Establishes the Customer Identification Policy

1. FRAMEWORK ..............................................................  2
2. OBJECTIVE AND SCOPE OF APPLICATION ...........................................  2
3. VERIFYING THE IDENTITY .................................................................  2
   3.1. Basic Principles ...........................................................................  2
   3.2. Data to obtain .............................................................................  3
4. ENTITIES .........................................................................................  4
   4.1. Individuals ..................................................................................  4
   4.2. Legal persons (civil or commercial companies, associations, foundations, etc) ..................  4
   4.3. Legal arrangements ......................................................................  5
5. SPECIAL RISK SITUATIONS .................................................................  6
   5.1. Execution by third parties of the identification duty ..................................  6
   5.2. Ultimate Beneficial Owner ...............................................................  7
   5.3. Deposits in cash amounting to or exceeding €10,000.00 or € 5,000.00 .......................  8
   5.4. Occasional transactions equal or exceeding €15,000.00 .........................................  8
   5.5. Supplementary procedures in remote transactions ...........................................  10
   5.6. Correspondent Banks .....................................................................  10
6. DOCUMENTS .....................................................................................  11
   6.1. Quality of the documents required ....................................................  11
   6.2. Periods for update and document archive ...........................................  11
1. FRAMEWORK

In order to comply with the domestic and European legislation and regulations in force, in terms of anti-money laundering and counter terrorism financing, bearing in mind the good practices followed internationally and the directives, recommendations and guidelines issued by entities with international technical authority over these matters, namely the Basel Committee, FATF/GAFI and Wolfsberg Group, the financial institutions must implement a group of policies and procedures to prevent the use of their operations for criminal purposes or for practices that may lead to increased operating and reputation risks.

Thus, the Basel Committee, in its guidelines (“Customer Due Diligence for Banks”, Basel Committee on Banking Supervision, October 2001), states that customer identification is an effective element in building the KYC - Know Your Customer process that the Banks must implement to be protected from reputation, operational and legal risks and, at the same time, as a fundamental instrument to comply with the legal requirements regarding money laundering and terrorism financing.

2. OBJECTIVE AND SCOPE OF APPLICATION

Amongst the policies suggested by the Basel Committee and by the domestic and international authorities for the Banks to implement, so as to promote high ethical and professional standards in their activities, is the Customer Identification Policy, whereby the Banks sets forth the fundamental requirements to observe while identifying Customers, their representatives and ultimate beneficial owners that, together with the application of the KYC - Know Your Customer principles, meet the conditions for adequately applying the Customer Acceptance Policy and subsequently monitor it.

This policy defines, namely:

i. The basic principles that must be followed when identifying the entities that establish a business relationship with the Banks;

ii. The set of documents to obtain, for the various categories of Customers, individuals, legal persons or legal arrangements that undertake operations with the Banks, as per the provisions of item 4.3;

iii. The quality requirements demandable to all documents presented to the Banks as evidence of the information pertaining to the customers, which is subject to verification;

iv. How often are updated the documents pertaining to the Customer Identification Policy, in the Bank's keeping, for Customers in a continuous business relation with it and the minimum periods of time for keeping such documents on file.

The Customer Identification Policy is applicable to the entire Group, in Portugal and in the operations abroad, although it may require adaptation to the local legal and regulatory framework, without prejudice to the mandatory compliance with the requirements applicable to group relations, in accordance with the Law.¹.

All the employees of the Banks and of the companies included in the consolidation perimeter of Group Banco Comercial Português are bound to comply with this policy, following the highest ethical standards and respecting the confidentiality of the information received while performing their duties.

3. VERIFYING THE IDENTITY

3.1. Basic Principles

Within the scope of the banking relation, the customers' identification must be considered in a broad sense since, to establish a stable and continuous business relation and comply with the highest ethical and

¹ As per Article 45 of Notice nr. 5/2013 of Banco de Portugal.
professional standards, it implies knowing certain features, described in greater detail below, that are far beyond the personal identification data alone.

The principles of truth, verification, specialty and update are fundamental to the Customer Identification Policy. Thus, regardless of the type and quality of the documents requested to the Customers for verification of their identity, in a broad sense, the principle of truth regards the need to know, at any given moment, that there are no real or possible suspicions that the data and information provided to the Bank are fake, nor try to hide situations that, if known, could prevent the commercial relation from being established as proposed.

Consequently, the principle of verification forces the Banks to ensure that the information obtained and gathered when the customer relation begins or when an occasional transaction is made, as well as throughout the entire business relation and that the data provided by the customers are based on the required and sufficient documents for effectively proving the truthfulness of the process.

The principle of specialty underlines the need to handle identification requisites differently, depending not only on the entity with whom the Banks are establishing a relation but also on various features associated to each entity that translate into different levels of risk in terms of money laundering and terrorism financing. Thus, the identification of customers and the maintenance of their identification data must be carried out, as some other actions, using a risk-based approach besides the strict legal and regulatory requirements for these matters.

At the beginning of the business relationship, on the making of an occasional transaction and during the business relation, if it lasts, the principle of update mandates that the documents evidencing the information of the identification process must be written down or received in due time, as near the act and the information they verify as possible and will not be admitted when expired or deemed inappropriate for the purposes they are meant to serve. Therefore, it must also be understood that the acts of identifying and verifying the identification data do not end when the relation is initiated, but constitute an on-going update process.

Complementarily, within the scope of the KYC - Know Your Customer process, the Banks must also obtain clear, complete and true information on:

i. the purpose of the business relation to be established;
ii. the origin and destination of the funds one intends to use;
iii. the sources of income and assets of the Customer, judging if they are licit and
iv. the expected transaction profile;

3.2. Data to obtain

The domestic legislation and regulations (in compliance with the best international practices) establish a number of Customer identification duties that must be part of the respective identification/update processes.

The Banks, in their internal regulations in force, set forth the fundamental data to obtain at the beginning of the business relation, at the moment an occasional transaction is made and also throughout the entire business relation.

Thus, below is a list of the fundamental data to collect during the identification of the various categories, described in greater detail in the rules of procedure in force.
4. ENTITIES

4.1. Individuals
In the case of individuals, the Banks must get from the Customer the following identification data:

i. full name and signature,

ii. date of birth,

iii. nationality, as appears in the identification document or, if more than one nationality, a statement issued by the individual concerning all other nationalities,

iv. complete permanent residence address and, when diverse, complete residence address for tax purposes,

v. profession and employer,

vi. public offices currently being held,

vii. type, number, date and issuer of the identification document, and

viii. place of birth.

The identity must be strictly verified by means of an original, valid, pre-signed identification document, with picture, which states the full name, date of birth and nationality of the customer (citizen card, identity card, passport, residence permit in the national territory or similar public document that complies with the same requisites - in accordance with the rules set forth in NP0054).

Concerning customers or transactions that, due to their type or features, may lead to a greater risk of money laundering or terrorism financing, the Banks promote a set of special procedures and prepare a reinforced KYC and monitoring. This situation includes distance business relations or transactions and relations established with Politically Exposed Persons (PEP), residing outside the national territory or with individuals holding other political or public offices (as per OS0036).

4.2. Legal persons (civil or commercial companies, associations, foundations, etc)
In the case of legal persons, the Banks must obtain from the Customer, at least, the following information data:

i. name,

ii. object,

iii. address of the registered office, full address of the branch or of the permanent establishment;

iv. legal person identification number,

v. identity of the members of the administration body or similar body;

vi. country of incorporation;

viii. code for classification of economic activities.

In the case of legal persons, the documentary evidencing of identification data is:

i. the denomination, object, full address of the registered office and full address of the branch or permanent establishment may be verified by one of the following means:

   o commercial Registry Certificate or other public document in a hard or soft copy, containing the data in question;
   o collection and verification of the respective electronic data near the competent entities responsible for their management;

ii. the legal person identification number may be verified by means of one of the following ways:

   o Legal person card, company's card or other public document showing that element, provided in a hard or soft copy;
o document equivalent to the ones mentioned in the above subparagraph, in the case of entities not domiciled in Portugal;

o collection and verification of the respective electronic data near the competent entities responsible for their management;

iii. the identity of the members of the administration body or similar body may be verified by a simple written statement, in a hard or soft copy, issued by the legal person, containing the following identification data concerning the holders of those positions:

o full name, date of birth and nationalities;

o type, number, validity date and issuer of the identification document;

o identification number for tax purposes;

iv. the country of incorporation and the data concerning the activity codes do not need to be verified by means of a document; the information provided by the legal person thereon is sufficient.

Whenever a member of an administration body or similar body acts as a representative of that legal person in banking deposit accounts, the Banks carry out the full identification process foreseen for individuals.

The confirmation of the veracity of the information obtained or requested to the representatives of the legal persons may also be complemented, for a stronger due diligence in legally admissible terms, by using commercial information services, lawyers, public access and independent databases, bank references, visits to the entities' premises and other actions deemed adequate and justifiable.

Simultaneously, the Banks must verify the identity and repute of any entity that tries to establish a business relationship representing a corporate person and, at the same time, verify the authenticity of the documents given as evidence and of the representation powers.

The verification of the customer's identification must be made when the business relation begins or previously, notably when occasional transactions are made.

The Banks can only open current accounts when, cumulatively, all the identification data that apply to that specific case in legal and regulatory terms, have been delivered to them, together with all the documentary evidence necessary for their verification.

The documentary evidence of the identification elements the presentation of which is not indispensable for the beginning of the business relation must be delivered within thirty days maximum after the account opening date, time during which the account will remain subject to the account use legal restrictions and all amounts therein deposited will remain totally unavailable. However, so as not to disrupt the Clients approach procedures, the Banks will privilege the collection of all documents currently required at the moment the business relation is established.

When opening current accounts included in the banking minimum services legal regime, the Banks may allow the establishment of the business relation prior to the presentation of any documentary evidence on the identification data. However, the amounts deposited in the account will remain unavailable, being mandatory the presentation of the missing documentary evidence within a maximum deadline of thirty days.

4.3. Legal arrangements

Legal arrangements are: the autonomous assets, the condominiums of real estate properties under a horizontal property regime, the estate in abeyance and the trusts ruled by foreign law when and under the terms they are recognised by the Portuguese law.

Concerning the opening of current accounts held by legal arrangements mentioned in the previous paragraph (as well as in the opening of accounts held by limited liability individual establishments) applies, with all due adjustments made to each specific case, the collection of identification data as foreseen for legal persons.
5. SPECIAL RISK SITUATIONS

Concerning the identification of customers, the Banks consider the situations mentioned hereunder as particularly risky and, therefore, adopt the following procedures.

5.1. Execution by third parties of the identification duty

The Banks may use a third party institution to comply with the identification duty concerning their Clients, provided that the latter is:

i. one of the entities foreseen by the Law \( \text{\textsuperscript{2}} \), exception made to currency exchange offices, payment institutions and e-money institutions;

ii. an entity, with registered office in the European Union or in an equivalent third country, possessing a nature similar to the entities foreseen in the previous subparagraph.

Other third parties also entitled to execute the identification duty are:

i. The branches, established in the national territory, in another EU member State or in an equivalent third country, of entities with a nature similar to the one of those foreseen by the law, exception made to currency exchange offices and e-money institutions;

ii. entities providing postal services, to the extent that they offer to the public financial services related with issues supervised by Banco de Portugal.

Whenever the Banks resort to the execution of the identification duty by third parties, they must:

i. ensure that such third parties, for being part of the categories mentioned above, are duly licensed to execute the identification duty;

ii. assess, based on public information, on the good repute and trustworthiness of the third party;

iii. ensure that the third party has an appropriate internal control system in terms of anti-money laundering and counter terrorism financing;

iv. obtain the necessary identification data at a moment prior to the establishment of the business relation, of the execution of the occasional transaction or the making of the operation, as well as ensure that the third party sends to the Bank the respective identification evidence immediately after the same is requested;

v. ensure that the identification data have been collected by the third party by means of a direct and personal contact established with the Customer;

vi. complement the information collected by the third party or carry out a new identification process, in case the information received is not sufficient or the associated risk so justifies.

The execution of the identification duty, in the capacity of a third party, by the entities mentioned above, must observe the following requirements:

i. be ruled by a contract establishing the relations between the financial institution and the third institution;

ii. be carried out in a specific physical location;

iii. be carried out by employees properly trained in anti-money laundering and counter terrorism financing, in accordance with the legislation in force.

The agency, representation or outsourcing relationships do not envisage the execution of the identification by third parties.

\( \text{\textsuperscript{2}} \) As per article 3 (1) of Law 25/2008 - “Credit institutions, investment companies and other financial entities, entities managing or marketing venture capital funds, undertakings for collective investment marketing their units, insurance companies and intermediaries exercising the insurance mediation activity, exception made to tied insurance intermediaries, pension fund management companies, credit securitization companies, venture capital companies and investors, investment advisory companies, companies pursuing activities dealing with contracts related to investment in tangible assets”.

Once printed, this document constitutes a non-controlled copy
Without prejudice to the responsibility of the third parties concerning the compliance with all legal requirements, the Banks, in this case, continue to be responsible for the full compliance with the identification duty executed by those third parties as if they were the direct performers of that duty.

5.2. Ultimate Beneficial Owner

1. The ultimate beneficial owner (UBO) is always the natural person on behalf of whom a transaction or activity is carried out or who, ultimately, owns or controls the Customer.

2. Whenever the Customer is a legal person or a legal arrangement or, in any case, whenever there is a grounded suspicion that a Customer is not acting on its own account, the Banks adopt, for the purpose of investigating who the UBO is, the following cumulative procedures:

   i. get information on the identity of the UBO and ensure the collection of all the identification data mentioned in Item 4;

   ii. adopt the appropriate measures to verify the identity in view of the money laundering and terrorism financing risks associated with that Customer and with the business relation.

3. Whenever the risk level is deemed relevant, the Banks must collect the documentary evidence of the identity and capacity of the UBO, which may be evidenced by a simple copy of the documents mentioned in 4.1. and described in detail in NP0054 or through a measure or diligence deemed sufficient and reliable by the Banks in view of the specific risk identified;

4. For the purpose of determining the relevant risk level mentioned in the previous number, the Banks must particularly take into account the indicative risk situations described in Annex I of the Policy for Risk Management in terms of Anti-Money Laundering and Counter Terrorism Financing (GR0006), without prejudice to other situations that are, internally, classified as such.

5. When identifying the UBO, the Banks must always request original documents in a hard or soft copy or certified copies of those documents, when:

   i. the documentary evidence referred in item 3 raises doubts;

   ii. there is the suspicion of money laundering or terrorism financing activities;

   iii. such is justified by the risk profile defined for that Client or by any other circumstance deemed relevant.

6. Without prejudice to other diligences that, by their own initiative, the Banks consider that they must autonomously adopt, the documents or records of the current account opening formalization process must mandatorily include specific information fields for the identification of the UBO on account of which the Customers act or that, ultimately, controls them.

7. While carrying out the verification measures mentioned in Item 2, the Banks should:

   i. when determining the UBO classified as a corporate legal person, consider the percentage of 25% therein mentioned as a sign to take into consideration, without disregarding the possibility that the effective control of the management may be carried out by other means, inclusive through a stake or the holding of voting rights under that percentage;

   ii. when determining the UBO classified as a non corporate legal person wherein the future beneficiaries have not yet been determined, the Banks must get sufficient information on the UBO of trusts ruled by foreign law, defined in view of their features or types, in order to ensure that they will be able to verify the respective identity at the moment of payment or when the UBO exercise their respective acquired rights;

   iii. adopt other reasonable measures to know the Client's ownership and control structure, whenever the Customer is a corporate person or a legal arrangement, notably, and without prejudice to the carrying out of other diligences, the collection of reliable documents, data or information on:
the respective chain of stakes, of control or domination;

- the identity, in the case of foreign law trusts, of the settlor, of the protector and of the trustees, when the same cannot be ascertained while complying with the provisions of item 4.

5.3. Deposits in cash amounting to or exceeding €10,000.00 or € 5,000.00

In the case of deposits in cash in accounts held by third parties and whenever the amounts to be deposited is equal or exceeds €10,000.00, the Banks must confer and register the following identification elements:

i. name of the depositor;

ii. type, number, validity date and issuer of the identification document of the depositor.

Whenever, in accordance with their own internal rulings, the Banks consider that a deposit in cash in an account held by a third party represents a high risk of money laundering or of terrorism financing, they must adopt the procedures foreseen in the previous paragraph when the amount to be deposited equals or exceeds €5,000.00.

Whenever the Banks have reasons to suspect that deposits in cash have been divided amongst accounts held by third parties so as not to reach the ceilings defined in the paragraphs above, they must obtain a copy of the identification document of the depositor or collect the identification document's electronic data.

In the case of deposits in cash in accounts held by self-employed individuals, by individual establishments with limited liability or by corporate legal persons, the Banks may waive the observance of the procedures foreseen in the first and second paragraphs of this item when the deposits are made in accounts held by a Customer that, according to their internal rulings, has been classified with a low risk level.

For that purpose, the following are not considered as third party depositors: the members of the corporate bodies of the holder of the current account, those exercising management functions, its employees, attorneys and other individuals that provide permanent, temporary or occasional services to it, including transportation, safekeeping, handling and distribution of funds and valuables.

5.4. Occasional transactions equal or exceeding €15,000.00

Whenever the Banks wish to make, in person or using a means of distance communication, occasional transactions involving amounts equal or exceeding €15,000.00, regardless of the fact that the transaction is made through a single or several operations that appear to be linked, or occasional transactions involving any amount, which are suspected to be possibly linked with money laundering or terrorism financing crimes, they must obtain, at least, the following identification data on their Customers and, if needed be, on their representatives:

i. in the case of individuals:
   - full name;
   - date of birth,
   - nationality as appears in the identification document;
   - type, number, validity date and issuer of the identification document.

ii. in the case of corporate entities:
   - name;
   - object;
   - legal person identification number;
   - identity of the members of the administration body or similar body;

When, in the context of an occasional transaction, the Banks verify that the Customer is a legal person or a legal arrangement or, in any case, whenever there is a grounded suspicion that a Customer is not acting on its own account, they must also obtain all information on the beneficial owners (item 5.2).
In occasional transactions wherein the associated risk is deemed relevant, the Banks must request the remaining identification data foreseen by the law, or any additional elements that enable them to achieve an increased knowledge on the Customer, its representative or on the beneficial owner.

For that purpose, and without prejudice to other situations that are classified as such by the Banks pursuant to their internal criteria, must be especially considered for the classification of a risk level as relevant, at least, the situations showing a potentially higher risk mentioned in Annex I of GR0006.

In the specific case of transfers of funds not related with any account held by, depending on the situation, the payer or by the payee, which are executed in person or using a means of distance communication, the Banks must, when acting as payer or payee institutions do the following:

i. whenever the individual or aggregate amount of the transfers equals or exceeds €15,000.00, comply with all the duties foreseen by the law for occasional transactions in general, relating to the payers or the payees of those transfers;

ii. whenever the individual or aggregate amount of the transfers exceeds €1,000.00 or less than €15,000.00 and these transfers are not comprised within the exclusions foreseen by the European legislation, identify the payers and the payees of the transfers, fully executing the identification process, being obliged to do the following:
   o obtain, at least, the full name and the type and number of the identification document of the legal or natural person;

---

2 Regulation 1781/2006 of the European Parliament and of the Council of 15-11 - Article 3 - Scope:
1. This Regulation shall apply to transfers of funds, in any currency, which are sent or received by a payment service provider established in the Community.
2. This Regulation shall not apply to transfers of funds carried out using a credit or debit card, provided that:
   a) the payee has an agreement with the payment service provider permitting payment for the provision of goods and services, and
   b) a unique identifier accompanies such transfer of funds, allowing the transaction to be traced back to the payer.
3. Where a Member State chooses to apply the derogation set out in Article 11(5)(d) of Directive 2005/60/EC, this Regulation shall not apply to transfers of funds using electronic money covered by that derogation, except where the amount transferred exceeds EUR 1 000.
4. Without prejudice to paragraph 3, this Regulation shall not apply to transfers of funds carried out by means of a mobile telephone or any other digital or Information Technology (IT) device, when such transfers are pre-paid and do not exceed EUR 150.
5. This Regulation shall not apply to transfers of funds carried out by means of a mobile telephone or any other digital or IT device, when such transfers are post-paid and meet all of the following conditions:
   a) the payee has an agreement with the payment service provider permitting payment for the provision of goods and services;
   b) a unique identifier accompanies the transfer of funds, allowing the transaction to be traced back to the payer; and
   c) the payment service provider is subject to the obligations set out in Directive 2005/60/EC.
6. Member States may decide not to apply this Regulation to transfers of funds within that Member State to a payee account permitting payment for the provision of goods or services if:
   a) the payment service provider of the payee is subject to the obligations set out in Directive 2005/60/EC.
   b) the payment service provider of the payee is able by means of a unique reference number to trace back, through the payee, the transfer of funds from the natural or legal person who has an agreement with the payee for the provision of goods and services; and
   c) the amount transacted is EUR 1 000 or less.
Member States making use of this derogation shall inform the Commission thereof.
7. This Regulation shall not apply to transfers of funds:
   a) where the payer withdraws cash from his or her own account;
   b) where there is a debit transfer authorization between two parties permitting payments between them through accounts, provided that a unique identifier accompanies the transfer of funds, enabling the natural or legal person to be traced back;
   c) where truncated cheques are used;
   d) to public authorities for taxes, fines or other levies within a Member State;
   e) where both the payer and the payee are payment service providers acting on their own behalf.
verify the veracity of those elements using documents, data or information provided by a reliable and independent source, being obliged to, under any circumstance, evidence before any competent authorities, the appropriate and trustworthy nature of the document evidence used.

When, in the context of a transfer, the Customer is a legal person or a legal arrangement, whenever there is a grounded suspicion that a Client is not acting on its own account, the Banks must also obtain all information on the ultimate beneficial owners (item 5.2 of this Policy).

In these transfers, wherein the associated risk is deemed relevant, the Banks must request the remaining identification data foreseen by the law, or any additional elements that enable to achieve an increased knowledge on the Customer, its representative or on the ultimate beneficial owner.

Also for that purpose, and without prejudice to other situations that are classified as such by the Banks pursuant to their internal criteria, must be especially taken into consideration for the classification of a risk level as relevant, at least, the situations showing a potentially higher risk mentioned in Annex I of GR0006 - Anti-Money Laundering and Counter Terrorism Financing Policy.

The cash exchange operations are considered occasional transactions when they are not executed in the scope of a business relation and the financial institutions must mandatorily comply with the identification duty.

5.5. Supplementary procedures in remote transactions

Whenever the financial institutions adopt the supplementary identification documentary evidence by making the first payment of the operation through an account opened in a credit institution in the Customer's name, the Banks must request their Customer that the first payment of the operation be made by means of a banking transfer or a direct debit originated at a current account opened in the name of the Customer at a bank with its registered office or establishment in a EU country or in an equivalent third country.

In the case of transfers of funds abroad, which are not part of a business relation, it is mandatory that the provision to the financial institutions of the funds to remit be always made by means of a transfer or of a direct debit made from a current account held by the payer with a bank with its registered office or establishment in a EU country or in an equivalent third country, while the verification of the identification data is not carried out through one of the following ways:

i. through evidence presented in person to the financial institution that is processing the remittance of the funds;

ii. through a written statement confirming that the information provided is true and up to date, issued by a financial entity with its registered office in a EU country or in an equivalent third country or by a financial entity part of the same group, pursuant to the requirements set forth above.

Without prejudice to the abstention duty foreseen by the law, the Banks must avoid establishing business relations or make occasional transactions using distance communication means whenever they have reasons to believe that the Customer, for any unexplainable reason, deliberately tries to avoid establishing personal contact with the institution.

5.6. Correspondent Banks

In case the correspondent relation involves transfer corresponding accounts, the Banks must confirm that the identity of the Customer having direct access to the account has been confirmed and that the due diligence duty is observed by the correspondent institution and also ensured that those elements can be provided to it pursuant to its request, in accordance with the law.
6. DOCUMENTS

6.1. Quality of the documents required

The documents and the identity documentary evidence defined by the laws, by regulations and by the applicable internal regulations must always be, when the first contact with the Customer is established, notably the opening of the account, original documents, in a hard or soft copy, or certified copies of those documents or obtained through the access by the Banks to the respective electronic equivalent information, namely through:

i. the electronic use of the Citizen’s card, by resorting to the interoperability platform between information systems belonging to the Public Administration or to devices that provide a qualified certification or an identical safety degree;

ii. collection and verification of the respective electronic data near the competent entities responsible for their management.

To confirm the identity of individuals when a current deposit account is opened, the Banks must always demand the presentation of a valid identification document, showing a picture and the signature of the respective holder, issued by a competent public authority (for example, the national identity card, citizen card or passport).

In the case of documents issued out of the country of the Group’s operation where they are presented, the Banks must enhance the care with which they verify their accuracy and nature. The documents presented must be original documents or, as for national documents, copies duly certified by public entities. In this case, and when applicable in view of the countries involved, the Banks will, in general, request that the certification of the copies includes the Hague Apostille as proof of authenticity.

Documents with strikes or visible damages to fundamental areas or that raise suspicions of forgery or adulteration will never be accepted.

Documents written in characters other than Latin characters must be transliterated into Latin characters, if there is no other manner of verifying the data included in such documents.

Generally, in case of doubt on the authenticity or quality of the documents presented, the Customer identification procedure must be deemed invalid, until the Compliance Office approves the process.

The verification of the documents concerning the information to update can be made by a simple copy. However, the Banks must request original documents, in a hard or soft copy, or certified copies of those documents or, alternatively, obtain equivalent electronic information, whenever:

i. the information in question has never been object of any previous confirmation in accordance with the legislation in force;

ii. the elements provided by the Customer for updating the identification data raise some doubts;

iii. the information update diligences were triggered by suspicions of money laundering or terrorism financing activities;

iv. such is justified by the risk profile defined for that Customer or by any other circumstance deemed relevant by the financial institution.

6.2. Periods for update and document archive

The Banks promote the periodical update of the information and of their respective documentary evidence, at most, every five years. The prioritization of the update of this information must be defined in view of the risk level associated to each Customer by the Banks and the periodical updates will be made in the reverse order in terms of the risk level identified and the update periodicity must not exceed 5 years concerning low risk Customers.
In any case, the financial institutions must immediately carry out the necessary information update diligences concerning filed information, whenever:

i. they have reasons to doubt the veracity, accuracy and up-to-dateness of the information provided;

ii. they suspect the practice of money laundering or terrorism financing activities, without prejudice to the compliance with the respective communication duty;

iii. they are aware of the occurrence of, at least, one of the following facts related with the Customer, his/her/its representative or ultimate beneficial owner, as the case may be:

   o alteration of the administration body or equivalent body;
   o alteration of the nature of the business activity or model pursued by the Customer;
   o alteration of the authorized signatures list for the use of bank accounts;
   o alteration of the respective chain of stakes, of control or domination when the same may imply the alteration of the ultimate beneficial owner;
   o end of the validity period of the identification documents.

The time limit for the archive/keeping of documents may be of 5 years but, in general, for specific situations duly foreseen by the laws the Banks may have to keep them for a longer period of time, as hereunder mentioned:

   o concerning the information and statement foreseen in the simplified identification duty - the same must be in a written document or record kept on file by the Banks for a period of 7 years after the end of the business relation;

   o the carrying out of the supplementary diligences for the appropriate verification of the identification data, namely through the consultation of public databases, in business relations that differ from the opening of current accounts, must involve documentary evidence and the Banks are obliged to keep that documentary evidence on file for, at least, 7 years;

   o the occasional relations or business relations established with PEP's residing outside the national territory must ensure the existence of documentary evidence and the Banks must keep that documentary evidence on file for, at least, 7 years;

   o the observance of the different requirements involving the establishment of correspondent relations must also be documentarily evidenced and the Banks must keep that documentary evidence on file for, at least, 7 years.

Additional Information

Decree -Law 145/2006, of 31-07
Law 25/2008 of 05-06.
Notice 1/2014 of 28-02 (republication of Notice 5/2013 of Banco de Portugal)