfulness or adequacy of the previously obtained customer identification data;
- with reference to customers already acquired, envisage renewal of the customer due diligence or assessment of the customer profile in the event that the risk linked to the same customer has increased, or in the event of major variations in their subjective or operational characteristics;
- identify the customers[11]and verify their identity based on the documents, data or information obtained by reliable and independent sources;
- identify the person who performs the transactions, if any, and the "beneficial owner" and verify their identity based on the documents, data or information obtained by reliable and independent sources.
- verify the actual existence of the power of representation, when the customer is a company or body, and acquire the necessary information to identify and verify the identity of the representatives with power of signature;

[7] Given the variability over time, the expression "threshold set by the legislation" shall be used in this Policy. At the date of entry into force of the Policy, the threshold in question is EUR 15,000, as set forth in Legislative Decree 231/07.
[8] The Regulations mentioned define as "fund transfer" a transaction made, at least partially, via electronic means on behalf of a transferor by a payment service provider, with the aim of making funds available to the beneficiary through a payment service provider, regardless of the fact that the transferor and the beneficiary are the same subject and that the transferor's payment service provider and that of the beneficiary coincide. Among these transactions we can mention: a) bank money transfer, as defined under Article 2, point 1), of (EU) Regulation no. 260/2012; b) direct debit, as defined under Article 2, point 2), of (EU) Regulation no. 260/2012; c) money remittance, both national or cross-border, as defined by Article 4, point 13), of directive 2007/64/EC; d) money transfer made using a payment card, an e-money tool or a mobile phone, or any other prepaid or post-paid digital or information device having similar characteristics.
[9] At the date of entry into force of the Policy, the threshold in question is EUR 1,000, as set forth in Legislative Decree 231/07.
[10] At the date of entry into force of the Policy, the threshold in question is EUR 15,000, as set forth in Legislative Decree 231/07.
[11] The identification procedure shall be carried out in the presence of the customer or, if this is not a private individual, of the person who performs transactions, subject to cases of "non-face-to-face transactions", governed by subsequent section 3.2.5.

- verify any political exposure of the subjects identified (the so called “politically exposed persons”) and namely the repeated presence of their names in the list of terrorism supporters, also by consulting the specific reference "black lists";
- acquire information on the scope and nature of ongoing relationships and transactions[12], 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;
- adopt "enhanced" customer due diligence measures if there is high risk of money laundering or terrorism financing in order to exclude, already when first establishing contact with the customer, any potential involvement in illegal activities (see, more specifically, subsequent section 3.2.3);
- evaluate the adoption of "simplified measures" for customer due diligence if low risk ratings are identified, as defined by art. 23 of Legislative Decree 231/07 (see, more specifically, subsequent section 3.2.4);
- perform continuous monitoring activities during ongoing relationships with the customers, by examining the overall transactions of that same customer, verifying and updating the data and information acquired also with regard to the origin of funds and resources available to the customer, keeping the documents, data and information owned up to date. As concerns the customers having a higher risk-rating, the information acquired shall be updated at least every year; for customers having a moderate (medium) risk rating, the information shall be updated at least every three 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, considering also the opportunity to submit a report to the FIU;
- refrain from executing transactions suspected of money laundering or terrorism financing. Should it not be possible to refrain from the above, due to legal obligations that provide for document reception, the obligation of immediate reporting of the suspicious transaction shall apply.

4.2 Obligations of customer risk profiling

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

- identify the money laundering "risk profile" of the customers and ensure this is updated, also in order to apply differentiated customer due diligence processes based on the risk linked to the same customers;
- to this end, adopt processing systems defined by the Parent company (or however shared with the same), based on the assessment criteria and on the risk factors defined by national reference legislation and by the provisions established by the Supervisory Authorities and weighted based on their relative importance;
- In relation to the above, consider as indicators of high risk, at least the following:
    - names listed in the national and international [13]counter-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";
    - fiduciary mandates and trusts;
    - subjects operating in a sector considered at greater risk of exposure to money laundering phenomena;

[12] 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 of the customer or gathered from the report.

[13] International lists refer to those published at EU (EU regulations) or UN level.

- consider as a low risk factor, with subsequent exclusion from the obligation of continuous revaluation 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[14];
    - the Public Administration and the European Union Institutions;
- adopt, for the same customer, the highest risk profile among those assigned by all the Group Companies (the so called "Group risk profile"), requesting the Parent Company - based on clear written motivations - to provide express authorisation if a lower risk profile is considered more appropriate than that assigned by the other Group companies;
- periodically assess the customer risk profile and, in addition to pre-established deadlines, such risk profile shall be assessed based on any higher risk rating attributed to the customer by the corporate Procedures, applicable when events or circumstances that may change the risk profile occur (e.g. when a person is identified as PEP, in the case of major changes in the customers' activity or in their corporate shareholding).

4.3 Enhanced due diligence obligations

In order to ensure full compliance with applicable legislation regarding customer due diligence, the Parent Company establishes for the Group, in addition to the provisions outlined above, the following behavioural and organisational guidelines:

- adopt "enhanced measures" for customer due diligence in the event of a high risk of money laundering and terrorism financing. To this end, the risk factors laid down by Article 24 of Legislative Decree 231/07[15] shall be taken into account. These refer to the customer (residency in high-risk geographical areas, business activities characterised by high use of cash money etc.), to products, services or transactions (products that may help anonymity, payments received by third parties without a clear connection with the customers or their business activities etc.) or are linked 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;
    - cross-border relationships with a correspondent banking or financial intermediary based in a third country, which involve the execution of payments;
    - customers residing in high-risk rated third countries, or transactions with the same 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 so- called national and international terrorism "black-lists";
    - the relationships established with organisations that may be identified as means of asset mediation, such as trust and fiduciary companies, i.e. companies incorporated or capitalised via bearer shares or with shares owned by trustees;
    - the transactions connected with public tenders and financing;

[14] Pursuant to Article 3, paragraph 8, of Legislative Decree 231/07.
[15] Further specified and supplemented by the Bank of Italy in the provisions on customer due diligence published on 30 July 2019.

- the relationships established with non-profit organisations;
- special transactions in cash or bearer securities, such as: cross-border movement of cash and bearer securities, 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:
  - repeated application, in relation to the customer, the beneficial owner or the person who performs the transactions, of negative reputation ratings (connected with criminal proceedings, damage to the tax authorities or administration responsibilities; repeated application of administrative fines due to violations of anti-money laundering provisions; existence of previous reporting of suspicious transactions sent to the Financial Intelligence Unit (FIU) or of negative news from public information sources), performing the following:
    (i) further analyse the content of said negative information, contacting the competent corporate departments or conducting further investigations on public sources, also in order to evaluate the opportunity to refrain from continuing current relationships;
    (ii) carry out more frequent and 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 money - such as, by way of example, cash-for-gold, money exchange, gaming and betting, money remittance sectors - by means of the following:
    (i) verification - 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, building, arms trade, defence, arms industry, mining, waste collection and disposal industries, production of renewable energies - or considered, owing to their characteristics, more exposed to the risk of money laundering or terrorism 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 proprietary and control assets, 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 both to customer identification and to the transactions recorded;
    (iii) keeping up-to-date the information on the origin/destination of funds used for the account activity, as well as 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);
  - repeated listing of customers/beneficial owners that hold public roles in fields that may not be defined as "politically exposed persons", but for whom a major exposure to the risk of corruption exists, performing the following:
    (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 customers who own high asset amounts, envisaging the following:
    (i) conducting specific in-depth analyses regarding the economic/equity situation of the Customer connected with the funds,

(ii) in addition to analysing the consistency of the service provided with respect to the position of the same customer
(iii) and continually and regularly updating the acquired data;

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

- submit the projects concerning the adoption of new products and commercial practices - that may potentially expose the Group to money laundering/terrorism financing risks - to prior assessment of the Anti-Money Laundering Department, so that they may verify the possible risks as well as consequent and appropriate mitigation actions.

4.4 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:

- the possibility of observing simplified due diligence methods is allowed in the event of low risk factors, such as:
  - opening relationships or performing transactions on behalf of Italian or EU entities considered lower risk listed in previous section 3.2.2. for which, despite the acquisition of ordinary information for due diligence purposes, the possibility of adopting simplified methods is recognised from the perspective of verification of the data provided, in addition to the adoption of a different calibration of the risk factors normally used in order to take account of the lower risk associated to said 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/the transaction refers to, for which a reduction of the information to gather[16] , 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 terrorism financing are suspected;
- it is established that, during the term of the relationship, the pre-requisites that allowed the observance of simplified due diligence simplified measures shall be verified to check whether they persist, and it is envisaged, if such prerequisites are no longer applicable, that ordinary due diligence methods 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 that a low risk level persists or, however, if money laundering or terrorism financing are suspected.

[16] 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 his own responsibility.

4.5 Identification and non-face-to-face transactions

In order to comply with reference legislation on customer due diligence, the Parent Company establishes that the following protection measures shall be observed in those cases where the identification or operational activities are identified when the customer (or the person who performs the transactions) are not physically present:

- observe the customer identification obligations by acquiring the identification data, alternatively:
    - from public documents, certified private deeds or eligible certificates used for generating digital signatures associated with information documents pursuant to Art. 24, Legislative Decree 82/2005;
    - by verifying ownership of a digital identity with the greatest security level or of a certificate used for generating digital signatures, 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;
    - a declaration issued by the Italian Diplomatic Mission or Consular authority[17];
- 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;
- aside from the above mentioned cases, meet the identification obligations by verifying the ID details information declared by the customer on the copy of a valid ID document sent by fax, mail, e-mail or other similar methods and by further verifying - in addition to the *standard* verification methods pursuant to section 3.2.1 - the data acquired, using 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 Department of the Parent Company.
  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[18], 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[19];
    - digital and remote video identification systems configured with an audio/video recording setting compliant and specifically regulated by the Bank of Italy[20];
    - video identity recognition through webcam by an operator responsible for remote identification with concurrent ID verification. ID must contain a picture and qualified certificate with digital signature;
    - issuance of a certificate, by an Italian or EU banking or financial intermediary, that confirms proper identification of the subject person 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;
    - feedback mechanisms based on innovative technological solutions that provide for forms of

[17] As indicated in art. 6, Legislative Decree 153/1997.
[18] 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.
[19] The considerations formulated in the previous note are valid.
[20] Reference is made to the video-identification procedure referenced in the Provisions published by the Bank of Italy on 30 July 2019 regarding customer due diligence, Annex 3. Respect for the guidelines and criteria reported therein makes it possible to consider the obligation of acquisition and verification customer identification data satisfied.

biometric recognition assisted by suitable security controls.

4.6 Obligations of data and information storage and of transmission of the aggregate data to the FIU (financial information unit)

In order to comply with the reference legislation concerning data and information storage and sending of aggregate data, the Parent Company establishes that the following protection measures be observed:

- store the documents, data, information and records concerning the transactions useful to prevent, identify or ascertain possible activities of money laundering or terrorism financing, and to allow performance of the analyses conducted by the FIU or by other competent Authorities;
- specifically, keep 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 applicable national legislation (articles 31 and 32, Legislative Decree 231/07) and of the Supervisory Authority;
- adopt storage methods suitable to assure prompt and full accessibility and acquisition, integrity and inalterability, transparency, clearness and completeness, as well as historical recording of the same documents;
- store the documents, data and information acquired[21]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[22] 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 functioning of the markets;
- notify the FIU of the aggregate data gathered in compliance with the methods established by the same (the so called S.AR.A. - Aggregate anti-money laundering reports 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 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 said authorities.

4.7 Personnel training obligations

In order to comply with the reference legislation concerning personnel training, the Parent Company establishes that the following protection measures be observed:

- comply with the updated guidelines on the methods of perpetration of money laundering and terrorism 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 differentiated by role and function, addressed to all employees and associates, so that they may receive appropriate knowledge of relevant legislation and related responsibilities, and so that they will be able to use the instruments and procedures adopted for proper application of the law provisions;
- define, for the persons in charge of risk protection measures at the central Departments, high-profile and suitable training, provided by external organisations;

[21] With regard to the Group foreign Companies, reference may be made to any other different period of time provided for by local legislation.

[22] Provisions for the storage and provision of documents, data and information for combatting money laundering and financing of terrorism published by the Bank of Italy on 24 March 2020.

- continually update the educational material in compliance with legislative and regulatory developments;
- monitor actual attendance of employees and associates to the training courses provided.

4.8 Reporting obligations for suspicious transactions

In order to comply with the reference legislation concerning 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;
- envisage procedures suitable to assure that all documentation concerning transactions which must be reported to the FIU is promptly sent to the Responsible Officer by the operators and managers of operational centres or organisational units that handle the relationships with the customers[23];
- envisage procedures suitable to assure traceability of the reporting processes and store evidence of the evaluations expressed by the operators and by 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 phenomena of money laundering or terrorism 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 terrorism financing (the so called “objective communications”)[24];
- store and keep the documentation regarding the data and information collected during the investigation 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 Responsible Officer 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 relation management, are bound to report, without delay, the transactions suspected of money laundering and terrorism financing to the Responsible Officer;
- identify a “Group Responsible Officer” as recipient of the information concerning the transactions reported by the Group foreign companies to their local Authorities, or the transactions filed by the same, in order to further analyse both the transactions reported as well as those filed, and evaluate

[23] Document transmission must be performed, for the Group Banks, 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 Department of the Parent Company (e.g., a Certified Electronic Mail box provided).

[24] As regards non-banking companies of the Group under Italian law and foreign Companies, the aforementioned obligation shall be complied with only if contemplated, respectively, by primary and secondary applicable legislation as well as by local legislation.

them from a Group viewpoint[25];

- entrust the "Anti-Money Laundering Department" with the responsibility of ensuring information flows for suspicious transaction reports, so that these may be addressed to the attention of the strategic function and supervisory function bodies of the Parent Company, of the Banks or of the Group Companies.

4.9 Compliance measures on counter-terrorism, freezing of funds and economic resources, and on countering the proliferation of mass destruction weapons

In order to comply with the reference legislation concerning freezing of funds, the Parent company establishes that the following protection measures be observed:

- financial services must not be provided to private individuals and legal persons included in the list of persons that commit, attempt to commit, take part in, or facilitate acts of terrorism;
- rule out altogether the possibility of placing, either directly or indirectly, funds or economic resources at the disposal of persons subject to freezing measures or of allocating them for their benefit, thus preventing the person, group or entity from obtaining funds, assets or services;
- adopt suitable protection measures aimed at preventing involvement in development programmes for the proliferation of weapons of mass destruction;
- in order to counter terrorism and international money laundering events, as well as the proliferation of mass destruction weapons, envisage specific supervisory procedures to verify that the legislation applicable to transactions involving assets classified as “dual use” assets are observed;
- refrain from taking part, knowingly and intentionally, in activities the object or effect of which is, directly or indirectly, to circumvent the freezing measures of the funds;
- prevent frozen funds from being transferred, made available or used. In any case, the freezing shall be without prejudice to the effects of any seizure or confiscation measures adopted within the scope of criminal or administrative proceedings;
- envisage procedures suitable to detect transactions or names of subjects that are potentially connected with the scope of the freezing obligations dealt with;
- notify the Financial Intelligence Unit and the Special Currency Police Unit of Guardia di Finanza (Italian tax police) of any freezing measures adopted in compliance with the provisions of applicable national legislation[26] and, to this end, envisage procedures suitable to assure that the Responsible Officer promptly receives the information notice regarding the identification of potential transactions subject to the obligations herein.

In order to ensure the sharing of information at Group level, the foreign Companies of the Group:

- send specific information to the Responsible Officer regarding the communications outlined in this paragraph sent to the competent local Authorities.

4.10 Limits on the use of cash and bearer securities

In order to comply with the reference legislation concerning reporting of suspicious transactions, the Parent company establishes that the following protection measures be observed:

- 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[27]:
    - the prohibition to transfer cash or bearer bankbooks or bearer securities in Euro or foreign

[25] The Foreign Companies shall promptly send, via Certified Electronic Mail (PEC) to the Group Representative, the documentation pertaining to the transactions reported to the competent local authorities as well as that pertaining to the transactions filed.
[26] Italian Legislative Decree no. 109 of 22 June 2007
[27] In the event of infringements regarding cheques, banker’s orders, bearer passbooks or similar securities, notification must be made both by the Bank accepting them for their deposit and by the Bank that extinguishes them, unless there is the certainty that this has already been performed by the other obligor.

currency[28], for any reason whatsoever between different persons, when the overall value being transferred exceeds or is equal to the threshold set by the legislator[29];

- the obligation to indicate the name or company name of the beneficial owner and affix the non-transferability clause on the bank cheques issued for amounts above or equal to the threshold set by legislator[30];
- the obligation to indicate the name or the company name of the beneficiary and to report the non-transferability clause on banker's orders. In the event of banker's orders below the threshold set by the legislation[31] the non-transferability clause may be omitted upon written request by the customer and payment of the stamp duty prescribed by law;
- the obligation to endorse bank 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 amount threshold set by legislator[32] for the money remittance service pursuant to art. 1, paragraph 1, letter b), no. 6) of Legislative Decree 11/2010 (so called "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 securities 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 orders indicating the name or the company name of the beneficiary and the non-transferability clause, subject to the above-mentioned exception concerning amounts below the threshold set by law;
- observe the obligation to issue savings bankbooks solely in the name of the bearer[33];
- comply with the prohibition to open - in whatever form - accounts or savings bankbooks in anonymous form or with fictitious names, as well as the issuance of anonymous electronic money products.

4.11 Protection measures for distribution networks and mediators

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

- define suitable organisation and IT procedures in order to ensure observance of the provisions on countering money laundering and terrorism financing;
- within the scope of "collaboration agreements" stipulated with financial agents and other external subjects connected with the Group Companies by means of contractual obligations designed to provide off-site products and services, define the rules of conduct aimed at complying with the reference legislation and therefore at countering money laundering and terrorism financing. Such rules shall be observed by the above subjects when performing activities on behalf of the Group, among which, with special reference to financial agents , when providing payment services or when issuing/distributing electronic money, the obligation to perform customer due diligence also in the event of occasional transactions involving amounts below EUR 15,000;

[28] The transfer shall be prohibited even when carried out with payments below the threshold, which appear to be artificially fractioned. 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..

[29] At the date of entry into force of the Policy, the threshold for the transfer of cash and bearer securities is EUR 2,000 (threshold introduced by Decree Law no. 124 of 26 October 2019).

[30] At the date of entry into force of the Policy, the amount threshold is EUR 1,000 (this threshold was introduced under Decree Law no. 201 of 6 December 2011, converted with amendments by Law no. 214 of 22 December 2011).

[31] At the date of entry into force of the Policy, the amount threshold is EUR 1,000 (this threshold was introduced under Decree Law no. 201 of 6 December 2011, converted with amendments by Law no. 214 of 22 December 2011).

[32] At the date of entry into force of the Policy, the amount threshold for money remittances is EUR 1,000.

[33] Pursuant to the provisions of Legislative Decree 231/07, art. 49, all bearer savings bankbooks have been extinguished by 31 December 2018.

- provide that the above-mentioned subjects promptly notify the reference Group Company of the Group of all relevant circumstances and information for the purpose of allowing the latter to evaluate appropriate reporting of suspicious transactions;
- provide the subjects concerned with the operational instruments and procedures that may support them in meeting the obligations envisaged for anti-money laundering purposes when performing transactions;
- provide for the interruption of all relationships with financial agents and other subjects connected with the Group Companies by contractual obligations for the provision of off-site products, should they have committed, as ascertained, anti-money laundering/counter-terrorism breaches;
- define specific training programmes for the subjects in question, so that they may be suitably knowledgeable with reference legislation and with the connected responsibilities, and so that they may use the instruments and procedures designed to support them in performing their obligations;
- continually monitor observance, by the sales network, of the rules of conduct within the scope of anti-money laundering/counter-terrorism as contractually laid down. In particular, it shall be verified that the financial agents appointed promptly notify the Group Companies[34] of the data and information provided by Art. 31 of Legislative Decree 231/07;
- perform, at regular intervals, inspections at the operations centres of the persons in charge of the sales network;
- verify how effectively associates apply the obligations of articles 24 and 25 of Legislative Decree 231/2007 – "Enhanced customer due diligence", in relation to which the Group Company provides its support.

In order to apply the above mentioned guidelines:

- the Italian Banks and non-banking companies of the Group that, for the off-site provision of their products, use networks of agents performing financial activities or other subjects linked to the same companies by contractual relationships, shall:
    - draw up "collaboration agreements" based on those defined by the Parent Company;
    - adopt training programmes consistent with the training objectives laid down by the Parent Company;
    - collaborate in performing the verification and monitoring activities conducted by the Parent Company;
- the foreign Companies that, for the off-site provision of their products, use networks of agents performing financial activities or other subjects, shall:
    - draw up "collaboration agreements" based on those defined by the Parent Company and taking into account applicable local legislation, as well as the operational and business specifications that characterise them;
    - prepare training programmes on the basis of those defined by the Parent Company and taking into account applicable local legislation, as well as the operational and business specifications that characterise them;
    - collaborate in performing the verification and monitoring activities conducted by the Parent Company.

4.12 Protection measures regarding the internal systems for reporting violations (so-called Whistleblowing)

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

- adopt specific procedures so that employees may report, internally, potential or actual violations of

[34] Authorised entities and agents pursuant to art. 1, paragraph 2, letter nn), of Legislative Decree 231/07 send to the reference intermediary the data acquired with reference to the customer, the person performing the transaction and the beneficial owner within twenty days of the execution of the transaction.

the provisions laid down to prevent money laundering and terrorism financing. Such procedures shall be capable of protecting the privacy of the subjects involved and of the reporting party.

5 Roles and Responsibilities of the Parent Company

5.1 Board of Directors

- defines, approves and periodically reviews the strategic guidelines and risk management policies connected with money laundering and terrorism financing for BPER Banca and for the Group; in compliance with a risk-based approach, such policies shall be suited to the extent and type of risk the business activity is actually exposed to. In this regard, also the results of the risk self-assessment practices - implemented by the Bank - in conformity with the indications received by the Supervisory Authority – shall be taken into account[35];
- approves the guidelines of the internal control system at an organic and coordinated Group level, designed to promptly detect and manage the risks of money laundering and terrorism financing, and assures its effectiveness over time;
- defines and approves the risk objectives and the tolerance threshold;
- evaluates the adequacy of the overall management of the risk of money laundering and terrorism financing implemented by the Group;
- approves the appointment of the Anti-Money Laundering Department, to provide compliance with anti-money laundering and counter-terrorism legislation. Such function has an independent nature and plays a centralised role at the Parent Company for managing second-level controls on the risk of money laundering and terrorism financing. The Board identifies its tasks and responsibilities, as well as the coordination and collaboration methods with other corporate control functions;
- approves appointment of the Chief Anti-Money Laundering Officer (CAMLO), of the Responsible Officer for reporting suspicious transactions - and of any substitute representatives - and of the Group Representative, and approves their subsequent revocation, if any, after consulting the Board of Statutory Auditors;
- assures, on an ongoing basis, that the responsibilities and tasks regarding anti-money laundering and countering terrorism financing are allocated within the Group in a clear and appropriate manner, at the same time assuring that the operating and control functions are distinct 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;
- 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 on the inspections carried out by the Anti-Money Laundering Department. The Board also approves the document on the results of the self-assessment procedure applicable to money laundering risks[36];
- assures that the deficiencies and anomalies found as a result of the inspections performed on different levels are promptly brought to their knowledge, and promotes the adoption of suitable corrective measures, evaluating their effectiveness;
- with this Policy, the Board approves the principles for managing the relationships with "high-risk" customers connected with the risk of money laundering and terrorism financing, and it identifies the protection measures to adopt in order to limit the risks linked to transactions with the highest risk third countries.

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

5.2 Board of Statutory Auditors

- audits the Internal Control System set up to monitor the risk of money laundering and terrorism financing;
- supervises that the anti-money laundering legislation is observed and that the System adopted is complete, appropriate and functional;
- evaluates the appropriateness of the existing procedures applicable to customer due diligence, to information storage and to the reporting of suspicious transactions;
- analyses the reasons for the deficiencies, anomalies and irregularities found and promotes the adoption of appropriate corrective measures;
- expresses its opinion on the decisions concerning the appointment of the Chief Anti-Money Laundering Officer (CAMLO) and on the reporting of suspicious transactions, as well as on the definition of the overall architecture for managing and controlling the risk of money laundering and terrorism financing;
- as regards the 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.

5.3 Chief Executive Officer[37]

- provides for the implementation of the strategic guidelines and risk management policies on money laundering and terrorism financing, as defined by the Board of Directors, and he/she is responsible for taking the necessary measures to assure the effectiveness of the organisation and monitoring systems on this matter;
- takes care of the implementation of an internal control system aimed at promptly detecting and managing the money laundering risk, observing the guidelines laid down by the Board of Directors, and ensures its effectiveness over time. In this regard, he/she also takes into account evidence resulting from risk self-assessment procedures carried out by the Bank, consistently with the instructions received by the Supervisory Authority[38];
- puts in place the initiatives and actions required to assure that the architecture of control functions is consistent with the complexity of the activities performed, the dimension of the internal organisation, the type of products and services offered and the extent of the risk that may be linked to the customer characteristics, thus 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 guidelines on anti-money laundering and financing of international terrorism;
- establishes the suitable instruments for allowing 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 adequate protection measures for the offences of money laundering and terrorism financing;
- defines the actions and procedures to ensure prompt fulfilment of the obligation to report to the Authorities, as laid down by the legislation on money laundering and the financing of terrorism;
- as regards reporting suspicious transactions, he/she defines and takes care of the implementation of a procedure capable of assuring reference certainty, homogeneous behaviour, generalised

[37] The Chief Executive Officer represents the body with management function pursuant to the Provisions of the Bank of Italy of 26 March 2019 "regarding anti-money laundering organisation, procedures and controls".
[38] See Bank of Italy provisions of 26 March 2019 on "anti-money laundering organisation, procedures and controls", Section Seven.

application to the entire organisation, complete use of the 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 instruments (including electronic instruments) used for detecting the anomalous transactions;
- defines and takes care of the implementation of information procedures aimed at ensuring that the employees, at all organisational levels, and the bodies with supervisory functions are aware of the risk factors and of the company protection measures on anti-money laundering and countering of terrorism connected with their tasks and related responsibilities;
- he/she defines the management procedures for the relationships with the customers identified as "high risk" subjects in connection with money laundering/terrorism financing, consistently with the principles laid down by the Board of Directors.

5.4 General Manager

The General Manager, or other holder of management and administrative functions, or person entrusted by the same[39]:

- assesses and authorises:
    - the opening of current accounts with correspondent bodies in third Countries for the Group Companies under Italian and foreign Law;
    - the establishment/continuation of an ongoing relationship, or performance of occasional transactions with "politically exposed persons" (so called "PEP") for the Parent Company;
- receives information on the authorisations provided by the Banks and by the Group Companies under Italian Law as regards the establishment/continuation of an ongoing relationship, or performance of occasional transactions with "politically exposed persons" (so called "PEP").

5.5 Responsible Officer

- evaluates the reports on suspicious transactions of money laundering or terrorism financing received or that came otherwise to his/her knowledge within the scope of his/her activity, and he/she notifies such transactions, if deemed well-founded, to the FIU, or he/she files them;
- manages the relationships with the FIU, promptly responding to any requests for further investigation submitted by the same;
- ensures promptness and confidentiality of the suspicious transactions reporting process by the Bank;
- keeps evidence of the assessments made, also if a report is not sent to the FIU;
- ensures that the policies and procedures for detecting and reporting suspicious transactions are observed, promptly notifying the Bank corporate bodies of any issues found;
- when requested, he/she submits a report on the detection, analysis and reporting of suspicious transactions to the FIU, to the Bank corporate Bodie;
- ensures observance of the procedures for identifying and reporting suspicious transactions;
- has free access, directly or through the organisation facilities he/she coordinates, to the information flows and archives (both on paper and electronic means), as well as to all information that may be relevant for performance of his/her tasks.

5.6 Group Responsible Officer

- analyses and evaluates, from a Group viewpoint, the reports filed and the transactions reported by the Italian Companies to the FIU, as well as those reported by the Group foreign Companies to their

[39] Or, nonetheless, subjects who perform an equivalent function.

competent local Authorities;

- at least every year, he/she submits - to the corporate Bodies of the Parent Company - a report on the identification, in-depth analysis and reporting of suspicious transactions from a Group viewpoint;
- has free access, directly or through the organisation facilities he/she coordinates, to the information flows and to all databases (both on paper and electronic means) of the Group, as well as to all information that may be relevant for performance of his/her tasks.