# Global Policy on the Prevention of Money Laundering and Financing of Terrorism of the BANKIA GROUP

**Approved by the Board of Directors on**

**28 April 2016**

# I. INTRODUCTION

- The Bankia Group, aware of the significance of money laundering and the financing of terrorism and the role that financial institutions play in preventing it, is fully collaborating with the relevant authorities and has joined the rest of the Spanish financial system in combatting all types of money laundering and terrorist financing.

- These efforts focus on establishing obligatory rules and procedures designed to:
  - Comply with current anti-money laundering laws at all times and with the recommendations issued by international organisations and national and international authorities.
  - Implement codes of conduct and appropriate control and communication systems to prevent its units from being used for money laundering.
  - Establish customer acceptance policies and Know-Your-Customer procedures, ensuring that all its employees understand and follow them.

- All references to "money laundering" included in this document shall also refer to the financing of terrorism. Nevertheless, when a specific policy, action or special measure is mentioned regarding the prevention of terrorist financing, it shall be specifically described and stated.

## I. 1. SCOPE OF APPLICATION

- The policy established in this document applies to the whole Group, its employees and collaborators, establishing the minimum standards that must be observed by Group companies that are subject to these regulations in the course of their business.

## I. 2. APPROVAL

- This policy will be approved by the Board of Directors of Bankia S.A. and published on the bank's intranet.

## I. 3. CONCEPTS OF MONEY LAUNDERING AND TERRORISM FINANCING

- Money laundering is considered as the following:

  - The conversion or transfer of goods in the knowledge that they come from a criminal activity or participation in a criminal activity, for the purpose of concealing or covering up the illegal source of the goods, or helping people that are involved to evade the legal consequences of their actions.

  - Concealing or covering up the characteristics, origin, location, availability, movement or the real ownership of goods or rights over goods, in the knowledge that these goods come from a criminal activity or participation in a criminal activity.

  - The acquisition, possession or use of goods, in the knowledge that, at the time of receiving these goods, they come from a criminal activity or participation in a criminal activity.

  - Participation in any of the aforementioned activities, the association to undertake these types of actions, attempts to perpetrate them and the act of abetting, instigating or advising someone to carry them out or facilitating such acts.

  Money laundering shall also be deemed to exist when the conducts described in the above points are carried out by the person or persons that committed the criminal acts that generated the goods.

  The goods resulting from a criminal activity shall be defined as all types of assets in which the acquisition or ownership originates from a crime, both material and immaterial, fixed or otherwise, tangible or intangible, as well as documents or legal instruments regardless of their format, including electronic or digital, which accredit ownership of these assets or a right over them, including in relation to tax evasion in the case of crimes against the tax authorities.

  Money laundering is also deemed to exist when the activities that generated the goods took place in the territory of another state.

- The financing of terrorism is defined as the supply, deposit, distribution or collection of funds or goods, by any means, directly or indirectly, with the intention of using them or in the knowledge that they will be used, wholly or partly, to commit any of the crimes of terrorism defined in the Spanish Criminal Code.

  The financing of terrorism is deemed to exist even when the supply or collection of funds or goods occurs in the territory of another state.

- For the purposes of the law and the Bankia Group's policy on the prevention of money laundering and the financing of terrorism, States, territories or jurisdictions that are identified by the Commission for the Prevention of Money Laundering and Monetary Offences as having requirements equivalent to those under Spanish legislation, shall be deemed to be equivalent third countries.

## II. INTERNAL REGULATIONS

i. To implement this Global Policy for the Prevention of Money Laundering and the Financing of Terrorism ("PML&FT"), each Group company that is subject to Law 10/2010 shall have its own Manual of Policies and Procedures on PML&FT that will establish the policies, procedures and internal controls designed to comply with prevailing legislation.

ii. The manuals of Group companies will be duly approved by the PML&FT Committee and by their respective Boards of Directors, ensuring that the company:

   i. Has the appropriate internal control measures, control bodies and reporting structures, approving in writing its suitable policies and procedures in relation to due diligence, information, document archiving, internal control, risk evaluation and management, compliance standards and reporting in order to prevent and frustrate transactions related to money laundering and the financing of terrorism.
   ii. Identifies and knows its customers; that it has implemented specific customer acceptance policies based on risk; and that it applies due diligence in accepting, identifying and knowing its customers.
   iii. Has personnel that are responsible for compliance with anti-money laundering regulations.
   iv. Complies with the requirements established by law for obtaining and retaining customers' identification documents, and the recording and reporting of transactions.
   v. Implements and puts into practice appropriate control methods based on the customer's characteristics and the operations it may perform in order to detect the activities of a suspicious customer; immediately analyse any identified transactions; and take the appropriate measures.
   vi. Bases its internal control procedures on a prior risk analysis, which is recorded in the self-assessment risk report and regularly reviewed.

vii. Performs and documents a specific risk analysis prior to launching a new product, providing a new service or distribution channel, or using a new technology, applying the appropriate measures to manage the risk.

viii. Specifically reports any event or transaction that has any of the following characteristics, carried out by or through BANKIA, to the internal bodies created for such purpose:

- Indications or certainty that it is related to money laundering and the financing of terrorism.
- Inconsistent with the customer's characteristics, business volume or transaction history, provided that a prior analysis of the transaction shows no apparent economic, professional or business explanation for carrying out such transactions.

ix. Refrains from executing suspicious transactions. When this is not possible or may complicate the investigation, the transaction may be executed, immediately followed by a communication explaining the reasons for the execution, which is supplementary to the sections of the suspicious transactions report.

x. Collaborates with the Commission for the Prevention of Money Laundering and Monetary Offences (SEPBLAC) and other authorities, providing them with the information that they may require to perform their duties. This information may relate to any data or knowledge obtained by these regulated companies regarding the transactions that they carry out and the people involved in them.

xi. Implement training programs on the prevention of money laundering and the financing of terrorism.

xii. Implement audit and quality systems for its anti-money laundering policies and procedures.

xiii. Establish a duty of confidentiality, so that the corresponding company as well as its executives and employees that hold information about transactions or activities classified as suspicious are completely forbidden from disclosing the actions being taken to the customer and third parties, with the exception of

the established internal anti-money laundering bodies. Any exceptions to this confidentiality will be handled by the appropriate internal body in accordance with the cases established by law.

xiv. Includes the procedures established in the regulations on the adaptation of internal control procedures in its manual on the prevention of money laundering and the financing of terrorism.

- The reporting of suspicious money laundering transactions to the Commission for the Prevention of Money Laundering and Monetary Offences (SEPBLAC) in response to requests for information from the Commission and submissions of the Obligatory Monthly Statement shall be centralised by the Group's representative for SEPBLAC, providing a comprehensive overview of a customer's positions and products across the whole Group.

- The bank will also apply anti-money laundering procedures to its activities, areas and sectors at highest risk to money laundering, which will be approved by the PML&FT Committee. These procedures will be included in specific anti-money laundering manuals.

- Furthermore, the following rules will be applied in relation to any agents, brokers and intermediaries that deal with a Group company:

  i. A section that requires the agent/intermediary to comply with legal obligations related to the prevention of money laundering and the financing of terrorism will be included in service agreements, in accordance with the bank's policy. In particular, this will include obtaining the necessary documents in order to sufficiently identify and know the customer, the obligation to train its employees in the prevention of money laundering and the financing of terrorism, and any analysis rules that the bank may establish in order to monitor its transactions.

  ii. The same control measures and KYC procedures applied by the bank will also apply to people that transact with the Group's companies through an agent or intermediary.

iii. The internal audit function will include a review of agent/intermediary compliance with PML&FT regulations in its audit plans.

iv. If an agent is subject to the requirements of Law 10/2010, the agreement must require the agent to provide the Group company that it has transacted with, with a copy of the annual independent expert report or a summary of the report prepared in accordance with Ministerial Order EHA/2444/2007 of 31 July, every year.

## III. ORGANIZATION AND INTERNAL CONTROL

i. The organisational structure will consist of an internal control body at the Group level called the Prevention of Money Laundering and Financing of Terrorism Committee (PML&FT Committee). The Group will have an operations unit within the Compliance Unit to ensure that all policies and actions in this area are coordinated, centralising all PML&FT activities regardless of the responsibilities that may be assigned to each of the business groups.

This will be in addition to effectively implementing an internal control system that, at a basic level, is linked to the business areas by strengthening regulatory knowledge in the most sensitive areas.

ii. The Group's SEPBLAC representative will be appointed from among the bank's directors or executives.

iii. The PML&FT Committee may appoint Money Laundering Prevention Managers for certain activities or centres in the Group who will manage operations that are considered to be at greatest risk of money laundering.

iv. The duties, functioning and composition of the PML&FT Committee, as well as the duties of the SEPBLAC representative, the Operations Unit and the PML&FT managers of the Group's subsidiaries, activities or centres with the highest risk of exposure to money laundering, shall be described in the PML&FT policies and

procedures manuals of the bank and any subsidiary companies subject to Law 10/2010.

v. Group companies will have appropriate internal control and reporting mechanisms in order to identify, prevent and frustrate transactions related to money laundering and the financing of terrorism, and to report to them as required by law.

vi. Group companies will apply internal control measures in accordance with these policies and the criteria established by the Group's PML&FT Committee, approving, in writing, suitable procedures in relation to due diligence, information, document archiving, internal control, risk evaluation and management, compliance and reporting. Branches and majority-owned subsidiaries in third countries will be informed of these policies and procedures.

The Group will adopt a PML&FT model that enables it to delegate specific tasks of the anti-money laundering function, so that certain processes that require less specialisation can be managed externally by prioritising tasks that have less added value and greater volatility in terms of their volumes, provided that responsibility for and performance of the associated tasks can be assured and continue to be subject to the supervision of the operating unit, which will continue to be responsible for compliance.

- The Group will have personnel that are responsible for compliance with anti-money laundering and financing of terrorism regulations.

- The Group will inform bank employees, and other people subject to the requirements under current legislation, by means of annual training plans designed in accordance with the risks of each person's business sector.

- The Group will establish procedures regarding the protection and suitability of employees, executives and agents.

## IV. POLICIES FOR APPLYING DUE DILIGENCE MEASURES: ACCEPTANCE, IDENTIFICATION AND KNOWLEDGE OF CUSTOMERS

i. The policies for accepting, identifying and knowing the customer help to protect the reputation of financial institutions and the integrity of banking systems by reducing the probability of them becoming a vehicle or victim of financial crime. They are also an essential part of effective risk management.

ii. The bank and Group companies subject to these regulations shall identify and know their customers according to the due diligence measures described below. They will also have a money laundering risk model that ultimately seeks to segment the customer portfolio in line with risk management criteria by calculating a money laundering and terrorist financing risk level for each customer or potential customer, which will enables them to identify the specific actions to implement in order to supervise and analyse their operations.

iii. Group companies that use this manual must prepare their own self-assessment PML&FT risk report, which will be reviewed on a regular basis and whenever there are significant changes that could influence the company's risk profile. These companies will check for potential significant changes at least once every year. The report will be sent to the Group PML&FT Committee and senior management.

iv. The bank and Group companies subject to these regulations shall not establish business relations or execute transactions if they are unable to apply the due diligence measures outlined in this section.

### IV. 1. CUSTOMER ACCEPTANCE POLICY

i. The customer acceptance policy must be applied to all customers of the bank and its financial institution subsidiaries before engaging in any commercial relations. Specific procedures will be implemented for non-financial subsidiaries to ensure they comply with regulations, depending on their core business and sector.

ii. In general, acceptance of a customer by one financial institution in the Group will be valid and sufficient for the remaining Group financial institutions.

iii. The Group has defined the following customer categories based on their level of money laundering risk:

**Group I - Categories of unacceptable customers**

**Group II - Categories of customers whose acceptance requires authorisation by a higher authority [enhanced due diligence measures]**

**Group III - Categories of customers whose acceptance requires authorisation by a higher authority and the enhanced due diligence measures expressly mentioned by law**

The types of customers in each category will be defined in the Manual on the prevention of money laundering and the financing of terrorism.

## IV. 2. CUSTOMER IDENTIFICATION POLICY

i. Group companies subject to these regulations must ask their customers to provide valid documents that verify their identity when initiating a business relationship or carrying out the transactions stipulated by prevailing legislation.

ii. They must also identify the real account holder and take sufficient measures to check his/her/its identity prior to entering into a business relationship or executing the transactions stipulated by prevailing legislation.

iii. In the case of legal entities, measures shall be taken to identify the ownership or control structure. Business relations may not be established or maintained with legal entities for which the ownership or control structure has not been identified. The aforementioned ban on relations shall apply to all companies in which the capital is represented by bearer shares, unless the institution subject to these regulations can determine the ownership or control structure by other means.

iv. Compliance with this policy is the responsibility of the business centres (branches or other business centres) of the institution subject to these regulations. This will apply to all persons (customers or otherwise) that request any type of service that requires identification. This identification process may be carried out in person or remotely, in accordance with the procedures established in the applicable regulations.

v. If indications or certainty of money laundering or terrorist financing arise during the process of establishing a business relationship, or once a relationship exists, or in the course of executing transactions, the identity of the customer and the real account holder must be obtained and verified prior to performing the special examination or reporting these indications, regardless of any exception, exemption or threshold.

## IV. 3. KNOW YOUR CUSTOMER POLICY

- Knowing the customer means knowing its activity and the source of its funds, as well as continuously monitoring the business relationship.

- Bankia Group companies must obtain information about **the purpose and nature of the business relationship**. In particular, they must obtain sufficient information from their customers (account holders and other participants) so as to understand the nature of their professional or business activities or the source of the funds, taking measures designed to reasonably check the accuracy of this information.

- The activity declared by the customer will always be checked in the following cases:
  - When the customer or business relationship has a higher-than-average risk, according to regulations or due to the results of the risk analysis.
  - When the monitoring of the business relationship shows that the customer's active or passive transactions are not consistent with its declared activity or transaction history.

- When circumstances require a special examination or notification of the indications.

- This verification shall be performed by obtaining the documents directly from the customer, by accessing public databases such as the Mercantile Registry, by signing up to the agreement between CECA/AEB and the General Treasury of the Social Security, or by obtaining information from reliable independent sources. Customers' professional or business activities can also be checked by visiting the offices, warehouses or commercial premises that are declared by the customer as locations for its commercial activities, recording the results of these visits in writing.

- Bankia Group companies will continuously monitor the business relationship, implementing measures to scrutinise transactions and updating documentation in order to ensure that these reflect their knowledge of the customer and the customer's business and risk profile. In particular, during the initial months when new customers start to use their accounts, as well as for transactions that involve new products or services that have not been previously offered by the regulated company, customers' activities must be specifically monitored in detail to ensure that their operations are consistent with the knowledge that the regulated company has of them and their business and risk profile.

- Group companies must also take measures to ensure that the documents, data and information that they have are up-to-date, setting reasonable time periods to update the documentation, data and information for each type of customer based on the assigned level of risk. The interval between document reviews shall depend on a customer's level of risk, although this must be at least annually for higher-than-average risk customers.

## IV. 4. USE OF SIMPLIFIED DUE DILIGENCE MEASURES

- The Bankia Group, in accordance with current legislation, may apply simplified due diligence measures to the following customers:

i. Entities governed by public law of EU member states or equivalent third countries.

ii. Companies or other legal entities that are controlled or majority owned by entities governed by public law of EU member states or equivalent third countries.

iii. Financial institutions, except payment institutions, domiciled in the European Union or in equivalent third countries that are subject to supervision of PML&FT compliance.

iv. Branches or subsidiaries of financial institutions, except payment institutions, domiciled in the European Union or in equivalent third countries, when they are subject to the parent company's PML&FT procedures.

v. Listed companies whose shares are listed for trading on a regulated market of the European Union or equivalent third countries, as well as their branches and majority owned subsidiaries.

- One or several of the following measures will apply to these customers based on their risk, replacing the normal due diligence measures:

  a. The purpose and nature of the customer's professional or business activity may be inferred from the type of transactions carried out or the established business relationship, instead of collecting information about the customer's activities.

  b. The frequency of the documentary review process may be reduced.

  c. The monitoring of the business relationship and analysis of transactions that do not exceed a quantitative threshold may be reduced.

- The documentation that justifies the customer's inclusion in one of the above groups must be duly recorded in the customer's file in order to prove that these measures should be applied for this reason.

## IV. 5. USE OF ENHANCED DUE DILIGENCE MEASURES

- In addition to the normal due diligence measures, Group companies subject to these regulations must apply additional KYC measures to control the risk of money laundering and terrorist financing in business areas, activities, products, services, distribution or marketing channels, business relations and transactions that have a higher risk of money laundering or terrorist financing.

- In addition to the cases established in current legislation, Group companies must apply enhanced due diligence measures in those cases established by the PML&FT Committee based on the risk analysis.

- The following factors should be taken into account when identifying these higher risk cases, among others:

    - Characteristics of the customer:

        - Customers that are not resident in Spain.

        - Companies that have a shareholding and control structure that is opaque, unusual or excessively complex.

        - Companies that are purely holding companies.

    - Characteristics of the transaction, business relationship or distribution channel:

        - Business relations and transactions in unusual circumstances.

        - Business relations and transactions with customers that regularly use bearer-based payment methods.

        - Business relations and transactions carried out through intermediaries.

## IV. 6. USE OF THIRD PARTY DUE DILIGENCE MEASURES

- Group companies may use third-parties that are subject to money laundering obligations to implement their due diligence measures, except for the requirement to continuously monitor the business relationship.

- The parties' respective obligations will include a written agreement that formally requires the third parties to apply the due diligence measures. Under this agreement, the company must always require third parties to:

  - Immediately send the company the information about the customer.
  - Immediately send the company a copy of the documents that verify the information provided by the customer, upon request.

- The annual independent expert assessment report must be requested from the third party to ensure that it is subject to anti-money laundering and terrorism financing obligations and supervision.

## V. POLICIES TO ENSURE COMPLIANCE WITH REPORTING OBLIGATIONS

- The bank and Group companies must:

  i. Assess any transaction that, due to its nature, may be associated with money laundering, regardless of its amount. In particular, any complex or unusual transaction or any transaction that does not have an obvious economic or lawful purpose must be examined in detail, recording the results of this assessment in writing.

  ii. Establish appropriate warnings based on transaction types, the parties involved and transaction amounts, in accordance with the corresponding risk, which will be reviewed to determine whether the transaction should be analysed in detail.

  iii. Facilitate the identification of risky transactions by employees, executives or agents in accordance with prevailing regulations.

  iv. Refrain from executing suspicious transactions. When this is not possible or may complicate the investigation, the transaction may be executed, immediately followed by a communication explaining the reasons for executing the transaction.

  v. Expressly report to SEPBLAC via the internal bodies created for such purpose, any event or transaction carried out by or through the bank in other Group companies, which shows indications or certainty of being related to money laundering and the financing of terrorism, or that is inconsistent with the customer's nature, business volume or transaction history, provided that a prior analysis of the transaction shows no apparent economic, professional or business justification for carrying out such transactions.

  vi. Report to SEPBLAC the transactions included in the legislation in relation to the systematic transaction reporting.

vii. Report to SEPBLAC the opening and cancellation of any current accounts, savings accounts, securities accounts and term deposits, via the Financial Account Holders File.

viii. Collaborate with SEPBLAC and its support bodies.

ix. Retain copies of the documents requested from its customers verifying the execution of transactions, business relations, customer identification and customers' professional and business activities, for a minimum period of ten years. Specifically, copies of identification documents must be stored on optical, magnetic or electronic supports that ensure the integrity of the data; that the data can be correctly read; cannot be manipulated and is appropriately conserved and located. Documents that formalise customers' compliance with reporting and internal control obligations must also be held for 10 years.

x. Comply with the duty of confidentiality, refraining from disclosing the actions being taken in relation to the prevention of money laundering and financing of terrorism to the customer or third party.

- The bank and Group companies will implement the necessary procedures to comply with these obligations, which will be included in their respective Manuals of Policies and Procedures on the Prevention of Money Laundering and the Financing of Terrorism.

## VI. SUPERVISION OF THE POLICY

The Corporate Compliance Directorate shall submit an annual report to the Audit and Compliance Committee in relation to compliance with this policy.

## VII. EVALUATION AND REVIEW OF THE POLICY

This policy will be appropriately updated and reviewed according to any organisational, legal and functional changes that may occur in the Group. Potential amendments will be made in

accordance with the validation and approval procedures of Bankia's Information Security Rules and shall also require the approval of Bankia's Board of Directors, upon receipt of the corresponding report from the Audit and Compliance Committee.

***